Introdução à Teoria dos Números: Funções Aritméticas

Fabio E. Brochero Martinez
Carlos Gustavo T. de A. Moreira
Nicolau C. Saldanha
Eduardo Tengan

Prefácio

Este livro é uma versão reduzida do livro "Teoria dos Números: um passeio pelo mundo inteiro com primos e outros números familiares", dos mesmos autores. Foi preparado especialmente para servir como texto do curso de "Funções Aritméticas", a ser dado por Carlos Gustavo Moreira no II Colóquio da Região Sul, em Londrina.

Rio de Janeiro, 30 de março de 2011

Conteúdo

Capítulo 0

Princípios

Neste capítulo preliminar veremos duas propriedades básicas dos números naturais, o *Princípio da Indução Finita* e o *Princípio da Casa dos Pombos.*

0.1 Princípio da Indução Finita

Seja $P(n)$ uma propriedade do número natural n, por exemplo:

- n pode ser fatorado em um produto de números primos;
- $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$;
- a equação $2x + 3y = n$ admite solução com x e y inteiros positivos.

Uma maneira de provar que $P(n)$ é verdadeira para todo natural $n \geq n_0$ é utilizar o chamado *Princípio da Indução Finita* (PIF), que é um dos axiomas que caracterizam o conjunto dos números naturais. O PIF consiste em verificar duas coisas:

1. (Base da Indução) $P(n_0)$ é verdadeira e
2. (Passo Indutivo) Se $P(n)$ é verdadeira para algum número natural $n \geq n_0$, então $P(n+1)$ também é verdadeira.

Na base da indução, verificamos que a propriedade é válida para um valor inicial $n = n_0$. O passo indutivo consiste em mostrar como utilizar a validade da propriedade para um dado n (a chamada *hipótese de indução*) para provar a validade da mesma propriedade para o inteiro seguinte $n + 1$. Uma vez verificados a base e o passo indutivo, temos uma "cadeia de implicações"

$$\begin{aligned} P(n_0) \text{ é verdadeira (base)} &\overset{\substack{\text{passo} \\ \text{indutivo}}}{\Longrightarrow} P(n_0+1) \text{ é verdadeira} \\ &\overset{\substack{\text{passo} \\ \text{indutivo}}}{\Longrightarrow} P(n_0+2) \text{ é verdadeira} \\ &\overset{\substack{\text{passo} \\ \text{indutivo}}}{\Longrightarrow} P(n_0+3) \text{ é verdadeira} \\ &\vdots \end{aligned}$$

de modo que $P(n)$ é verdadeira para todo natural $n \geq n_0$.

Vejamos alguns exemplos.

Exemplo 0.1. *Demonstrar que, para todo inteiro positivo* n,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

SOLUÇÃO: Observemos que $1 = \frac{1 \cdot 2}{2}$ donde a igualdade vale para $n = 1$ (base da indução). Agora suponha que a igualdade valha para $n = k$ (hipótese de indução):

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Somando $k + 1$ a ambos lados da igualdade, obtemos

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2},$$

de modo que a igualdade também vale para $n = k + 1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$. □

Exemplo 0.2. *Demonstrar que, para todo número natural* n,

$$M_n = n(n^2 - 1)(3n + 2)$$

é múltiplo de 24.

SOLUÇÃO: Veja que se $n = 0$ então $M_0 = 0$, que é um múltiplo de 24 (base da indução).

Agora, suponhamos que para certo inteiro k o número M_k é divisível por 24 (hipótese de indução) e vamos mostrar que M_{k+1} também é divisível por 24 (passo indutivo). Calculamos primeiramente a diferença

$$\begin{aligned} M_{k+1} - M_k &= (k+1)\big((k+1)^2 - 1\big)\big(3(k+1) + 2\big) - k(k^2 - 1)(3k + 2) \\ &= k(k+1)[(k+2)(3k+5) - (k-1)(3k+2)] \\ &= 12k(k+1)^2. \end{aligned}$$

Um dos números naturais consecutivos k e $k + 1$ é par donde $k(k+1)^2$ é sempre par e $12k(k+1)^2$ é divisível por 24. Por hipótese de indução, M_k é divisível por 24 e temos portanto que $M_{k+1} = M_k + 12k(k+1)^2$ também é divisível por 24, como se queria demonstrar. □

Uma variante do PIF é a seguinte versão (às vezes apelidada de *princípio de indução forte* ou *princípio de indução completa*), em que se deve mostrar

1. (Base da Indução) $P(n_0)$ é verdadeira e
2. (Passo Indutivo) Se $P(k)$ é verdadeira para todo natural k tal que $n_0 \leq k \leq n$, então $P(n+1)$ também é verdadeira.

Exemplo 0.3. *A* sequência de Fibonacci F_n *é a sequência definida recursivamente por*

$$F_0 = 0, \quad F_1 = 1 \quad e \quad F_n = F_{n-1} + F_{n-2} \text{ para } n \geq 2.$$

Assim, seus primeiros termos são

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ \ldots$$

Mostre que

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

onde $\alpha = \frac{1+\sqrt{5}}{2}$ *e* $\beta = \frac{1-\sqrt{5}}{2}$ *são as raízes de* $x^2 = x + 1$.

Solução: Temos que $F_0 = \frac{\alpha^0-\beta^0}{\alpha-\beta} = 0$ e $F_1 = \frac{\alpha^1-\beta^1}{\alpha-\beta} = 1$ (base de indução). Agora seja $n \geq 1$ e suponha que $F_k = \frac{\alpha^k-\beta^k}{\alpha-\beta}$ para todo k com $0 \leq k \leq n$ (hipótese de indução). Assim,

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &= \frac{\alpha^n - \beta^n}{\alpha - \beta} + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \\ &= \frac{(\alpha^n + \alpha^{n-1}) - (\beta^n + \beta^{n-1})}{\alpha - \beta} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \end{aligned}$$

pois $\alpha^2 = \alpha + 1 \implies \alpha^{n+1} = \alpha^n + \alpha^{n-1}$ e analogamente $\beta^{n+1} = \beta^n + \beta^{n-1}$.

Observe que, neste exemplo, como o passo indutivo utiliza os valores de dois termos anteriores da sequência de Fibonacci, a base requer verificar a fórmula para os dois termos iniciais F_0 e F_1 e não apenas para o primeiro termo. □

Exemplo 0.4. *Demonstrar que, para quaisquer naturais $n \geq m$, o coeficiente binomial*

$$\binom{n}{m} \stackrel{\text{def}}{=} \frac{n!}{m!(n-m)!}$$

é inteiro.

Solução: Procederemos por indução sobre a soma $m + n$. Se $m + n = 0$ então $m = n = 0$ e $\binom{0}{0} = 1$ é inteiro (base de indução). Para o passo indutivo, observe primeiramente que para $0 < m < n$ temos a seguinte identidade de binomiais

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

que segue diretamente das definições:

$$\begin{aligned} \binom{n-1}{m} + \binom{n-1}{m-1} &= \frac{(n-1)!}{m!(n-m-1)!} + \frac{(n-1)!}{(m-1)!(n-m)!} \\ &= \frac{\big((n-m)+m\big)(n-1)!}{m!(n-m)!} = \binom{n}{m}. \end{aligned}$$

Agora suponhamos que $\binom{n}{m}$ é inteiro para $m + n \leq k$ (hipótese de indução). Note que podemos supor também que $0 < m < n$, já que se $m = n$ ou $m = 0$ temos $\binom{n}{m} = 1$ e o resultado vale trivialmente. Assim, se $m + n = k + 1$, temos que $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$ é inteiro também pois cada somando da direita é inteiro pela hipótese de indução. □

Um terceiro disfarce do PIF é o chamado *princípio da boa ordenação* (PBO) dos números naturais, que afirma que todo subconjunto A não vazio de $\mathbb{N}$ tem um elemento mínimo. (Você sabe dizer por que o princípio da boa ordem não vale para o conjunto $\mathbb{Z}$ de todos os inteiros?)

Vejamos a equivalência entre os dois princípios. Assuma primeiramente o PBO e seja $P(n)$ uma propriedade para a qual $P(0)$ é verdadeira e $P(n)$ verdadeira implica $P(n+1)$ verdadeira. Seja B o conjunto dos n tais que $P(n)$ é falsa; devemos mostrar que $B = \emptyset$. Suponha que não; pelo PBO o conjunto B possui um menor elemento b. Como $0 \notin B$ (pois $P(0)$ é verdadeira por hipótese) temos que $b \geq 1$ e assim $b-1 \in \mathbb{N}$ e pela minimalidade de b temos que $b - 1 \notin B$, ou seja, $P(b-1)$ é verdadeira. Mas por hipótese temos então que $P(b)$ também é verdadeira, o que é um absurdo, logo $B = \emptyset$.

Assuma agora o PIF e seja $A \subset \mathbb{N}$ um subconjunto não vazio. Defina agora o conjunto $B = \{b \in \mathbb{N} \mid a \notin A \text{ para todo } a < b\}$. Trivialmente $0 \in B$. Afirmamos que existe $k \in B$ tal que $k+1 \notin B$ e nesse caso k será o menor elemento de A. De fato, se isto não acontecer, teremos que $0 \in B$ e $k \in B$ implica que $k+1 \in B$. Logo, pelo PIF, $B = \mathbb{N}$ e $A = \emptyset$, o que é absurdo.

Exemplo 0.5. *Demonstrar que toda função $f : \mathbb{N} \to \mathbb{N}$ monótona não-crescente (isto é, $n \le m \implies f(n) \ge f(m)$) é constante a partir de um certo número natural.*

Solução: Seja $A \subset \mathbb{N}$ a imagem de f. Pelo PBO, tal conjunto possui elemento mínimo a_0. Seja n_0 um natural tal que $f(n_0) = a_0$. Como a função é monótona não-crescente então para todo $n \ge n_0$ temos que $f(n) \le f(n_0)$, mas pela definição de a_0 temos $f(n) \ge a_0$. Logo $f(n) = a_0$ para todo $n \ge n_0$, como queríamos demonstrar. $\square$

Observação 0.6. *Dado um conjunto S, uma relação $\prec$ em S é chamada de* ordem parcial *em S se ela satisfaz os seguintes axiomas:*

1. *(Reflexividade) $a \prec a$ para todo $a \in S$.*
2. *(Anti-simetria) se $a \prec b$ e $b \prec a$ então $a = b$.*
3. *(Transitividade) se $a \prec b$ e $b \prec c$ então $a \prec c$.*

Dizemos que $\prec$ é uma ordem total *se, dados quaisquer $a, b \in S$, ou $a \prec b$ ou $b \prec a$. Uma ordem total $\prec$ em S é uma* boa ordem *se todo subconjunto A de S possui um elemento mínimo, isto é, um elemento $a \in A$ tal que $a \prec b$ para todo $b \in A$. É possível demonstrar que para todo conjunto S podemos definir uma ordem total em S que é uma boa ordem. Este fato usa o axioma da escolha (e na verdade é equivalente a ele) e está fora do propósito deste livro. Veja por exemplo [22].*

Problemas Propostos

0.1. *Demonstrar por indução que para $n \ge 1$ natural*

(a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(b) $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

(c) $(1^5 + 2^5 + \cdots + n^5) + (1^7 + 2^7 + \cdots + n^7) = 2(1 + 2 + \cdots + n)^4$.

(d) $\operatorname{sen} x + \operatorname{sen} 2x + \cdots + \operatorname{sen} nx = \dfrac{\operatorname{sen} \frac{(n+1)x}{2} \cdot \operatorname{sen} \frac{nx}{2}}{\operatorname{sen} \frac{x}{2}}$.

0.2. *Seja F_n o n-ésimo termo da sequência de Fibonacci. Demonstrar que para todo natural $n \ge 1$ temos*

(a) $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

(b) $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$.

(c) $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$.

(d) $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \cdots = F_{n+1}$, *onde na soma interpretamos* $\binom{m}{k} = 0$ *se $k > m$.*

0.3. *Demonstrar que*

(a) $n^3 - n$ *é um múltiplo de* 6 *para todo natural* n*.*

(b) $5^n - 1$ *é múltiplo de* 24 *para todo número natural* n *par.*

(c) $2^n + 1$ *é múltiplo de* 3 *para todo natural ímpar* n*.*

0.4. *Definimos a sequência* $\{a_n\}$ *por* $a_1 = 2$ *e para* $n \geq 2$ *o termo* a_n *é o produto dos termos anteriores mais um. Mostre que*

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = 1 - \frac{1}{a_1 a_2 \cdots a_n}.$$

0.5. *Mostre que* $7^{2n} - 48n - 1$ *é divisível por* 48^2 *para todo valor* n*.*

0.6. *Mostre que para todo natural* $n \geq 4$

(a) $2^n < n!$*.*

(b) $2n^3 > 3n^2 + 3n + 1$*.*

0.7. *Dado um inteiro positivo* n*, definimos* $T(n,1) = n$ *e, para todo* $k \geq 1$*,* $T(n,k+1) = n^{T(n,k)}$*. Prove que existe* $c \in \mathbb{N}$ *tal que, para todo* $k \geq 1$*,* $T(2010,k) < T(2,k+c)$*. Determine o menor inteiro positivo* c *com essa propriedade.*

0.8. *Mostre que para todo* n *e* k *inteiros positivos*

$$\binom{n}{n} + \binom{n+1}{n} + \binom{n+2}{n} + \cdots + \binom{n+k}{n} = \binom{n+k+1}{n+1}.$$

0.9. *Demonstre a fórmula do* binômio de Newton *para* n *natural:*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

0.10. *Encontrar com demonstração uma expressão para o multinômio*

$$(x_1 + x_2 + \cdots + x_k)^n$$

em termos dos coeficientes multinomiais

$$\binom{n}{i_1, \ldots, i_k} \stackrel{\text{def}}{=} \frac{n!}{i_1! \cdots i_k!}$$

onde $i_1 + \cdots + i_k = n$*.*

0.11. *Considere* n *retas em posição geral em um plano, isto é, sem que haja duas retas paralelas ou três retas concorrentes em um mesmo ponto.*

(a) Determine em função de n *o número de regiões em que as retas dividem o plano.*

(b) Demonstre que é possível colorir essas regiões com duas cores sem que duas regiões vizinhas tenham a mesma cor (duas regiões são vizinhas se elas possuem um segmento de reta em comum).

0.12. *Sejam* $x_1, \ldots, x_n$ *números reais positivos. Neste exercício vamos provar que*

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}.$$

Tal desigualdade é conhecida como desigualdade das médias aritmética e geométrica.

(a) Utilize o PIF para mostrar a desigualdade das médias para $n = 2^k$*.*

(b) *Sejam $x_1, \ldots, x_n$ reais positivos fixados e $A = \frac{x_1+\cdots+x_n}{n}$ a média aritmética destes números. Suponha que a desigualdade valha para $n+1$ números reais positivos quaisquer; aplicando-a para $x_1, \ldots, x_n, A$, conclua que a desigualdade vale também para quaisquer n números reais positivos.*

(c) *Combinando os itens anteriores, prove a desigualdade para todo n natural.*

Primeiro observemos que se $a, b > 0$ então

$$0 \leq (a-b)^2 = a^2 - 2ab + b^2 = (a+b)^2 - 4ab,$$

logo $\sqrt{ab} \leq \frac{a+b}{2}$, assim a desigualdade vale para $n = 2$. Agora mostremos que se a desigualdade vale para k então a desigualdade vale para $2k$. De fato

$$\begin{aligned}\frac{x_1 + \cdots + x_{2k}}{2k} &= \frac{\frac{x_1+\cdots+x_k}{k} + \frac{x_{k+1}+\cdots+x_{2k}}{k}}{2} \\ &\geq \frac{\sqrt[k]{x_1 \cdots x_k} + \sqrt[k]{x_{k+1} \cdots x_{2k}}}{2} \\ &\geq \sqrt{\sqrt[k]{x_1 \cdots x_k}\,\sqrt[k]{x_{k+1} \cdots x_{2k}}} = \sqrt[2k]{x_1 \cdots x_{2k}}.\end{aligned}$$

Assim a desigualdade é verdadeira para $2, 4, 8, \ldots, 2^n, \ldots$. Suponhamos que a desigualdade é verdadeira para $n+1$, e sejam $x_1, \ldots, x_n$ reais positivos, definamos $A = \frac{x_1+\cdots+x_n}{n}$ e $G = \sqrt[n]{x_1 \cdots x_n}$, temos que mostrar que $A \geq G$, mas de fato sabemos que

$$A = \frac{x_1 + \cdots + x_n + A}{n+1} \geq \sqrt[n+1]{x_1 \cdots x_n A} = G^{\frac{n}{n+1}} A^{\frac{1}{n+1}}.$$

Daqui facilmente concluímos o que queríamos demonstrar.

0.13. *Demonstrar que para cada número natural n existe um número natural M satisfazendo simultaneamente as seguintes duas condições:*

(i) *M possui n dígitos pertencentes ao conjunto $\{1, 2\}$.*

(ii) *M é divisível por 2^n.*

0.14 (IMO1987). *Mostre que não existe uma função $f\colon \mathbb{N} \to \mathbb{N}$ tal que $f(f(n)) = n + 1987$ para todo $n \in \mathbb{N}$.*

0.2 Princípio da Casa dos Pombos

É intuitivamente claro que se colocamos $n+1$ objetos em n gavetas então haverá ao menos uma gaveta com mais de um objeto. Isto é exatamente o que afirma o chamado *Princípio da Casa dos Pombos* (PCP) ou *Princípio das Gavetas de Dirichlet*: se temos $kn+1$ pombos e n casinhas, então existirá uma casinha onde haverá pelo menos $k+1$ pombos. De fato, se em todas as casas houvesse no máximo k pombos, então o número de pombos não poderia ultrapassar kn.

O PCP parece bastante inocente, mas tem muitas aplicações interessantes, especialmente em argumentos de *existência* em que não se determina o objeto procurado explicitamente. Como exemplos falam mais do que 10^3 palavras, vejamos alguns.

Exemplo 0.7. *Do conjunto $A = \{1, 2, \ldots, 99, 100\}$, escolhemos ao acaso 51 números. Demonstrar que entre os números escolhidos sempre existem dois que são consecutivos.*

Solução: Para provar isto, primeiro escolhamos gavetas adequadas ao problema. Distribuímos os números de A em 50 "gavetas" assim construídas:

$$\{1,2\} \quad \{3,4\} \quad \{5,6\} \quad \cdots \quad \{99,100\}.$$

Como há 50 gavetas das quais retiramos 51 números, sempre existirá uma gaveta da qual escolhemos dois números e estes, graças à nossa construção, serão consecutivos. Podemos generalizar este resultado considerando os números $\{1,2,\ldots,2n\}$ e escolhendo dentre eles $n+1$ números ao acaso. $\square$

Exemplo 0.8. *Do conjunto $A=\{1,2,\ldots,99,100\}$, escolhemos ao acaso 55 números. Demonstrar que entre os números escolhidos sempre existem dois tais que sua diferença é 9.*

Solução: Como no exemplo anterior o problema é descobrir como formar as gavetas. Consideremos as gavetas numeradas $0,1,2,\ldots,8$, onde o número n é colocado na gaveta i se, e só se, o resto na divisão de n por 9 é i. Como escolhemos $55=9\times 6+1$ números, pelo PCP existirá uma gaveta j na qual há 7 ou mais números escolhidos. Mas em cada gaveta há no máximo 12 números (por exemplo, o conjunto $\{1,10,19,28,37,46,55,64,73,82,91,100\}$ possui exatamente 12 elementos). Segue, como no problema anterior, que existirão dois números que serão "consecutivos" em tal conjunto, isto é, dois números cuja diferença é 9. $\square$

Exemplo 0.9. *Demonstrar que qualquer conjunto de n inteiros possui um subconjunto não vazio cuja soma dos elementos é divisível por n.*

Solução: Sejam $a_1,a_2,\ldots,a_n$ os elementos do conjunto, e definamos as "somas parciais" $s_j=a_1+\cdots+a_j$ para $j=1,\ldots,n$. Se algum dos s_j é divisível por n o problema fica resolvido. Se nenhum é divisível por n, então os possíveis restos na divisão por n são $1,2,\ldots,n-1$ e como há n somas parciais pelo PCP existem duas s_j e s_k com $j<k$ que deixam o mesmo. Portanto $s_k-s_j=a_{j+1}+\cdots+a_k$ é divisível por n e $\{a_{j+1},a_{j+2},\ldots,a_k\}$ é o subconjunto procurado.

Por outro lado, observemos que n é a quantidade mínima de elementos para que se verifique tal condição, no sentido em que existem conjuntos A com $n-1$ elementos tais que a soma dos elementos de todo subconjunto não vazio de A não é divisível por n. Por exemplo, $A=\{1,n+1,2n+1,\ldots,(n-2)n+1\}$ é um destes conjuntos (verifique!). $\square$

Exemplo 0.10. *Seja α um número real. Demonstrar que, para todo inteiro $n\geq 2$, existe um inteiro $0<k<n$ tal que o módulo da diferença entre $k\alpha$ e seu inteiro mais próximo é menor ou igual a $\frac{1}{n}$.*

Solução: Vamos denotar por $\{x\}$ a *parte fracionária* do número real x, isto é, o único real que satisfaz $0\leq\{x\}<1$ e $x=m+\{x\}$ para algum $m\in\mathbb{Z}$.

Considere $\{k\alpha\}$ para $k=1,2,\ldots,n-1$. Particione o intervalo $[0,1)$ em n partes de tamanho $\frac{1}{n}$:

$$[0,1)=\Big[0,\frac{1}{n}\Big)\cup\Big[\frac{1}{n},\frac{2}{n}\Big)\cup\Big[\frac{2}{n},\frac{3}{n}\Big)\cup\cdots\Big[\frac{n-1}{n},1\Big)$$

Se $\{k\alpha\}\in[0,\frac{1}{n})$ ou $\{k\alpha\}\in[\frac{n-1}{n},1)$ para algum $k=1,\ldots,n-1$, o problema acabou. Caso contrário, pelo PCP haverá duas partes fracionárias $\{j\alpha\}$ e $\{k\alpha\}$

com $1 \leq j < k \leq n-1$ pertencentes a um mesmo intervalinho dentre os $n-2$ restantes. Sendo $x = (k-j)\alpha$, teremos

$$\{x\} = \begin{cases} \{k\alpha\} - \{j\alpha\} & \text{se } \{k\alpha\} \geq \{j\alpha\} \\ 1 + \{k\alpha\} - \{j\alpha\} & \text{se } \{k\alpha\} < \{j\alpha\} \end{cases}$$

e portanto $\{x\} \in [0, \frac{1}{n})$ ou $\{x\} \in [\frac{n-1}{n}, 1)$, assim $k-j$ satisfaz as condições do problema. □

Problemas Propostos

0.15. *Escolhem-se* 7 *pontos no interior de um retângulo de dimensões* 2×3*. Demonstrar que sempre é possível encontrar dois pontos tal que sua distância é menor ou igual a* $\sqrt{2}$*.*

0.16. *Escolhem-se 9 pontos no interior de um quadrado de lado* 1*. Demonstrar que é possível escolher 3 deles de tal forma que a área do triângulo que formam é menor ou igual a* $\frac{1}{8}$*.*

0.17. *Dadas 6 pessoas numa festa, demonstrar que necessariamente existem 3 pessoas que se conhecem mutuamente ou 3 pessoas que não se conhecem mutuamente. Suponha que a relação de conhecer é simétrica. Este é um caso particular do teorema de Ramsey, veja por exemplo [14].*

0.18. *Do conjunto* $A = \{1, 2, \ldots, 99, 100\}$ *escolhemos* 51 *números. Demonstrar que, entre os 51 números escolhidos, existem dois tais que um é múltiplo do outro.*

0.19. *Dado um número irracional u, demonstrar que sempre é possível encontrar infinitos números racionais* $\frac{p}{q}$*,* $p, q \in \mathbb{Z}$*, de tal forma que*

$$\left| u - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Um problema mais difícil é demonstrar existem racionais $\frac{p}{q}$ *de tal forma que*

$$\left| u - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

Veja o teorema **??** *e a seção correspondente para este e outros resultados relacionados à aproximação de números reais por números racionais.*

0.20 (IMO1985)**.** *Dado um conjunto M com 1985 inteiros positivos distintos, nenhum dos quais tem divisores primos maiores do que* 23*, mostre que há* 4 *elementos em M cujo produto é uma quarta potência.*

0.21 (OIbM1998)**.** *Determinar o mínimo valor de n para o qual, de todo subconjunto de* $\{1, 2, \ldots, 999\}$ *com n elementos, é possível selecionar quatro inteiros diferentes* a, b, c, d *tais que* $a + 2b + 3c = d$*.*

0.22. *Demonstrar que de qualquer conjunto de* $2^{n+1} - 1$ *números inteiros positivos é possível escolher* 2^n *elementos de tal forma que sua soma é divisível por* 2^n*.*

0.23 (IMO2001)**.** *Sejam* $n_1, n_2, \ldots, n_m$ *inteiros com m ímpar. Denotemos por* $x = (x_1, \ldots, x_m)$ *uma permutação dos inteiros* $1, 2, \ldots, m$*, e definamos* $f(x) = x_1 n_1 + \cdots + x_m n_m$*. Demonstre que existem duas permutações a e b tais que* $f(a) - f(b)$ *é divisível por* $m!$*.*

0.24. *Demonstrar que dados* 7 *números reais sempre é possível escolher* 2 *deles, digamos* a *e* b*, tais que*

$$\left|\frac{a-b}{1+ab}\right| < \frac{1}{\sqrt{3}}.$$

Para resolver o anterior problema, vejamos que a função $y = \tan x$ *é crescente entre* $(-\frac{\pi}{2}, \frac{\pi}{2})$*, como se mostra na figura, e além disso, para cada real* r *existe um único ângulo* θ *em este mesmo intervalo de tal forma que* $r = \tan\theta$*.*

Portanto, dados os 7 números reais, a cada um deles podemos fazer corresponder um ângulo no intervalo $(-\frac{\pi}{2}, \frac{\pi}{2})$*, e dividindo tal intervalo em 6 partes iguais, i.e., em 6 intervalos de comprimento* $\frac{\pi}{6}$ *, abertos à esquerda, existirão 2 ângulos* θ *e* γ *que estejam no mesmo intervalo, e portanto,* $|\theta - \gamma| < \frac{\pi}{6}$*.*

Podemos supor sem perda de generalidade que $a = \tan\theta > \tan\gamma = b$ *e como a função tangente é crescente,*

$$\frac{a-b}{1+ab} = \frac{\tan\theta - \tan\gamma}{1+\tan\theta\tan\gamma} = \tan(\theta-\gamma) < \tan\frac{\pi}{6} = \frac{1}{\sqrt{3}},$$

como queríamos demonstrar.

0.25 (IMO1991)**.** *Seja* $S = \{1, 2, \ldots, 280\}$*. Encontrar o menor inteiro* n *para o qual todo subconjunto de* S *com* n *elementos contém cinco números que são dois a dois primos entre si.*

0.26 (Erdős)**.** *Mostrar que toda a sequência com* n^2+1 *números reais contém ou uma subsequência crescente com* $n+1$ *termos ou uma subsequência decrescente com* $n+1$ *termos.*

0.27. *Pintamos todos os pontos do plano de azul, verde ou preto. Mostrar que existe no plano um retângulo cujos vértices têm todos a mesma cor.*

0.28. *Em um tabuleiro* 9×9 *são colocados todos os números de* 1 *até* 81*. Mostre que exite um* k *tal que o produto dos números na* k*-ésima linha é* diferente ao produto dos números da k-ésima coluna.

Capítulo 1

Divisibilidade e Congruências

Neste primeiro capítulo veremos os tópicos básicos de Teoria dos Números, como divisibilidade, congruências e aritmética módulo n.

1.1 Divisibilidade

Dados dois inteiros d e a, dizemos que d *divide* a ou que d é um *divisor* de a ou ainda que a é um *múltiplo* de d e escrevemos

$$d \mid a$$

se existir $q \in \mathbb{Z}$ com $a = qd$. Caso contrário, escrevemos $d \nmid a$. Por exemplo, temos que $-5 \mid 10$ mas $10 \nmid -5$.

Eis algumas propriedades importantes da divisibilidade:

Lema 1.1. *Sejam $a, b, c, d \in \mathbb{Z}$. Temos*

(i) ("d divide") Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.

(ii) (Limitação) Se $d \mid a$, então $a = 0$ ou $|d| \le |a|$.

(iii) (Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração: Se $d \mid a$ e $d \mid b$, então podemos escrever $a = dq_1$ e $b = dq_2$ com $q_1, q_2 \in \mathbb{Z}$, logo $ax + by = d(q_1x + q_2y)$. Como $q_1x + q_2y \in \mathbb{Z}$, temos $d \mid ax + by$. Para mostrar *(ii)*, suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \ge 1$ e $|a| = |d||q| \ge |d|$. Finalmente, se $a \mid b$ e $b \mid c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto $a \mid c$. $\square$

Vejamos como utilizar estas propriedades para resolver alguns problemas de divisibilidade.

Exemplo 1.2. *Encontre todos os inteiros positivos n tais que $2n^2+1 \mid n^3+9n-17$.*

Solução: Utilizando o "$2n^2+1$ divide" para reduzir o grau de $n^3+9n-17$, temos que

$$\begin{aligned}
&\begin{cases} 2n^2 + 1 \mid n^3 + 9n - 17 \\ 2n^2 + 1 \mid 2n^2 + 1 \end{cases} \\
\Longrightarrow\ & 2n^2 + 1 \mid (n^3 + 9n - 17) \cdot 2 + (2n^2 + 1) \cdot (-n) \\
\Longleftrightarrow\ & 2n^2 + 1 \mid 17n - 34.
\end{aligned}$$

Como o grau de $17n-34$ é menor do que o de $2n^2+1$, podemos utilizar a "limitação" para obter uma lista finita de candidatos a n. Temos $17n-34=0 \iff n=2$ ou $|2n^2+1| \leq |17n-34| \iff n=1,4$ ou 5. Destes candidatos, apenas $n=2$ e $n=5$ são soluções. □

Exemplo 1.3 (IMO1994). *Determine todos os pares* (m,n) *de inteiros positivos para os quais* $\frac{n^3+1}{mn-1}$ *é inteiro.*

Solução: Vamos tentar reduzir o grau em n utilizando o "d divide". Temos

$$\begin{aligned} mn-1 \mid n^3+1 &\implies mn-1 \mid (n^3+1)\cdot m-(mn-1)\cdot n^2 \\ &\iff mn-1 \mid n^2+m. \end{aligned}$$

Da mesma forma,

$$\begin{aligned} mn-1 \mid n^2+m &\implies mn-1 \mid (n^2+m)\cdot m-(mn-1)\cdot n \\ &\iff mn-1 \mid m^2+n \end{aligned}$$

e, finalmente,

$$\begin{aligned} mn-1 \mid m^2+n &\implies mn-1 \mid (m^2+n)\cdot m-(mn-1) \\ &\iff mn-1 \mid m^3+1 \end{aligned}$$

que é a mesma expressão com que começamos, trocando n por m. Assim, temos que a condição é simétrica em m e n e as divisibilidades acima são todas equivalentes entre si. Portanto podemos supor sem perda de generalidade que $m \geq n$. Utilizando a "limitação" temos

$$mn-1 \mid n^2+m \implies mn-1 \leq n^2+m \iff m(n-1) \leq n^2+1.$$

Se $n \neq 1$ temos $m \leq \frac{n^2+1}{n-1} = n+1+\frac{2}{n-1}$. Como estamos assumindo $m \geq n$, se $n \geq 4$ temos apenas duas possibilidades: $m=n$ ou $m=n+1$. Agora temos alguns casos a analisar.

- Se $m \geq n = 1$ devemos ter $m-1 \mid 1^2+m \implies m-1 \mid m+1-(m-1) \iff m-1 \mid 2$ e portanto $m=2$ ou $m=3$, ambos os casos fornecendo soluções.
- Se $m \geq n = 2$ devemos ter $2m-1 \mid 2^2+m \implies 2m-1 \mid 2(m+4)-(2m-1) \iff 2m-1 \mid 9 \iff m=2$ ou $m=5$, ambos os casos fornecendo soluções.
- Se $m \geq n = 3$ devemos ter $3m-1 \mid 3^2+m \implies 3m-1 \mid 3(m+9)-(3m-1) \iff 3m-1 \mid 28 \iff m=5$, que fornece uma solução.
- Se $m = n \geq 4$ devemos ter

  $$\begin{aligned} n^2-1 \mid n^2+n &\iff n-1 \mid n \\ &\implies n-1 \mid n-(n-1) \iff n-1 \mid 1 \end{aligned}$$

  o que não é possível pois $n \geq 4$.
- Se $m = n+1 \geq 5$ devemos ter

  $$\begin{aligned} &(n+1)n-1 \mid n^2+(n+1) \\ \iff &n^2+n-1 \mid (n^2+n+1)-(n^2+n-1) \\ \iff &n^2+n-1 \mid 2 \end{aligned}$$

  o que novamente não é possível pois $n \geq 4$.

Logo as soluções (m,n) são $(1,2)$, $(2,1)$, $(1,3)$, $(3,1)$, $(2,2)$, $(2,5)$, $(5,2)$, $(3,5)$ e $(5,3)$. □

1.2 mdc, mmc e Algoritmo de Euclides

Dados dois números inteiros a e b com $a \neq 0$ ou $b \neq 0$, a cada um deles pode-se associar seu conjunto de divisores positivos, D_a e D_b respectivamente, e a intersecção de tais conjuntos $D_a \cap D_b$ é finita (pela "limitação") e não vazia (já que 1 pertence à intersecção). Por ser finito, $D_a \cap D_b$ possui elemento máximo, que é chamado de *máximo divisor comum* (mdc) dos números a e b. Denotamos este número por $\mathrm{mdc}(a, b)$ (alguns autores usam a notação (a, b)). Para $a = b = 0$ convencionamos $\mathrm{mdc}(0, 0) = 0$. Quando $\mathrm{mdc}(a, b) = 1$ dizemos que a e b são *primos entre si*.

Por outro lado, se denotamos por M_n o conjunto dos múltiplos positivos de n, dados dois números inteiros a e b com $a \neq 0$ e $b \neq 0$, então a intersecção $M_a \cap M_b$ é não vazia (já que $|ab|$ está na intersecção). Como os naturais são bem ordenados, $M_a \cap M_b$ possui elemento mínimo. Tal número é chamado *mínimo múltiplo comum* (mmc) de a e b e o denotaremos por $\mathrm{mmc}(a, b)$ (alguns autores escrevem $[a, b]$).

Para calcularmos o mdc e o mmc de maneira eficiente, vamos descrever o chamado *algoritmo de Euclides* ou *algoritmo das divisões sucessivas*. Primeiramente, vamos relembrar o conceito de *divisão euclidiana*, ou *divisão com resto*, que é uma das quatro operações que toda criança aprende na escola. Sua formulação precisa é: dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ com

$$a = bq + r \qquad \text{e} \qquad 0 \le r < |b|.$$

Tais q e r estão unicamente determinados pelas duas condições acima (veja o argumento a seguir) e são chamados o *quociente* e *resto* da divisão de a por b. O resto r é também denotado por $a \bmod b$.

Para $x \in \mathbb{R}$, definimos o *piso* ou *parte inteira* $\lfloor x \rfloor$ de x como sendo o único $k \in \mathbb{Z}$ tal que $k \le x < k + 1$; definimos o *teto* $\lceil x \rceil$ de x como o único $k \in \mathbb{Z}$ tal que $k - 1 < x \le k$. Por exemplo, temos $\lfloor \sqrt{2} \rfloor = 1$, $\lceil \sqrt{2} \rceil = 2$, $\lfloor 10 \rfloor = \lceil 10 \rceil = 10$, $\lfloor -\pi \rfloor = -4$ e $\lceil -\pi \rceil = -3$. Podemos agora mostrar a existência de q e r satisfazendo as duas condições acima: basta tomar

$$q = \begin{cases} \lfloor a/b \rfloor & \text{se } b > 0 \\ \lceil a/b \rceil & \text{se } b < 0 \end{cases} \qquad \text{e} \qquad r = a - bq \quad \text{em ambos os casos}$$

e é fácil verificar que $0 \le r < |b|$ a partir das definições das funções piso e teto. Por outro lado, se $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \le r_1, r_2 < |b|$, então temos que $r_2 - r_1 = b(q_1 - q_2)$ é um múltiplo de b com $|r_2 - r_1| < |b|$, portanto $r_2 - r_1 = 0$ e assim $q_1 = q_2$ também, o que prova a unicidade.

Podemos agora descrever o *algoritmo de Euclides* para calcular o mdc, que se baseia na seguinte simples observação:

Lema 1.4 (Euclides)**.** *Se $a = bq + r$, então $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, r)$.*

Demonstração: Basta mostrar que $D_a \cap D_b = D_b \cap D_r$, já que se estes conjuntos forem iguais em particular os seus máximos também serão iguais. Se $d \in D_a \cap D_b$ temos $d \mid a$ e $d \mid b$, logo $d \mid a - bq \iff d \mid r$ e portanto $d \in D_b \cap D_r$. Da mesma forma, se $d \in D_b \cap D_r$ temos $d \mid b$ e $d \mid r$, logo $d \mid bq + r \iff d \mid a$ e assim $d \in D_a \cap D_b$. $\square$

O algoritmo de Euclides consiste na aplicação reiterada do lema acima onde q e r são o quociente e o resto na divisão de a por b (note que o lema vale mesmo sem a condição $0 \le r < |b|$). Como os restos formam uma sequência estritamente decrescente, o algoritmo eventualmente para quando atingimos o resto 0.

Exemplo 1.5. *Calcule* $\mathrm{mdc}(1001, 109)$.

Solução: Realizando as divisões sucessivas, temos

$$\begin{aligned} 1001 &= 109 \cdot 9 + 20 \\ 109 &= 20 \cdot 5 + 9 \\ 20 &= 9 \cdot 2 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Assim, temos $\operatorname{mdc}(1001, 109) = \operatorname{mdc}(109, 20) = \operatorname{mdc}(20, 9) = \operatorname{mdc}(9, 2) = \operatorname{mdc}(2, 1) = \operatorname{mdc}(1, 0) = 1$. □

Exemplo 1.6. *Sejam $m \neq n$ dois números naturais. Demonstrar que*

$$\operatorname{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \textit{se } a \textit{ é par,} \\ 2 & \textit{se } a \textit{ é ímpar.} \end{cases}$$

Solução: Suponha sem perda de generalidade que $m > n$ e observe a fatoração

$$a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-2}} + 1)(a^{2^{m-3}} + 1) \ldots (a^{2^n} + 1)(a^{2^n} - 1).$$

Logo $a^{2^m} + 1 = (a^{2^n} + 1) \cdot q + 2$ com $q \in \mathbb{Z}$ e assim

$$\operatorname{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \operatorname{mdc}(a^{2^n} + 1, 2)$$

que é igual a 2 se $a^{2^n} + 1$ for par, isto é, se a for ímpar, e é igual a 1 caso contrário. □

Além de servir de ferramenta computacional para o cálculo do mdc, a divisão euclidiana tem consequências teóricas importantes. O próximo teorema mostra que é sempre possível escrever o mdc de dois números como combinação linear destes (com coeficientes inteiros).

Teorema 1.7 (Bachet-Bézout)**.** *Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com*

$$ax + by = \operatorname{mdc}(a, b).$$

Portanto se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid \operatorname{mdc}(a, b)$.

Demonstração: O caso $a = b = 0$ é trivial (temos $x = y = 0$). Nos outros casos, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b:

$$I(a, b) \stackrel{\text{def}}{=} \{ax + by : x, y \in \mathbb{Z}\}.$$

Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$ (há pelo menos um elemento positivo, verifique!). Afirmamos que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \le r < d$. Temos

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

Mas como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e portanto $d \mid m$.

Em particular, como $a, b \in I(a, b)$ temos que $d \mid a$ e $d \mid b$, logo $d \le \operatorname{mdc}(a, b)$. Note ainda que se $c \mid a$ e $c \mid b$, então $c \mid ax_0 + by_0 \iff c \mid d$. Tomando $c = \operatorname{mdc}(a, b)$ temos que $\operatorname{mdc}(a, b) \mid d$ o que, juntamente com a desigualdade $d \le \operatorname{mdc}(a, b)$, mostra que $d = \operatorname{mdc}(a, b)$. □

Corolário 1.8. *Sejam* $a, b, c \in \mathbb{Z}$. *A equação*

$$ax + by = c$$

admite solução inteira em x *e* y *se, e somente se,* $\operatorname{mdc}(a, b) \mid c$.

DEMONSTRAÇÃO: Se a equação admite solução inteira, então $\operatorname{mdc}(a, b)$ divide o lado esquerdo, logo deve dividir o direito também. Reciprocamente, se $\operatorname{mdc}(a, b) \mid c$, digamos $c = k \cdot \operatorname{mdc}(a, b)$ com $k \in \mathbb{Z}$, pelo teorema acima existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = \operatorname{mdc}(a, b)$ e multiplicando tudo por k obtemos que $x = kx_0$ e $y = ky_0$ são soluções da equação dada. □

Temos uma outra importante consequência do teorema anterior:

Proposição 1.9. *Se* $\operatorname{mdc}(a, b) = 1$ *e* $a \mid bc$, *então* $a \mid c$.

DEMONSTRAÇÃO: Como $\operatorname{mdc}(a, b) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1 \implies a \cdot cx + (bc) \cdot y = c$. Do fato de a dividir cada termo do lado esquerdo, temos que $a \mid c$. □

Lembramos que um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de p são 1 e p e um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e n. Observemos que 1 não é nem primo nem composto.

Claramente, se p é primo e $p \nmid a$ temos $\operatorname{mdc}(p, a) = 1$. Usando a proposição anterior e indução temos o seguinte resultado:

Corolário 1.10. *Seja* p *um número primo e sejam* $a_1, \ldots a_m \in \mathbb{Z}$. *Se* $p \mid a_1 \cdots a_m$, *então* $p \mid a_i$ *para algum* i, $1 \le i \le m$.

O próximo lema resume algumas propriedades úteis do mdc:

Lema 1.11. *Temos*

1. *Se* p *é primo, então* $\operatorname{mdc}(a, p)$ *é* 1 *ou* p.
2. *Se* k *é um inteiro, então* $\operatorname{mdc}(a, b) = \operatorname{mdc}(a - kb, b)$.
3. *Se* $a \mid c$, *então* $\operatorname{mdc}(a, b) \mid \operatorname{mdc}(c, b)$.
4. *Se* $\operatorname{mdc}(a, b) = 1$, *então* $\operatorname{mdc}(ac, b) = \operatorname{mdc}(c, b)$.

DEMONSTRAÇÃO: O primeiro item é claro e o segundo é apenas uma reformulação do lema 1.4. Para provar o terceiro item, observe que $\operatorname{mdc}(a, b) \mid a$ e $a \mid c$ implicam que $\operatorname{mdc}(a, b) \mid c$. Como também temos $\operatorname{mdc}(a, b) \mid b$, concluímos que $\operatorname{mdc}(a, b) \mid \operatorname{mdc}(b, c)$ por Bachet-Bézout. Finalmente, para mostrar o último item, note primeiro que $\operatorname{mdc}(c, b) \mid \operatorname{mdc}(ac, b)$ pois $\operatorname{mdc}(c, b)$ divide simultaneamente ac e b. Reciprocamente, para mostrar que $\operatorname{mdc}(ac, b) \mid \operatorname{mdc}(c, b)$, podemos escrever $ax + by = 1$ com $x, y \in \mathbb{Z}$ por Bachet-Bézout. Assim, $\operatorname{mdc}(ac, b)$ divide $ac \cdot x + b \cdot cy = c$ e também divide b, logo divide $\operatorname{mdc}(c, b)$. □

Vejamos como podemos usar as propriedades acima para solucionar o seguinte

Exemplo 1.12. *Sejam* $a_n = 100 + n^2$ *e* $d_n = \operatorname{mdc}(a_n, a_{n+1})$. *Calcular* d_n *para todo* n.

SOLUÇÃO: Aplicando a propriedade 2 temos que

$$d_n = \operatorname{mdc}(100 + n^2, 100 + (n + 1)^2) = \operatorname{mdc}(100 + n^2, 2n + 1).$$

Como $2n+1$ é ímpar, $\operatorname{mdc}(4, 2n+1) = 1$ e pelas propriedades 4 e 2 temos que

$$\begin{aligned} d_n &= \operatorname{mdc}(400 + 4n^2, 2n+1) \\ &= \operatorname{mdc}(400 + 4n^2 - (2n+1)(2n-1), 2n+1) \\ &= \operatorname{mdc}(401, 2n+1). \end{aligned}$$

Como 401 é primo, então $\operatorname{mdc}(401, 2n+1) = 401$ se $2n+1 = 401k$ (com $k = 2r+1$ inteiro ímpar) e $\operatorname{mdc}(401, 2n+1) = 1$ caso contrário, ou seja,

$$d_n = \begin{cases} 401 & \text{se } n = 401r + 200 \text{ com } r \in \mathbb{Z} \\ 1 & \text{caso contrário.} \end{cases}$$

□

A próxima proposição conecta o mdc e o mmc de dois inteiros e pode ser utilizada, juntamente com o algoritmo de Euclides, para o cálculo eficiente do mmc.

Proposição 1.13. *Sejam a e b dois números naturais, então*

$$\operatorname{mdc}(a, b) \cdot \operatorname{mmc}(a, b) = a \cdot b.$$

DEMONSTRAÇÃO: Escreva $d = \operatorname{mdc}(a, b)$ e $a = a_1 d$ e $b = b_1 d$ onde $a_1, b_1 \in \mathbb{Z}$ são tais que $\operatorname{mdc}(a_1, b_1) = 1$. Temos $\operatorname{mmc}(a, b) = al$ para algum $l \in \mathbb{Z}$; além disso, $b \mid \operatorname{mmc}(a, b) \iff b_1 d \mid a_1 dl \iff b_1 \mid a_1 l$. Como $\operatorname{mdc}(a_1, b_1) = 1$, isto implica que $b_1 \mid l$ pela proposição 1.9. Pela definição de mínimo múltiplo comum, temos que l deve ser o mínimo número divisível por b_1, assim concluímos que $l = b_1$ e portanto $\operatorname{mmc}(a, b) = b_1 a$. Logo $\operatorname{mdc}(a, b) \cdot \operatorname{mmc}(a, b) = d \cdot b_1 a = a \cdot b$. □

A demonstração que demos do teorema de Bachet-Bézout não mostra como efetivamente encontrar uma solução de $ax + by = \operatorname{mdc}(a, b)$. Porém, isto pode ser feito utilizando-se o algoritmo de Euclides, como mostra o exemplo a seguir. De fato, este exemplo pode servir como ponto de partida para uma segunda demonstração do teorema de Bachet-Bézout (veja os exercícios).

Exemplo 1.14. *Encontre todos os $x, y \in \mathbb{Z}$ tais que*

$$1001x + 109y = \operatorname{mdc}(1001, 109).$$

SOLUÇÃO: Fazemos as divisões sucessivas para o cálculo de mdc(1001, 109) = 1 utilizando o algoritmo de Euclides (veja o exemplo 1.5). Em seguida, isolamos os restos:

$$\begin{aligned} \boxed{20} &= \boxed{1001} - \boxed{109} \cdot 9 \\ \boxed{9} &= \boxed{109} - \boxed{20} \cdot 5 \\ \boxed{2} &= \boxed{20} - \boxed{9} \cdot 2 \\ \boxed{1} &= \boxed{9} - \boxed{2} \cdot 4 \end{aligned}$$

Note que a última divisão permite expressar o mdc 1 como combinação linear de 9 e 2:

$$\boxed{9} \cdot 1 - \boxed{2} \cdot 4 = 1.$$

Mas da penúltima divisão, temos que $\boxed{2} = \boxed{20} - \boxed{9} \cdot 2$, logo substituindo esta expressão na combinação linear acima, temos

$$\boxed{9} - (\boxed{20} - \boxed{9} \cdot 2) \cdot 4 = 1 \iff \boxed{9} \cdot 9 - \boxed{20} \cdot 4 = 1$$

e agora expressamos 1 como combinação linear de 20 e 9. Repetindo este procedimento, eventualmente expressaremos 1 como combinação linear de 1001 e 109. Tomamos o cuidado de $\boxed{\text{lembrar}}$ quais são os "coeficientes" a e b nas equações $ax + by = \operatorname{mdc}(a, b)$ durante as simplificações. Continuando, obtemos

$$\begin{aligned} 1 &= (\boxed{109} - \boxed{20} \cdot 5) \cdot 9 - \boxed{20} \cdot 4 = \boxed{109} \cdot 9 - \boxed{20} \cdot 49 \\ 1 &= \boxed{109} \cdot 9 - (\boxed{1001} - \boxed{109} \cdot 9) \cdot 49 = \boxed{1001} \cdot (-49) + \boxed{109} \cdot 450. \end{aligned}$$

Logo uma solução da equação $1001x + 109y = 1$ é $(x_0, y_0) = (-49, 450)$. Para encontrar as demais, escrevemos o lado direito desta equação utilizando a solução particular que acabamos de encontrar:

$$1001x + 109y = 1001x_0 + 109y_0 \iff 1001(x - x_0) = -109(y - y_0).$$

Como $\operatorname{mdc}(1001, 109) = 1$ temos pela proposição 1.9 que 1001 divide $y - y_0$, ou seja, $y - y_0 = 1001t$ para algum $t \in \mathbb{Z}$ e, portanto, $x - x_0 = -109t$. Assim, as soluções da equação dada são todos os pontos da reta $1001x + 109y = 1$ da forma

$$(x, y) = (x_0 - 109t, y_0 + 1001t) = (-49, 450) + (-109, 1001) \cdot t$$

com $t \in \mathbb{Z}$. $\square$

Em geral, o raciocínio do exemplo acima mostra que se $\operatorname{mdc}(a, b) = 1$ e (x_0, y_0) é uma solução da equação $ax + by = c$, então todas as soluções inteiras são dadas por $x = x_0 - bk$ e $y = y_0 + ak$ com $k \in \mathbb{Z}$.

Exemplo 1.15. *Sejam a, b inteiros positivos com* $\operatorname{mdc}(a, b) = 1$. *Mostre que para todo $c \in \mathbb{Z}$ com $c > ab - a - b$, a equação $ax + by = c$ admite soluções inteiras com $x, y \geq 0$.*

Solução: Seja (x_0, y_0) uma solução inteira (que existe pelo teorema de Bachet-Bézout). Devemos mostrar a existência de um inteiro k tal que

$$x = x_0 - bk > -1 \qquad \text{e} \qquad y = y_0 + ak > -1,$$

ou seja,

$$-\frac{y_0 + 1}{a} < k < \frac{x_0 + 1}{b}.$$

Mas isto segue do fato de o intervalo $(-\frac{y_0+1}{a}, \frac{x_0+1}{b})$ ter tamanho maior do que 1:

$$\frac{x_0 + 1}{b} - \left(-\frac{y_0 + 1}{a}\right) = \frac{ax_0 + by_0 + a + b}{ab} = \frac{c + a + b}{ab} > 1.$$

$\square$

1.3 O Teorema Fundamental da Aritmética

Estamos agora prontos para enunciar o teorema que caracteriza todo número natural em termos de seus "constituintes" primos.

Teorema 1.16 (Teorema Fundamental da Aritmética)**.** *Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \ldots \leq p_m$ são primos.

Demonstração: Mostramos a existência da fatoração de n em primos por indução. Se n é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n.

Vamos agora mostrar a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \ldots \leq p_m$, $q_1 \leq \ldots \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 \mid q_1 \cdots q_{m'}$ temos $p_1 \mid q_i$ para algum valor de i pelo corolário 1.10. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, pela minimalidade de n, donde $m = m'$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações. □

Outra forma de escrever a fatoração acima é

$$n = p_1^{e_1} \ldots p_m^{e_m},$$

com $p_1 < \cdots < p_m$ e $e_i > 0$. Ainda outra formulação é escrever

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \ldots p^{e_p} \ldots$$

onde o produto é tomado sobre *todos* os primos mas apenas um número finito de expoentes é maior do que zero. Vamos nos referir a qualquer destas expressões como a *fatoração canônica* de n em primos.

A fatoração única em primos se aplica em contextos mais gerais, como veremos mais tarde. Aqui, como aplicação imediata do Teorema Fundamental da Aritmética, vamos mostrar a prova atribuída a Euclides para a existência de infinitos primos (uma prova com mais de 2000 anos e que ainda funciona!).

Teorema 1.17 (Euclides). *Existem infinitos primos.*

Demonstração: Suponha por absurdo que $p_1, p_2, \ldots, p_m$ fossem *todos* os primos. O número $N = p_1 p_2 \ldots p_m + 1 > 1$ não seria divisível por nenhum primo p_i, o que contradiz o Teorema Fundamental da Aritmética. □

Observe que *não* provamos que $p_1 p_2 \ldots p_m + 1$ é primo para algum conjunto finito de primos (por exemplo, os m primeiros primos). Aliás, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ não é primo. Não se conhece nenhuma fórmula simples que gere sempre números primos (veja a seção **??** para uma discussão sobre este assunto).

Embora a quantidade de primos seja infinita, uma questão natural é saber o quão "raros" ou "frequentes" eles são. Na segunda parte do livro, discutiremos mais a fundo esta questão sobre a distribuição dos primos. Por outro lado, é interessante notar que existem cadeias arbitrariamente longas de números compostos consecutivos: na sequência

$$(k+1)! + 2, (k+1)! + 3, (k+1)! + 4, \ldots, (k+1)! + (k+1),$$

nenhum termo é primo, pois eles admitem fatores próprios $2, 3, 4, \ldots, k+1$, respectivamente.

Uma interessante prova alternativa, devida a Erdős, de que existem infinitos primos é a seguinte:

Suponha, por contradição, que existe um número finito de primos, digamos $p_1, p_2, \ldots, p_k$. Seja n um número natural. Então podemos escrever qualquer número $m \leq n$ na forma $m = m_1^2 m_2$, onde $m_1^2 \leq n$ e

$$m_2 = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \qquad \text{onde } a_k = 0 \text{ ou } 1 \text{ para cada } k.$$

Assim, considerando todas as possíveis maneiras de escrever os naturais $m \leq n$, temos: 2^k escolhas para m_2 e no máximo $\lfloor \sqrt{n} \rfloor$ escolhas para m_1. Ou seja, para todo n natural, vale que

$$n \leq 2^k \sqrt{n}$$

absurdo, pois esta desigualdade não vale para n suficientemente grande. □

Exemplo 1.18 (OIbM1987). *A sequência p_n é definida da seguinte forma:*

(i) $p_1 = 2$.

(ii) Para todo $n \geq 2$, p_n é o maior divisor primo da expressão

$$p_1 p_2 p_3 \cdots p_{n-1} + 1.$$

Demonstrar que p_n é diferente de 5.

Solução: Dado que $p_1 = 2$, $p_2 = 3$, $p_3 = 7$, segue-se que para qualquer $n \geq 3$, $p_1 p_2 \cdots p_{n-1}$ é múltiplo de 2 e de 3, portanto $p_1 p_2 \cdots p_{n-1} + 1$ não é múltiplo nem de 2 nem de 3. Além disso, como $p_1 = 2$, então p_n é ímpar para todo $n \geq 2$, assim $p_1 p_2 \cdots p_{n-1}$ não é múltiplo de 4.

Suponhamos que exista n tal que $p_n = 5$, isto é, o maior divisor primo de $p_1 p_2 \cdots p_{n-1} + 1$ é 5. Como 2 e 3 não dividem $p_1 p_2 \cdots p_{n-1} + 1$, temos que

$$p_1 p_2 \cdots p_{n-1} + 1 = 5^k.$$

Portanto

$$p_1 p_2 \cdots p_{n-1} = 5^k - 1 = (5-1)(5^{k-1} + 5^{k-2} + \cdots + 5 + 1),$$

donde $4 \mid p_1 p_2 \cdots p_{n-1}$, uma contradição. □

Exemplo 1.19. *Determine todas as ternas (a, b, c) de inteiros positivos tais que $a^2 = 2^b + c^4$.*

Solução: Como $a^2 = 2^b + c^4 \iff (a - c^2)(a + c^2) = 2^b$, pelo Teorema Fundamental da Aritmética existem dois naturais $m > n$ tais que $m + n = b$, $a - c^2 = 2^n$ e $a + c^2 = 2^m$. Subtraindo as duas últimas equações, obtemos que $2c^2 = 2^m - 2^n$, assim $c^2 = 2^{n-1}(2^{m-n} - 1)$. Como 2^{n-1} e $2^{m-n} - 1$ são primos entre si e o seu produto é um quadrado perfeito (i.e. os expoentes das potências de primos distintos são pares), novamente pelo Teorema Fundamental da Aritmética 2^{n-1} e $2^{m-n} - 1$ devem ser ambos quadrados perfeitos, logo $n - 1$ é par e $2^{m-n} - 1 = (2k-1)^2$ para algum inteiro positivo k. Como $2^{m-n} = (2k-1)^2 + 1 = 4k(k-1) + 2$ é divisível por 2 mas não por 4, temos $m - n = 1$. Assim, fazendo $n - 1 = 2t$, temos que todas as soluções são da forma $(a, b, c) = (3 \cdot 2^{2t}, 4t + 3, 2^t)$ com $t \in \mathbb{N}$ e é fácil verificar que todos os números desta forma são soluções. □

Segue do Teorema Fundamental da Aritmética que todo divisor de $n = p_1^{e_1} \dots p_m^{e_m}$ é da forma

$$p_1^{d_1} \dots p_m^{d_m}$$

com $0 \le d_i \le e_i$. Assim, obtemos o outro algoritmo usual para calcular o mdc de dois números: fatoramos os dois números em primos e tomamos os fatores comuns com os menores expoentes. Este algoritmo é bem menos eficiente do que o de Euclides para inteiros grandes (que em geral não sabemos fatorar de forma eficiente computacionalmente) mas é instrutivo saber que os dois algoritmos dão o mesmo resultado. Além disso, este algoritmo tem consequências teóricas importantes, como por exemplo o

Corolário 1.20. *Se* $\operatorname{mdc}(a, n) = \operatorname{mdc}(b, n) = 1$, *então* $\operatorname{mdc}(ab, n) = 1$.

Demonstração: Evidente a partir do algoritmo descrito acima. □

Para encerrar esta seção, vejamos ainda algumas outras aplicações do Teorema Fundamental da Aritmética.

Proposição 1.21. *Seja* $n = p_1^{e_1} \dots p_m^{e_m}$ *a fatoração de* n *em potências de primos distintos* p_i *e seja* $\sigma_k(n) \stackrel{\text{def}}{=} \sum_{d \mid n,\ d>0} d^k$ *a soma das* k*-ésimas potências dos divisores positivos de* n*. Então*

$$\sigma_k(n) = \frac{p_1^{(e_1+1)k} - 1}{p_1^k - 1} \cdot \ldots \cdot \frac{p_m^{(e_m+1)k} - 1}{p_m^k - 1}.$$

Para $k = 0$*, a fórmula acima deve ser interpretada tomando-se o limite* $k \to 0$*, de modo que a quantidade de divisores positivos de* n *é* $\sigma_0(n) = (e_1 + 1) \cdots (e_m + 1)$.

Demonstração: Como a soma na definição de $\sigma_k(n)$ percorre todos os números da forma $d^k = p_1^{d_1 k} \dots p_m^{d_m k}$ com $0 \le d_i \le e_i$, temos a seguinte fatoração:

$$\sigma_k(n) = (1 + p_1^k + p_1^{2k} + \cdots + p_1^{e_1 k}) \cdot \ldots \cdot (1 + p_m^k + p_m^{2k} + \cdots + p_m^{e_m k}).$$

Somando as progressões geométricas $1 + p_i^k + p_i^{2k} + \cdots + p_i^{e_i k} = \frac{p_i^{(e_i+1)k} - 1}{p_i^k - 1}$, o resultado segue. □

Proposição 1.22 (Fatores do Fatorial)**.** *Seja* p *um primo. Então a maior potência de* p *que divide* $n!$ *é* p^α *onde*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Observe que a soma acima é finita pois os termos $\left\lfloor \frac{n}{p^i} \right\rfloor$ são eventualmente zero.

Demonstração: No produto $n! = 1 \cdot 2 \cdot \ldots \cdot n$, apenas os múltiplos de p contribuem com um fator p. Há $\left\lfloor \frac{n}{p} \right\rfloor$ tais múltiplos entre 1 e n. Destes, os que são múltiplos de p^2 contribuem com um fator p extra e há $\left\lfloor \frac{n}{p^2} \right\rfloor$ tais fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p e assim por diante, resultando na fórmula acima. □

Exemplo 1.23. *Determine com quantos zeros termina* $1000!$.

Solução: O problema é equivalente a determinar qual a maior potência de 10 que divide $1000!$ e como há muito mais fatores 2 do que 5 em $1000!$, o expoente desta potência coincide com o da maior potência de 5 que divide $1000!$, ou seja,

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 249.$$

Assim, $1000!$ termina com 249 zeros. □

Problemas Propostos

1.1 (IMO1959). *Mostre que a fração* $\frac{21n+4}{14n+3}$ *é irredutível para todo* n *natural.*

1.2. *Encontre todos os inteiros positivos tais que*

(a) $n+1 \mid n^3-1$

(b) $2n-1 \mid n^3+1$

(c) $\frac{1}{n}+\frac{1}{m}=\frac{1}{143}$

(d) $2n^3+5 \mid n^4+n+1$

1.3. *Demonstre:*

(a) se $m \mid a-b$, *então* $m \mid a^k-b^k$ *para todo natural* k.

(b) se $f(x)$ *é um polinômio com coeficientes inteiros e* a *e* b *são inteiros quaisquer, então* $a-b \mid f(a)-f(b)$.

(c) se k *é um natural ímpar, então* $a+b \mid a^k+b^k$.

1.4. *Mostre que*

(a) $2^{15}-1$ *e* $2^{10}+1$ *são primos entre si.*

(b) $2^{32}+1$ *e* 2^4+1 *são primos entre si.*

1.5. *Demonstrar que* $(n-1)^2 \mid n^k-1$ *se, e só se,* $n-1 \mid k$.

1.6 (IMO1992). *Encontrar todos os inteiros* a, b, c *com* $1 < a < b < c$ *tais que* $(a-1)(b-1)(c-1)$ *é divisor de* $abc-1$.

Dica: Mostrar primeiro que $a \leq 4$ *e considerar os possíveis casos.*

1.7 (IMO1998). *Determine todos os pares de inteiros positivos* (a, b) *tais que* ab^2+b+7 *divide* a^2b+a+b.

Dica: Mostre que $ab^2+b+7 \mid 7a-b^2$ *e considerar três casos:* $7a-b^2$ *maior, menor ou igual a zero.*

1.8. *Mostre que, se* $n > 1$, *então*

$$\sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

não é um número inteiro.

1.9 (OBM1997). *Sejam* $c \in \mathbb{Q}$, $f(x) = x^2 + c$. *Definimos*

$$f^0(x) = x, \quad f^{n+1}(x) = f(f^n(x)), \forall n \in \mathbb{N}.$$

Dizemos que $x \in \mathbb{R}$ *é pré-periódico se* $\{f^n(x), n \in \mathbb{N}\}$ *é finito. Mostre que* $\{x \in \mathbb{Q} \mid x$ *é pré-periódico*$\}$ *é finito.*

1.10. *Demonstrar que se* $\operatorname{mdc}(a, 2^{n+1}) = 2^n$ *e* $\operatorname{mdc}(b, 2^{n+1}) = 2^n$, *então* $\operatorname{mdc}(a+b, 2^{n+1}) = 2^{n+1}$.

1.11. *Demonstrar que se* a, b, c, d, m *e* n *são inteiros tais que* $ad-bc=1$ *e* $mn \neq 0$, *então*

$$\operatorname{mdc}(am+bn, cm+dn) = \operatorname{mdc}(m, n).$$

1.12. *Seja F_n o n-ésimo termo da sequência de Fibonacci.*

(a) Encontrar dois números inteiros a e b tais que $233a + 144b = 1$ (observe que 233 e 144 são termos consecutivos da sequência de Fibonacci).

(b) Mostre que $\operatorname{mdc}(F_n, F_{n+1}) = 1$ para todo $n \geq 0$.

(c) Determine x_n e y_n tais que $F_n \cdot x_n + F_{n+1} \cdot y_n = 1$.

1.13. *Sejam a e b dois inteiros positivos e d seu máximo divisor comum. Demonstrar que existem dois inteiros positivos x e y tais que $ax - by = d$.*

1.14. *Definimos a* sequência de frações de Farey *de ordem n como o conjunto de frações reduzidas $\frac{a}{b}$ tais que $0 \leq \frac{a}{b} \leq 1$, $1 \leq b \leq n$. Por exemplo a sequência de Farey de ordem 3 é $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$.*

(a) Demonstrar que se $\frac{a}{b}$ e $\frac{c}{d}$ são dois termos consecutivos de uma sequência de Farey, então $cb - ad = 1$.

(b) Demonstrar que se $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}$ são três termos consecutivos de uma sequência de Farey, então $\frac{a_2}{b_2} = \frac{a_1+a_3}{b_1+b_3}$.

1.15. *Utilize indução em $\min\{a, b\}$ e o algoritmo de Euclides para mostrar que $ax + by = \operatorname{mdc}(a, b)$ admite solução com $x, y \in \mathbb{Z}$, obtendo uma nova demonstração do teorema de Bachet-Bézout.*

1.16. *Sejam a e b números inteiros positivos. Considere o conjunto*

$$C = \{ax + by \mid x, y \in \mathbb{N}\}.$$

Lembre-se de que já mostramos no exemplo 1.15 que todo número maior que $ab-a-b$ pertence a C.

(a) Demonstre que o número $ab - a - b$ não pertence a C.

(b) Achar a quantidade de números inteiros positivos que não pertencem a C.

1.17 (IMO1984). *Dados os inteiros positivos a, b e c, dois a dois primos entre si, demonstrar que $2abc - ab - bc - ca$ é o maior número inteiro que não pode expressar-se na forma $xbc + yca + zab$ com x, y e z inteiros não negativos.*

1.18 (IMO1977). *Sejam a, b inteiros positivos. Quando dividimos $a^2 + b^2$ por $a + b$, o quociente é q e o resto é r. Encontrar todos os a, b tais que $q^2 + r = 1977$.*

1.19. *Demonstrar que $\operatorname{mdc}(2^a - 1, 2^b - 1) = 2^{\operatorname{mdc}(a,b)} - 1$ para todo $a, b \in \mathbb{N}$.*

Pelo algoritmo de Euclides aplicado aos expoentes, basta mostrar que $\operatorname{mdc}(2^{bq+r} - 1, 2^b - 1) = \operatorname{mdc}(2^b - 1, 2^r - 1)$. Mas isto segue novamente do lema de Euclides, pois $2^{bq+r} - 1 = 2^r(2^{bq} - 1) + 2^r - 1$ e $2^{bq} - 1 = (2^b - 1)(2^{b(q-1)} + 2^{b(q-2)} + \cdots + 2^b + 1)$ é um múltiplo de $2^b - 1$.

1.20. *Encontrar todas as funções $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ satisfazendo simultaneamente as seguintes propriedades*

(i) $f(a, a) = a$.

(ii) $f(a, b) = f(b, a)$.

(iii) Se $a > b$, então $f(a, b) = \frac{a}{a-b} f(a - b, b)$.

1.21. *Mostre que se n é um número natural composto, então n é divisível por um primo p com $p \leq \lfloor \sqrt{n} \rfloor$.*

1.22 (IMO1989). *Prove que, para todo inteiro positivo n, existem n inteiros positivos consecutivos, nenhum dos quais é potência de primo.*

1.23 (Chi1998). *Encontrar todos os n para os quais $1+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}$ divide 2^{2000}.*

1.24 (IMO2002). *Sejam $d_1 < d_2 < \cdots < d_k$ os divisores positivos de um inteiro $n > 1$. Seja $d = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$. Mostre que $d < n^2$ e encontrar todos os n para os quais $d \mid n^2$. Temos $d = \frac{n^2}{d_kd_{k-1}} + \frac{n^2}{d_{k-1}d_{k-2}} + \cdots + \frac{n^2}{d_2d_1} < n^2 \cdot (\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots) = n^2 \cdot (\frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \cdots) = n^2$. Por outro lado, se p é o menor primo que divide n^2, temos que $d \geq d_{k-1}d_k = \frac{n^2}{p}$. Como $\frac{n^2}{p}$ é o maior divisor próprio de n^2 e $d > d_{k-1}d_k$ se $k > 2$, temos que $d \mid n^2$ se, e só se, $n = p$ é primo.*

1.25 (IMO1997). *Encontrar todos os pares (x, y) de inteiros positivos tais que $x^{y^2} = y^x$.*
Dica: Sejam $x = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ e $y = p_1^{\beta_1} \dots p_n^{\beta_n}$ as fatorações canônicas de x e y. Mostre que $\alpha_j = t\beta_j$ e $x = y^t$ para algum $t \in \mathbb{Q}$ e limite os valores de t.

1.26. *Generalizar o resultado anterior para $x^{y^n} = y^x$, onde x e y são inteiros positivos.*

1.27 (IMO1984). *Sejam a, b, c, d inteiros ímpares tais que $0 < a < b < c < d$ e $ad = bc$. Demonstre que se $a + d = 2^k$ e $b + c = 2^m$ para inteiros k e m, então $a = 1$.*

1.4 Congruências

Sejam $a, b, n \in \mathbb{Z}$. Dizemos que *a é congruente a b módulo n*, e escrevemos

$$a \equiv b \pmod{n}$$

se $n \mid a - b$, ou seja, se a e b deixam o mesmo resto na divisão por n. Por exemplo, temos que $17 \equiv 3 \pmod 7$ e $10 \equiv -5 \pmod 3$.

Proposição 1.24. *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$ temos:*

1. *(Reflexividade) $a \equiv a \pmod n$;*
2. *(Simetria) se $a \equiv b \pmod n$, então $b \equiv a \pmod n$;*
3. *(Transitividade) se $a \equiv b \pmod n$ e $b \equiv c \pmod n$, então $a \equiv c \pmod n$;*
4. *(Compatibilidade com a soma e diferença) Podemos somar e subtrair "membro a membro":*

$$\begin{cases} a \equiv b \pmod n \\ c \equiv d \pmod n \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod n \\ a - c \equiv b - d \pmod n \end{cases}$$

   Em particular, se $a \equiv b \pmod n$, então $ka \equiv kb \pmod n$ para todo $k \in \mathbb{Z}$.

5. *(Compatibilidade com o produto) Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b \pmod n \\ c \equiv d \pmod n \end{cases} \implies ac \equiv bd \pmod n$$

   Em particular, se $a \equiv b \pmod n$, então $a^k \equiv b^k \pmod n$ para todo $k \in \mathbb{N}$.

6. *(Cancelamento) Se* $\mathrm{mdc}(c,n)=1$, *então*

$$ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n}.$$

Demonstração: Para o item *(1)* basta observar que $n \mid a-a=0$. Em *(2)*, se $n \mid a-b$, então $n \mid -(a-b) \iff n \mid b-a$. Em *(3)*, se $n \mid a-b$ e $n \mid b-c$, então $n \mid (a-b)+(b-c) \iff n \mid a-c$. Em *(4)* e *(5)*, se $n \mid a-b$ e $n \mid c-d$, então $n \mid (a-b)+(c-d) \iff n \mid (a+c)-(b+d)$, $n \mid (a-b)-(c-d) \iff n \mid (a-c)-(b-d)$ e $n \mid (a-b)c+(c-d)b \iff n \mid ac-bd$. Finalmente, como $\mathrm{mdc}(c,n)=1$ temos que $n \mid ac-bc \iff n \mid (a-b)c \iff n \mid a-b$ pela proposição 1.9. □

As propriedades acima mostram que a relação $\equiv \pmod{n}$ ("ser congruente módulo n") tem um comportamento muito similar à relação de igualdade usual. São estas propriedades que tornam as congruências tão úteis em problemas de divisibilidade. Vejamos alguns exemplos.

Exemplo 1.25. *Demonstrar que* $31 \mid 20^{15}-1$.

Solução: Isto é equivalente a demonstrar que $20^{15} \equiv 1 \pmod{31}$. Para isso observemos que

$$20 \equiv -11 \pmod{31} \qquad (*)$$

e assim $20^2 \equiv (-11)^2 \pmod{31} \iff 20^2 \equiv 121 \pmod{31}$. Como $121 \equiv -3 \pmod{31}$ temos

$$20^2 \equiv -3 \pmod{31}. \qquad (**)$$

Multiplicando $(*)$ e $(**)$ membro a membro, obtemos $20^3 \equiv 33 \pmod{31}$ e, como $33 \equiv 2 \pmod{31}$,

$$20^3 \equiv 2 \pmod{31}.$$

Elevando a 5, temos que $20^{15} \equiv 32 \pmod{31}$ e como $32 \equiv 1 \pmod{31}$, obtemos $20^{15} \equiv 1 \pmod{31}$, como desejado. □

Exemplo 1.26. *Encontre os restos das divisões de*

1. 3^{1000} *por* 101
2. $5^{3^{20}}$ *por* 13

Solução: Como $3^4 \equiv -20 \pmod{101}$, elevando ao quadrado obtemos $3^8 \equiv 400 \pmod{101} \iff 3^8 \equiv -4 \pmod{101}$. Multiplicando por 3^2, obtemos $3^{10} \equiv -36 \pmod{101}$. Portanto

$$\begin{aligned}
3^{20} \equiv 1296 \pmod{101} &\iff 3^{20} \equiv -17 \pmod{101}\\
3^{40} \equiv 289 \pmod{101} &\iff 3^{40} \equiv -14 \pmod{101}\\
3^{80} \equiv 196 \pmod{101} &\iff 3^{80} \equiv -6 \pmod{101}\\
3^{80}\cdot 3^{20} \equiv (-6)\cdot(-17) \pmod{101} &\iff 3^{100} \equiv 1 \pmod{101}.
\end{aligned}$$

Assim, elevando a última congruência a 10, obtemos $3^{1000} \equiv 1 \pmod{101}$, ou seja, 3^{1000} deixa resto 1 na divisão por 101.

Para encontrar o resto da divisão de $5^{3^{20}}$ por 13, note que como $5^4 \equiv 1 \pmod{13}$, os restos de 5^n por 13 se repetem com período 4:

$$\begin{array}{llll}
5^0 \equiv 1 \pmod{13} & 5^4 \equiv 1 \pmod{13} & \\
5^1 \equiv 5 \pmod{13} & 5^5 \equiv 5 \pmod{13} & \\
5^2 \equiv -1 \pmod{13} & 5^6 \equiv -1 \pmod{13} & \\
5^3 \equiv -5 \pmod{13} & 5^7 \equiv -5 \pmod{13} & \cdots
\end{array}$$

Por outro lado, temos $3 \equiv -1 \pmod{4} \implies 3^{20} \equiv 1 \pmod{4}$, isto é, 3^{20} deixa resto 1 na divisão por 4. Assim, $5^{3^{20}} \equiv 5^1 \pmod{13}$, ou seja, $5^{3^{20}}$ deixa resto 5 na divisão por 13. □

O problema a seguir tem uma história interessante. Em um artigo publicado em 1969, D. J. Lewis afirmava que a equação $x^3 - 117y^3 = 5$ tem no máximo 18 soluções inteiras. Na verdade, ela não possui nenhuma, como foi provado dois anos mais tarde por R. Finkelstein e H. London, utilizando métodos de Teoria Algébrica dos Números. Em 1973, F. Halter-Koch e V. Şt. Udresco observaram independentemente que existe uma prova muito mais simples deste fato, como mostra o exemplo a seguir.

Exemplo 1.27. *Mostre que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras.*

Solução: Observe que como 117 é múltiplo de 9, qualquer solução inteira deve satisfazer

$$x^3 - 117y^3 \equiv 5 \pmod 9 \iff x^3 \equiv 5 \pmod 9.$$

Porém, x só pode deixar resto $0, 1, \ldots, 8$ na divisão por 9. Analisando estes 9 casos, temos

$x \bmod 9$	0	1	2	3	4	5	6	7	8
$x^3 \bmod 9$	0	1	8	0	1	8	0	1	8

Ou seja, x^3 só pode deixar resto 0, 1 ou 8 na divisão por 9. Logo $x^3 \equiv 5 \pmod 9$ é impossível e a equação não possui soluções inteiras. □

Exemplo 1.28 (AusPol2002)**.** *Encontrar todas as ternas (a, b, c) de inteiros não negativos tais que $2^a + 2^b + 1$ é múltiplo de $2^c - 1$.*

Solução: O problema pede para determinar quando $2^a + 2^b + 1 \equiv 0 \pmod{2^c - 1}$. Note que como $2^c \equiv 1 \pmod{2^c - 1}$, escrevendo $a = cq_1 + a'$ e $b = cq_2 + b'$ com $0 \le a', b' < c$ temos que

$$\begin{aligned} & 2^a + 2^b + 1 \equiv 0 \pmod{2^c - 1} \\ \iff & (2^c)^{q_1} \cdot 2^{a'} + (2^c)^{q_2} \cdot 2^{b'} + 1 \equiv 0 \pmod{2^c - 1} \\ \iff & 2^{a'} + 2^{b'} + 1 \equiv 0 \pmod{2^c - 1} \end{aligned}$$

que é o mesmo problema com a' e b' no lugar de a e b. Assim, basta resolver o problema supondo $0 \le a, b < c$. Temos alguns casos a analisar.

Não há soluções com $c = 0$ e para $c = 1$ temos que $(a, b, 1)$ é solução para todos os $a, b \ge 0$. Se $c = 2$, temos que apenas $(0, 0, 2)$ é solução com $0 \le a, b < c = 2$, o que dá origem às soluções $(2m, 2n, 2)$ para todos os m e n naturais. Se $c = 3$, temos que apenas $(1, 2, 3)$ e $(2, 1, 3)$ são soluções com $0 \le a, b < c = 3$, o que nos fornece soluções $(1+3m, 2+3n, 3)$ e $(2+3m, 1+3n, 3)$ para todos os m e n naturais. Finalmente, para $c \ge 4$, temos que se $a < c - 1$ ou $b < c - 1$, então

$$3 \le 2^a + 2^b + 1 \le 2^{c-1} + 2^{c-2} + 1 = 3 \cdot 2^{c-2} + 1 < 2^c - 1$$

e assim $2^a + 2^b + 1$ não pode ser múltiplo de $2^c - 1$. Neste caso devemos ter $a = b = c - 1$ e $2^{c-1} + 2^{c-1} + 1 \equiv 0 \pmod{2^c - 1} \iff 2^c + 1 \equiv 0 \pmod{2^c - 1} \iff 2 \equiv 0 \pmod{2^c - 1}$, o que não ocorre pois $2^c - 1 \ge 15$ não pode dividir 2. Logo não há soluções neste último caso.

Resumindo, as ternas pedidas são $(m, n, 1)$, $(2m, 2n, 2)$, $(1 + 3m, 2 + 3n, 3)$ e $(2 + 3m, 1 + 3n, 3)$ onde m e n são naturais arbitrários. □

1.5 Bases

A notação usual para naturais é a chamada base 10, com algarismos $0, \ldots, 9$. Isto significa, por exemplo, que

$$196883 = 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0.$$

O teorema abaixo mostra como escrever qualquer natural em qualquer base d.

Teorema 1.29. *Seja $n \geq 0$ e $d > 1$. Então existe uma única sequência (os "dígitos" de n na base d) $a_0, \ldots, a_k, \ldots$ com as seguintes propriedades:*

1. *para todo k, $0 \leq a_k < d$,*
2. *existe m tal que se $k \geq m$, então $a_k = 0$,*
3. *$n = \sum_{k \geq 0} a_k d^k$.*

Demonstração: Escrevemos $n = n_0 = n_1 d + a_0$, $0 \leq a_0 < d$, $n_1 = n_2 d + a_1$, $0 \leq a_1 < d$ e em geral $n_k = n_{k+1} d + a_k$, $0 \leq a_k < d$. Nossa primeira afirmação é que $n_k = 0$ para algum valor de k. De fato, se $n_0 < d^m$, então $n_1 = \lfloor \frac{n_0}{d} \rfloor < d^{m-1}$ e mais geralmente, por indução, $n_k < d^{m-k}$; fazendo $k \geq m$ temos $n_k < 1$ donde $n_k = 0$. Segue daí que $a_k = 0$ para $k \geq m$. A identidade do item *3* é facilmente demonstrada por indução.

Para a unicidade, suponha $\sum_{k \geq 0} a_k d^k = \sum_{k \geq 0} b_k d^k$. Se as sequências a_k e b_k são distintas existe um menor índice, digamos j, para o qual $a_j \neq b_j$. Podemos escrever $a_j + \sum_{k > j} a_k d^{k-j} = b_j + \sum_{k > j} b_k d^{k-j}$ donde $a_j \equiv b_j \pmod{d}$, o que é uma contradição, pois $0 < |a_j - b_j| < d$ e portanto $a_j - b_j$ não pode ser um múltiplo de d. $\square$

Ignorando os dígitos 0's iniciais, denotamos por $(a_n a_{n-1} \cdots a_1 a_0)_d$ o natural cuja representação na base d tem dígitos a_k como no teorema acima:

$$(a_n a_{n-1} \cdots a_1 a_0)_d \stackrel{\text{def}}{=} \sum_{0 \leq k \leq n} a_k d^k.$$

Muitos dos famosos critérios de divisibilidade que aprendemos na escola decorrem diretamente da representação acima. Por exemplo, se $N = (a_n a_{n-1} \cdots a_1 a_0)_{10}$, como $10 \equiv 1 \pmod{9}$, temos que $10^k \equiv 1 \pmod{9}$, donde

$$N = \sum_{0 \leq k \leq n} a_k 10^k \equiv \sum_{0 \leq k \leq n} a_k \pmod{9}.$$

Segue que N e a soma de seus dígitos na base 10 possuem o mesmo resto na divisão por 9; em particular N é divisível por 9 se, e só se, a soma de seus dígitos $a_0 + \cdots + a_n$ é divisível por 9.

De forma similar, para o critério de divisibilidade por 11, observemos que $10 \equiv -1 \pmod{11}$, logo

$$N = \sum_{0 \leq k \leq n} a_k 10^k \equiv \sum_{0 \leq k \leq n} (-1)^k a_k \pmod{11}$$

e assim um número é divisível por 11 se, e só se, a soma dos dígitos em posição par menos a soma dos dígitos em posição ímpar é divisível por 11. De igual forma, podemos encontrar critérios de divisibilidade por 7, 13 e 37, que deixamos como exercício para o leitor enunciá-los e demonstrá-los (utilize o fato que $10^3 \equiv -1 \pmod{7}$, $10^3 \equiv -1 \pmod{13}$ e $10^3 \equiv 1 \pmod{37}$).

Exemplo 1.30. *Encontrar os últimos dois algarismos em representação decimal de* 3^{200}.

SOLUÇÃO: Como

$$\begin{aligned}(a_n a_{n-1} \cdots a_1 a_0)_{10} &= 10^2 \cdot (a_n \cdot 10^{n-2} + \cdots + a_2) + (10 \cdot a_1 + a_0) \\ &= 100 \cdot (a_n \ldots a_2)_{10} + (a_1 a_0)_{10}\end{aligned}$$

temos que o número formado pelos dois últimos algarismos de $(a_n \cdots a_1 a_0)_{10}$ é o resto da divisão deste número por 100, logo o problema se resume a calcular 3^{200} módulo 100. Podemos utilizar o binômio de Newton para simplificar as contas:

$$3^{200} = 9^{100} = (10-1)^{100} = \sum_{0 \le k \le 100} \binom{100}{k} 10^{100-k} (-1)^k,$$

logo $3^{200} \equiv -\binom{100}{99} 10 + \binom{100}{100} \pmod{100} \iff 3^{200} \equiv 1 \pmod{100}$ e assim os dois últimos dígitos de 3^{200} são 01. □

Exemplo 1.31. *Demonstrar que, para todo n natural ímpar,*

$$s_n = 2^{2n} \cdot (2^{2n+1} - 1)$$

termina em 28 *quando escrito em notação decimal.*

SOLUÇÃO: Vamos mostrar por indução em n que s_n termina em 28. Para $n = 1$ temos que $s_1 = 28$. Suponhamos que para algum $n \ge 1$ ímpar s_n termina em 28 e vamos mostrar que s_{n+2} termina em 28 ou, equivalentemente, que $100 \mid s_{n+2} - s_n$. Temos

$$\begin{aligned}s_{n+2} - s_n &= 2^{2(n+2)} \cdot (2^{2(n+2)+1} - 1) - 2^{2n} \cdot (2^{2n+1} - 1) \\ &= 2^{2n} \cdot (16 \cdot 2^{2n+5} - 16 - 2^{2n+1} + 1) \\ &= 5 \cdot 2^{2n} \cdot (51 \cdot 2^{2n+1} - 3).\end{aligned}$$

Como, para n ímpar,

$$\begin{aligned}2^2 \equiv -1 \pmod 5 &\implies 2^{2n} \equiv -1 \pmod 5 \\ &\implies 2^{2n+1} \equiv -2 \pmod 5,\end{aligned}$$

temos que $51 \cdot 2^{2n+1} - 3 \equiv 1 \cdot (-2) - 3 \pmod 5 \iff 51 \cdot 2^{2n+1} - 3 \equiv 0 \pmod 5$. Assim, $s_{n+2} - s_n$ é divisível por $5 \cdot 4 \cdot 5 = 100$. □

1.6 O Anel de Inteiros Módulo n

As semelhanças entre as relações de congruência módulo n e igualdade não são mero fruto do acaso, ambas são instâncias de *relações de equivalência* em $\mathbb{Z}$. Em geral, uma relação $\sim$ sobre um conjunto X é dita de *equivalência* se ela é reflexiva ($x \sim x$ para todo $x \in X$), simétrica ($x \sim y \iff y \sim x$) e transitiva ($x \sim y$ e $y \sim z \implies x \sim z$).

Dar uma relação de equivalência em X é o mesmo que dar uma *partição* $X = \coprod_{\lambda \in \Lambda} X_\lambda$ de X, i.e., uma coleção de subconjuntos $X_\lambda \neq \emptyset$, dois a dois disjuntos, cuja união é X. De fato, dada a partição acima, podemos definir uma relação de equivalência $\sim$ declarando que $x \sim y$ se, e somente se, x e y pertencem a um mesmo X_λ. Reciprocamente, se $\sim$ é uma relação de equivalência, dado um elemento $x \in X$ podemos definir a *classe de equivalência* $\overline{x}$ de x como o conjunto de todos os elementos equivalentes a x:

$$\overline{x} = \{y \in X \mid y \sim x\}.$$

Observe que ou $\overline{x} \cap \overline{y} = \emptyset$ (se $x \not\sim y$) ou $\overline{x} = \overline{y}$ (se $x \sim y$). Assim, as distintas classes de equivalência $\overline{x}$ formam uma partição de X. O conjunto $\{\overline{x} \mid x \in X\}$ das classes de equivalência de $\sim$ é chamado de *quociente* de X por $\sim$ e é denotado por $X/\sim$. Intuitivamente, $X/\sim$ é o conjunto obtido "igualando-se" elementos equivalentes entre si.

Agora aplicamos esta construção geral ao nosso caso. O quociente de $\mathbb{Z}$ pela relação $\equiv \pmod{n}$ é chamado de *anel de inteiros módulo* n e é denotado por uma das notações $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/n$ ou às vezes $\mathbb{Z}_n$. Por exemplo, para $n = 2$, temos que $\mathbb{Z}/2\mathbb{Z}$ possui apenas dois elementos, $\overline{0}$ e $\overline{1}$ (popularmente conhecidos como conjunto dos pares e ímpares, respectivamente).

A definição de $\overline{a}$ como um subconjunto de $\mathbb{Z}$ raramente será importante, sendo apenas uma maneira de formalizar o fato de que estamos "identificando" todos os inteiros que deixam o mesmo resto na divisão por n (como no exemplo dos pares e ímpares acima). Assim, o importante é sabermos que

$$\begin{aligned} \overline{a} = \overline{a'} &\iff a \equiv a' \pmod{n} \\ &\iff a \text{ e } a' \text{ deixam o mesmo resto na divisão por } n. \end{aligned}$$

Se $n > 0$, a divisão euclidiana diz que todo inteiro a é côngruo a um único inteiro a' com $0 \le a' < n$; podemos reescrever este fato na nossa nova linguagem como

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Os itens *(4)* e *(5)* da proposição 1.24 dizem que as operações de soma, diferença e produto são compatíveis com a relação de congruência. Uma formulação mais abstrata da mesma ideia é dizer que as operações $+$, $-$ e $\cdot$ *passam ao quociente*, i.e., que podemos definir a soma, subtração e o produto de classes de congruência por

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} - \overline{b} &= \overline{a-b} \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b} \end{aligned}$$

respectivamente. A dúvida à primeira vista seria se a escolha de a e b não afeta a resposta: afinal existem infinitos inteiros a' e b' com $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Os itens *(4)* e *(5)* da proposição são exatamente o que precisamos: eles nos dizem que nestas condições $\overline{a \pm b} = \overline{a' \pm b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$, de modo que as operações acima estão bem definidas.

Por exemplo, em $\mathbb{Z}/6\mathbb{Z}$ temos as seguintes tabelas de soma e produto:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

e

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A próxima proposição diz quando podemos "dividir" por a módulo n, isto é, quando o "inverso multiplicativo" de a módulo n está definido:

Proposição 1.32. *Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod{n}$ se, e somente se,* $\mathrm{mdc}(a, n) = 1$.

DEMONSTRAÇÃO: Temos que $ab \equiv 1 \pmod{n}$ admite solução na variável b se, e somente se, existem $b, k \in \mathbb{Z}$ tais que $ab - 1 = nk \iff ab - nk = 1$. Pelo corolário 1.8 do teorema de Bachet-Bézout, isto ocorre se, e só se, $\mathrm{mdc}(a, n) = 1$. □

Dizemos portanto que a é *invertível* módulo n quando $\mathrm{mdc}(a, n) = 1$ e chamamos b com $ab \equiv 1 \pmod{n}$ de *inverso multiplicativo* de a módulo n. O inverso é sempre único módulo n: se $ab \equiv ab' \equiv 1 \pmod{n}$ temos

$$b \equiv b \cdot 1 \equiv b \cdot (ab') \equiv (ba) \cdot b \equiv 1 \cdot b' \equiv b' \pmod{n}.$$

Assim, $\overline{b}$ está bem definido e, em termos de classes de congruência, temos que $\overline{a} \cdot \overline{b} = \overline{1}$; denotamos $\overline{b}$ por $(\overline{a})^{-1}$. Note que pela demonstração da proposição acima calcular $(\overline{a})^{-1}$ é equivalente a resolver a equação diofantina linear $ax + ny = 1$ e para isto podemos utilizar o método do exemplo 1.14.

Definimos o *grupo de unidades* $(\mathbb{Z}/n\mathbb{Z})^\times \subset \mathbb{Z}/n\mathbb{Z}$ do anel de inteiros módulo n como o subconjunto formado pelos elementos invertíveis de $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{mdc}(a, n) = 1\}.$$

Observe que o produto de elementos de $(\mathbb{Z}/n\mathbb{Z})^\times$ é sempre um elemento de $(\mathbb{Z}/n\mathbb{Z})^\times$. Por exemplo, temos a seguinte tabela de multiplicação em $(\mathbb{Z}/15\mathbb{Z})^\times$:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{14}$	$\overline{1}$	$\overline{7}$	$\overline{11}$	$\overline{13}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{13}$	$\overline{2}$	$\overline{14}$	$\overline{7}$	$\overline{11}$
$\overline{7}$	$\overline{7}$	$\overline{14}$	$\overline{13}$	$\overline{4}$	$\overline{11}$	$\overline{2}$	$\overline{1}$	$\overline{8}$
$\overline{8}$	$\overline{8}$	$\overline{1}$	$\overline{2}$	$\overline{11}$	$\overline{4}$	$\overline{13}$	$\overline{14}$	$\overline{7}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{14}$	$\overline{2}$	$\overline{13}$	$\overline{1}$	$\overline{8}$	$\overline{4}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\overline{7}$	$\overline{1}$	$\overline{14}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{14}$	$\overline{14}$	$\overline{13}$	$\overline{11}$	$\overline{8}$	$\overline{7}$	$\overline{4}$	$\overline{2}$	$\overline{1}$

Uma aplicação do inverso multiplicativo é o famoso *teorema de Wilson.* Primeiramente precisamos de um lema.

Lema 1.33. *Se p é primo, então as únicas soluções de $x^2 = \overline{1}$ em $\mathbb{Z}/(p)$ são $\overline{1}$ e $-\overline{1}$. Em particular, se $x \in (\mathbb{Z}/(p))^\times - \{1, -1\}$, então $x^{-1} \neq x$ em $\mathbb{Z}/(p)$.*

DEMONSTRAÇÃO: Temos

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\iff p \mid (x^2 - 1) \iff p \mid (x-1)(x+1) \\ &\iff p \mid x - 1 \text{ ou } p \mid x + 1 \\ &\iff x \equiv 1 \pmod{p} \text{ ou } x \equiv -1 \pmod{p} \end{aligned}$$

donde o resultado segue. □

Teorema 1.34 (Wilson)**.** *Seja $n > 1$. Então $n \mid (n-1)! + 1$ se, e só se, n é primo. Mais precisamente,*

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \textit{se } n \textit{ é primo} \\ \ \ 0 \pmod{n} & \textit{se } n \textit{ é composto e } n \neq 4. \end{cases}$$

Demonstração: Se n é composto mas não é o quadrado de um primo podemos escrever $n = ab$ com $1 < a < b < n$. Neste caso tanto a quanto b são fatores de $(n-1)!$ e portanto $(n-1)! \equiv 0 \pmod{n}$. Se $n = p^2$, $p > 2$, então p e $2p$ são fatores de $(n-1)!$ e novamente $(n-1)! \equiv 0 \pmod{n}$; isto demonstra que para todo $n \neq 4$ composto temos $(n-1)! \equiv 0 \pmod{n}$.

Se n é primo podemos escrever $(n-1)! \equiv -2 \cdot 3 \cdot \ldots \cdot (n-2) \pmod{n}$; mas pelo lema anterior podemos juntar os inversos aos pares no produto do lado direito, donde $(n-1)! \equiv -1 \pmod{n}$. □

Vejamos uma aplicação do teorema de Wilson.

Teorema 1.35 (Teorema de Wolstenholme)**.** *Seja $p > 3$ um número primo. Então o numerador do número*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

é divisível por p^2.

Demonstração: Note que somando os “extremos” temos

$$\sum_{1 \le i \le p-1} \frac{1}{i} = \sum_{1 \le i \le \frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i}\right) = p \sum_{1 \le i \le \frac{p-1}{2}} \frac{1}{i(p-i)}.$$

Como o mmc dos números de 1 a $p-1$ não é divisível por p, basta mostrar que o numerador da última soma é múltiplo de p. Equivalentemente, como $p \nmid (p-1)!$, devemos mostrar que o inteiro

$$S \stackrel{\text{def}}{=} \sum_{1 \le i \le \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)}$$

é um múltiplo de p. Para $1 \le i \le p-1$, denote por r_i o inverso de i mod p, ou seja, $ir_i \equiv 1 \pmod{p}$. Note que $r_{p-i} \equiv -r_i \pmod{p}$, assim

$$\begin{aligned} S &\equiv \sum_{1 \le i \le \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)} \cdot ir_i(p-i)r_{p-i} \\ &\equiv \sum_{1 \le i \le \frac{p-1}{2}} (p-1)! r_i r_{p-i} \equiv \sum_{1 \le i \le \frac{p-1}{2}} r_i^2 \pmod{p} \end{aligned}$$

pelo teorema de Wilson. Note que como cada r_i é congruente a um dos números $\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, temos que os r_i^2 são congruentes a um dos números $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ módulo p. Vamos mostrar que todos eles aparecem. De fato, se $r_i^2 \equiv r_j^2 \pmod{p}$, então $p \mid (r_i - r_j)(r_i + r_j)$, isto é, $r_i \equiv \pm r_j \pmod{p}$. Multiplicando por ij, temos que $j \equiv \pm i \pmod{p}$, o implica $i = j$ pois $1 \le i, j \le \frac{p-1}{2}$.

Assim, $S \equiv \sum_{1 \le i \le \frac{p-1}{2}} i^2 \pmod{p}$ e como $\sum_{1 \le i \le \frac{p-1}{2}} i^2 = \frac{p(p^2-1)}{24}$ é um múltiplo de p (pois $\mathrm{mdc}(p, 24) = 1$), o resultado segue. □

O teorema de Wilson produz ainda resultados interessantes sobre os coeficientes binomiais. Suponhamos que k e h são inteiros positivos tais que $k + h = p - 1$ onde p é primo. Então

$$\begin{aligned} h!k! &\equiv (-1)^h (p-1)(p-2) \cdots (p-h) k! = (-1)^k (p-1)! \\ &\equiv (-1)^{k+1} \pmod{p}. \end{aligned}$$

Portanto

$$\begin{aligned} & h!k!\binom{p-1}{k} \equiv (p-1)! \pmod{p} \\ \iff & (-1)^{k+1}\binom{p-1}{k} \equiv -1 \pmod{p} \\ \iff & \binom{p-1}{k} \equiv (-1)^k \pmod{p}. \end{aligned}$$

Exemplo 1.36. *Demonstrar que se $p > 3$ é primo, então $p^3 \mid \binom{2p}{p} - 2$.*

Solução: Primeiramente, vamos relembrar algumas identidades com coeficientes binomiais bem conhecidas. Para todo $1 \le i \le p-1$, temos que $\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$ (basta utilizar a definição) enquanto que

$$\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \cdots + \binom{p}{p}^2$$

pois podemos escolher p objetos dentre $2p$ escolhendo i objetos dentre os p primeiros e $p-i$ dos p últimos para todo i entre 0 e p, logo

$$\binom{2p}{p} = \sum_{0\le i\le p}\binom{p}{i}\binom{p}{p-i} = \sum_{0\le i\le p}\binom{p}{i}^2.$$

Utilizando estas identidades, temos que

$$\binom{2p}{p} - 2 = \sum_{1\le i\le p-1}\frac{p^2}{i^2}\binom{p-1}{i-1}^2 = p^2\sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2.$$

Note que $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ é um múltiplo de p para $1 \le i \le p-1$ pois o denominador desta fração não é divisível por p. Assim, $\frac{1}{i^2}\binom{p-1}{i-1}^2 = \frac{1}{p^2}\binom{p}{i}^2$ é inteiro e portanto a soma $\sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2$ é inteira e devemos mostrar que ela é um múltiplo de p. Para isto observemos que cada $1 \le i \le p-1$ é invertível módulo p; seja r_i tal que $1 \le r_i \le p-1$ e $ir_i \equiv 1 \pmod{p}$. Pela unicidade de r_i módulo p, temos que os r_i's formam uma permutação de $1, 2, \ldots, p-1$. Assim, como $\binom{p-1}{i-1} \equiv (-1)^{i-1} \pmod{p}$, temos

$$\begin{aligned} & \sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2 \equiv \sum_{1\le i\le p-1}\frac{(ir_i)^2}{i^2}\binom{p-1}{i-1}^2 \pmod{p} \\ \iff & \sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2 \equiv \sum_{1\le i\le p-1} r_i^2 = \sum_{1\le i\le p-1} i^2 \pmod{p}. \end{aligned}$$

Como $\sum\limits_{1\le i\le p-1} i^2 = \frac{p(p-1)(2p-1)}{6}$ é um múltiplo de p (pois $\mathrm{mdc}(p, 6) = 1$), a prova acaba. □

Os termos grupo e anel empregados nesta seção estão em conformidade com o jargão usualmente utilizado em Álgebra. *Grupo* é o nome emprestado a um conjunto G juntamente com uma operação binária $\cdot$ (produto) que satisfaz os seguintes três axiomas:

1. (Associatividade) Para quaisquer $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

2. (Existência de elemento neutro) Existe um elemento $e \in G$ tal que, para todo $a \in G$, $a \cdot e = e \cdot a = a$.

3. (Existência de inverso) Para qualquer elemento $a \in G$ existe um elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Se, além dos três axiomas acima, o grupo G satisfaz

4. (Comutatividade) Para quaisquer $a, b \in G$, $a \cdot b = b \cdot a$.

então G é chamado de *grupo abeliano*.

Um *anel* é um conjunto A com duas operações binárias $+$ (soma) e $\cdot$ (produto) satisfazendo axiomas que abstraem as propriedades usuais dos inteiros (por exemplo). Estes axiomas são

1. $(A, +)$ é um grupo abeliano com elemento neutro 0.

2. (Associatividade do produto) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a, b, c \in A$.

3. (Elemento neutro do produto) Existe um elemento $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in A$.

4. (Distributividade) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ para todo $a, b, c \in A$.

Se $a \cdot b = b \cdot a$ para todo $a, b \in A$, dizemos que o anel A é *comutativo*. Um anel comutativo $A \neq 0$ (isto é, $0 \neq 1$ em A) é chamado de *domínio* se, para $a, b \in A$, $a \cdot b = 0 \implies a = 0$ ou $b = 0$. Por outro lado, se um anel comutativo $A \neq 0$ é tal que todo elemento não nulo possui inverso multiplicativo (ou seja, $(A \setminus \{0\}, \cdot)$ é um grupo) então dizemos que o anel A é um *corpo*. Um importante resultado é a seguinte

Proposição 1.37. *O anel $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e só se, n é primo.*

Demonstração: Temos que $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e somente se, todo elemento $\overline{a} \neq \overline{0}$ é invertível, ou seja, se e somente se, $\text{mdc}(a, n) = 1$ para todo a com $0 < a < n$. Mas isto é equivalente a n ser primo, pois se n é composto e $a \mid n$ com $1 < a < n$, então $\text{mdc}(a, n) = a \neq 1$. □

Um fato curioso e muito útil quando trabalhamos no corpo $\mathbb{Z}/p\mathbb{Z}$ (p primo) é a seguinte

Proposição 1.38 ("Sonho de todo estudante")**.** *Seja p um primo. Então em $\mathbb{Z}/p\mathbb{Z}$ temos*

$$(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$$

para quaisquer $\overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$.

Demonstração: Devemos mostrar que $(a + b)^p \equiv a^p + b^p \pmod{p}$ para todo $a, b \in \mathbb{Z}$. Temos que se $0 < k < p$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \equiv 0 \pmod{p}$$

pois há um fator p no numerador que não pode ser cancelado com nada que apareça no denominador. Assim, utilizando o binômio de Newton, temos

$$(a + b)^p = \sum_{0 \le k \le p} \binom{p}{k} a^{p-k} b^k \equiv a^p + b^p \pmod{p}$$

como queríamos mostrar. □

1.7 A Função de Euler e o Teorema de Euler-Fermat

Dizemos que um conjunto de n números inteiros $a_1, \dots, a_n$ forma um *sistema completo de restos módulo* n (scr) se

$$\{\overline{a_1}, \overline{a_2}, \dots, \overline{a_n}\} = \mathbb{Z}/(n),$$

isto é, se os a_i representam todas as classes de congruência módulo n. Por exemplo, $0, 1, 2, \dots, n-1$ formam um scr módulo n. Equivalentemente, podemos dizer que $a_1, a_2, \dots, a_n$ formam um scr módulo n se, e somente se, $a_i \equiv a_j \pmod{n}$ implicar $i = j$.

De igual forma, dizemos que os números inteiros $b_1, b_2, \dots, b_{\varphi(n)}$ formam um *sistema completo de invertíveis módulo* n (sci) se

$$\{\bar{b}_1, \bar{b}_2, \dots, \bar{b}_{\varphi(n)}\} = (\mathbb{Z}/(n))^\times,$$

onde $\varphi(n)$ representa o número de elementos de $(\mathbb{Z}/(n))^\times$. Em outras palavras, $b_1, b_2, \dots, b_{\varphi(n)}$ formam um sci módulo n se, e somente se, representam todas as classes de congruência invertíveis módulo n ou, equivalentemente, $\mathrm{mdc}(b_i, n) = 1$ para todo i e $b_i \equiv b_j \pmod{n}$ implica $i = j$. O conjunto $\{k \in \mathbb{Z} \mid 1 \le k \le n \text{ e } \mathrm{mdc}(n, k) = 1\}$ é um exemplo de sci módulo n.

Definição 1.39. *A função*

$$\varphi(n) \overset{\text{def}}{=} |(\mathbb{Z}/n\mathbb{Z})^\times|$$

é chamada de função phi de Euler*.*

Temos $\varphi(1) = \varphi(2) = 1$ e, para $n > 2$, $1 < \varphi(n) < n$. Se p é primo, $\varphi(p) = p - 1$; mais geralmente $\varphi(p^k) = p^k - p^{k-1}$ pois $\mathrm{mdc}(a, p^k) = 1$ se, e somente se, a não é múltiplo de p e há p^{k-1} múltiplos de p no intervalo $1 \le a \le p^k$. Para calcular a função φ no caso geral, vamos mostrar que se $\mathrm{mdc}(n, m) = 1$, então $\varphi(nm) = \varphi(n)\varphi(m)$. Consideremos os números $1, 2, \dots, nm$, onde $\mathrm{mdc}(n, m) = 1$ e os arrumamos em forma matricial assim:

$$\begin{array}{ccccc}
1 & 2 & 3 & \dots & n \\
n+1 & n+2 & n+3 & \dots & 2n \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
n(m-1)+1 & n(m-1)+2 & n(m-1)+3 & \dots & n(m-1)+n
\end{array}$$

Note que, como $\mathrm{mdc}(ni + j, n) = \mathrm{mdc}(j, n)$, se um número nesta tabela é primo relativo com n, então todos os números nessa coluna são primos relativos com n. Logo existem $\varphi(n)$ colunas nas quais todos os números são primos relativos com n. Por outro lado, toda coluna possui um conjunto completo de restos módulo m: se duas entradas são tais que $ni_1 + j \equiv ni_2 + j \pmod{m}$, então $i_1 \equiv i_2 \pmod{m}$ pois n é invertível módulo m já que $\mathrm{mdc}(m, n) = 1$, logo como $0 \le i_1, i_2 < m$ devemos ter $i_1 = i_2$. Desta forma, em cada coluna existem exatamente $\varphi(m)$ números que são primos relativos com m e portanto o total de números nesta tabela que são simultaneamente primos relativos com m e n (i.e. primos com nm) é $\varphi(nm) = \varphi(n)\varphi(m)$.

Assim, se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ é a fatoração de n em potências de primos distintos p_i, temos que

$$\varphi(n) = \prod_{1 \le i \le k} \varphi(p_i^{\alpha_i}) = \prod_{1 \le i \le k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{1 \le i \le k} \left(1 - \frac{1}{p_i}\right).$$

Agora estamos prontos para enunciar e provar o importante

Teorema 1.40 (Euler-Fermat)**.** *Sejam a e m dois inteiros com $m > 0$ e $\operatorname{mdc}(a, m) = 1$. Então*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demonstração: Observemos que se $r_1, r_2, \ldots, r_{\varphi(m)}$ é um sistema completo de invertíveis módulo m e a é um número natural tal que $\operatorname{mdc}(a, m) = 1$, então $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ também é um sistema completo de invertíveis módulo m. De fato, temos que $\operatorname{mdc}(ar_i, m) = 1$ para todo i e se $ar_i \equiv ar_j \pmod{m}$, então $r_i \equiv r_j \pmod{m}$ pois a é invertível módulo m, logo $r_i = r_j$ e portanto $i = j$. Consequentemente cada ar_i deve ser congruente com algum r_j e, portanto,

$$\begin{aligned} \prod_{1\le i\le\varphi(m)} (ar_i) &\equiv \prod_{1\le i\le\varphi(m)} r_i \pmod{m} \\ \iff a^{\varphi(m)} \cdot \prod_{1\le i\le\varphi(m)} r_i &\equiv \prod_{1\le i\le\varphi(m)} r_i \pmod{m}. \end{aligned}$$

Mas como cada r_i é invertível módulo m, simplificando o fator $\prod_{1\le i\le\varphi(m)} r_i$, obtemos o resultado desejado. ☐

Como caso particular do teorema anterior obtemos o

Teorema 1.41 (Pequeno Teorema de Fermat)**.** *Seja a um inteiro positivo e p um primo, então*

$$a^p \equiv a \pmod{p}$$

Demonstração: De fato, observemos que se $p \mid a$ o resultado é evidente. Então, podemos supor que $\operatorname{mdc}(a, p) = 1$. Como $\varphi(p) = p-1$, pelo teorema de Euler temos $a^{p-1} \equiv 1 \pmod{p}$, logo multiplicando por a obtemos o resultado desejado. ☐

Observação 1.42. *O teorema de Euler-Fermat também pode ser provado utilizando-se o seguinte corolário do teorema de Lagrange em Teoria dos Grupos: se G é um grupo finito e $g \in G$, então $g^{|G|} = e$ (identidade). Aplicando este resultado para $G = (\mathbb{Z}/m\mathbb{Z})^\times$, temos que $\overline{a}^{\varphi(m)} = \overline{1}$ para todo $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$, que é uma formulação equivalente para o teorema de Euler-Fermat.*

Observemos que o teorema de Euler-Fermat pode ser otimizado da seguinte forma:

Proposição 1.43. *Sejam a e n números inteiros tais que $\operatorname{mdc}(a, n) = 1$ e n se fatora como $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ em potências de primos distintos. Então*

$$a^M \equiv 1 \pmod{n} \quad \textit{onde} \quad M = \operatorname{mmc}(\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \ldots, \varphi(p_k^{\alpha_k})).$$

Demonstração: Pelo teorema de Euler-Fermat sabemos que $a^{\varphi(p_j^{\alpha_j})} \equiv 1 \pmod{p_j^{\alpha_j}}$ para todo $j = 1, \ldots k$. Elevando a $M/\varphi(p_j^{\alpha_j})$, obtemos $a^M \equiv 1 \pmod{p_j^{\alpha_j}}$. Assim, $a^M - 1$ é múltiplo de $p_j^{\alpha_j}$ para todo j e como estes números são dois a dois primos entre si concluímos que $n \mid a^M - 1 \iff a^M \equiv 1 \pmod{n}$, como desejado. ☐

Vejamos agora algumas aplicações do teorema de Euler-Fermat.

Exemplo 1.44. *Mostre que existem infinitos números da forma* $20000\ldots009$ *que são múltiplos de* 2009.

Demonstração: O problema é equivalente a encontrar infinitos naturais k tais que

$$\begin{aligned} 2\cdot 10^k+9\equiv 0 \pmod{2009} &\iff 2\cdot 10^k+9\equiv 2009 \pmod{2009}\\ &\iff 10^{k-3}\equiv 1 \pmod{2009}\end{aligned}$$

pois 2000 é invertível módulo 2009. Como $\text{mdc}(10,2009)=1$, pelo teorema de Euler-Fermat temos que $10^{\varphi(2009)}\equiv 1 \pmod{2009} \implies 10^{\varphi(2009)t}\equiv 1 \pmod{2009}$ para todo $t\in\mathbb{N}$, logo basta tomar $k=\varphi(2009)t+3$. □

Exemplo 1.45. *Encontre um número $n\in\mathbb{N}$ tal que $2^n>10^{2000}$ e 2^n tenha entre suas 2000 últimas casas decimais pelo menos 1000 zeros consecutivos.*

Solução: Sabemos que $2^{\varphi(5^{2000})}\equiv 1 \pmod{5^{2000}}$ pelo teorema de Euler-Fermat. Portanto existe $b\in\mathbb{N}$ com

$$2^{\varphi(5^{2000})}=5^{2000}b+1 \implies 2^{2000+\varphi(5^{2000})}=10^{2000}b+2^{2000}.$$

Portanto os 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coincidem com a representação decimal de 2^{2000}, que tem no máximo 667 dígitos pois $2^{2000}<(2^3)^{667}<10^{667}$. Desta forma, há pelo menos $2000-667=1333$ zeros consecutivos dentre as 2000 últimas casas decimais de $2^{2000+\varphi(5^{2000})}$ e assim $n=\varphi(5^{2000})+2000=4\cdot 5^{1999}+2000$ satisfaz as condições do enunciado. □

Exemplo 1.46. *Mostre que não existe inteiro x tal que $103\mid x^3-2$.*

Solução: Note primeiramente que 103 é primo. Agora suponha que $x^3\equiv 2 \pmod{103}$, de modo que $103\nmid x$. Elevando ambos os lados desta congruência a $(103-1)/3=34$, obtemos $x^{102}\equiv 2^{34} \pmod{103}$ e sabemos pelo teorema de Euler-Fermat que $x^{102}\equiv 1 \pmod{103}$. Porém, fazendo as contas, obtemos que $2^{34}\equiv 46 \pmod{103}$, uma contradição. Logo não há inteiro x tal que $103\mid x^3-2$. □

Utilizando o mesmo raciocínio do exemplo anterior, temos que se p é um primo tal que $p\equiv 1 \pmod 3$ e $p\nmid a$, então uma condição necessária para que $x^3\equiv a \pmod p$ tenha solução em x é que $a^{(p-1)/3}\equiv 1 \pmod p$. Esta condição também é suficiente, pela existência de raízes primitivas módulo p, como mostraremos no final deste capítulo.

Exemplo 1.47. *Demonstrar que se $p>2$ é primo, então*

$$1^{p-1}+2^{p-1}+3^{p-1}+\cdots+(p-1)^{p-1}\equiv p+(p-1)! \pmod{p^2}.$$

Solução: Pelo pequeno teorema de Fermat, sabemos que $i^{p-1}\equiv 1 \pmod p$ para todo $1\le i\le p-1$, isto é, que $i^{p-1}=k_ip+1$ onde k_i é um inteiro. Assim, $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}=(k_1+k_2+\cdots+k_{p-1})p+p-1$ e portanto devemos mostrar que $(k_1+k_2+\cdots+k_{p-1})p\equiv (p-1)!+1 \pmod{p^2}$.

Multiplicando as equações $i^{p-1}=k_ip+1$, temos

$$(k_1p+1)(k_2p+1)\cdots(k_{p-1}p+1)=1^{p-1}2^{p-1}\cdots(p-1)^{p-1}=((p-1)!)^{p-1}.$$

Por um lado, $(k_1p+1)(k_2p+1)\cdots(k_{p-1}p+1)\equiv(k_1+k_2+\cdots+k_{p-1})p+1 \pmod{p^2}$. Por outro, pelo teorema de Wilson sabemos que $(p-1)!\equiv -1 \pmod p$, ou seja, $(p-1)!=Kp-1$ para algum K inteiro. Segue que

$$\begin{aligned} &(k_1+k_2+\cdots+k_{p-1})p+1\equiv(Kp-1)^{p-1} \pmod{p^2}\\ \implies &(k_1+k_2+\cdots+k_{p-1})p+1\equiv 1-\binom{p-1}{1}Kp \pmod{p^2}\\ \implies &(k_1+k_2+\cdots+k_{p-1})p\equiv Kp \pmod{p^2}\\ \implies &(k_1+k_2+\cdots+k_{p-1})p\equiv (p-1)!+1 \pmod{p^2}\end{aligned}$$

o que encerra a prova. □

Concluímos esta seção apresentando brevemente uma aplicação do Teorema de Euler que tem particular interesse prático: a *Criptografia RSA*. Trata-se de um método de criptografia com chave pública, isto é, um método que permite a qualquer pessoa transmitir mensagens por uma via insegura (ou seja, que pode ser monitorada por espiões) de modo que, na prática, apenas o legítimo destinatário, que conhece uma *chave*, pode recuperar a mensagem original. A sigla vem dos nomes de Ron Rivest, Adi Shamir, e Leonard Adleman, que desenvolveram esse método.

Para isso, o receptor publica um inteiro N que é o produto de dois primos razoavelmente grandes p e q (aproximadamente da mesma ordem de grandeza); N é público mas a sua fatoração pq só é conhecida pelo receptor. O receptor também publica um expoente s (em geral não muito grande) com $\mathrm{mdc}(s,(p-1)(q-1)) = 1$. O receptor calcula (usando o algoritmo de Euclides) o inverso de s mod $(p-1)(q-1) = \varphi(N)$, isto é, um natural $r < (p-1)(q-1)$ com $rs \equiv 1 \pmod{(p-1)(q-1)}$ (donde $rs = 1 + k\varphi(N)$, para algum natural k). Note que apesar de N e s serem públicos, não parece ser fácil calcular $\varphi(N)$ ou r (neste contexto, calcular $\varphi(N) = (p-1)(q-1)$ dado $N = pq$ é equivalente a fatorar N, i.e., a encontrar os fatores primos p e q).

Uma mensagem é um número natural $m < N$. O emissor envia (ou publica) $\tilde{m} := m^s \pmod N$, com $0 < \tilde{m} < N$. O receptor recupera m via

$$m \equiv \tilde{m}^r \pmod N.$$

Para verificar essa equivalência, podemos observar que

$$\tilde{m}^r \equiv (m^s)^r = m^{rs} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \pmod p;$$

note que, se $p \mid m$, os dois lados são 0 mod p, e, caso contrário, $m^{p-1} \equiv 1 \pmod p$; analogamente $\tilde{m}^r \equiv m \pmod q$, donde $\tilde{m}^r \equiv m \pmod N$. Essas tarefas são relativamente rápidas computacionalmente. Mais precisamente, veremos a seguir que existem algoritmos polinomiais para testar primalidade, assim como para as demais operações necessárias (veja o capítulo 7, especialmente a seção sobre o teste de Agrawal, Kayal e Saxena que garante que testar primalidade de um número da ordem de N leva tempo no máximo polinomial em $\log N$).

Se existem algoritmos polinomiais para testar primalidade, não é verdade que sejam conhecidos algoritmos polinomiais (e *determinísticos*) para obter primos "novos" de uma determinada ordem de grandeza. Pelo teorema dos números primos (capítulo 5 e apêndice A), para todo N grande, a probabilidade de um número escolhido ao acaso entre N e $2N$ ser primo é $(1 + o(1))/\log N$, o que implica que, se testarmos $C \log N$ números ao acaso entre N e $2N$, a probabilidade de algum deles ser primo é da ordem de $1 - \exp(-C(1 + o(1)))$, que está muito perto de 1 para C grande. Se ao invés de sortear números procurarmos o menor primo maior ou igual a N (testando um por um) então, novamente pelo teorema dos números primos, *em média* o número de tentativas será da ordem de $\log(n)$. Entretanto, há gaps bem maiores do que $\log N$ e sabe-se muito pouco sobre o tamanho dos gaps (para um primo p, o gap $g(p)$ é igual a $q - p$ onde q é o menor primo maior do que p). Por exemplo, Harald Cramér conjectura que $g(p) < C(\log(p))^2$ (para algum $C > 0$; [3]): se isto for verdade então o algoritmo proposto acima é realmente polinomial. Pode ser que outra estratégia permita encontrar primos sem demonstrar esta conjectura, mas nada de tempo polinomial é conhecido. Há um projeto Polymath sobre este assunto: veja o preprint [17] e as páginas indicadas juntamente nas referências. Ainda assim, podemos considerar que o problema de obter primos é razoavelmente fácil e rápido para aplicações práticas pois aí devemos permitir algoritmos que dependem de sorteios e que obtêm o que é pedido em tempo polinomial com probabilidade quase igual a 1. No interessante artigo de divulgação [20] é discutido o problema de gerar primos grandes, e em particular é apresentado um algoritmo que funciona em muitos casos e gera primos grandes cuja primalidade pode ser verificada por critérios bem mais simples que o teste de Agrawal, Kayal e Saxena, como o teste de Pocklington (veja o capítulo 7).

Não se conhecem algoritmos polinomiais para fatorar inteiros (grandes). A maioria dos especialistas duvida que exista tal algoritmo mas é preciso enfatizar que a não-existência de um tal algoritmo não é um teorema. Mais do que isso, a não-existência de tal algoritmo implica diretamente em $P \neq NP$ (um dos mais importantes problemas em aberto da matemática) mas $P \neq NP$ não parece implicar a não existência do algoritmo.

Existe ainda a possibilidade de que não exista um algoritmo rápido, mas que ainda assim exista uma máquina (no sentido literal) capaz de fatorar inteiros rapidamente. De fato, a mecânica quântica parece permitir a construção de um *computador quântico* e Peter Shor encontrou um "algoritmo" que permite a um computador quântico fatorar inteiros em tempo polinomial [23]. Até 2010 foram construídos computadores quânticos mínimos, suficientes para fatorar o número 15 pelo algoritmo de Shor mas insuficientes para números maiores [16]. Não é claro se será possível construir computadores quânticos maiores.

Resumindo, a criptografia RSA é eficiente e segura pois é muito mais rápido achar primos grandes do que fatorar números grandes e ele é bastante utilizado para encriptar mensagens transmitidas pela internet. Para mais informações sobre a criptografia RSA, veja [2].

Problemas Propostos

1.28. *Demonstrar que*

(a) $61 \mid 20^{15} - 1$.

(b) $13 \mid 2^{70} + 3^{70}$.

1.29. *Encontrar os últimos três dígitos de* 3^{2009} *em notação decimal.*

1.30. *Verificar se* 987654321 *é divisível por* 9*,* 11*,* 13*,* 17 *ou* 19*.*

1.31. *Calcule o resto da divisão de* $2^{2^{2011}}$ *por* 97*.*

1.32. *Determine um valor inteiro positivo de* k *tal que* $5^k \equiv 97 \pmod{101}$*.*

1.33. *Demonstrar que todo número palíndromo com um número par de dígitos é divisível por* 11*. O que acontece com os números palíndromos com um número ímpar de dígitos?*

1.34. *Encontrar todos os números* N *de três dígitos em representação decimal, tais que* N *é divisível por* 11 *e além disso* $N/11$ *é igual à soma dos quadrados dos dígitos de* N*.*

1.35. *Mostre que o dígito das dezenas de qualquer potência de* 3 *é um número par (por exemplo, o dígito das dezenas de* $3^6 = 729$ *é* 2*).*

1.36. *Mostre que, para todo* $n \geq 0$*, vale que* $13 \mid 7^{2n+1} + 6^{2n+1}$*.*

1.37. *Mostre que*

$$a^{12} \equiv b^{12} \pmod{91} \iff \mathrm{mdc}(a, 91) = \mathrm{mdc}(b, 91).$$

1.38. *(P. Sabini) Mostre que entre os números da forma*

$$14, \quad 144, \quad 1444, \quad 14444, \quad 144\cdots 44, \ldots$$

os únicos quadrados perfeitos são $144 = 12^2$ *e* $1444 = 38^2$*.*

1.39. *Seja* $f : \mathbb{N}_{>0} \to \mathbb{N}$ *uma função definida do conjunto dos inteiros positivos no conjunto dos números naturais tal que*

(a) $f(1) = 0$*;*

(b) $f(2n) = 2f(n) + 1$*;*

(c) $f(2n + 1) = 2f(n)$*.*

Utilize a representação em base 2 *de* n *para encontrar uma fórmula não recursiva para* $f(n)$*.*

1.40. *Mostre que todo número racional positivo pode ser escrito de maneira única na forma*

$$\frac{a_1}{1!} + \frac{a_2}{2!} + \cdots + \frac{a_k}{k!}$$

onde:

$$0 \le a_1, \quad 0 \le a_2 < 2, \quad 0 \le a_3 < 3, \quad \ldots, \quad 0 < a_k < k.$$

1.41 (OBM1991)**.** *Demonstrar que existem infinitos múltiplos de* 1991 *que são da forma* $19999\ldots 99991$*.*

1.42 (IMO1983)**.** *É possível escolher 1983 inteiros positivos distintos, todos menores que* 10^5*, tal que não existam três que sejam termos consecutivos de uma progressão aritmética?*

Dica: Usar base 3*.*

1.43. *Seja* $S(n)$ *a soma dos dígitos de* n*. Encontrar* $S(S(S(2^{2^5} + 1)))$*.*

1.44 (Chi2003)**.** *Encontrar todas as ternas* (d, m, n) *de inteiros positivos tais que* $d^m + 1$ *divide* $d^n + 203$*.*

1.45. *Seja* $p > 2$ *um número primo. Demonstrar que*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \pmod p.$$

1.46 (AusPol1996)**.** *Mostrar que não existem inteiros não negativos* m, n *tais que* $m! + 48 = 48(m + 1)n$

1.47. *Seja* p *um número primo. Demonstrar que* $(p - 1)! + 1$ *é uma potência de* p *se, e só se,* $p = 2$*,* 3 *ou* 5*.*

1.48. *Demonstrar que para todo número primo* $p > 3$*, o número* $\binom{np}{p} - n$ *é divisível por* p^{3+r} *onde* p^r *é a maior potência de* p *que divide* n*.*

1.49. *Demonstrar que*

$$\sum_{\substack{1 \le k \le n \\ \mathrm{mdc}(n,k)=1}} k = \frac{n\varphi(n)}{2}.$$

1.50. *Demonstrar que se* $\mathrm{mdc}(a, b) = 1$*, então todos os divisores primos de* $a^2 + b^2$ *são da forma* $4k + 1$*.*

Dica: Utilize o teorema de Euler-Fermat.

1.51. *Demonstrar que existem infinitos primos da forma* $4k + 1$.

1.52. *Sejam* m, n *inteiros positivos. Demonstrar que* $4mn - m - n$ *nunca pode ser o quadrado de um número inteiro.*

1.53 (IMO1985). *Seja* d *um número positivo distinto de* 2, 5 *e* 13. *Demonstrar que é possível encontrar dois números diferentes* a *e* b *que pertençam ao conjunto* $\{2, 5, 13, d\}$ *tais que* $ab - 1$ *não é um quadrado perfeito.*

1.54. *Demonstrar que se* $p \mid (a^p - b^p)$, *então* $p^2 \mid (a^p - b^p)$.

1.55 (IMO1984). *Encontre todos os pares de inteiros positivos* a, b *tais que* $ab(a+b)$ *não é divisível por* 7, *mas* $(a + b)^7 - a^7 - b^7$ *é divisível por* 7^7.
$(a + b)^7 - a^7 - b^7 = 7ab(a + b)(a^2 + ab + b^2)^2$.

1.56 (OIbM2001). *Demonstrar que para cada inteiro positivo* n *existe um inteiro* m *tal que* 2^m *tem no mínimo* $\frac{2}{3}n - 1$ *zeros entre seus últimos* n *algarismos em notação base* 10.

1.57 (IMO2003). *Seja* p *um número primo. Demonstre que existe um primo* q *tal que para todo* n, *o número* $n^p - p$ *não é divisível por* q.

1.58 (IMO1979). *Sejam* m *e* n *inteiros positivos tais que*

$$\frac{m}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Mostrar que m *é divisível por* 1979.

1.59. *Seja* p *um número primo ímpar e sejam* a *e* b *inteiros não divisíveis por* p *tais que* $p \mid a - b$. *Mostrar que* $p^k \mid a^n - b^n \iff p^k \mid n(a - b)$.

1.8 Polinômios

Dado um anel comutativo K, definimos o anel comutativo $K[x]$ como sendo o conjunto das expressões da forma $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ com $a_i \in K$, chamados de *polinômios* com coeficientes em K. A soma e o produto em $K[x]$ são definidos da maneira usual: dados $f(x) = \sum_i a_ix^i$ e $g(x) = \sum_i b_ix^i$ elementos de $K[x]$ temos

$$f(x) + g(x) \stackrel{\text{def}}{=} \sum_i (a_i + b_i)x^i;$$
$$f(x) \cdot g(x) \stackrel{\text{def}}{=} \sum_k c_kx^k \text{ onde } c_k = \sum_{i+j=k} a_ib_j.$$

Definimos o *grau* $\deg f(x)$ de um polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ como sendo o maior i tal que $a_i \neq 0$; o grau do polinômio nulo 0 é definido como sendo $-\infty$. Tal convenção visa a tornar válidas as seguintes identidades para todos os polinômios $f(x), g(x) \in K[x]$:

$$\deg\bigl(f(x) \cdot g(x)\bigr) = \deg f(x) + \deg g(x) \qquad \text{e}$$
$$\deg\bigl(f(x) + g(x)\bigr) \leq \max\{\deg f(x), \deg g(x)\}.$$

O coeficiente do termo de maior grau de um polinômio é chamado de *coeficiente líder*. Um polinômio cujo coeficiente líder é igual a 1 é chamado de *mônico*.

Observe que nas definições acima x é um símbolo formal e não um elemento de K. Apesar disso, cada polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ define uma *função polinomial*

$$\begin{aligned} f\colon K &\to K \\ c &\mapsto f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n \end{aligned}$$

também chamada de f. A distinção entre um polinômio e uma função polinomial é bem ilustrada pelo polinômio $f(x) = x^p - x \in (\mathbb{Z}/(p))[x]$: este polinômio é não nulo pois seus coeficientes são não nulos, mas para todo $c \in \mathbb{Z}/(p)$ temos $f(c) = 0$ pelo pequeno teorema de Fermat. Dado um polinômio $f(x) \in K[x]$, qualquer $c \in K$ tal que $f(c) = 0$ é chamado de *raiz* ou *zero* de $f(x)$.

Como veremos nesta seção, polinômios guardam muitas semelhanças com números inteiros. Por exemplo, podemos definir divisibilidade de polinômios de maneira completamente análoga: $d(x) \mid f(x)$ em $K[x]$ se, e só se, existe $g(x) \in K[x]$ tal que $f(x) = d(x) \cdot g(x)$. Temos também uma generalização da divisão euclidiana:

Proposição 1.48 (Algoritmo da divisão)**.** *Seja K um corpo. Dados polinômios $f(x), g(x) \in K[x]$, com $g(x) \neq 0$, existem $q(x), r(x) \in K[x]$ (chamados respectivamente de* quociente *e* resto *da divisão de $f(x)$ por $g(x)$), unicamente determinados, tais que*

$$f(x) = q(x) \cdot g(x) + r(x) \quad \textit{com} \quad \deg r(x) < \deg g(x).$$

Demonstração: Sejam $n = \deg f(x)$ e $m = \deg g(x)$. Para demonstrar a existência de $q(x)$ e $r(x)$, procederemos por indução sobre n. Note que se $m > n$, então basta tomar $q(x) = 0$ e $r(x) = f(x)$, logo podemos supor que $m \leq n$. Se $n = m = 0$, então $f(x) = a$ e $g(x) = b$ são ambos constantes não nulas, logo basta tomar $q(x) = a/b$ e $r(x) = 0$ neste caso.

Agora suponha que $n \geq 1$. Escreva $f(x) = a_nx^n + f_1(x)$ e $g(x) = b_mx^m + g_1(x)$ com $a_n \neq 0$, $b_m \neq 0$ e $\deg f_1(x) < n$, $\deg g_1(x) < m$. Observemos que o polinômio $f(x) - \frac{a_n}{b_m}x^{n-m}g(x) = f_1(x) - \frac{a_n}{b_m}x^{n-m}g_1(x)$ é de grau menor que n. Por hipótese de indução existem dois polinômios $q(x)$ e $r(x)$ tais que

$$f(x) - \frac{a_n}{b_m}x^{n-m}g(x) = q(x)g(x) + r(x) \quad \text{com} \quad \deg r(x) < \deg g(x).$$

Logo podemos escrever $f(x) = (\frac{a_n}{b_m}x^{n-m} + q(x)) \cdot g(x) + r(x)$, que era o que se queria demonstrar.

Para demonstrar que os polinômios $q(x)$ e $r(x)$ são únicos, suponha que

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

com $q_1(x) \neq q_2(x)$ e $\deg r_1(x), \deg r_2(x) < \deg g(x)$. Então $r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x) \neq 0$ é um múltiplo de $g(x)$ de grau estritamente menor do que $\deg g(x)$, o que é um absurdo. □

Corolário 1.49. *Seja K um corpo, $f(x) \in K[x]$ e $a \in K$. Então*

$$x - a \mid f(x) \iff f(a) = 0.$$

Demonstração: Como $\deg(x - a) = 1$, dividindo $f(x)$ por $x - a$ temos que $f(x) = (x - a)q(x) + r$ com $r \in K$. Assim, substituindo x por a, temos que $f(a) = r$ donde o resultado segue. □

Proposição 1.50. *Seja K um corpo. Um polinômio $f(x) \in K[x]$ não nulo de grau n tem no máximo n raízes em K.*

Demonstração: A demonstração é feita por indução em $n = \deg f(x)$; os casos $n = 0$ e $n = 1$ são triviais. Se $f(x)$ tivesse $n+1$ raízes distintas $a_1, \ldots, a_{n+1}$, então $f(x) = (x - a_{n+1})g(x)$ para algum $g(x) \in K[x]$ pelo corolário anterior. Assim, para $i \neq n+1$, teríamos $0 = f(a_i) = (a_i - a_{n+1})g(a_i) \implies g(a_i) = 0$ pois $(a_i - a_{n+1}) \neq 0$ é invertível em K. Logo $g(x)$, de grau $n-1$, teria n raízes distintas $a_1, \ldots, a_n$, contradizendo a hipótese de indução. $\square$

Note que o teorema anterior é falso se K não é um corpo. Por exemplo, o polinômio $f(x) = x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[x]$ tem 4 raízes em $\mathbb{Z}/8\mathbb{Z}$, a saber $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.

Vejamos uma aplicação dos resultados anteriores quando $K = \mathbb{Z}/(p)$, p primo. A primeira é uma nova demonstração do teorema de Wilson:

Teorema 1.51. *Seja p um primo. Considere a função simétrica elementar σ_i em $1, 2, \ldots, p-1$ dada pela soma de todos os $\binom{p-1}{i}$ produtos de i termos distintos dentre $1, 2, \ldots, p-1$:*

$$\begin{aligned}
\sigma_1 &= 1 + 2 + \cdots + (p-1) \\
\sigma_2 &= 1 \cdot 2 + 1 \cdot 3 + \cdots + (p-2)(p-1) \\
&\vdots \\
\sigma_{p-1} &= 1 \cdot 2 \cdot \ldots \cdot (p-1).
\end{aligned}$$

Então $\sigma_1, \ldots, \sigma_{p-2}$ são todos múltiplos de p e $\sigma_{p-1} = (p-1)! \equiv -1 \pmod p$ (teorema de Wilson).

Demonstração: Pelo teorema de Fermat e pela proposição anterior, temos que $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ são todas as raízes de $x^{p-1} - \overline{1}$ em $\mathbb{Z}/(p)$. Logo aplicando o corolário e comparando coeficientes líderes obtemos a fatoração

$$x^{p-1} - \overline{1} = (x - \overline{1})(x - \overline{2}) \cdot \ldots \cdot (x - \overline{p-1}).$$

Mas o polinômio do lado direito é igual a $x^{p-1} - \overline{\sigma}_1 x^{p-2} + \overline{\sigma}_2 x^{p-3} - \cdots + (-1)^{p-1}\overline{\sigma}_{p-1}$. Comparando coeficientes, obtemos o resultado. $\square$

Seja K um corpo. Podemos considerar também congruências de polinômios em $K[x]$: se $a(x), b(x), m(x) \in K[x]$, escrevemos

$$a(x) \equiv b(x) \pmod{m(x)} \iff m(x) \mid a(x) - b(x).$$

As mesmas demonstrações do caso inteiro mostram que as congruências módulo $m(x)$ definem uma relação de equivalência em $K[x]$ compatível com as operações de soma, subtração e produto. Assim, podemos formar o *anel quociente*

$$\frac{K[x]}{\big(m(x)\big)}$$

cujos elementos são os conjuntos da forma

$$\overline{a(x)} \stackrel{\text{def}}{=} \{b(x) \in K[x] \mid b(x) \equiv a(x) \pmod{m(x)}\}$$

e as operações no anel quociente são dadas por

$$\overline{f(x)} + \overline{g(x)} \stackrel{\text{def}}{=} \overline{f(x) + g(x)} \qquad \text{e} \qquad \overline{f(x)} \cdot \overline{g(x)} \stackrel{\text{def}}{=} \overline{f(x) \cdot g(x)}$$

sendo independentes das escolhas dos representantes de classe $f(x)$ e $g(x)$. Se $\deg m(x) = n$, um sistema completo de resíduos módulo $m(x)$ é dado pelos polinômios de grau menor do que n (os possíveis restos na divisão euclidiana por $m(x)$):

$$\{a_0 + a_1x + \cdots + a_nx^{n-1} \mid a_i \in K\}$$

Em particular, $\frac{K[x]}{(m(x))}$ é infinito se K também o é.

Exemplo 1.52. *Determine o resto da divisão de* $(x+1)^{2010}$ *por* x^2+x+1 *em* $\mathbb{Q}[x]$.

Solução: Multiplicando por $x-1$ a congruência $x^2+x+1 \equiv 0 \pmod{x^2+x+1}$, obtemos $x^3 \equiv 1 \pmod{x^2+x+1}$. Assim, temos

$$\begin{aligned} &(x+1)^2 \equiv x \pmod{x^2+x+1} \\ \Longrightarrow\ &(x+1)^{2010} \equiv x^{1005} = (x^3)^{335} \pmod{x^2+x+1} \\ \Longrightarrow\ &(x+1)^{2010} \equiv 1 \pmod{x^2+x+1} \end{aligned}$$

Assim, o resto da divisão é 1. □

Podemos tentar definir o mdc $d(x)$ de dois polinômios $f(x)$ e $g(x)$ (com $f(x) \neq 0$ ou $g(x) \neq 0$) de maneira análoga ao mdc de inteiros, tomando o polinômio $d(x)$ de maior grau que divide $f(x)$ e $g(x)$ simultaneamente. Entretanto, $d(x)$ não está bem determinado, pois qualquer múltiplo $c \cdot d(x)$ com $c \neq 0$ constante ainda satisfaz as condições acima. Para evitar esta ambiguidade, definimos o mdc de $f(x)$ e $g(x)$ como sendo o polinômio *mônico* de maior grau que divide $f(x)$ e $g(x)$ simultaneamente. Analogamente, define-se o mmc de $f(x)$ e $g(x)$ (com $f(x) \neq 0$ e $g(x) \neq 0$) como o polinômio mônico de menor grau que é divisível tanto por $f(x)$ como por $g(x)$.

A divisão euclidiana permite estender resultados de $\mathbb{Z}$ para $K[x]$ de maneira quase trivial. Por exemplo, temos

Teorema 1.53 (Bachet-Bézout)**.** *Seja $d(x)$ o máximo divisor comum de dois polinômios $f(x)$ e $g(x)$. Então existem dois polinômios $m(x)$ e $n(x)$ tais que $f(x)m(x) + g(x)n(x) = d(x)$.*

Demonstração: Análoga ao teorema 1.7; como naquele teorema $d(x)$ será o polinômio mônico de menor grau no conjunto

$$I(f,g) \stackrel{\text{def}}{=} \{f(x)m(x) + g(x)n(x) \mid m(x), n(x) \in K[x]\}.$$

□

Definição 1.54. *Seja K um corpo. Dizemos que um polinômio não constante $f(x) \in K[x]$ é* irredutível *em $K[x]$ se $f(x)$ não é o produto de dois polinômios em $K[x]$ de graus estritamente menores do que* $\deg f(x)$.

Polinômios irredutíveis fazem o papel de números primos para polinômios. Por exemplo, $x^2+1 \in \mathbb{R}[x]$ é irredutível em $\mathbb{R}[x]$, pois caso contrário ele poderia ser escrito como produto de polinômios de grau 1 em $\mathbb{R}[x]$, contradizendo o fato de $x^2+1 = 0$ não possuir raízes reais. Por outro lado, x^2+1 é *redutível* em $\mathbb{C}[x]$ já que $x^2+1 = (x-i)(x+i)$. Isto mostra que irredutibilidade é um conceito que depende do anel de polinômios sobre o qual estamos trabalhando.

Os exemplos mais evidentes de polinômios irredutíveis em $K[x]$ são os lineares mônicos, i.e., os da forma $x-a$, $a \in K$. Quando estes são os únicos polinômios irredutíveis em $K[x]$ dizemos que o corpo K é *algebricamente fechado*. Observe que em geral polinômios de graus 2 ou 3 são irredutíveis em $K[x]$ se, e somente se, não têm raízes em K.

A partir do teorema de Bachet-Bézout, como no caso dos inteiros, obtemos (c.f. proposição 1.10 e teorema 1.16):

Proposição 1.55. *Seja K um corpo e sejam $p(x), a_1(x), \ldots a_m(x) \in K[x]$ com $p(x)$ irredutível em $K[x]$. Se $p(x) \mid a_1(x) \cdot \ldots \cdot a_m(x)$, então $p(x) \mid a_i(x)$ para algum i.*

Teorema 1.56 (Fatoração Única)**.** *Seja K um corpo. Todo polinômio não nulo em $K[x]$ pode ser fatorado como um produto de polinômios irredutíveis em $K[x]$; esta fatoração é única a menos da ordem dos fatores e multiplicação por constantes não nulas.*

Outra importante consequência do teorema de Bachet-Bézout é o seguinte (c.f. teorema 1.37)

Teorema 1.57. *Seja K um corpo e $f(x)$ um polinômio irredutível em $K[x]$. Então $K[x]/(f(x))$ é um corpo.*

Demonstração: Assim como na demonstração de que $\mathbb{Z}/p\mathbb{Z}$ é um corpo para p primo, a dificuldade aqui é mostrar que todo elemento $\overline{a(x)} \neq 0$ é invertível em $K[x]/(f(x))$. Temos que $\operatorname{mdc}(a(x), f(x)) = 1$ pois $f(x)$ é irredutível e $f(x)$ não divide $a(x)$, caso contrário teríamos $\overline{a(x)} = 0$. Logo, pelo teorema de Bachet-Bézout, existem $r(x), s(x) \in K[x]$ tais que

$$a(x)r(x) + f(x)s(x) = 1 \implies a(x)r(x) \equiv 1 \pmod{f(x)}$$

Portanto $\overline{r(x)}$ é o inverso multiplicativo de $\overline{a(x)}$. □

Por exemplo, seja $K = \mathbb{Z}/(2)$ e $f(x) = x^2 + x + \overline{1} \in K[x]$. Temos que $f(x)$ é irredutível pois ele tem grau 2 e não possui raízes em K. Assim, $K[x]/(f(x))$ é um corpo, que possui 4 elementos. As tabelas de adição e multiplicação deste corpo são as seguintes:

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Encerramos esta seção com um importante critério de irredutibilidade para polinômios com coeficientes inteiros. Primeiro, precisamos de uma

Definição 1.58. *Um polinômio não nulo $f(x) \in \mathbb{Z}[x]$ é dito* primitivo *se o mdc de seus coeficientes é* 1.

Lema 1.59. *O produto de dois polinômios primitivos é primitivo.*

Demonstração: Sejam $g(x)$ e $h(x)$ dois polinômios primitivos. Seja p um primo e suponha por absurdo que p divida todos os coeficientes de $g(x)h(x)$. Assim, em $\mathbb{Z}/p\mathbb{Z}[x]$ teríamos que $\overline{g(x)h(x)} = \overline{g}(x)\overline{h}(x) = \overline{0}$, onde a barra denota o polinômio obtido reduzindo-se seus coeficientes módulo p. Por outro lado, $\overline{g}(x) \neq \overline{0}$ e $\overline{h}(x) \neq \overline{0}$, já que por hipótese p não divide todos os coeficientes de $g(x)$ e o mesmo para $h(x)$. Assim, temos uma contradição pois $\mathbb{Z}/p\mathbb{Z}[x]$ é um domínio, isto é, o produto de dois polinômios não nulos em $\mathbb{Z}/p\mathbb{Z}[x]$ é diferente de zero (de fato, olhe por exemplo para os coeficientes líderes e use o fato de que $\mathbb{Z}/p\mathbb{Z}$ é um corpo). □

O lema anterior é o passo essencial na prova do famoso *lema de Gauß*, que permite reduzir a questão da irredutibilidade de um polinômio em $\mathbb{Q}[x]$ para a mesma questão em $\mathbb{Z}[x]$.

Teorema 1.60 (Lema de Gauß)**.** *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Então $f(x)$ é irredutível em $\mathbb{Q}[x]$ se, e somente se, $f(x)$ é irredutível em $\mathbb{Z}[x]$ (isto é, não podemos escrever $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Z}[x]$ não constantes).*

Demonstração: É claro que se $f(x)$ é irredutível sobre $\mathbb{Q}[x]$, então ele é irredutível sobre $\mathbb{Z}[x]$. Reciprocamente, suponha por contradição que $f(x)$ seja irredutível sobre $\mathbb{Z}[x]$ mas que $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Q}[x]$, ambos não constantes. Multiplicando esta última igualdade por um inteiro conveniente $d > 0$, podemos escrever

$$d \cdot f(x) = e \cdot g_0(x)h_0(x)$$

com $g_0(x), h_0(x) \in \mathbb{Z}[x]$ primitivos e $e \in \mathbb{N}$. Como $f(x)$ e $g_0(x)h_0(x)$ (pelo lema anterior) são primitivos, temos que d é o mdc dos coeficientes de $d \cdot f(x)$, enquanto que e é o mdc dos coeficientes de $e \cdot g_0(x)h_0(x)$. Logo $d = e$ e assim $f(x) = g_0(x)h_0(x)$ é redutível sobre $\mathbb{Z}[x]$, uma contradição. $\square$

Finalmente, para polinômios em $\mathbb{Z}[x]$, podemos aplicar o

Proposição 1.61 (Critério de Eisenstein)**.** *Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Suponha que exista um número primo p tal que $p \nmid a_n$, $p \mid a_j$ para todo $0 \le j < n$ e $p^2 \nmid a_0$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.*

Demonstração: Suponha por absurdo que $f(x)$ é redutível, i.e., existem $g(x), h(x) \in \mathbb{Z}[x]$ tais que $f(x) = g(x)h(x)$ e $0 < \deg g(x), \deg h(x) < n$. Em $\mathbb{Z}/p\mathbb{Z}[x]$, temos então $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$, onde a barra denota o polinômio obtido reduzindo-se os seus coeficientes módulo p. Porém, como $p \mid a_j$ para todo $0 \le j < n$, temos que $\overline{f}(x) = \overline{a}_n x^n$ e portanto, pela fatoração única em $\mathbb{Z}/p\mathbb{Z}[x]$ (teorema 1.56), devemos ter $g(x) = \overline{b}x^i$ e $h(x) = \overline{c}x^j$ com $0 < i, j < n$, $i + j = n$ e $\overline{b} \cdot \overline{c} = \overline{a}_n$. Mas isto significa que os coeficientes de x^0 em $g(x)$ e $h(x)$ são múltiplos de p, e como $f(x) = g(x)h(x)$, que a_0 é múltiplo de p^2, absurdo. $\square$

Exemplo 1.62. *Seja p um primo. Demonstrar que o polinômio $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ é irredutível em $\mathbb{Q}[x]$.*

Solução: Pelo lema de Gauß, basta provar a irredutibilidade sobre $\mathbb{Z}[x]$ e para isto utilizaremos o critério de Eisenstein. Observemos que $f(x) = \frac{x^p - 1}{x - 1}$, logo

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}$$

e, com exceção do coeficiente líder, todos os coeficientes deste polinômio são múltiplos de p, sendo que o termo independente $\binom{p}{p-1} = p$ não é múltiplo de p^2. Pelo critério de Eisenstein, $f(x+1)$ é irredutível em $\mathbb{Z}[x]$ e, portanto, $f(x)$ também o é. $\square$

Observação 1.63. *Existem polinômios primitivos irredutíveis $f(x) \in \mathbb{Z}[x]$ mas que são redutíveis módulo p para todo primo p, por exemplo $f(x) = x^4 - 10x^2 + 1$ (veja o exemplo 2.10). Por outro lado, se $f(x) \in \mathbb{Z}[x]$ admite raiz módulo p para todo primo p suficientemente grande, então $f(x)$ possui raiz em $\mathbb{Z}$! Veja o excelente artigo de Serre [21] para uma demonstração deste fato.*

Problemas Propostos

1.60. *Seja $f(x) \in \mathbb{C}[x]$ um polinômio que deixa restos 10 e 1 quando dividido por $x-1$ e $x-10$ respectivamente. Encontrar o resto de $f(x)$ na divisão por $(x-1)(x-10)$.*

1.61. *Seja $\theta \in \mathbb{R}$ e n um inteiro positivo. Calcule o resto da divisão do polinômio $(\cos\theta + x\sin\theta)^n \in \mathbb{R}[x]$ por x^2+1.*

1.62. *Seja $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ um polinômio de grau n. Mostre que se p/q é uma raiz racional de $f(x)$, com $p, q \in \mathbb{Z}$ e $\operatorname{mdc}(p,q) = 1$, então $p \mid a_0$ e $q \mid a_n$.*

1.63 (IMO1993)**.** *Seja $f(x) = x^n + 5x^{n-1} + 3$ onde $n > 1$. Demonstrar que $f(x)$ não pode se expressar como produto de dois polinômios não constantes com coeficientes inteiros.*

1.64. *Seja α uma raiz de $x^3 - 3x + 1 = 0$. Mostre que $\alpha^2 - 2$ também é uma raiz deste polinômio.*

1.65. *Encontrar todos os pares $(c, P(x))$ onde c é um real e $P(x)$ é um polinômio não nulo tal que*

$$P(x^4 + x^2 + x) = (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)P(cx).$$

1.66 (AusPol1998)**.** *Encontrar todos os inteiros positivos n e m tais que todas as soluções de $x^3 - 17x^2 + mx - n^2 = 0$ são inteiras.*

1.67. *Dados $x, y \in \mathbb{N}$, defina $a := x(y+1) - (y!+1)$. Mostre que imagem da função $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por*

$$f(x,y) = \frac{y-1}{2}\left(|a^2-1| - (a^2-1)\right) + 2$$

é exatamente o conjunto dos números primos.

1.68. *Prove a seguinte modificação do Critério de Eisenstein: seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ um polinômio primitivo não constante e sem raízes racionais. Suponha que exista um número primo p tal que $p \nmid a_n$, $p \mid a_j$ para todo $0 \le j < n$ e $p^2 \nmid a_1$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.*

1.69. *(Zagier) Dado um número primo, associe a ele um polinômio cujos coeficientes são os dígitos decimais desse primo (por exemplo, $9x^3 + 4x^2 + 3$ para o primo 9403). Mostre que este polinômio é sempre irredutível em $\mathbb{Z}[x]$.*

1.70. *Encontrar todos os valores de k para os quais o polinômio $x^{2k+1} + x + 1$ é divisível por $x^k + x + 1$.*

1.71 (IMO2002)**.** *Encontrar todos os pares de inteiros $m, n > 2$ tais que existam infinitos valores de k para os quais*

$$\frac{k^m + k - 1}{k^n + k^2 - 1}$$

é inteiro.

1.9 Ordem e Raízes Primitivas

Dado $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, definimos a *ordem de* $\overline{a}$, denotado por $\operatorname{ord}\overline{a}$, como o menor inteiro $t > 0$ tal que $\overline{a}^t = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$. Se $a, n \in \mathbb{Z}$ com $\operatorname{mdc}(a,n) = 1$, definimos a *ordem de* a *módulo* n, denotado por $\operatorname{ord}_n a$, como a ordem de $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note que pelo teorema de Euler-Fermat, temos que $\operatorname{ord}_n a \le \varphi(n)$. Se $\operatorname{ord}_n a = \varphi(n)$, dizemos que a é *raiz primitiva módulo* n. Por exemplo, 2 é raiz primitiva módulo 5, pois $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, que é a primeira potência de 2 congruente a 1 módulo 5 e $4 = \varphi(5)$.

O resultado básico mais importante sobre ordem é a seguinte

Proposição 1.64. *Temos que* $a^t \equiv 1 \pmod{n}$ *se, e só se,* $\operatorname{ord}_n a \mid t$.

Demonstração: Como $a^{\operatorname{ord}_n a} \equiv 1 \pmod{n}$, para todo $k \in \mathbb{N}$ tem-se $a^{k \operatorname{ord}_n a} \equiv 1 \pmod{n}$. Por outro lado, se $a^t \equiv 1 \pmod{n}$, pelo algoritmo da divisão existem inteiros q e r tais que $0 \le r < \operatorname{ord}_n a$ e $t = q \operatorname{ord}_n a + r$. Portanto

$$1 \equiv a^t = a^{q \operatorname{ord}_n a + r} = (a^{\operatorname{ord}_n a})^q \cdot a^r \equiv a^r \pmod{n}$$

Ou seja, $a^r \equiv 1 \pmod{n}$. Pela minimalidade de $\operatorname{ord}_n a$, temos que $r = 0$, i.e., $\operatorname{ord}_n a \mid t$. □

Corolário 1.65. $\operatorname{ord}_n a \mid \varphi(n)$.

Exemplo 1.66. *Demonstrar que* $n \mid \varphi(a^n - 1)$ *para todo inteiro positivo* $a > 1$.

Solução: Já que $\operatorname{mdc}(a, a^n - 1) = 1$, pelo teorema de Euler-Fermat temos que $a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}$; por outro lado, n é a ordem de a módulo $a^n - 1$ já que $a^n \equiv 1 \pmod{a^n - 1}$ e se $0 < t < n$ temos $0 < a^t - 1 < a^n - 1$ e assim $a^n - 1 \nmid a^t - 1$. Pela proposição, temos portanto $n \mid \varphi(a^n - 1)$. □

Exemplo 1.67. *Demonstrar que não existe um inteiro* $n > 1$ *tal que* $n \mid 2^n - 1$.

Solução: Suponhamos o contrário; seja p o menor divisor primo de n e $r = \operatorname{ord}_p 2$. Sabemos que $2^n \equiv 1 \pmod{p}$ e além disso, pelo teorema de Fermat, $2^{p-1} \equiv 1 \pmod{p}$.

Portanto $r \mid n$ e $r \mid p-1$, o que implica que $r \mid \operatorname{mdc}(n, p-1)$. Mas $\operatorname{mdc}(n, p-1) = 1$ pois p é o menor divisor primo de n e assim os divisores primos de $p-1$ são menores que os divisores primos de n. Isto mostra que $r = 1$, isto é $2^1 \equiv 1 \pmod{p}$, donde $p \mid 1$, uma contradição. □

Exemplo 1.68. *Sejam* a, m *e* n *inteiros positivos; defina* m' *e* n' *por* $m = \operatorname{mdc}(m,n) \cdot m'$ *e* $n = \operatorname{mdc}(m,n) \cdot n'$, *de modo que* $\operatorname{mdc}(m', n') = 1$. *Mostre que*

$$\operatorname{mdc}(a^m + 1, a^n + 1) = \begin{cases} a^{\operatorname{mdc}(m,n)} + 1 & \textit{se } m' \textit{ e } n' \textit{ são ímpares.} \\ 2 & \textit{se } m' + n' \textit{ e } a \textit{ são ímpares.} \\ 1 & \textit{se } m' + n' \textit{ é ímpar e } a \textit{ é par.} \end{cases}$$

Solução: Como

$$\operatorname{mdc}(a^m + 1, a^n + 1) = \operatorname{mdc}\big((a^{\operatorname{mdc}(m,n)})^{m'} + 1, (a^{\operatorname{mdc}(m,n)})^{n'} + 1\big),$$

o resultado no caso geral seguirá do caso em que $\operatorname{mdc}(m,n) = 1$. Assim, vamos supor m e n são primos entre si e seja $d = \operatorname{mdc}(a^n + 1, a^m + 1)$. Temos

$$\begin{cases} a^n \equiv -1 \pmod{d} \\ a^m \equiv -1 \pmod{d} \end{cases} \Longrightarrow \begin{cases} a^{2n} \equiv 1 \pmod{d} \\ a^{2m} \equiv 1 \pmod{d} \end{cases}$$
$$\Longrightarrow \operatorname{ord}_d a \mid \operatorname{mdc}(2n, 2m) = 2.$$

Assim, $a^2 \equiv 1 \pmod d$. Digamos que m seja ímpar (como estamos supondo $\text{mdc}(m,n)=1$, não podemos ter m e n ambos pares), de modo que

$$\begin{aligned} a\cdot(a^2)^{(m-1)/2} = a^m \equiv -1 \pmod d &\implies a \equiv -1 \pmod d \\ &\iff d \mid a+1. \end{aligned}$$

Se n é ímpar também, então $d = a+1$ já que $a+1 \mid a^m+1$ e $a+1 \mid a^n+1$ neste caso (utilize a fatoração $a^m+1 = (a+1)(a^{m-1}-a^{m-2}+a^{m-3}-\cdots+1)$ ou a implicação $a \equiv -1 \pmod{a+1} \implies a^m \equiv -1 \pmod{a+1}$). Por outro lado, se n é par, temos

$$\begin{aligned} (a^2)^{n/2} = a^n \equiv -1 \pmod d &\implies 1 \equiv -1 \pmod d \\ &\implies d=1 \text{ ou } d=2. \end{aligned}$$

O caso $d=2$ ocorre se, e só se, a^m+1 e a^n+1 são ambos pares, ou seja, quando a é ímpar. Isto encerra a análise de casos e com isso o problema. □

Uma outra caracterização de raiz primitiva é dada pela

Proposição 1.69. *O número a é raiz primitiva módulo n se, e somente se, $\{\overline{a}^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^\times$.*

Demonstração: Para todo $a \in \mathbb{Z}$ com $\text{mdc}(a,n)=1$ temos $\{\overline{a}^t, t\in\mathbb{N}\} \subset (\mathbb{Z}/n\mathbb{Z})^\times$. Note que $\{\overline{a}^t, t\in\mathbb{N}\} = \{\overline{1}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{\text{ord}_n a-1}\}$ é um conjunto com $\text{ord}_n a$ elementos. De fato, para qualquer $t\in\mathbb{N}$ temos $\overline{a}^t = \overline{a}^r$ onde r é o resto na divisão de t por $\text{ord}_n a$; por outro lado, os elementos $\overline{1}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{\text{ord}_n a-1}$ são distintos pois caso $\overline{a}^i = \overline{a}^j$ com $0 \le i < j < \text{ord}_n a$, então $\overline{a}^{j-i} = \overline{1}$ com $0 < j-i < \text{ord}_n a$, o que é absurdo.

Assim, $\{\overline{a}^t, t\in\mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^\times$ se, e só se, $\text{mdc}(a,n)=1$ e $\text{ord}_n a = \varphi(n)$, isto é, se, e só se, a é uma raiz primitiva módulo n. □

Corolário 1.70. *Se m divide n e a é raiz primitiva módulo n, então a é raiz primitiva módulo m.*

Demonstração: Como o mapa natural $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ que leva $x \bmod n$ em $x \bmod m$ é sobrejetor, temos que se as potências de $a \bmod n$ cobrem todo o $(\mathbb{Z}/n\mathbb{Z})^\times$, então as potências de $a \bmod m$ também cobrem todo o $(\mathbb{Z}/m\mathbb{Z})^\times$. Pela proposição, isto implica o corolário. □

Raízes primitivas são muito úteis em diversas questões de Teoria dos Números. Entretanto elas nem sempre existem para qualquer módulo n. O resto desta seção é dedicado a provar o seguinte importante

Teorema 1.71. *Existe alguma raiz primitiva módulo n se, e só se, $n=2$, $n=4$, $n=p^k$ ou $n=2p^k$ onde p é primo ímpar.*

A demonstração deste teorema é longa e é composta de vários passos. Começamos com a seguinte

Proposição 1.72. *Se $k \ge 3$, então não existe nenhuma raiz primitiva módulo 2^k.*

Demonstração: Pelo corolário anterior, basta provar que não existe raiz primitiva módulo 8, e isso segue do fato de que se $\text{mdc}(a,8)=1$, isto é, $a=2r+1$, $r\in\mathbb{N}$, então $a^2 = 4r(r+1)+1 \equiv 1 \pmod 8$ (sendo $r(r+1)$ par, visto que é o produto de dois números consecutivos). Assim, não há elemento de ordem $\varphi(8)=4$ módulo 8. □

Proposição 1.73. *Se $n = ab$, com $a \geq 3$ e $b \geq 3$ inteiros tais que* $\mathrm{mdc}(a, b) = 1$, *então não existe raiz primitiva módulo n.*

Demonstração: Como $\varphi(n) = \varphi(a)\varphi(b)$ e $a \geq 3$ e $b \geq 3$, segue que $\varphi(a)$ e $\varphi(b)$ são pares (verifique!). Se $\mathrm{mdc}(k, n) = 1$, então temos

$$\begin{aligned} k^{\varphi(n)/2} &= (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod{a} \qquad \text{e} \\ k^{\varphi(n)/2} &= (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \pmod{b}. \end{aligned}$$

Assim, $k^{\varphi(n)/2} \equiv 1 \pmod{n}$ e portanto $\mathrm{ord}_n k \leq \varphi(n)/2 < \varphi(n)$ para todo k primo com n. □

Proposição 1.74. *Se p é um número primo e $a \in \mathbb{Z}$ é uma raiz primitiva módulo p, então a ou $a + p$ é raiz primitiva módulo p^2.*

Demonstração: Por hipótese, $\mathrm{ord}_p a = \mathrm{ord}_p(a + p) = \varphi(p) = p - 1$. Portanto $p - 1 \mid \mathrm{ord}_{p^2} a$, pois $a^t \equiv 1 \pmod{p^2}$ implica $a^t \equiv 1 \pmod{p}$. Além disso, como $\mathrm{ord}_{p^2} a \mid \varphi(p^2) = p(p-1)$, devemos ter $\mathrm{ord}_{p^2} a = p-1$ ou $\mathrm{ord}_{p^2} a = p(p-1) = \varphi(p^2)$. Do mesmo modo, $\mathrm{ord}_{p^2}(a + p) = p - 1$ ou $\mathrm{ord}_{p^2}(a + p) = p(p - 1) = \varphi(p^2)$. Basta provar, portanto, que $\mathrm{ord}_{p^2} a \neq p - 1$ ou $\mathrm{ord}_{p^2}(a + p) \neq p - 1$. Suponha que $\mathrm{ord}_{p^2} a = p - 1$. Portanto $a^{p-1} \equiv 1 \pmod{p^2}$ e assim

$$\begin{aligned} (a + p)^{p-1} &= a^{p-1} + \binom{p-1}{1} a^{p-2} p + \binom{p-1}{2} a^{p-3} p^2 + \cdots \\ &\equiv 1 - pa^{p-2} \pmod{p^2}. \end{aligned}$$

Portanto $(a + p)^{p-1}$ não é congruente a 1 módulo p^2, pois p^2 não divide pa^{p-2} (lembre-se de que $\mathrm{mdc}(a, p) = 1$), donde $\mathrm{ord}_{p^2}(a + p) \neq p - 1$. □

Proposição 1.75. *Se p é um número primo ímpar e a é raiz primitiva módulo p^2, então a é raiz primitiva módulo p^k para todo $k \in \mathbb{N}$.*

Demonstração: Como $a^{p-1} \equiv 1 \pmod{p}$, mas a^{p-1} não é congruente a 1 módulo p^2 (já que a é raiz primitiva módulo p^2), temos $a^{p-1} = 1 + b_1 p$, onde p não divide b_1. Vamos mostrar por indução que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, onde p não divide b_k, para todo $k \geq 1$. De fato, para $k \geq 1$ e $p > 2$ primo,

$$\begin{aligned} a^{p^k(p-1)} = (1 + b_k p^k)^p &= 1 + \binom{p}{1} b_k p^k + \binom{p}{2} b_k^2 p^{2k} + \cdots \\ &= 1 + p^{k+1}(b_k + pt) \end{aligned}$$

para algum $t \in \mathbb{Z}$ e assim $b_{k+1} = b_k + pt$ também não é divisível por p pois $p \nmid b_k$.

Vamos agora mostrar por indução que a é raiz primitiva módulo p^k para todo $k \geq 2$. Suponha que a seja raiz primitiva módulo p^k. Como $a^{\mathrm{ord}_{p^{k+1}} a} \equiv 1 \pmod{p^{k+1}} \implies a^{\mathrm{ord}_{p^{k+1}} a} \equiv 1 \pmod{p^k}$ temos

$$p^{k-1}(p - 1) = \varphi(p^k) = \mathrm{ord}_{p^k} a \mid \mathrm{ord}_{p^{k+1}} a \mid \varphi(p^{k+1}) = p^k(p - 1).$$

Portanto $\mathrm{ord}_{p^{k+1}} a = p^{k-1}(p-1)$ ou $\mathrm{ord}_{p^{k+1}} a = p^k(p-1) = \varphi(p^{k+1})$, mas o primeiro caso é impossível pois $a^{p^{k-1}(p-1)} = 1 + b_k p^k$ com $p \nmid b_k$. Logo $\mathrm{ord}_{p^{k+1}} a = \varphi(p^{k+1})$ e a é raiz primitiva módulo p^{k+1}. □

Por exemplo 2 é raiz primitiva módulo 5^k para todo $k \geq 1$. De fato, 2 é raiz primitiva módulo 5 e, como $2^4 = 16 \not\equiv 1 \pmod{25}$, 2 é raiz primitiva módulo $25 = 5^2$ também. Portanto, pela proposição anterior, 2 é raiz primitiva módulo 5^k para todo $k \geq 1$.

Proposição 1.76. *Se p é primo ímpar e a é um inteiro ímpar tal que a é raiz primitiva módulo p^k, então a é raiz primitiva módulo $2p^k$. Em particular, se a é raiz primitiva qualquer módulo p^k, então a ou $a + p^k$ é raiz primitiva módulo $2p^k$ (pois um deles é ímpar).*

Demonstração: Temos, como nas provas acima, $\varphi(p^k) = \operatorname{ord}_{p^k} a \mid \operatorname{ord}_{2p^k} a$ e $\operatorname{ord}_{2p^k} a \mid \varphi(2p^k) = \varphi(p^k)$, logo $\operatorname{ord}_{2p^k} a = \varphi(2p^k)$. □

Para completar a prova do teorema 1.71, falta provar que se p é primo ímpar, então existe raiz primitiva módulo p. Para isto, precisamos de dois lemas.

Lema 1.77. $\sum_{d\mid n} \varphi(d) = n$ *para todo* $n \in \mathbb{N}$.

Demonstração: Seja d um divisor de n. A quantidade de a's tais que $1 \leq a \leq n$ e $d = \operatorname{mdc}(n, a)$ é igual a $\varphi(\frac{n}{d})$ pois $d = \operatorname{mdc}(n,a) \iff d \mid a$ e $1 = \operatorname{mdc}(\frac{n}{d}, \frac{a}{d})$. Como $\varphi(\frac{n}{d})$ conta justamente a quantidade de inteiros entre 1 e $\frac{n}{d}$ (inclusive) que são primos com $\frac{n}{d}$, temos que $\sum_{d\mid n} \varphi(\frac{n}{d}) = \sum_{d\mid n} \varphi(d)$ conta a quantidade de números a entre 1 e n (inclusive), particionados segundo os valores de $\operatorname{mdc}(a, n)$. □

Lema 1.78. *Seja p um primo e d um divisor de $p - 1$. Defina $N(d)$ como a quantidade de elementos $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ com $\operatorname{ord} \overline{a} = d$. Então $N(d) \leq \varphi(d)$.*

Demonstração: Podemos supor que $N(d) > 0$, logo existe a tal que $\operatorname{ord}_p a = d$. Logo $\overline{a}^d = \overline{1}$ e, para $0 \leq k < d$, as classes de a^k são todas distintas módulo p. Como $(\overline{a}^k)^d = 1$ e a equação $x^d - \overline{1} = 0$ tem no máximo d raízes distintas em $\mathbb{Z}/p\mathbb{Z}$ (pois $\mathbb{Z}/p\mathbb{Z}$ é um corpo), suas raízes são exatamente $\overline{a}^k$, $0 \leq k < d$. Por outro lado, se $\operatorname{ord}_p a^k = d$, então $\operatorname{mdc}(k, d) = 1$, pois caso $r = \operatorname{mdc}(k, d) > 1$, então $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1 \pmod{p}$, logo $\operatorname{ord}_p(a^k) \leq d/r < d$. Desta forma,

$$\{b \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \operatorname{ord}_p b = d\} \subset \{\overline{a}^k \mid 0 \leq k < d \text{ e } \operatorname{mdc}(k, d) = 1\},$$

portanto $N(d) \leq \varphi(d)$ (na verdade, os dois conjuntos acima são iguais, como ficará claro a partir da demonstração da proposição abaixo). □

Proposição 1.79. *Se p é um primo, então existe uma raiz primitiva módulo p.*

Demonstração: Para cada $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, tem-se $\operatorname{ord}_p a \mid p-1$ e portanto $p - 1 = \sum_{d\mid p-1} N(d)$. Por outro lado, temos pelos dois lemas acima que

$$p - 1 = \sum_{d\mid p-1} N(d) \leq \sum_{d\mid p-1} \varphi(d) = p - 1.$$

Logo devemos ter $N(d) = \varphi(d)$ para todo d. Em particular, $N(p-1) = \varphi(p-1) > 0$, logo existem raízes primitivas módulo p. □

Corolário 1.80. *Seja p um primo. Para cada $d \mid p - 1$, existem exatamente $\varphi(d)$ elementos em $(\mathbb{Z}/p\mathbb{Z})^\times$ com ordem d. Em particular, p possui exatamente $\varphi(p - 1)$ raízes primitivas.*

Com isto, encerramos a demonstração do teorema 1.71. Vejamos algumas aplicações.

Exemplo 1.81. *Mostre que existe n natural tal que os mil últimos dígitos de 2^n pertencem a $\{1, 2\}$.*

Solução: Observamos inicialmente que para todo $k \in \mathbb{N}$ existe um número m_k de k algarismos, todos 1 ou 2, divisível por 2^k. De fato, $m_1 = 2$ e $m_2 = 12$ satisfazem o enunciado. Seja $m_k = 2^k r_k$, $r_k \in \mathbb{N}$. Se r_k é par, tome $m_{k+1} = 2\times 10^k + m_k = 2^{k+1}(5^k + r_k/2)$, e se r_k é ímpar, tome $m_{k+1} = 10^k + m_k = 2^{k+1}(5^k + r_k)/2$.

Como $m_{1000} \equiv 2 \pmod{10}$, 5 não divide $r_{1000} = \frac{m_{1000}}{2^{1000}}$. Portanto, como 2 é raiz primitiva módulo 5^{1000} pela proposição 1.75, existe $k \in \mathbb{N}$ com $2^k \equiv r_{1000} \pmod{5^{1000}}$. Logo $2^k = b5^{1000} + r_{1000}$ para algum $b \in \mathbb{N}$ e assim

$$2^{k+1000} = b10^{1000} + 2^{1000} r_{1000} = b10^{1000} + m_{1000},$$

e as 1000 últimas casas de 2^{k+1000} são as 1000 casas de m_{1000}, que pertencem todas a $\{1, 2\}$. □

Observação 1.82. *Um grupo G é chamado de* cíclico *se existe um elemento g tal que $G = \{g^n \mid n \in \mathbb{Z}\}$. O fato de p^n e $2p^n$, p primo ímpar, admitirem raízes primitivas equivale a dizer que os grupos $(\mathbb{Z}/p^n\mathbb{Z})^\times$ e $(\mathbb{Z}/2p^n\mathbb{Z})^\times$ são cíclicos, ou ainda que há isomorfismos de grupos $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p^n)$ e $(\mathbb{Z}/2p^n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(2p^n)$ onde a operação nos grupos da direita é a adição.*

O leitor não deve ter dificuldades para adaptar a prova acima a fim de mostrar que todo corpo K com um número finito de elementos (tal como o construído no exemplo após o teorema 1.57) admite raiz primitiva, isto é, o seu grupo de unidades $K^\times = K \setminus \{0\}$ é um grupo cíclico.

Problemas Propostos

1.72. *Encontrar as ordens de 2 e 5 módulo 101. Encontrar também todos os elementos de ordem 20 em $(\mathbb{Z}/101\mathbb{Z})^\times$.*

1.73. *Determine um elemento de $(\mathbb{Z}/99\mathbb{Z})^\times$ de ordem 30.*

1.74. *Determine todos os valores de n para os quais $|(\mathbb{Z}/n\mathbb{Z})^\times| = 24$.*

1.75. *Determine um gerador de $(\mathbb{Z}/242\mathbb{Z})^\times$.*

1.76. *Demonstrar que $2n \mid \varphi(a^n + 1)$ para todo inteiro positivo a.*

1.77 (IMO1978). *Sejam m e n inteiros positivos com $m < n$. Se os três últimos algarismos de 1978^m são os mesmos que os três últimos algarismos de 1978^n, encontrar m e n tais que $m + n$ assume o menor valor possível.*

1.78. *Sejam d e n números naturais tais que $d \mid 2^{2^n} + 1$. Demonstre que existe um inteiro k tal que $d = k2^{n+1} + 1$.*

1.79. *Seja $k \geq 2$ e $n_1, n_2, \ldots, n_k \geq 1$ números naturais que tem a propriedade*

$$n_2 \mid (2^{n_1} - 1), \quad n_3 \mid (2^{n_2} - 1), \ldots, n_k \mid (2^{n_{k-1}} - 1) \text{ e } n_1 \mid (2^{n_k} - 1)$$

Demonstrar que $n_1 = n_2 = \cdots = n_k = 1$.

1.80. *Mostrar que $x^3 - x + \overline{1}$ é irredutível em $\mathbb{Z}/3\mathbb{Z}[x]$. Encontrar todas as raízes primitivas do corpo finito $\frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^3 - x + \overline{1})}$.*

1.81 (Teorema de Lagrange). *Seja G um grupo com número finito de elementos. Seja H um* subgrupo *de G, i.e., um subconjunto de G tal que $a, b \in H \implies a \cdot b \in H$ e $a \in H \implies a^{-1} \in H$, de modo que o produto de G se restringe a H e faz de H um grupo também.*

(a) Mostre que os subconjuntos de G do tipo

$$g \cdot H \stackrel{\text{def}}{=} \{g \cdot h \mid h \in H\}$$

formam uma partição de G, ou seja, todo elemento de G pertence a algum $g \cdot H$ e que se $g_1 \cdot H \cap g_2 \cdot H \neq \emptyset$, então $g_1 \cdot H = g_2 \cdot H$.

(b) Mostre que $|g_1 \cdot H| = |g_2 \cdot H|$ para quaisquer $g_1, g_2 \in G$ e que portanto $|H|$ divide $|G|$ (teorema de Lagrange).

(c) Seja $g \in G$. Mostre que existe $t > 0$ tal que $g^t = e$. Se $\operatorname{ord} g$ *é o menor t positivo com esta propriedade, mostre que*

$$H = \{g^n \mid n \in \mathbb{N}\}$$

é um subgrupo de G com $\operatorname{ord} g$ *elementos.*

(d) Aplicando o teorema de Lagrange ao subgrupo do item anterior, prove que $g^{|G|} = e$ para todo $g \in G$. Observe que isto fornece uma nova prova do teorema de Euler-Fermat no caso em que $G = (\mathbb{Z}/(n))^\times$.

1.82 (APMO1997). *Encontrar um n no conjunto $\{100, 101, \ldots 1997\}$ tal que n divide $2^n + 2$.*

1.83. *Definimos a* função de Carmichael $\lambda \colon \mathbb{N} \to \mathbb{N}$ *como o menor inteiro positivo tal que $a^{\lambda(n)} \equiv 1 \pmod n$ para todo a primo com n. Observe que, pelo teorema 1.71, $\lambda(p^l) = p^{l-1}(p-1)$ para todo p primo ímpar. Mostrar que*

(a) $\lambda(2) = 1$, $\lambda(4) = 2$ e $\lambda(2^l) = 2^{l-2}$ para todo $l \geq 3$.

(b) Se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ é a fatoração em primos de n, então

$$\lambda(n) = \operatorname{mmc}\{\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})\}.$$

1.84 (IMO2000). *Existe um inteiro N divisível por exatamente 2000 primos diferentes e tal que N divide $2^N + 1$?*

Sim. Vamos construir indutivamente um inteiro N divisível por exatamente k primos distintos e tal que $N \mid 2^N + 1$.

1.85 (IMO1990). *Encontrar todos os números naturais n tais que $n^2 \mid 2^n + 1$.*

1.86 (IMO1999). *Encontrar todos os pares (n, p) de inteiros positivos tais que p é primo, $n \leq 2p$ e $(p-1)^n + 1$ é divisível por n^{p-1}.*

1.87 (Banco-IMO2000). *Determine todas as triplas (a, m, n) de inteiros positivos tais que $a^m + 1 \mid (a+1)^n$.*

Capítulo 2

Equações Módulo m

Neste capítulo estudaremos equações do tipo

$$f(x) \equiv 0 \pmod{m}$$

na variável x, onde $f(x)$ é um polinômio com coeficientes inteiros.

2.1 Equações Lineares Módulo m

Se $\mathrm{mdc}(a, m) = 1$, como a é invertível módulo m, a equação

$$ax \equiv b \pmod{m},$$

tem solução única módulo m, dada por $x \equiv a^{\varphi(m)-1}b \pmod{m}$ (utilizando o teorema de Euler-Fermat para encontrar o inverso de $\overline{a} \in \mathbb{Z}/(m)$). Assim, todas as soluções da equação acima são da forma $x = a^{\varphi(m)-1}b + km$ onde $k \in \mathbb{Z}$. No caso geral, se $\mathrm{mdc}(a, m) = d > 1$ temos que

$$ax \equiv b \pmod{m} \implies ax \equiv b \pmod{d} \iff b \equiv 0 \pmod{d}.$$

Logo uma condição necessária para que a congruência linear $ax \equiv b \pmod{m}$ tenha solução é que $d \mid b$. Esta condição é também suficiente, já que escrevendo $a = da'$, $b = db'$ e $m = dm'$, temos que

$$ax \equiv b \pmod{m} \iff a'x \equiv b' \pmod{m'}.$$

Como $\mathrm{mdc}(a', m') = 1$, há uma única solução $(a')^{\varphi(m')-1}b'$ módulo m', isto é, há d soluções distintas módulo m, a saber $x \equiv (a')^{\varphi(m')-1}b' + km' \pmod{m}$ com $0 \leq k < d$. Note ainda que como resolver $ax \equiv b \pmod{m}$ é equivalente a resolver a equação diofantina linear $ax + my = b$, poderíamos também ter utilizado o teorema de Bachet-Bézout e o algoritmo de Euclides para encontrar as soluções desta congruência linear como no exemplo 1.14. Resumimos esta discussão na seguinte

Proposição 2.1. *A congruência linear*

$$ax \equiv b \pmod{m}$$

admite solução se, e somente se, $\mathrm{mdc}(a, m) \mid b$. *Neste caso, há exatamente* $\mathrm{mdc}(a, m)$ *soluções distintas módulo* m.

Agora queremos encontrar condições para que um sistema de congruências lineares tenha solução. O seguinte teorema nos garante a existência de tais soluções.

Teorema 2.2 (Teorema Chinês dos Restos)**.** *Se $b_1, b_2, \ldots, b_k$ são inteiros quaisquer e $a_1, a_2, \ldots, a_k$ são primos relativos dois a dois, o sistema de equações*

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

admite solução, que é única módulo $A = a_1 a_2 \ldots a_k$.

DEMONSTRAÇÃO: Daremos duas provas do teorema chinês dos restos. Para a primeira, consideremos os números $M_i = \frac{A}{a_i}$. Como $\mathrm{mdc}(a_i, M_i) = 1$, logo existe X_i tal que $M_i X_i \equiv 1 \pmod{a_i}$. Note que se $j \neq i$ então M_j é múltiplo de a_i e portanto $M_j X_j \equiv 0 \pmod{a_i}$. Assim, temos que

$$x_0 = M_1 X_1 b_1 + M_2 X_2 b_2 + \cdots + M_k X_k b_k$$

é solução do sistema de equações, pois $x_0 \equiv M_i X_i b_i \equiv b_i \pmod{a_i}$. Além disso, se x_1 é outra solução, então $x_0 \equiv x_1 \pmod{a_i} \iff a_i \mid x_0 - x_1$ para todo a_i, e como os a_i's são dois a dois primos, temos que $A \mid x_0 - x_1 \iff x_0 \equiv x_1 \pmod{A}$, mostrando a unicidade módulo A.

Para a segunda prova, considere o mapa natural

$$\begin{aligned} f \colon \mathbb{Z}/(A) &\to \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_k) \\ b \bmod A &\mapsto (b \bmod a_1, b \bmod a_2, \ldots, b \bmod a_k). \end{aligned}$$

Note que este mapa está bem definido, isto é, o valor de $f(b \bmod A)$ independe da escolha do representante da classe de $b \bmod A$, pois quaisquer dois representantes diferem de um múltiplo de A, que tem imagem $(0 \bmod a_1, \ldots, 0 \bmod a_k)$ no produto $\mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_k)$. Observemos agora que o teorema chinês dos restos é equivalente a mostrar que f é uma bijeção: o fato de f ser sobrejetor corresponde à existência da solução do sistema, enquanto que o fato de f ser injetor corresponde à unicidade módulo A. Como o domínio e o contradomínio de f têm mesmo tamanho (ambos têm A elementos), para mostrar que f é uma bijeção basta mostrarmos que f é injetora. Suponha que $f(b_1 \bmod A) = f(b_2 \bmod A)$, então $b_1 \equiv b_2 \pmod{a_i}$ para todo i, e como na primeira demonstração temos que isto implica $b_1 \equiv b_2 \pmod{A}$, o que encerra a prova. □

Observação 2.3. *Como* $\mathrm{mdc}(b, a_1 a_2 \ldots a_k) = 1 \iff \mathrm{mdc}(b, a_j) = 1, \forall j \leq k$*, a bijeção f definida na segunda prova do teorema anterior satisfaz $f((\mathbb{Z}/(A))^\times) = (\mathbb{Z}/(a_1))^\times \times (\mathbb{Z}/(a_2))^\times \times \cdots \times (\mathbb{Z}/(a_k))^\times$.*

Em particular, isso nos dá uma nova prova de que
$\varphi(a_1 a_2 \ldots a_k) = \varphi(a_1)\varphi(a_2)\ldots\varphi(a_k)$ *sempre que* $\mathrm{mdc}(a_i, a_j) = 1, \forall i \neq j$.

Por exemplo, para $k = 2$, $a_1 = 3$ e $a_2 = 5$, temos a seguinte tabela, que mostra, para cada i e j com $0 \leq i < 3$ e $0 \leq j < 5$, a única solução x com $0 \leq x < 3 \cdot 5 = 15$ tal que $x \equiv i \pmod 3$ e $x \equiv j \pmod 5$:

	0 mod 5	1 mod 5	2 mod 5	3 mod 5	4 mod 5
0 mod 3	0	6	12	3	9
1 mod 3	10	1	7	13	4
2 mod 3	5	11	2	8	14

Vejamos algumas aplicações.

Exemplo 2.4. *Um inteiro é* livre de quadrados *se ele não é divisível pelo quadrado de nenhum número inteiro maior do que 1. Demonstrar que existem intervalos arbitrariamente grandes de inteiros consecutivos, nenhum dos quais é livre de quadrados.*

SOLUÇÃO: Seja n um número natural qualquer. Sejam $p_1, \dots, p_n$ primos distintos. O teorema chinês dos restos nos garante que o sistema

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2} \\ x &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -n \pmod{p_n^2} \end{aligned}$$

tem solução. Se x_0 é uma solução positiva do sistema, então cada um dos números $x_0 + 1, x_0 + 2, \dots, x_0 + n$ é divisível pelo quadrado de um inteiro maior do que 1, logo nenhum deles é livre de quadrados. □

Exemplo 2.5. *Seja $P(x)$ um polinômio não constante com coeficientes inteiros. Demonstrar que para todo inteiro n, existe um inteiro i tal que*

$$P(i), P(i+1), P(i+2), \dots, P(i+n)$$

são números compostos.

SOLUÇÃO: Demonstraremos primeiro o seguinte

Lema 2.6. *Seja $P(x)$ um polinômio não constante com coeficientes inteiros. Para todo par de inteiros k, i, tem-se que $P(i) \mid P(k\,P(i) + i)$.*

DEMONSTRAÇÃO: Dado que $(kP(i)+i)^n \equiv i^n \pmod{P(i)}$ para todo n inteiro não negativo, é fácil ver que $P(kP(i) + i) \equiv P(i) \equiv 0 \pmod{P(i)}$. □

Suponhamos por contradição que a sequência $P(i), P(i+1), \dots, P(i+n)$ contém um número primo para cada i. Então a sequência $\{P(i)\}_{i \geq 1}$ assume infinitos valores primos. Consideremos os $n+1$ primos distintos $P(i_0), P(i_1), \dots, P(i_n)$. Pelo teorema chinês dos restos segue que existem infinitas soluções x do sistema de equações

$$\begin{aligned} x &\equiv i_0 \pmod{P(i_0)} \\ x &\equiv i_1 - 1 \pmod{P(i_1)} \\ x &\equiv i_2 - 2 \pmod{P(i_2)} \\ &\vdots \\ x &\equiv i_n - n \pmod{P(i_n)} \end{aligned}$$

onde, se x_0 é uma solução, então $x = x_0 + k(P(i_0) \cdots P(i_n))$ também é solução para todo $k \geq 0$. Assim, pelo lema anterior, podemos dizer que $P(x), P(x+1), \dots, P(x+n)$ são números compostos quando k é suficientemente grande, múltiplos respectivamente de $P(i_0), P(i_1), \dots, P(i_n)$.

□

Exemplo 2.7. *Uma* potência não trivial *é um número da forma* m^k*, onde* m*,* k *são inteiros maiores do que ou iguais a 2. Dado* $n \in \mathbb{N}$*, prove que existe um conjunto* $A \subset \mathbb{N}$ *com* n *elementos tal que para todo subconjunto* $B \subset A$ *não vazio,* $\sum\limits_{x \in B} x$ *é uma potência não trivial. Em outras palavras, se* $A = \{x_1, x_2, \ldots, x_n\}$ *então todas as somas* $x_1, x_2, \ldots, x_n$*,* $x_1 + x_2, x_1 + x_3, \ldots, x_{n-1} + x_n$*,* $\ldots$*,* $x_1 + x_2 + \cdots + x_n$ *são potências não triviais.*

Solução: Vamos provar a existência de um tal conjunto por indução em n. Para $n = 1$, $A = \{4\}$ é solução e, para $n = 2$, $A = \{9, 16\}$ é solução. Suponha agora que $A = \{x_1, \ldots, x_n\}$ é um conjunto com n elementos e para todo $B \subset A$, $B \neq \emptyset$, $\sum\limits_{x \in B} x = m_B^{k_B}$. Vamos mostrar que existe $c \in \mathbb{N}$ tal que o conjunto $\tilde{A} = \{cx_1, cx_2, \ldots, cx_n, c\}$ satisfaz o enunciado. Seja $\lambda = \operatorname{mmc}\{k_B \mid B \subset A, B \neq \emptyset\}$, o mínimo múltiplo comum de todos os expoentes k_B. Para cada $B \subset A$, $B \neq \emptyset$, associamos um número primo $p_B > \lambda$, de forma que $B_1 \neq B_2$ implica $p_{B_1} \neq p_{B_2}$. Pelo teorema chinês dos restos existe um natural r_B com

$$\begin{aligned} r_B &\equiv 0 \pmod{p_X} \text{ para todo subconjunto } X \subset A,\ X \neq B \\ \lambda \cdot r_B &\equiv -1 \pmod{p_B}. \end{aligned}$$

(λ é invertível módulo p_B). Tomemos

$$c = \prod_{\substack{X \subset A \\ X \neq \emptyset}} (1 + m_X^{k_X})^{\lambda r_X}$$

e vamos mostrar que $\tilde{A} = \{cx_1, cx_2, \ldots, cx_n, c\}$ continua a satisfazer as condições do enunciado.

Dado $B' \subset \{cx_1, cx_2, \ldots, cx_n\}$, temos que $B' = \{cx \mid x \in B\}$ para algum $B \subset A$. Como c é uma potência λ-ésima, c também é uma potência k_B-ésima, portanto, $\sum_{x \in B'} x = c m_B^{k_B}$ será uma potência k_B-ésima para todo $B' \neq \emptyset$. Além disso, para subconjuntos de $\tilde{A}$ da forma $B' \cup \{c\}$, temos

$$\sum_{x \in B' \cup \{c\}} x = c \cdot (1 + m_B^{k_B}) = \Big(\prod_{\substack{X \subset A \\ X \neq \emptyset, B}} (1 + m_X^{k_X})^{\lambda r_X} \Big) (1 + m_B^{k_B})^{\lambda r_B + 1},$$

que é uma potência p_B-ésima, pois $\lambda r_B + 1$ e r_X ($X \neq B$) são múltiplos de p_B. □

Problemas Propostos

2.1. *Resolver as equações lineares*

(a) $7x \equiv 12 \pmod{127}$

(b) $12x \equiv 5 \pmod{122}$

(c) $40x \equiv 64 \pmod{256}$

2.2. *Resolver o sistema de congruências lineares*

$$\begin{aligned} x &\equiv 0 \pmod{7} \\ x &\equiv 1 \pmod{12} \\ x &\equiv -5 \pmod{17} \end{aligned}$$

2.3. *Determine um valor de s tal que $1024s \equiv 1 \pmod{2011}$ e calcule o resto da divisão de 2^{2000} por 2011.*

2.4. *Um inteiro positivo n é chamado de* auto-replicante *se os últimos dígitos de n^2 formam o número n. Por exemplo, 25 é auto-replicante pois $25^2 = 625$. Determine todos os números auto-replicantes com exatamente 4 dígitos.*

2.5. *Sejam $a, n \in \mathbb{N}_{>0}$ e considere a sequência (x_k) definida por $x_1 = a$, $x_{k+1} = a^{x_k}$ para todo $k \in \mathbb{N}$. Demonstrar que existe $N \in \mathbb{N}$ tal que $x_{k+1} \equiv x_k \pmod{n}$ para todo $k \geq N$.*

2.6. *Demonstrar que o sistema de equações*

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

tem solução se, e só se, para todo i e j, $\operatorname{mdc}(a_i, a_j) \mid (b_i - b_j)$. (No caso particular em que $\operatorname{mdc}(a_i, a_j) = 1$, o problema se reduz ao teorema chinês dos restos).

2.7. *Demonstrar que, para k e n números naturais, é possível encontrar k números consecutivos, cada um dos quais tem ao menos n divisores primos diferentes.*

2.8. *Demonstrar que se a, b e c são três inteiros diferentes, então existem infinitos valores de n para os quais $a+n$, $b+n$ e $c+n$ são primos relativos.*

2.9. *Demonstrar que para todo inteiro positivo m e todo número par $2k$, este último pode ser escrito como a diferença de dois inteiros positivos, cada um dos quais é primo relativo com m.*

2.10. *Demonstrar que existem progressões aritméticas de comprimento arbitrário formadas por inteiros positivos tais que cada termo é a potência de um inteiro positivo com expoente maior do que 1.*

2.2 Congruências de Grau 2

Seja $p > 2$ um número primo e $a, b, c \in \mathbb{Z}$ com a não divisível por p. Resolver a equação quadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

é o mesmo que resolver (completando quadrados)

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

(note que 2 e a são invertíveis módulo p). Assim, estamos interessados em encontrar critérios de existência de soluções da equação

$$X^2 \equiv d \pmod{p}.$$

Se a equação acima admite solução (i.e. se $\overline{d}$ é um "quadrado perfeito" em $\mathbb{Z}/p\mathbb{Z}$) então dizemos que d é um *resíduo ou resto quadrático* módulo p. Há exatamente $(p+1)/2$ resíduos quadráticos módulo p, a saber

$$0^2, 1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p$$

já que todo inteiro x é congruente a $\pm i$ mod p para algum i tal que $0 \leq i \leq (p-1)/2$, de modo que x^2 é congruente a um dos números da lista acima. Note que módulo p estes números são todos distintos: de fato, temos que

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} &\implies p \mid (i-j)(i+j) \\ &\iff p \mid i-j \text{ ou } p \mid i+j \\ &\iff i \equiv \pm j \pmod{p} \end{aligned}$$

Mas como $0 \leq i, j \leq (p-1)/2 \implies 0 < i+j \leq p-1$ ou $i = j = 0$, temos que a única possibilidade é $i \equiv j \pmod{p}$.

Embora saibamos a lista completa dos resíduos quadráticos, na prática pode ser difícil reconhecer se um número é ou não resíduo quadrático. Por exemplo, você sabe dizer se 2 é resíduo quadrático módulo 1019? Veremos a seguir o teorema da reciprocidade quadrática, que permite responder estas questões de maneira bastante eficiente.

2.2.1 Resíduos Quadráticos e Símbolo de Legendre

Seja $p > 2$ um número primo e a um inteiro qualquer. Para simplificar cálculos e notações definiremos o chamado *símbolo de Legendre*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ 0 & \text{se } p \mid a \\ -1 & \text{caso contrário} \end{cases}$$

Proposição 2.8 (Critério de Euler)**.** *Seja $p > 2$ um primo e a um inteiro qualquer. Então*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

DEMONSTRAÇÃO: Para $a \equiv 0 \pmod{p}$ o resultado é claro, de modo que podemos supor $p \nmid a$. Pelo teorema de Fermat temos que $a^{p-1} \equiv 1 \pmod{p}$, donde

$$\begin{aligned} (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p} &\iff p \mid a^{\frac{p-1}{2}} - 1 \text{ ou } p \mid a^{\frac{p-1}{2}} + 1 \\ &\iff a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}. \end{aligned}$$

Assim, devemos mostrar que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se, e só se, a é um resíduo quadrático módulo p.

Se a é um resíduo quadrático, digamos $a \equiv i^2 \pmod{p}$, novamente pelo teorema de Fermat temos que

$$a^{\frac{p-1}{2}} \equiv i^{p-1} \equiv 1 \pmod{p}.$$

Assim, os resíduos quadráticos $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ módulo p são raízes do polinômio $f(x) = x^{\frac{p-1}{2}} - \overline{1}$ em $\mathbb{Z}/(p)[x]$. Mas $\mathbb{Z}/(p)$ é corpo, logo $f(x)$ pode ter no máximo $\deg f = (p-1)/2$ raízes em $\mathbb{Z}/(p)$. Isto mostra que as raízes de $f(x)$ são exatamente os resíduos quadráticos não congruentes a zero módulo p e que, portanto, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se, e só se, a é um resíduo quadrático módulo p. □

Corolário 2.9. *O símbolo de Legendre possui as seguintes propriedades:*

1. *se $a \equiv b \pmod{p}$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

2. *$\left(\frac{a^2}{p}\right) = 1$ se $p \nmid a$.*

3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, *ou seja,* -1 *é resíduo quadrático módulo* p *se, e só se,* $p \equiv 1 \pmod 4$.

4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Demonstração: Os itens *1* e *2* são imediatos a partir da definição e *3* segue do critério de Euler: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p \implies \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ já que $p > 2$ e ambos os lados da congruência são iguais a ± 1. Da mesma forma, aplicando o critério de Euler temos que

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p,$$

o que mostra que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, pois novamente ambos os lados da congruência são iguais a ± 1. ◻

Exemplo 2.10. *Mostre que o polinômio* $f(x) = x^4 - 10x^2 + 1$ *é irredutível em* $\mathbb{Z}[x]$, *mas é redutível módulo* p *para todo primo* p.

Solução: Vejamos que $f(x)$ é irredutível em $\mathbb{Z}[x]$. Observe inicialmente que as raízes de $f(x)$ são todas irracionais: se $p, q \in \mathbb{Z}$ são tais que $\operatorname{mdc}(p,q) = 1$ e $f(p/q) = 0 \iff p^4 - 10p^2q^2 + q^4 = 0$, temos da última igualdade que $q \mid p^4 \implies q = \pm 1$ e $p \mid q^4 \implies p = \pm 1$ já que p e q são primos entre si, logo $p/q = \pm 1$, nenhuma das quais é raiz de $f(x)$ (cujos zeros são $\pm\sqrt{2} \pm \sqrt{3}$).

Logo se $f(x)$ for redutível ele é o produto de dois polinômios de grau 2, que podemos supor mônicos. Como o produto dos coeficientes independentes destes dois fatores deve ser igual ao coeficiente independente de $f(x)$, que é 1, temos apenas duas possibilidades:

$$\begin{aligned} f(x) &= (x^2 + ax + 1)(x^2 + bx + 1) \qquad \text{ou} \\ f(x) &= (x^2 + ax - 1)(x^2 + bx - 1) \end{aligned}$$

com $a, b \in \mathbb{Z}$. Em ambos os casos, temos $a + b = 0$ (coeficiente de x^3). Logo, no primeiro caso, comparando o coeficiente de x^2 temos $ab + 2 = -10 \iff a^2 = 12$, o que é impossível. O segundo caso é análogo.

Agora, para $p = 2$ e $p = 3$ temos

$$f(x) \equiv (x+1)^4 \pmod 2 \qquad \text{e} \qquad f(x) \equiv (x^2+1)^2 \pmod 3.$$

Agora se $p > 3$ é um primo, temos que ou $\left(\frac{2}{p}\right) = 1$, ou $\left(\frac{3}{p}\right) = 1$ ou $\left(\frac{6}{p}\right) = 1$ já que $\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{6}{p}\right)$. No primeiro caso, se $a^2 \equiv 2 \pmod p$ temos

$$f(x) \equiv (x^2 + 2ax - 1)(x^2 - 2ax - 1) \pmod p.$$

Já no segundo caso, se $b^2 \equiv 3 \pmod p$ temos

$$f(x) \equiv (x^2 + 2bx + 1)(x^2 - 2bx + 1) \pmod p.$$

Finalmente, no último caso, se $c^2 \equiv 6 \pmod p$ temos

$$f(x) \equiv (x^2 + 2c - 5)(x^2 - 2c - 5) \pmod p.$$

Isto mostra que $f(x)$ é redutível módulo p para todo primo p. ◻

2.2.2 Lei de Reciprocidade Quadrática

O critério de Euler já nos fornece uma maneira de identificar resíduos quadráticos. Entretanto, vamos provar um resultado muito mais forte, que é a famosa

Teorema 2.11 (Reciprocidade Quadrática)**.**

1. *Sejam p e q primos ímpares distintos. Então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

2. *Seja p um primo ímpar. Então*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \textit{se } p \equiv \pm 1 \pmod 8 \\ -1 & \textit{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

Antes de apresentar a prova, vejamos algumas aplicações.

Exemplo 2.12. *Determinar se* -90 *é resíduo quadrático módulo* 1019 *ou não.*

SOLUÇÃO:

$$\begin{aligned}\left(\frac{-90}{1019}\right) &= \left(\frac{-1}{1019}\right)\left(\frac{2}{1019}\right)\left(\frac{3^2}{1019}\right)\left(\frac{5}{1019}\right)\\ &= (-1)\cdot(-1)\cdot 1\cdot\left(\frac{1019}{5}\right)\\ &= \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1.\end{aligned}$$

Ou seja, -90 é resíduo quadrático módulo 1019. □

Exemplo 2.13. *Seja p um número primo. Mostre que*

1. *se p é da forma $4n+1$ então $p \mid n^n - 1$.*

2. *se p é da forma $4n-1$ então $p \mid n^n + (-1)^{n+1}\cdot 2n$.*

SOLUÇÃO: No primeiro item, $4n \equiv -1 \pmod p$, donde elevando a n obtemos

$$(4n)^n = 2^{2n}n^n \equiv (-1)^n \pmod p.$$

Por outro lado, pelo critério de Euler e pela reciprocidade quadrática temos

$$2^{2n} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \equiv (-1)^{n(2n+1)} \equiv (-1)^n \pmod p.$$

Portanto $n^n \equiv 1 \pmod p$, como queríamos demonstrar.

No segundo item, temos $4n \equiv 1 \pmod p$ e assim

$$(4n)^n = 2^{2n}n^n \equiv 1 \pmod p,$$

mas $2^{2n-1} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} = (-1)^{n(2n-1)} \pmod p$, donde $2^{2n} \equiv 2\cdot(-1)^n \pmod p$. Concluímos que $2n^n \equiv (-1)^n \pmod p$ e multiplicando por $2n$ e utilizando $4n \equiv 1 \pmod p$ obtemos $n^n \equiv 2n\cdot(-1)^n \pmod p$, como desejado. □

O primeiro passo da demonstração da lei de reciprocidade quadrática é o seguinte

Lema 2.14 (Gauß)**.** *Sejam $p > 2$ um número primo e a um inteiro positivo primo relativo com p. Seja s o número de elementos do conjunto*

$$\left\{a, 2a, 3a, \ldots, \tfrac{p-1}{2} \cdot a\right\}$$

tais que seu resto módulo p é maior do que $\frac{p-1}{2}$. Então

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Demonstração: A ideia é imitar a prova do teorema de Euler-Fermat. Como o conjunto $\{\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}\}$ é um sistema completo de invertíveis módulo p, para cada $j = 1, 2, \ldots, \frac{p-1}{2}$ podemos escrever $a \cdot j \equiv \epsilon_j m_j \pmod{p}$ com $\epsilon_j \in \{-1, 1\}$ e $m_j \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Temos que se $i \neq j$ então $m_i \neq m_j$ donde $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. De fato, se $m_i = m_j$ temos $a \cdot i \equiv a \cdot j \pmod{p}$ ou $a \cdot i \equiv -a \cdot j \pmod{p}$; como a é invertível módulo p e $0 < i, j \le (p-1)/2$, temos que a primeira possibilidade implica $i = j$ e a segunda é impossível. Assim, multiplicando as congruências $a \cdot j \equiv \epsilon_j m_j \pmod{p}$, obtemos

$$\begin{aligned}
(a \cdot 1)(a \cdot 2) \cdots (a \cdot \tfrac{p-1}{2}) &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} m_1 m_2 \cdots m_{\frac{p-1}{2}} \pmod{p} \\
a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \\
\iff \left(\frac{a}{p}\right) &\equiv \epsilon_1 \epsilon_2 \ldots \epsilon_{\frac{p-1}{2}} \pmod{p},
\end{aligned}$$

donde $(\frac{a}{p}) = \epsilon_1 \epsilon_2 \ldots \epsilon_{\frac{p-1}{2}}$, pois ambos os lados pertencem a $\{-1, 1\}$. Assim, $(\frac{a}{p}) = (-1)^s$ já s é o número de elementos j de $\{1, 2, \ldots, \frac{p-1}{2}\}$ tais que $\epsilon_j = -1$. □

O lema de Gauß já nos permite provar a fórmula para $\left(\frac{2}{p}\right)$. Se $p \equiv 1 \pmod{4}$, digamos $p = 4k+1$, temos $\frac{p-1}{2} = 2k$. Como $1 \le 2j \le \frac{p-1}{2}$ para $j \le k$ e $\frac{p-1}{2} < 2j \le p-1$ para $k+1 \le j \le 2k$, temos

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} 1, & \text{se } p \equiv 1 \pmod{8}, \\ -1, & \text{se } p \equiv 5 \pmod{8}. \end{cases}$$

Se $p \equiv 3 \pmod{4}$, digamos $p = 4k+3$, temos $\frac{p-1}{2} = 2k+1$. Para $1 \le j \le k$ temos $1 \le 2j \le \frac{p-1}{2}$ e para $k+1 \le j \le 2k+1$ temos $\frac{p-1}{2} < 2j \le p-1$, donde

$$\left(\frac{2}{p}\right) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod{8}, \\ 1, & \text{se } p \equiv 7 \pmod{8}. \end{cases}$$

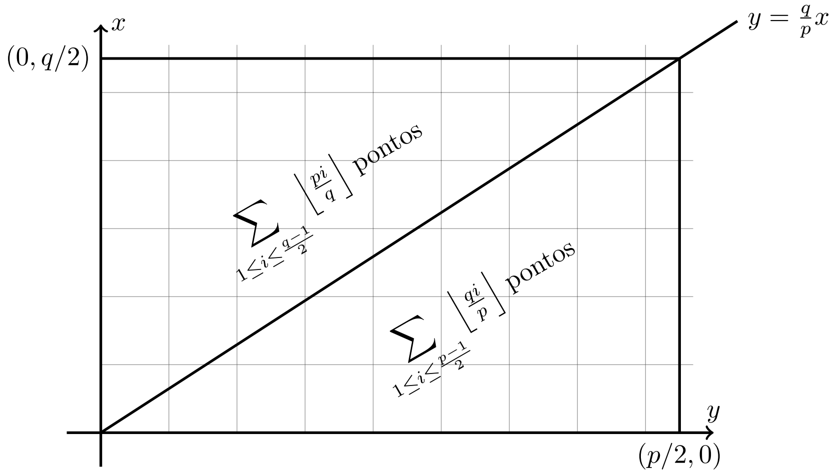
Agora, para provar o item *1* da lei de reciprocidade quadrática, vamos mostrar que

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{1 \le i \le \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{1 \le i \le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \tag{$*$}$$

e que

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{1 \le i \le \frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor} \quad \text{e} \quad \left(\frac{q}{p}\right) = (-1)^{\sum_{1 \le i \le \frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor}. \tag{$**$}$$

A fórmula $(*)$ é apenas uma contagem: o lado esquerdo é o número de pontos com ambas as coordenadas inteiras no interior do retângulo de vértices $(0,0)$, $(p/2, 0)$, $(0, q/2)$ e $(p/2, q/2)$.



Por outro lado, o primeiro somatório do lado direito conta o número de tais pontos que estão acima da diagonal $x = \frac{p}{q}y$ do retângulo, enquanto o segundo somatório conta o número de tais pontos abaixo desta diagonal (note que como p e q são primos, não há pontos com ambas as coordenadas inteiras na diagonal). Por exemplo, no primeiro somatório cada termo $\left\lfloor \frac{ip}{q} \right\rfloor$ representa a quantidade de pontos na reta $y = i$ acima da diagonal $x = \frac{p}{q}y$.

Finalmente, para mostrar $(**)$, basta checar que $\sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2$, onde s é como no lema de Gauß aplicado para $a = q$. Seja r_i o resto da divisão de iq por p, de modo que $iq = \left\lfloor \frac{iq}{p} \right\rfloor p + r_i$. Somando e utilizando a notação da demonstração do lema de Gauß, obtemos

$$q \sum_{1\le i\le \frac{p-1}{2}} i = p \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (p - m_i).$$

Como p e q são ímpares, módulo 2 temos

$$\sum_{1\le i\le \frac{p-1}{2}} i \equiv \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (1 + m_i) \pmod 2,$$

e como $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$, concluímos assim que

$$\sum_{1\le i\le \frac{p-1}{2}} i \equiv \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{1\le i\le \frac{p-1}{2}} i + \sum_{r_i>p/2} 1 \pmod 2$$

$$\iff \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2$$

o que encerra a prova. Para uma outra prova da lei de reciprocidade quadrática, veja a seção **??**.

Observação 2.15. *O símbolo de Legendre* $\left(\frac{a}{p}\right)$ *pode ser estendido para o símbolo de Jacobi* $\left(\frac{a}{n}\right)$, *que está definido para* a *inteiro arbitrário e* n *inteiro positivo ímpar por* $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \ldots \left(\frac{a}{p_k}\right)^{\alpha_k}$ *se* $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *é a fatoração prima de* n *(onde os* $\left(\frac{a}{p_j}\right)$ *são dados pelo símbolo de Legendre usual); temos* $\left(\frac{a}{1}\right) = 1$ *para todo inteiro* a. *Não é difícil provar as seguintes propriedades do símbolo de Jacobi, que podem ser usadas para calcular rapidamente símbolos de Legendre (e de Jacobi):*

1. *Se* $a \equiv b \pmod n$ *então* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

2. $\left(\frac{a}{n}\right) = 0$ *se* $\operatorname{mdc}(a,n) \neq 1$ *e* $\left(\frac{a}{n}\right) \in \{-1, 1\}$ *se* $\operatorname{mdc}(a,n) = 1$.

3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$*; em particular,* $\left(\frac{a^2}{n}\right) \in \{0, 1\}$.

4. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$*; em particular,* $\left(\frac{a}{n^2}\right) \in \{0, 1\}$.

5. *Se* m *e* n *são positivos e ímpares, então* $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right)$.

6. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

7. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Os três últimos fatos, que generalizam a lei de reciprocidade quadrática, podem ser provados usando a multiplicatividade em a *e em* n *do símbolo de Jacobi* $\left(\frac{a}{n}\right)$ *e a lei de reciprocidade quadrática para o símbolo de Legendre.*

Como para o símbolo de Legendre, se $\left(\frac{a}{n}\right) = -1$*,* a *não é resíduo quadrático módulo* n*, mas (diferentemente do que acontece para o símbolo de Legendre) é possível que* $\left(\frac{a}{n}\right)$ *seja igual a* 0 *ou a* 1 *sem que* a *seja resíduo quadrático módulo* n*. Por exemplo,* $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$ *e* $\left(\frac{3}{15}\right) = \left(\frac{3}{3}\right)\left(\frac{3}{5}\right) = 0\cdot(-1) = 0$*, mas* 2 *e* 3 *não são resíduos quadráticos módulo* 15.

Problemas Propostos

2.11. *Calcular* $\left(\frac{44}{103}\right)$, $\left(\frac{-60}{1019}\right)$ *e* $\left(\frac{2010}{1019}\right)$.

2.12. *Determine todas as soluções de* $x^{10} \equiv 1 \pmod{49}$.

2.13. *Sejam* p *um primo ímpar e* c *um inteiro que não é múltiplo de* p*. Prove que*

$$\sum_{a=0}^{p-1}\left(\frac{a(a+c)}{p}\right) = -1.$$

2.14. *Existem inteiros* m *e* n *tais que*

$$5m^2 - 6mn + 7n^2 = 1985\ ?$$

2.15. *Demonstrar que a congruência* $6x^2 + 5x + 1 \equiv 0 \pmod m$ *tem solução para todo valor natural de* m.

2.16. *Demonstrar que existem infinitos primos da forma* $3k + 1$ *e* $3k - 1$.

2.17. *Demonstrar que se* $\operatorname{mdc}(a,b) = 1$ *o número* $a^2 + b^2$ *não pode ter fatores primos da forma* $4k - 1$ *e se além disso* $\operatorname{mdc}(a,3) = 1$ *então o número* $a^2 + 3b^2$ *não pode ter fatores da forma* $3k - 1$*. Que podemos dizer sobre os fatores primos de* $a^2 + pb^2$ *onde* p *é um primo?*

2.18. *Demonstrar que, para* $p = 1093$,

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}.$$

2.19. *a) (Euler) Seja* $F_n = 2^{2^n} + 1$ *o* n*-ésimo número de Fermat. Prove que todo fator primo de* F_n *é da forma* $k\cdot 2^{n+1} + 1$.

b) (Lucas) Prove que, se $n \geq 2$*, então todo fator primo de* F_n *é da forma* $k\cdot 2^{n+2} + 1$.

c) Mostre que $2^{2^5} + 1$ *é composto.*

2.20 (IMO1996). *Sejam a, b inteiros positivos tais que $15a + 16b$ e $16a - 15b$ sejam quadrados perfeitos. Encontrar o menor valor que pode tomar o menor destes quadrados.*

2.21. *Seja p um número primo ímpar. Mostrar que o menor não resto quadrático positivo de p é menor que $\sqrt{p} + 1$.*

2.22. *Sejam M um número inteiro e p um número primo maior do que 25. Mostrar que a sequência $M, M+1, \cdots, M + 3\lfloor\sqrt{p}\rfloor - 1$ contém um resto não quadrático módulo p.*

2.23 (Putnam 1991). *Seja p um primo ímpar. Quantos elementos tem o conjunto*

$$\{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\} \cap \{y^2 + 1 \mid y \in \mathbb{Z}/p\mathbb{Z}\}?$$

2.24 (IMO2008). *Prove que existe um número infinito de inteiros positivos n tais que $n^2 + 1$ tem um divisor primo maior do que $2n + \sqrt{2n}$.*

2.3 Congruências de Grau Superior

Dado um polinômio $f(x) \in \mathbb{Z}[x]$ e um número natural n, vamos estudar condições para que a congruência

$$f(x) \equiv 0 \pmod{n}$$

tenha solução. O primeiro resultado diz que basta considerar o caso em que $n = p^k$ é a potência de um primo p.

Proposição 2.16. *Suponhamos que $n = p_1^{k_1} \cdots p_l^{k_l}$ onde os p_j são primos distintos. Temos uma equivalência*

$$f(x) \equiv 0 \pmod{n} \iff \begin{cases} f(x) & \equiv 0 \pmod{p_1^{k_1}} \\ & \vdots \\ f(x) & \equiv 0 \pmod{p_l^{k_l}} \end{cases}$$

de modo que $f(x) \equiv 0 \pmod{n}$ admite solução se, e somente se, $f(x) \equiv 0 \pmod{p_j^{k_j}}$ tem solução para cada j.

Demonstração: Como as potências $p_j^{k_j}$ são coprimas duas a duas, temos que n divide um inteiro M se, e só se, $p_j^{k_j} \mid M$ para cada j, o que demonstra a equivalência. Assim, a existência de solução para $f(x) \equiv 0 \pmod{n}$ implica a existência de solução para o sistema acima. Reciprocamente, se cada $f(x) \equiv 0 \pmod{p_j^{k_j}}$ tem uma solução $x \equiv a_j \pmod{p_j^{k_j}}$, pelo teorema chinês dos restos existe a tal que $a \equiv a_j \pmod{p_j^{k_j}}$ para todo j, de modo que $f(a) \equiv f(a_j) \equiv 0 \pmod{p_j^{k_j}}$ para todo j e logo $f(a) \equiv 0 \pmod{n}$ pela equivalência acima. Note em particular que o número de soluções distintas módulo n de $f(x) \equiv 0 \pmod{n}$ é igual ao produto do número de soluções módulo $p_j^{k_j}$ de $f(x) \equiv 0 \pmod{p_j^{k_j}}$. □

A próxima proposição indica como, a partir de uma solução de $f(x) \equiv 0 \pmod{p^{k_0}}$, obter soluções para $f(x) \equiv 0 \pmod{p^k}$ para todo $k \geq k_0$.

Proposição 2.17 (Lema de Hensel). *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio, p um número primo. Seja $a \in \mathbb{Z}$ tal que $f(a) \equiv 0 \pmod{p^{k_0}}$ e cuja maior potência p^{l_0} de p com*

$p^{l_0} \mid f'(a)$ *satisfaz* $0 \le 2l_0 < k_0$. *Então existe uma sequência de inteiros* $(a_k)_{k \ge k_0}$ *com*

$$\begin{aligned} &a_{k_0} = a, \quad a_{k+1} \equiv a_k \pmod{p^{k-l_0}} \qquad \textit{e} \\ &f(a_k) \equiv 0 \pmod{p^k} \ \textit{para todo}\ k \ge k_0. \end{aligned}$$

Em particular, se existe um inteiro a *tal que* $f(a) \equiv 0 \pmod p$ *mas* $f'(a) \not\equiv 0 \pmod p$ *então* $f(x) \equiv 0 \pmod{p^k}$ *admite solução para todo* $k \in \mathbb{N}$.

DEMONSTRAÇÃO: Construímos a sequência indutivamente. Seja $k \ge k_0$ e suponha por indução que $p^k \mid f(a_k)$, ou seja, $f(a_k) = r_k p^k$ para um certo $r_k \in \mathbb{Z}$ e $p^{l_0} \mid f'(a_k)$ mas $p^{l_0+1} \nmid f'(a_k)$, ou seja, $f'(a_k) = s_k p^{l_0}$ onde $p \nmid s_k$. Estamos procurando um número da forma $a_{k+1} = a_k + t_k p^{k-l_0}$, com $t_k \in \mathbb{Z}$, que satisfaz $p^{k+1} \mid f(a_{k+1})$, $p^{l_0} \mid f'(a_{k+1})$ mas $p^{l_0+1} \nmid f'(a_{k+1})$. Vamos utilizar a expansão em série de Taylor $f(x+t) = \sum_{0 \le j \le m} \frac{f^{(j)}(x)}{j!} t^j$, onde m é o grau de $f(x)$; note que a partir da expressão $\frac{1}{j!}\frac{d^j}{(dx)^j}(x^n) = \binom{n}{j} x^{n-j}$ temos que $\frac{f^{(j)}(x)}{j!}$ é um polinômio com coeficientes inteiros. Como a hipótese $0 \le 2l_0 < k_0$ implica $2(k - l_0) \ge k+1$, temos

$$\begin{aligned} f(a_{k+1}) &= f(a_k) + f'(a_k) t_k p^{k-l_0} + \sum_{2 \le j \le m} \frac{f^{(j)}(a_k)}{j!} (t_k p^{k-l_0})^j \\ &\equiv r_k p^k + s_k t_k p^k \pmod{p^{k+1}}. \end{aligned}$$

Logo para que $p^{k+1} \mid f(a_{k+1})$ devemos encontrar t_k tal que $r_k + s_k t_k \equiv 0 \pmod p$, o que é possível pois s_k é invertível módulo p. Finalmente, temos que

$$\begin{aligned} &f'(a_{k+1}) \equiv f'(a_k) = s_k p^{l_0} \pmod{p^{k-l_0}} \\ \Longrightarrow &\begin{cases} f'(a_{k+1}) & \equiv 0 \pmod{p^{l_0}} \\ f'(a_{k+1}) & \not\equiv 0 \pmod{p^{l_0+1}} \end{cases} \end{aligned}$$

o que completa a indução. □

Observemos que a condição sobre a derivada de f no lema de Hensel é necessária. Para isto, consideremos $f(x) = x^m + 3$ com $m \ge 2$, $a = 0$ e $p = 3$. Assim, temos que $f(0) = 3 \equiv 0 \pmod 3$, mas $f'(0) = 0$ é divisível por potências arbitrariamente grandes de 3, logo $f(x)$ não satisfaz a segunda hipótese da proposição. E de fato, se $b \in \mathbb{Z}$ e $f(b) = b^m + 3 \equiv 0 \pmod 3$ então $b \equiv 0 \pmod 3$, donde $b^m \equiv 0 \pmod 9$ e $f(b) = b^m + 3 \equiv 3 \pmod 9$, o que mostra que nenhuma raiz módulo 3 "levanta" para uma raiz módulo 9.

Agora vamos nos concentrar em equações módulo p. Para o próximo resultado, necessitamos de um

Lema 2.18. *Seja* p *um primo. Então*

$$1^k + 2^k + \cdots + (p-1)^k \bmod p = \begin{cases} 0 & \textit{se}\ (p-1) \nmid k, \\ p-1 & \textit{se}\ (p-1) \mid k. \end{cases}$$

DEMONSTRAÇÃO: Se $(p-1) \mid k$, temos que cada termo da soma acima é congruente a 1 módulo p e o resultado segue. Suponha agora que $(p-1) \nmid k$ e seja g uma raiz primitiva módulo p. Temos portanto

$$1^k + 2^k + \cdots + (p-1)^k \equiv 1 + g^k + g^{2k} + \cdots + g^{(p-2)k} \pmod p$$

Sendo $S = 1 + g^k + g^{2k} + \cdots + g^{(p-2)k}$, multiplicando por g^k e observando que $g^{(p-1)k} \equiv 1 \pmod p$ temos

$$g^k S \equiv g^k + g^{2k} + \cdots + g^{(p-1)k} \pmod p$$
$$\iff g^k S \equiv S \pmod p \iff (g^k - 1)S \equiv 0 \pmod p$$

Como g é uma raiz primitiva e $(p-1) \nmid k$ temos que $g^k - 1 \not\equiv 0 \pmod p$, ou seja, $g^k - 1$ é invertível módulo p e portanto $S \equiv 0 \pmod p$, o que encerra a prova. □

Teorema 2.19 (Chevalley-Warning)**.** *Seja p um primo e sejam*

$$f_1(x_1,\dots,x_n),\dots,f_k(x_1,\dots,x_n) \in \mathbb{Z}[x_1,\dots,x_n]$$

polinômios em n variáveis com coeficientes inteiros tais que $f_i(0,\dots,0) \equiv 0 \pmod p$ para todo $i \le k$. Suponha que $\sum\limits_{1\le i\le k} \deg(f_i) < n$. Então a quantidade de "pontos" em

$$A = \{(x_1,\dots,x_n) \in (\mathbb{Z}/p\mathbb{Z})^n \mid f_i(x_1,\dots,x_n) = \overline{0} \quad \forall i = 1,\dots,k\}$$

é um múltiplo de p. Em particular, existem pontos $(x_1,\dots,x_n) \neq (\overline{0},\dots,\overline{0})$ em $(\mathbb{Z}/p\mathbb{Z})^n$ tais que $f_i(x_1,\dots,x_n) = \overline{0}$ para todo i.

Demonstração: Usaremos o lema anterior para determinar $|A| \bmod p$. Para isso, notemos que pelo teorema de Euler-Fermat $f_j(x_1,\dots,x_n) \not\equiv 0 \pmod p \iff f_j(x_1,\dots,x_n)^{p-1} \equiv 1 \pmod p$. Definamos

$$g(x_1,\dots,x_n) = \prod_{1\le j\le k} \bigl(1 - f_j(x_1,\dots,x_n)^{p-1}\bigr).$$

Observemos que $g(x_1,\dots,x_n) \equiv 0 \pmod p$ se, e somente se, existe j tal que $f_j(x_1,\dots,x_n) \not\equiv 0 \pmod p$. Por outro lado, se $f_j(x_1,\dots,x_n) \equiv 0 \pmod p$ para todo j então $g(x_1,\dots,x_n) \equiv 1 \pmod p$, portanto

$$\sum_{(x_1,\dots,x_n)\in(\mathbb{Z}/p\mathbb{Z})^n} g(x_1,\dots,x_n) \equiv |A| \pmod p.$$

Notemos agora que $\deg(g) \le \sum_{1\le j\le k}(p-1)\deg(f_j) < (p-1)n$. Portanto cada monômio $cx_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ de g é tal que $\sum_{1\le j\le n} i_j < (p-1)n$, donde pelo Princípio da Casa dos Pombos sempre existe algum r com $0 \le i_r < p-1$. Assim, pelo lema anterior, $\sum_{x_r\in\mathbb{Z}/p\mathbb{Z}} x_r^{i_r} \equiv 0 \pmod p$ donde

$$\begin{aligned}\sum_{(x_1,\dots,x_n)\in(\mathbb{Z}/p\mathbb{Z})^n} cx_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} &\equiv c\sum_{x_1\in\mathbb{Z}/p\mathbb{Z}} x_1^{i_1}\sum_{x_2\in\mathbb{Z}/p\mathbb{Z}} x_2^{i_2}\cdots\sum_{x_n\in\mathbb{Z}/p\mathbb{Z}} x_n^{i_n}\\ &\equiv 0 \pmod p\end{aligned}$$

Isso mostra que $\sum_{(x_1,\dots,x_n)\in(\mathbb{Z}/p\mathbb{Z})^n} g(x_1,\dots,x_n) \equiv 0 \pmod p$ e, portanto, $|A|$ é múltiplo de p. Como $(\overline{0},\overline{0},\dots,\overline{0}) \in A$, há pelo menos $p-1$ outros pontos nesse conjunto, o que prova o teorema.

□

Como aplicação, provemos o seguinte resultado, devido a Erdős, Ginzburg e Ziv.

Proposição 2.20. *Seja n um inteiro positivo. Dados inteiros $x_1,\dots,x_{2n-1}$ existem $1 \le i_1 < i_2 < \cdots < i_n \le 2n-1$ tais que $x_{i_1} + x_{i_2} + \cdots + x_{i_n}$ é divisível por n.*

Demonstração: Mostremos primeiro que se o resultado vale para m e para n então vale para mn. Sejam $x_1, x_2, \dots, x_{2mn-1} \in \mathbb{Z}$. Por hipótese temos que, para cada subconjunto A de $\{1, 2, \dots, 2mn-1\}$ com $2n-1$ elementos, existe um subconjunto $B \subset A$ com n elementos tal que $\sum_{i \in B} x_i$ é divisível por n. Assim, construímos B_j indutivamente para todo $1 \le j \le 2m-1$, seguindo os seguintes passos

- Escolhemos um subconjunto A_j de $\{1, 2, \dots, 2mn-1\} \setminus \bigcup\limits_{k<j} B_k$ com $2n-1$ elementos.
- De A_j escolhemos um subconjunto B_j com n elementos tal que $\sum_{i \in B_j} x_i$ é divisível por n.

Observemos que se $j \le 2m-1$ então

$$\begin{aligned}\Big|\{1, 2, \dots, 2mn-1\} \setminus \bigcup_{k<j} B_j\Big| &= 2mn - 1 - (j-1)n \\ &\ge 2mn - 1 - (2m-2)n = 2n - 1,\end{aligned}$$

o que garante a construção até $j = 2m-1$. Definamos agora os inteiros $y_j = \frac{1}{n}\sum_{i \in B_j} x_i$ para $1 \le j \le 2m-1$. De novo por hipótese, existe um subconjunto de índices $C \subset \{1, \dots, 2m-1\}$ com m elementos tal que $\sum_{j \in C} y_j$ é divisível por m e portanto

$$\sum_{j \in C} \sum_{i \in B_j} x_i = n \sum_{j \in C} y_j$$

é uma soma com $|C||B_j| = mn$ somandos que é divisível por mn.

Assim, basta provar a proposição para n primo. Para isso, consideremos os polinômios

$$\begin{aligned} f_1(x_1, \dots, x_{2n-1}) &= x_1^{n-1} + x_2^{n-1} + \cdots + x_{2n-1}^{n-1} \qquad \text{e} \\ f_2(x_1, \dots, x_{2n-1}) &= a_1 x_1^{n-1} + a_2 x_2^{n-1} + \cdots + a_{2n-1} x_{2n-1}^{n-1} \end{aligned}$$

onde $a_1, \dots, a_{2n-1}$ são os inteiros dados. A soma dos graus de f_1 e f_2 é $2(n-1) < 2n-1$. Pelo teorema de Chevalley-Warning, existem $x_1, \dots, x_{2n-1} \in \mathbb{Z}/(n)$ não todos nulos com

$$f_1(x_1, \dots, x_{2n-1}) \equiv f_2(x_1, \dots, x_{2n-1}) \equiv 0 \pmod{n}.$$

Como $x^{n-1} \equiv 1 \pmod{n}$ para todo $x \in (\mathbb{Z}/(n))^\times$, $f_1(x_1, \dots, x_{2n-1}) \equiv 0 \pmod{n}$ implica que existem exatamente n valores $i \le 2n-1$ com $x_i \not\equiv 0 \pmod{n}$. Sejam $1 \le i_1 < i_2 < \cdots < i_n \le 2n-1$ tais valores de i, como $x_{i_s}^{n-1} \equiv 1 \pmod{n}$ para todo $s \le n$ temos que

$$a_1 x_1^{n-1} + a_2 x_2^{n-1} + \cdots + a_{2n-1} x_{2n-1}^{n-1} \equiv a_{i_1} + a_{i_2} + \cdots + a_{i_n} \pmod{n},$$

pois $x_j \equiv 0 \pmod{n}$ se $j \ne i_s$ para todo $s \le n$. Assim, $a_{i_1} + a_{i_2} + \cdots + a_{i_n}$ é divisível por n, o que prova o resultado. □

Problemas Propostos

2.25 (OBM2007). *Para quantos inteiros c, $-2007 \le c \le 2007$, existe um inteiro x tal que $x^2 + c$ é múltiplo de 2^{2007}?*

2.26. *Seja p um primo e seja n tal que $p^k \nmid n$. Demonstrar: se a equação $y^n \equiv a \pmod{p^k}$ tem solução com $\operatorname{mdc}(y,p)=1$, então para todo $m > k$ a equação $y^n \equiv a \pmod{p^m}$ possui solução. Seja y_0 solução de $y^n \equiv a \pmod{p^k}$, com $\operatorname{mdc}(y_0,p)=1$ e g raiz primitivo modulo p^m se $p>2$, e $g=5$ se $p=2$. Logo existe $b_0 \in \mathbb{N}$ tal que*

$$g^b y_0^n \equiv a \pmod{p^m}, \text{ para todo } b = b_0 + tp^{m-1}(p-1),\ t \in \mathbb{Z}.$$

Segue se que $g^{b_0} \equiv 1 \pmod{p^k}$ e $b_0 = \varphi(p^k) b_1$, assim

$$b_0 + tp^{m-1}(p-1) = p^{k-1}(p-1)(b_1 + tp^{m-k}).$$

como $n = p^l n_1$ com $l < k$ e $\operatorname{mdc}(n_1,p)=1$, então existe um número natural t_0 tal que $n_1 \mid b_1 + t_0 p^{m-k}$, e portanto

$$y = g^{p^{k-1-l}(p-1)\frac{b_1+t_0p^{m-k}}{n_1}} y_0$$

é a solução procurada.

2.27. *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio, p um número primo, a um inteiro tal que $f(a) \equiv 0 \pmod p$ mas $f'(a) \not\equiv 0 \pmod p$ e k um inteiro positivo. Prove que, se a_k é um inteiro tal que $a_k \equiv a \pmod p$ e $f(a_k) \equiv 0 \pmod{p^k}$, então, tomando b tal que $b \equiv a_k - f(a_k)\cdot f'(a_k)^{-1} \pmod{p^{2k}}$, então $f(b) \equiv 0 \pmod{p^{2k}}$.*

2.28. *Seja p um primo ímpar, a um inteiro e n um inteiro positivo. Sejam α e β inteiros não negativos, com $\alpha > 0$. Prove:*

(a) Se p^β e p^α são as maiores potências de p que dividem n e $a-1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência de p que divide $a^n - 1$ (atenção, p deve dividir $a-1$ pois $\alpha > 0$! Mas note que p não precisa dividir n)

(b) Se n é ímpar e p^β e p^α são as maiores potências de p que dividem n e $a+1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência de p que divide a^n+1 (mesma ressalva do item (i)).

2.29. *Encontre todos os inteiros não negativos x e y tais que*

$$7^y - 2\cdot 3^x = 1$$

2.30. *Encontre todas as ternas (a,m,n) de inteiros positivos tais que a^m+1 divide $(a+1)^n$.*

2.31. *Seja p um número primo e n, k e $a = p^t a_1$ números naturais tais que $\operatorname{mdc}(p,a_1)=1$. Prove: a congruência $x^n \equiv a \pmod{p^k}$ tem solução se, e só se, $k \le t$ ou*

$$k > t, \quad n \mid t \quad e \quad a_1^{\frac{p^{k-1}(p-1)}{\operatorname{mdc}(n,p^{k-1}(p-1))}} \equiv 1 \pmod{p^{k-t}}.$$

Claramente se $k \le t$, então $x = p^r$ com $rn > k$ é solução, assim podemos supor que $k > t$. Suponhamos que $t = sn + r$ com $0 \le r < t$. Como x^n tem que ser divisível por p^k logo $p^r \mid x^n$ portanto $x = a^{s+j} y$ com $j \ge 0$. Mas se $j > 0$ então $x^n - a = p^t(p^{jn-r}y - a_1)$ não é divisível por p^k, portanto $j = 0$ e $r = 0$, segue que $t = sn$. Assim o problema se transforma em determinar as soluções da congruência

$$y^n = a_1 \pmod{p^{k-t}}$$

Elevando esta equação $\frac{\varphi(p^{k-t})}{(n,\varphi(p^{k-t}))}$ obtemos como condição necessária que

$$a_1^{\frac{\varphi(p^{k-t})}{(n,\varphi(p^{k-t}))}} \equiv 1 \pmod{p^{k-t}}$$

2.32 (Irlanda 1997). *Seja A um subconjunto de $\{1, 2, \ldots 2n-1\}$ com n elementos. Prove que A contém uma potência de 2 ou dois elementos distintos cuja soma é uma potência de 2.*

2.33 (Romênia 1996). *Determinar o maior inteiro positivo n com a seguinte propriedade: existem inteiros não negativos $x_1, \ldots, x_n$ tais que, para toda sequência $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ de elementos de $\{-1, 0, 1\}$, não todos zero, o número*

$$\epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_n x_n$$

não é divisível por n^3.

2.34 (Erdős). *Mostrar que todo número inteiro positivo pode ser expresso como soma de números da forma $2^a 3^b$ de modo que nenhum termo é divisível por outro.*

2.35 (Romênia 1998). *Mostrar que para todo $n \geq 2$ existe um subconjunto S de $\{1, 2, \ldots, n\}$ com no máximo $2\lfloor\sqrt{n}\rfloor + 1$ elementos tal que todo número natural menor do que n pode ser representado como diferença de dois elementos de S.*

2.36 (IMO2007). *Seja n um inteiro positivo. Considere*

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\}, \quad x + y + z > 0\}$$

como um conjunto de $(n+1)^3 - 1$ pontos no espaço tridimensional. Determine o menor número de planos, a união dos quais contém S mas não inclui $(0, 0, 0)$.

Capítulo 3

Funções Aritméticas

Neste capítulo estudaremos o comportamento assintótico de algumas das mais importantes funções aritméticas, muitas delas já introduzidas em capítulos anteriores. Frequentemente resultados mais precisos sobre o crescimento dessas funções dependem de estimativas precisas sobre números primos, algumas das quais desenvolveremos neste capítulo, que é fortemente inspirado nos capítulos XVIII e XXII de [8].

Notação: dadas duas funções $f\colon \mathbb{N} \to \mathbb{R}$ e $g\colon \mathbb{N} \to (0, +\infty)$, escrevemos

$$\begin{aligned} f = o(g) &\text{ se } \lim_{n\to\infty} \frac{f(n)}{g(n)} = 0 \text{ e} \\ f = O(g) &\text{ se existe } C > 0 \text{ com } |f(n)| < Cg(n) \text{ para } n \gg 0. \end{aligned}$$

Em todo o livro, a menos que se afirme o contrário, log denota o logaritmo natural. Neste capítulo, divisor de um número natural significará divisor positivo.

3.1 Funções Multiplicativas

Uma função f definida sobre $\mathbb{N}_{>0}$ é dita *multiplicativa* se dados dois números naturais a e b tais que $\mathrm{mdc}(a, b) = 1$ então $f(ab) = f(a)f(b)$, e *totalmente multiplicativa* se $f(ab) = f(a)f(b)$ para todo a e b. Vejamos algumas funções multiplicativas importantes.

Proposição 3.1. *Seja n um número inteiro positivo e k um real qualquer. As funções*

$$\sigma_k(n) \stackrel{\text{def}}{=} \sum_{d|n} d^k \qquad e \qquad \varphi(n) = \text{função } \varphi \text{ de Euler}$$

são multiplicativas. Em particular, as funções

$$\begin{aligned} d(n) &\stackrel{\text{def}}{=} \sigma_0(n) &=& \text{ número de divisores de } n \\ \sigma(n) &\stackrel{\text{def}}{=} \sigma_1(n) &=& \text{ soma dos divisores de } n \end{aligned}$$

são multiplicativas.

Demonstração: Já vimos na seção 1.7 que φ é multiplicativa. Por outro lado, pela proposição 1.21, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ é a fatoração canônica de n em primos então temos uma fórmula explícita

$$\sigma_k(n) = \frac{p_1^{(\alpha_1+1)k} - 1}{p_1^k - 1} \cdot \ldots \cdot \frac{p_m^{(\alpha_m+1)k} - 1}{p_m^k - 1},$$

donde é fácil provar que σ_k é multiplicativa. □

Uma função totalmente multiplicativa f fica completamente determinada por seus valores nos números primos. Impondo algumas restrições adicionais, temos o seguinte resultado

Teorema 3.2. *Seja $f\colon \mathbb{N}_{>0} \to \mathbb{R}_{>0}$ uma função totalmente multiplicativa e monótona, então existe $\alpha \in \mathbb{R}$ tal que $f(n) = n^\alpha$.*

Demonstração: Trocando f por $1/f$, podemos supor sem perda de generalidade que f é estritamente crescente, e definamos $\alpha = \log_2 f(2)$. Vejamos que $f(n) = n^\alpha$. Para isto observemos que, aplicando f, para todo $m \in \mathbb{N}_{>0}$ temos

$$\begin{aligned} & 2^{\lfloor m \log_2 n \rfloor} \le n^m < 2^{\lfloor m \log_2 n \rfloor + 1} \\ \Longrightarrow\ & 2^{\alpha \lfloor m \log_2 n \rfloor} \le (f(n))^m < 2^{\alpha(\lfloor m \log_2 n \rfloor + 1)} \end{aligned}$$

Assim,

$$2^{\frac{\alpha \lfloor m \log_2 n \rfloor}{m}} \le f(n) < 2^{\frac{\alpha(\lfloor m \log_2 n \rfloor + 1)}{m}} \quad \text{para todo } m \in \mathbb{N}_{>0}.$$

Mas

$$\lim_{m\to\infty} \frac{\alpha \lfloor m \log_2 n \rfloor}{m} = \lim_{m\to\infty} \frac{\alpha(\lfloor m \log_2 n \rfloor + 1)}{m} = \alpha \log_2 n,$$

donde concluímos que $f(n) = 2^{\alpha \log_2 n} = n^\alpha$. □

Para uma extensão desse resultado para funções multiplicativas veja o exercício 3.18

Exemplo 3.3. *Encontrar condições necessárias e suficientes sobre m e n para que $n\varphi(m) = m\varphi(n)$.*

Solução: Se $n\varphi(m) = m\varphi(n)$ então

$$n\varphi(m) = mn \prod_{\substack{p|m \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right) = mn \prod_{\substack{q|n \\ q \text{ primo}}} \left(1 - \frac{1}{q}\right) = m\varphi(n).$$

Daí temos que n e m devem ter os mesmos divisores primos; caso contrário, consideremos $\{p_i\}$ e $\{q_j\}$ os fatores primos de n e m respectivamente que não são comuns aos dois números, então

$$\prod(p_i - 1)\prod q_j = \prod(q_j - 1)\prod p_i.$$

Mas, como $p_i \nmid q_j$ e $q_j \nmid p_i$ para todos os fatores primos, concluímos que

$$\prod p_i \,\Big|\, \prod(p_i - 1) \qquad \text{e} \qquad \prod q_j \,\Big|\, \prod(q_j - 1),$$

o que é impossível. Agora, se n e m tem os mesmos fatores primos prova-se diretamente da fórmula acima que $n\varphi(m) = m\varphi(n)$.

□

O seguinte teorema nos mostra uma forma de construir funções multiplicativas.

Teorema 3.4. *Se f é uma função multiplicativa então a função*

$$F(n) = \sum_{d|n} f(d)$$

é também multiplicativa.

Demonstração: Sejam a e b inteiros tais que $\text{mdc}(a, b) = 1$ então

$$\begin{aligned} F(ab) &= \sum_{d|ab} f(d) = \sum_{d_1|a, d_2|b} f(d_1 d_2) = \sum_{d_1|a, d_2|b} f(d_1) f(d_2) \\ &= \sum_{d_1|a}\sum_{d_2|b} f(d_1) f(d_2) = \sum_{d_1|a} f(d_1) \sum_{d_2|b} f(d_2) \\ &= F(a)F(b). \end{aligned}$$

Segue que F também é multiplicativa. □

Com o resultado anterior obtemos outro método para demonstrar que $\sigma_k(n)$ é multiplicativa, já que $f(n) = n^k$ é claramente uma função multiplicativa.

Exemplo 3.5. *Demonstrar que $\varphi(n)d(n) \geq n$.*

Solução: Se $\alpha \geq \beta \geq 0$ então para qualquer primo p temos $\varphi(p^\alpha) \geq \varphi(p^\beta)$, logo como φ é multiplicativa temos que $\varphi(n) \geq \varphi(d)$ para todo divisor d de n. Então, pelo lema 1.77,

$$\varphi(n)d(n) = \sum_{d|n} \varphi(n) \geq \sum_{d|n} \varphi(d) = n,$$

como queríamos demonstrar. Note que a igualdade só se obtém quando $n = 1$ ou $n = 2$. □

Exemplo 3.6. *Encontrar todos os inteiros n para os quais $\varphi(n) = d(n)$.*

Solução: Se $p \geq 3$ é um primo, temos que

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1} \geq 2(1+2)^{\alpha-1} \geq 2\big(1 + 2(\alpha - 1)\big) \geq \alpha + 1 = d(p^\alpha),$$

onde a igualdade só se dá quando $p = 3$ e $\alpha = 1$. Portanto, pela multiplicatividade das funções $\varphi(n)$ e $d(n)$, os únicos ímpares que satisfazem $\varphi(n) = d(n)$ são $n = 1$ e

$n = 3$. Por outro lado, se $\alpha > 3$ temos $\varphi(2^\alpha) = 2^{\alpha-1} > \alpha + 1 = d(2^\alpha)$; para $\alpha = 3$ obtemos as soluções $n = 1 \cdot 8 = 8$ e $n = 3 \cdot 8 = 24$.

Assim, só nos falta resolver os casos $\varphi(2n) = d(2n) \iff \varphi(n) = 2d(n)$ e $\varphi(4n) = d(4n) \iff 2\varphi(n) = 3d(n)$ onde n é ímpar. Temos $\varphi(5) = 4 = 2d(5)$, $\varphi(15) = 8 = 2d(15)$ e $\varphi(9) = 6 = 2d(9)$, donde $2 \cdot 5 = 10$, $2 \cdot 9 = 18$ e $2 \cdot 15 = 30$ também são soluções da equação inicial. Demonstremos agora que não existem mais soluções. Se $n = p^\alpha$ é potência de um primo ímpar p então para $p = 3$ e $\alpha \geq 3$, ou para para $p = 5$ e $\alpha \geq 2$, ou para $p \geq 7$, temos como acima que

$$\varphi(n) = p^{\alpha-1}(p-1) > 2\alpha + 2 = 2d(n) > \frac{3}{2}d(n).$$

Por outro lado, já sabemos que $\varphi(n) \geq d(n)$ para todo n ímpar. Assim, da multiplicatividade das funções $\varphi(n)$ e $d(n)$, obtemos que se n é divisível por 3^3, 5^2 ou por algum primo $p \geq 7$, então $\varphi(n) > 2d(n) > \frac{3}{2}d(n)$ e analisando os casos restantes obtemos apenas as soluções apresentadas anteriormente.

Em conclusão, as únicas soluções de $\varphi(n) = d(n)$ são 1, 3, 8, 10, 18, 24, 30. $\square$

O seguinte teorema relaciona a função $d(n)$ com a função $\lfloor x \rfloor$.

Teorema 3.7. *Seja n um inteiro positivo, então*

$$\sum_{k=1}^{2n} d(k) - \sum_{k=1}^{n} \left\lfloor \frac{2n}{k} \right\rfloor = n.$$

Demonstração: Seja

$$f(i) \stackrel{\text{def}}{=} \sum_{1 \leq k \leq i} \left\lfloor \frac{2i}{k} \right\rfloor.$$

Observemos que para $i, k > 1$

$$\left\lfloor \frac{2i}{k} \right\rfloor - \left\lfloor \frac{2i-2}{k} \right\rfloor = \begin{cases} 1 & \text{se } k \mid 2i \text{ ou } k \mid 2i-1 \\ 0 & \text{caso contrário.} \end{cases}$$

Portanto para $i \geq 2$ temos

$$\begin{aligned} f(i) - f(i-1) &= \lfloor 2i \rfloor - \lfloor 2i-2 \rfloor + \sum_{2 \leq k \leq i} \left(\left\lfloor \frac{2i}{k} \right\rfloor - \left\lfloor \frac{2i-2}{k} \right\rfloor \right) + \left\lfloor \frac{2i-2}{i} \right\rfloor \\ &= 2 + (d(2i) - 2) + (d(2i-1) - 2) + 1 \\ &= d(2i) + d(2i-1) - 1, \end{aligned}$$

donde

$$\begin{aligned} \sum_{k=1}^{2n} d(k) &= d(2) + d(1) + \sum_{i=2}^{n} \big(f(i) - f(i-1) + 1\big) \\ &= 3 + f(n) - f(1) + n - 1 \\ &= f(n) + n \end{aligned}$$

que era o que queríamos demonstrar. $\square$

3.2 Função de Möbius e Fórmula de Inversão

Definimos a *função de Möbius* $\mu\colon \mathbb{N}_{>0} \to \mathbb{Z}$ por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } a^2 \mid n \text{ para algum } a > 1 \\ (-1)^k & \text{se } n \text{ é produto de } k \text{ primos distintos.} \end{cases}$$

Facilmente se comprova que a função de Möbius é multiplicativa. Além disso

Lema 3.8. *Para todo inteiro positivo n temos*

$$\sum_{d\mid n} \mu(d) = \begin{cases} 1 & \textit{se } n = 1 \\ 0 & \textit{se } n > 1. \end{cases}$$

Demonstração: No caso $n = 1$ não temos nada para provar. Como a função $\sum_{d\mid n} \mu(d)$ é multiplicativa pelo teorema 3.4, basta mostra o lema para $n = p^k$ onde p é um número primo. De fato,

$$\sum_{d\mid p^k} \mu(d) = \sum_{j=0}^{k} \mu(p^j) = 1 - 1 = 0$$

como queríamos demonstrar. $\square$

Teorema 3.9 (Fórmula de inversão de Möbius)**.** *Seja $f(n)$ uma função sobre os inteiros positivos e $F(n) = \sum_{d\mid n} f(d)$, então para todo n inteiro positivo,*

$$f(n) = \sum_{d\mid n} \mu(d) F\left(\frac{n}{d}\right).$$

Demonstração: Vejamos que

$$\begin{aligned}
\sum_{d\mid n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d\mid n} \mu(d) \sum_{d_1 \mid \frac{n}{d}} f(d_1) \\
&= \sum_{d\mid n} \sum_{d_1 \mid \frac{n}{d}} \mu(d) f(d_1) \\
&= \sum_{d_1\mid n} \sum_{d \mid \frac{n}{d_1}} \mu(d) f(d_1) \\
&= \sum_{d_1\mid n} f(d_1) \sum_{d \mid \frac{n}{d_1}} \mu(d) = f(n)\mu(1) = f(n),
\end{aligned}$$

como queríamos demonstrar. $\square$

Exemplo 3.10. *Uma pulseira é formada por pedras coloridas, de mesmo tamanho, pregadas em volta de um círculo de modo a ficarem igualmente espaçadas. Duas pulseiras são consideradas iguais se, e só se, suas configurações de pedras coincidem por uma rotação. Se há pedras disponíveis de $k \geq 1$ cores distintas, mostre que o número de pulseiras diferentes possíveis com n pedras é dado pela expressão*

$$\frac{1}{n} \sum_{d\mid n} \varphi(d) \cdot k^{n/d}.$$

Solução: No que segue o número k de cores de pedras estará sempre fixo. A cada pulseira podemos associar um *período*, que é definido como o menor divisor positivo d de n tal que a sequência das n pedras da pulseira é obtida a partir de uma sequência de d pedras repetida n/d vezes. Se o problema fosse contar pulseiras fixas, sem indentificar pulseiras que coincidem por uma rotação, a resposta seria claramente k^n. Ao considerarmos as n rotações de uma pulseira de período d, obtemos d pulseiras fixas distintas (i.e., distintas como pulseiras fixas, mas iguais a menos de rotação). Dizemos que uma pulseira com n pedras é *primitiva* se seu período é n. Se denotarmos por $g(n)$ o número de pulseiras primitivas com n pedras, temos que, para cada divisor d de n, o número de pulseiras com n pedras e período d é $g(d)$ (se o período é d, podemos tomar d pedras consecutivas e unir as pontas criando uma pulseira com d pedras, que será primitiva), e elas dão origem a $d.g(d)$ pulseiras fixas. Assim, temos, para todo inteiro positivo n, $\sum_{d|n} d.g(d) = k^n$, donde, pelo teorema anterior, $n.g(n) = \sum_{d|n} \mu(d)k^{n/d}$.

O número de pulseiras que queremos contar, como no enunciado, é

$$\sum_{d|n} g(d) = \sum_{d|n} \frac{1}{d} \sum_{s|d} \mu(s)k^{d/s}.$$

Fazendo $t = d/s$ na última expressão, temos $d = st$, e $d \mid n$ equivale a $s \mid n/t$. Assim, podemos escrever a última expressão como

$$\sum_{t|n} \sum_{s|n/t} \frac{1}{st}\mu(s)k^t = \sum_{t|n} \frac{k^t}{t} \sum_{s|n/t} \frac{\mu(s)}{s},$$

que, pelo exemplo anterior, é igual a $\sum_{t|n} \frac{k^t}{t} \cdot \frac{t}{n}\varphi(n/t) = \sum_{t|n} \frac{k^t}{n} \cdot \varphi(n/t)$, que, por sua vez (fazendo $r = n/t$), é igual a $\frac{1}{n} \sum_{r|n} \varphi(r) \cdot k^{n/r}$. □

Agora, observemos que para todo número natural m, f e F definidas como antes,

$$\sum_{n=1}^{m} F(n) = \sum_{n=1}^{m} \sum_{d|n} f(d) = \sum_{d=1}^{m} \sum_{\substack{d|n \\ 1\le n\le m}} f(d)$$

Como $f(d)$ é somado $\left\lfloor \frac{m}{d} \right\rfloor$ vezes, então

$$\sum_{n=1}^{m} F(n) = \sum_{d=1}^{m} f(d) \left\lfloor \frac{m}{d} \right\rfloor.$$

No caso particular em que $f(n) = \varphi(n)$ temos que $F(n) = n$ pelo lema 1.77 e assim

$$\frac{m(m+1)}{2} = \sum_{n=1}^{m} \varphi(n) \left\lfloor \frac{m}{n} \right\rfloor.$$

Se $f(n) = \mu(n)$, então $F(n) = 0$ se $n > 1$ e $F(1) = 1$ pelo lema 3.8, portanto

$$1 = \sum_{n=1}^{m} \mu(n) \left\lfloor \frac{m}{n} \right\rfloor.$$

A igualdade anterior nos permite resolver o seguinte

Exemplo 3.11. *Demonstrar que, para todo inteiro $m > 1$,*

$$\left| \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < 1.$$

Solução: Como $-1 < \mu(k)\left(\left\lfloor \frac{m}{k}\right\rfloor - \frac{m}{k}\right) < 1$ e $\left\lfloor \frac{m}{k}\right\rfloor - \frac{m}{k} = 0$ quando $k = 1, m$, então

$$\left|\sum_{k=1}^{m} \mu(k)\left\lfloor \frac{m}{k}\right\rfloor - m\sum_{k=1}^{m}\frac{\mu(k)}{k}\right| < m-1$$

Usando a identidade acima provada temos que

$$\left|1 - m\sum_{k=1}^{m}\frac{\mu(k)}{k}\right| < m-1,$$

logo $\left|m\sum_{k=1}^{m}\frac{\mu(k)}{k}\right| < m$ e simplificando m obtemos o que queríamos demonstrar. É conhecido (Mangoldt 1897) que se m tende para infinito, então a soma anterior converge para 0. $\square$

Teorema 3.12 (Segunda fórmula de inversão de Möbius)**.** *Sejam f, g funções reais com domínio $(0, +\infty)$ tais que*

$$g(x) = \sum_{k=1}^{\infty} f\left(\frac{x}{k}\right)$$

para todo x, então

$$f(x) = \sum_{k=1}^{\infty} \mu(k) g\left(\frac{x}{k}\right).$$

Demonstração: Observemos que

$$f(x) = \sum_{k=1}^{\infty}\mu(k)\Big(\sum_{r=1}^{\infty} f\left(\frac{x}{kr}\right)\Big) = \sum_{m=1}^{\infty}\Big(\sum_{k\mid m}\mu(k)\Big) f\Big(\frac{x}{m}\Big) = f(x),$$

como queríamos demonstrar. $\square$

A seguinte é uma das formulações da famosa hipótese de Riemann, um dos problemas em aberto mais importantes da Matemática. O Clay Mathematics Institute oferece um prêmio de 1 milhão de dólares para a a primeira demonstração da Hipótese de Riemann (ver a página web `http://www.claymath.org/millennium/`).

Conjetura 3.13 (Hipótese de Riemann)**.** *Se $\alpha > 1/2$, então*

$$\lim_{n\to\infty} \frac{1}{n^{\alpha}} \sum_{m=1}^{n} \mu(m) = 0.$$

Podemos reenunciar esta conjectura assim: seja $f\colon (0, +\infty) \to \mathbb{R}$ definida por

$$\begin{cases} f(t) = 0 & \text{se } t < 1 \\ \sum_{k=1}^{\infty} f(t/k) = 1 & \text{se } t \geq 1. \end{cases}$$

Então, para todo $\alpha > 1/2$,

$$\lim_{t\to\infty} \frac{f(t)}{t^{\alpha}} = 0.$$

De fato, pela segunda fórmula de inversão de Möbius, temos

$$f(t) = \sum_{m=1}^{\lfloor t\rfloor} \mu(m).$$

Problemas Propostos

3.1. *Encontrar todos os inteiros positivos n tais que*

$$n = d_6^2 + d_7^2 - 1,$$

onde $1 = d_1 < d_2 < \cdots < d_k = n$ são todos os divisores positivos do número n.

3.2. *Seja r o número de fatores primos diferentes de n, demonstrar que*

$$\sum_{d|n} |\mu(d)| = 2^r.$$

3.3. *Seja n um inteiro positivo que não é primo e tal que $\varphi(n) \mid n-1$. Demonstrar que n possui ao menos quatro fatores primos distintos.*

3.4. *Dados dois números reais α e β tais que $0 \leq \alpha < \beta \leq 1$, demonstrar que existe um número natural m tal que*

$$\alpha < \frac{\varphi(m)}{m} < \beta.$$

3.5. *Seja m um inteiro positivo. Dizemos que um inteiro $m \geq 1$ é "superabundante" se*

$$\forall k \in \{1, 2, \dots, m-1\} \qquad \frac{\sigma(m)}{m} > \frac{\sigma(k)}{k}.$$

Demonstrar que existe um número infinito de números superabundantes.

3.6. *Demonstrar que $d(n) < 2\sqrt{n}$. Poderia melhorar esta cota?*

3.7. *Demonstrar que*

$$\frac{\sigma(n)}{d(n)} \geq \sqrt{n}.$$

3.8. *Encontrar todos os valores de n para os quais $\varphi(n) \mid n$.*

3.9. *Dois números a e b são* amigáveis *se $\sigma(a) = b$ e $\sigma(b) = a$. Por exemplo* 1184 *e* 1210 *são amigáveis (verificar!). Encontrar outra dupla de números amigáveis.*

3.10. *Demonstrar que $m \mid \sigma(mn-1)$ para todo n se, e só se, $m = 2, 3, 4, 6, 8, 12$ ou 24.*

3.11. *Demonstrar que*

$$\frac{\sigma(n!)}{n!} > 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

3.12. *Demonstrar que existem infinitos números naturais n para os quais $\sigma(x) = n$ não tem solução.*

3.13. *Demonstrar que para todo $m > 1$*

$$\left| \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < \frac{2}{3}.$$

3.14 (IMO1998)**.** *Para cada inteiro positivo n, $d(n)$ denota o número de divisores de n. Determine todos os inteiros positivos k tais que $d(n^2) = kd(n)$ para algum n.*

3.15. *Se n é composto, mostre que $\varphi(n) \leq n - \sqrt{n}$.*

3.16. *Determinar todos os números inteiros positivos n tais que $n = d(n)^2$.*

3.17. *Mostrar que* $\varphi(n) + \sigma(n) \geq 2n$ *para todo inteiro positivo* n.

3.18. *Seja* $f : \mathbb{N}^+ \to \mathbb{R}^+$ *uma função multiplicativa e crescente.*

(a) Prove que, para todo inteiro $M > 1$ *e todo inteiro positivo* n,

$$f(M^{n+1} - 1) \geq f(M^n - 1)f(M) \text{ e } f(M^{n+1} + 1) \leq f(M^n + 1)f(M).$$

Conclua que

$$\lim_{n\to\infty} \sqrt[n]{f(M^n)} = f(M).$$

(b) Utilize o item anterior para M *potência de primo para concluir que* $f(p^k) = f(p)^k$ *para todo primo* p.

(c) Conclua que f *é totalmente multiplicativa, e portanto existe* $\alpha > 0$ *tal que* $f(n) = n^\alpha$ *para todo inteiro positivo* n.

3.19. *Dadas duas funções* $f, g : \mathbb{N}_{>0} \to \mathbb{C}$, *definimos o produto de Dirichlet (ou convolução de Dirichlet)* $f * g : \mathbb{N}_{>0} \to \mathbb{C}$ *de* f *e* g *por*

$$f * g(n) \stackrel{\text{def}}{=} \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = \sum_{d_1 d_2 = n} f(d_1)g(d_2).$$

(a) Prove que, se $s \in \mathbb{R}$ *(ou* $s \in \mathbb{C}$*) e as séries* $\sum_{n\geq 1} \frac{f(n)}{n^s}$ *e* $\sum_{n\geq 1} \frac{g(n)}{n^s}$ *convergem absolutamente então*

$$\sum_{n\geq 1} \frac{f(n)}{n^s} \cdot \sum_{n\geq 1} \frac{g(n)}{n^s} = \sum_{n\geq 1} \frac{f * g(n)}{n^s}.$$

(b) Prove que, para quaisquer funções $f, g, h : \mathbb{N}_{>0} \to \mathbb{C}$, *temos* $f * g = g * f$ *e* $f*(g*h) = (f*g)*h$ *(isto é, o produto de Dirichlet é comutativo e associativo), e que a função* $I : \mathbb{N}_{>0} \to \mathbb{C}$ *dada por* $I(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}$ *é o elemento neutro do produto* $*$, *i.e.,* $I * f = f * I = f$, $\forall f : \mathbb{N}_{>0} \to \mathbb{C}$.

(c) Prove que se f *e* g *são multiplicativas então* $f * g$ *é multiplicativa.*

(d) Prove que, se $f : \mathbb{N}_{>0} \to \mathbb{C}$ *é tal que* $f(1) \neq 0$, *então existe uma única função* $f^{(-1)} : \mathbb{N}_{>0} \to \mathbb{C}$ *tal que* $f * f^{(-1)} = f^{(-1)} * f = I$, *a qual é dada recursivamente por* $f^{(-1)}(1) = 1/f(1)$ *e, para* $n > 1$,

$$f^{(-1)}(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} f\Big(\frac{n}{d}\Big) f^{(-1)}(d).$$

(e) Prove que, se f *é multiplicativa, então a função* $f^{(-1)}$ *definida no item anterior também é multiplicativa.*

3.3 Algumas Estimativas sobre Primos

Para estudar o comportamento assintótico das funções aritméticas da seção anterior, precisaremos de algumas estimativas sobre o crescimento dos primos.

3.3.1 O Teorema de Chebyshev

Começamos com um

Lema 3.14. *Sejam n um número natural e p um número primo. Seja θ_p o inteiro tal que $p^{\theta_p} \leq 2n < p^{\theta_p+1}$. Então o expoente da maior potência de p que divide $\binom{2n}{n}$ é menor ou igual a θ_p. Em particular, se $p > \sqrt{2n}$ então o expoente desta máxima potência de p é menor do que ou igual a 1. Além disso, se $\frac{2}{3}n < p < n$ então p não divide $\binom{2n}{n}$.*

Demonstração: Sejam α e β os expoentes das maiores potências de p que dividem $(2n)!$ e $n!$ respectivamente. Sabemos da proposição 1.22 que

$$\alpha = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \cdots \qquad \text{e} \qquad \beta = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots .$$

Portanto o expoente da máxima potência de p que divide $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é

$$\alpha - 2\beta = \sum_{i=1}^{\theta_p} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor .$$

Mas como

$$\frac{2n}{p^i} \geq \left\lfloor \frac{2n}{p^i} \right\rfloor > \frac{2n}{p^i} - 1 \qquad \text{e} \qquad -2\left(\frac{n}{p^i} - 1\right) > -2\left\lfloor \frac{n}{p^i} \right\rfloor \geq -2\frac{n}{p^i},$$

somando teremos que

$$2 > \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor > -1.$$

Portanto esta última expressão só pode tomar os valores 1 e 0. Concluímos que

$$\alpha - 2\beta \leq \sum_{i=1}^{\theta_p} 1 = \theta_p.$$

Além disso, se $\frac{2n}{3} < p < n$ então $\alpha = 2$ e $\beta = 1$, logo $\alpha - 2\beta = 0$. □

Corolário 3.15. *Para todo inteiro positivo n, o mínimo múltiplo comum dos números $1, 2, \ldots, 2n$ é maior ou igual a $\binom{2n}{n}$.*

Podemos agora mostrar a seguinte

Proposição 3.16 (Chebyshev)**.** *Seja $\pi(x)$ a quantidade de primos menores do que ou iguais a x. Existem constantes positivas $c < C$ tais que*

$$c\frac{x}{\log x} < \pi(x) < C\frac{x}{\log x}$$

para todo $x \geq 2$.

Demonstração: Observemos inicialmente que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é múltiplo de todos os primos p que satisfazem $n < p \leq 2n$. Como

$$\binom{2n}{n} < \sum_{0 \leq k \leq 2n} \binom{2n}{k} = 2^{2n},$$

segue que o produto dos primos entre n e $2n$ é menor do que 2^{2n}. Como há $\pi(2n) - \pi(n)$ primos como esses segue que $n^{\pi(2n)-\pi(n)} < 2^{2n}$ (pois todos esses primos são maiores que n), donde $(\pi(2n) - \pi(n)) \log n < 2n \log 2$ e

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}.$$

Isso implica facilmente, por indução, que

$$\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k}$$

(começando com $k = 5$; até $k = 5$ segue de $\pi(n) \leq n/2$ para $n \geq 4$). Daí segue que se $2^k < x \leq 2^{k+1}$ então

$$\pi(x) \leq \frac{5 \cdot 2^k}{k} \leq \frac{5x \log 2}{\log x}$$

pois $f(x) = x \log 2 / \log x$ é uma função crescente para $x \geq 3$.

Vamos agora provar a outra desigualdade. Se $\binom{2n}{n} = \prod_{p<2n} p^{\alpha_p}$ é a fatoração canônica de $\binom{2n}{n}$ então pelo lema 3.14 temos $p^{\alpha_p} \leq 2n \iff \alpha_p \log p \leq \log 2n$ e portanto

$$\log \binom{2n}{n} = \sum_{p<2n} \alpha_p \log p \leq \pi(2n) \log(2n),$$

donde

$$\pi(2n) \geq \frac{\log \binom{2n}{n}}{\log(2n)} \geq \frac{n \log 2}{\log(2n)}$$

pois

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} \geq 2^n,$$

assim,

$$\pi(x) \geq \frac{x \log 2}{2 \log x}$$

para todo x par, o que implica na mesma estimativa para todo x inteiro, pois $\pi(2k-1) = \pi(2k)$. □

Corolário 3.17. *Seja p_n o n-ésimo número primo. Existem constantes $C' > c' > 0$ tais que*

$$c' n \log n < p_n < C' n \log n$$

para todo $n \geq 2$.

Demonstração: Se $\limsup_{n\to\infty} \frac{p_n}{n \log n} > C'$, então

$$\begin{aligned}\liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} &\leq \liminf_{n\to\infty} \frac{\pi(p_n)}{p_n/\log p_n} \\ &\leq \liminf_{n\to\infty} \frac{n(\log C' + \log n + \log\log n)}{C' n \log n} = \frac{1}{C'}\end{aligned}$$

já que $x/\log x$ é crescente para $x \geq 3$. Assim, como $\liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} > 0$ pelo teorema anterior, temos que existe C' tal que $p_n < C' n \log n$ para todo $n \geq 2$. Analogamente se prova a existência de c'. □

Temos ainda o seguinte corolário do teorema de Chebyshev, que deixamos como exercício para o leitor.

Corolário 3.18. *Seja $f\colon \mathbb{N} \to [0, +\infty)$ uma função decrescente. A série*

$$\sum_{p \text{ primo}} f(p)$$

converge se, e somente se, a série

$$\sum_{n=2}^{\infty} \frac{f(n)}{\log n}$$

converge. Em particular,

$$\sum_{p \text{ primo}} \frac{1}{p} = +\infty.$$

Observação 3.19. *Um interessante argumento devido a Erdős dá uma outra prova da divergência da série dos inversos dos primos: supondo que $\sum_{p \text{ primo}} \frac{1}{p} < +\infty$, existe $N \in \mathbb{N}$ tal que*

$$\sum_{\substack{p \text{ primo} \\ p \geq N}} \frac{1}{p} < \frac{1}{2}.$$

Vamos considerar a decomposição $\mathbb{N} = A \cup B$ em que $A = \{n \in \mathbb{N} \mid$ todos os fatores primos de n são menores que $N\}$ e $B = \mathbb{N} \setminus A$. Sejam $p_1, p_2, \ldots, p_k$ todos os primos menores que N. Fixemos $M \in \mathbb{N}$. Se $n \in A$ e $n \leq M$, então n se fatora como $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, onde $\alpha_j \leq \frac{\log M}{\log 2}, \forall j \leq k$. Assim, $|A \cap [1, M]| \leq (1 + \frac{\log M}{\log 2})^k$. Por outro lado, todo elemento de B tem um fator primo maior ou igual a N, donde

$$|B \cap [1, M]| \leq \sum_{\substack{p \text{ primo} \\ p \geq N}} \left\lfloor \frac{M}{p} \right\rfloor \leq M \sum_{\substack{p \text{ primo} \\ p \geq N}} \frac{1}{p} < \frac{M}{2}.$$

Como $M = |\mathbb{N} \cap [1, M]| = |A \cap [1, M]| + |B \cap [1, M]| < (1 + \frac{\log M}{\log 2})^k + \frac{M}{2}$, temos $\frac{M}{2} < (1 + \frac{\log M}{\log 2})^k$ para todo $M \in \mathbb{N}$, o que é absurdo, pois

$$\lim_{M \to +\infty} \frac{1}{M} \left(1 + \frac{\log M}{\log 2}\right)^k = 0.$$

□

3.3.2 O Postulado de Bertrand

Sabemos que há sequências arbitrariamente grandes de números consecutivos que não contém primos, por exemplo

$$k! + 2, k! + 3, k! + 4, \ldots, k! + k$$

Nosso próximo resultado é o seguinte teorema, também devido a Chebyshev, que afirma que os primos não são tão "esparsos" assim. Ele é chamado de "postulado" por razões históricas.

Teorema 3.20 (Postulado de Bertrand)**.** *Seja n um inteiro positivo. Então sempre existe um primo p tal que $n \leq p \leq 2n$.*

Lema 3.21. *Para todo $n \geq 2$, temos*

$$\prod_{\substack{p \leq n \\ p \text{ primo}}} p < 4^n.$$

Demonstração: A prova é por indução em n. Para isso, vemos que para n pequeno tal desigualdade é válida. Além disso, se o resultado vale para $n = 2m+1$ então também vale para $n = 2m+2$ pois não agregamos novos primos ao produto quando passamos de $2m+1$ para $2m+2$. Logo basta provar a desigualdade para um valor ímpar $n = 2m+1$.

Dado que para todo primo p tal que $m+1 < p \leq 2m+1$ tem-se que p divide $(2m+1)!$ mas não divide $(m+1)!$ nem $m!$ então

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m+1} = \binom{2m}{m+1} + \binom{2m}{m} < (1+1)^{2m} = 4^m.$$

Portanto da hipótese de indução temos que

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \prod_{m+1<p\leq 2m+1} p < 4^{m+1}4^m = 4^{2m+1},$$

como queríamos demonstrar. □

Demonstração: (do postulado de Bertrand) Suponhamos que esta afirmação é falsa para algum valor de n e mostraremos que n não pode ser muito grande.

Seja p_i o i-ésimo primo e α_i máximo tal que $p_i^{\alpha_i} \mid \binom{2n}{n}$. Como estamos supondo que não há primos entre n e $2n$ e como nenhum primo entre $\frac{2}{3}n$ e n divide $\binom{2n}{n}$ pelo lema 3.14, temos $\binom{2n}{n} = \prod_{p_i \leq \frac{2n}{3}} p_i^{\alpha_i}$. Ainda pelo lema 3.14, $p_i^{\alpha_i} \leq 2n$ e $\alpha_j \leq 1$ para $p_j > \sqrt{2n}$, logo

$$\binom{2n}{n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{\alpha_i} \prod_{\sqrt{2n} < p_j \leq \frac{2n}{3}} p_j \leq \prod_{p_i \leq \sqrt{2n}} 2n \prod_{p_j \leq \frac{2n}{3}} p_j.$$

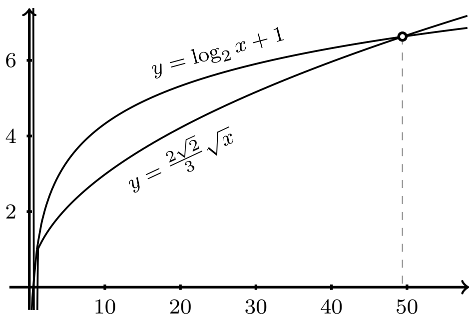
Utilizando o lema anterior, e supondo que n é suficientemente grande de modo que o número de primos entre 1 e $\sqrt{2n}$ é menor que $\sqrt{n/2} - 1$ ($n = 100$ é suficiente e a partir deste valor esta hipótese se cumpre já que metade dos números neste intervalo são pares), temos

$$\binom{2n}{n} < (2n)^{\sqrt{n/2}-1} 4^{2n/3}.$$

Por outra parte, $n\binom{2n}{n} = n\binom{2n-1}{n} + n\binom{2n-1}{n-1} > (1+1)^{2n-1} = 2^{2n-1}$ e assim a desigualdade anterior implica

$$\frac{2^{2n-1}}{n} < (2n)^{\sqrt{n/2}-1} 4^{2n/3} \implies 2^{2n/3} < (2n)^{\sqrt{n/2}}.$$

Tomando logaritmo na base 2, obtemos a desigualdade $\frac{2\sqrt{2}}{3}\sqrt{n} < \log_2 n + 1$, que é falsa para todo $n \geq 50$.



Portanto, se existe um contra-exemplo do postulado de Bertrand, este deve ser menor do que 100. Para terminar a demonstração só falta mostrar um primo que cumpra as condições do teorema para todo inteiro menor que 100: tome

$$\begin{array}{lll} p=2 & \text{para} & 1 \le n \le 2 \\ p=5 & \text{para} & 3 \le n \le 5 \\ p=11 & \text{para} & 6 \le n \le 11 \\ p=23 & \text{para} & 12 \le n \le 23 \\ p=47 & \text{para} & 24 \le n \le 47 \\ p=79 & \text{para} & 48 \le n \le 79 \\ p=101 & \text{para} & 80 \le n \le 100 \end{array}$$

□

Exemplo 3.22. *Seja $n > 2^k$. Demonstrar que os k primeiros números que são maiores do que n e primos relativos com $n!$ são primos.*

Solução: Como $n > 2^k$ então $n^2 > 2^k n$. Então entre dois termos consecutivos da sequência $n, 2n, 4n, \ldots, 2^k n$ existe ao menos um primo. Portanto, entre n e n^2 existem ao menos k primos. Em particular, os k primeiros números maiores que n que são primos relativos com $n!$ estarão entre n e n^2. Se um de tais números não fora primo, digamos $l = ab$, supondo $a \le b$, teremos que $a^2 \le l \le n^2$, logo $a \le n$, o que contradiz o fato de que $n!$ e l são primos relativos. □

3.3.3 Outras estimativas

Precisaremos também das seguintes estimativas:

Lema 3.23. *1.* $\sum\limits_{1\le j\le n} \frac{1}{j} = \log n + \gamma + O(\frac{1}{n}) = \log n + O(1)$, *onde*

$$\gamma = \lim_{n\to\infty}\Big(\Big(\sum_{1\le j\le n}\frac{1}{j}\Big) - \log n\Big) = 0{,}5772156649015328606065 12\ldots$$

é a constante de Euler-Mascheroni (ver [1] por exemplo).

2. $\sum\limits_{j=1}^{n} \log j = \big(n + \frac{1}{2}\big)\log n - n + O(1)$.

3. $\sum\limits_{j=2}^{n} \frac{1}{j\log j} = \log\log n + O(1)$.

Demonstração: Para estimativa mais precisa da primeira soma, veja por exemplo [6]. Aqui provaremos apenas a segunda estimativa, que nos será suficiente na maioria das aplicações. Para isto, observemos que a função $g(x) = \frac{1}{x}$ é estritamente decrescente e côncava para cima, assim para todo inteiro $j > 1$, no intervalo $[j-1, j]$ a reta $y = \frac{1}{j}$ fica embaixo de $y = g(x)$, que por sua vez fica embaixo da reta que passa pelos pontos $(j-1, \frac{1}{j-1})$ e $(j, \frac{1}{j})$. Portanto calculando as áreas sob as curvas temos que

$$\frac{1}{j} < \int_{j-1}^{j} \frac{1}{x} dx < \frac{1}{2}\left(\frac{1}{j-1} + \frac{1}{j}\right),$$

Somando todas estas desigualdades desde 2 até n temos que

$$\sum_{j=2}^{n} \frac{1}{j} < \int_{1}^{n} \frac{1}{x} dx < \sum_{j=2}^{n} \frac{1}{2}\left(\frac{1}{j-1} + \frac{1}{j}\right) = \frac{1}{2} - \frac{1}{2n} + \sum_{j=2}^{n} \frac{1}{j}$$

e assim

$$\frac{1}{2} + \frac{1}{2n} + \log n < \sum_{j=1}^{n} \frac{1}{j} < 1 + \log n.$$

Para estimar o segundo somatório, observemos que a função $h(x) = \log x$ é estritamente crescente e côncava para baixo. Como antes, temos que para todo inteiro $j > 1$, no intervalo $[j-1, j]$ a reta que contém o ponto $(j, \log j)$ e tem inclinação $m_j = h'(j) = \frac{1}{j}$ fica por cima de $y = h(x)$, que por sua vez fica acima da reta que passa pelos pontos $(j-1, \log(j-1))$, $(j, \log j)$. Logo

$$\log j - \frac{1}{2j} > \int_{j-1}^{j} \log x \, dx > \frac{1}{2}(\log(j-1) + \log j).$$

Somando estas desigualdades desde 2 até n temos que

$$\begin{aligned} \sum_{j=2}^{n} \log j - \sum_{j=2}^{n} \frac{1}{2j} &> \int_{1}^{n} \log x \, dx \\ &> \sum_{j=2}^{n} \frac{1}{2}(\log(j-1) + \log j) = \sum_{j=2}^{n} \log j - \frac{1}{2} \log n. \end{aligned}$$

Ou seja,

$$\left(n + \frac{1}{2}\right) \log n - n + 1 > \sum_{j=1}^{n} \log j > n \log n - n + \frac{1}{2} + \frac{1}{2} \sum_{j=1}^{n} \frac{1}{j}.$$

Assim, concluímos que

$$\left(n + \frac{1}{2}\right) \log n - n + 1 > \sum_{j=1}^{n} \log j > \left(n + \frac{1}{2}\right) \log n - n + \frac{1}{4n} + \frac{3}{4}$$

e o resultado segue.

A terceira soma é estimada comparando-a com a integral $\int_2^n \frac{dx}{x \log x} = \log\log n - \log\log 2$, e é deixada como exercício para o leitor. □

Agora, mostremos algumas estimativas sobre números primos.

Proposição 3.24. $\sum\limits_{\substack{p \text{ primo} \\ p \le n}} \frac{\log p}{p} = \log n + O(1).$

Demonstração: Pela proposição 1.22, temos

$$n! = \prod_{\substack{p \text{ primo} \\ p \le n}} p^{v_p} \quad \text{onde} \quad v_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Tomando logaritmos, temos $\sum_{k=1}^n \log k = \sum_{\substack{p \text{ primo} \\ p \le n}} v_p \log p$, e como $\frac{n}{p} - 1 < \lfloor \frac{n}{p} \rfloor \le v_p < \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1}$,

$$\sum_{\substack{p \text{ primo} \\ p \le n}} \left(\frac{n}{p} - 1 \right) \log p \le \sum_{k=1}^{n} \log k \le \sum_{\substack{p \text{ primo} \\ p \le n}} \frac{n}{p-1} \log p.$$

Ou seja,

$$-\frac{1}{n} \sum_{\substack{p \text{ primo} \\ p \le n}} \log p \le \frac{1}{n} \sum_{k=1}^{n} \log k - \sum_{\substack{p \text{ primo} \\ p \le n}} \frac{\log p}{p} \le \sum_{\substack{p \text{ primo} \\ p \le n}} \frac{\log p}{p(p-1)}.$$

Pelo teorema de Chebyshev 3.16, temos $\sum_{\substack{p \text{ primo} \\ p \le n}} \log p \le \pi(n) \log n = O(n)$. Por outro lado, $\sum_{\substack{p \text{ primo} \\ p \le n}} \frac{\log p}{p(p-1)} \le \sum_{n \ge 1} \frac{1}{n^{3/2}} = O(1)$. O resultado segue, pois $\frac{1}{n} \sum_{k=1}^{n} \log k = \log n + O(1)$ pelo lema anterior. $\square$

A proposição anterior nos permite estimar a ordem de crescimento da soma dos inversos dos primos.

Teorema 3.25. $\sum_{\substack{p \text{ primo} \\ p \le n}} \frac{1}{p} = \log \log n + O(1)$.

Demonstração: Defina

$$a_k = \begin{cases} \frac{\log k}{k} & \text{se } k \text{ é primo} \\ 0 & \text{caso contrário} \end{cases} \qquad \text{e} \qquad S_n = \sum_{k=1}^{n} a_k.$$

Pela proposição anterior, temos que $S_k = \sum_{\substack{p \text{ primo} \\ p \le k}} \frac{\log p}{p} = \log k + O(1)$. Assim, temos por "integração por partes" discreta

$$\begin{aligned}
\sum_{\substack{p \text{ primo} \\ p \le n}} \frac{1}{p} &= \sum_{k=2}^{n} \frac{a_k}{\log k} = \sum_{k=2}^{n} \frac{S_k - S_{k-1}}{\log k} \\
&= \sum_{k=2}^{n} S_k \left(\frac{1}{\log k} - \frac{1}{\log(k+1)} \right) + \frac{S_n}{\log(n+1)} \\
&= \sum_{k=2}^{n} \log k \left(\frac{1}{\log k} - \frac{1}{\log(k+1)} \right) + O(1) \\
&= \sum_{k=2}^{n} \frac{\log(k+1) - \log k}{\log(k+1)} + O(1) \\
&= \sum_{k=2}^{n} \frac{1}{(k+1)\log(k+1)} + O(1)
\end{aligned}$$

onde a última igualdade segue de

$$\begin{aligned}
& \frac{1}{k+1} \le \int_k^{k+1} \frac{dx}{x} \le \frac{1}{k} \\
\Longrightarrow\ & \frac{1}{(k+1)\log(k+1)} \le \frac{\log(k+1) - \log k}{\log(k+1)} \le \frac{1}{k \log(k+1)}
\end{aligned}$$

e

$$\left|\sum_{k=2}^{n} \frac{1}{k\log(k+1)} - \sum_{k=2}^{n} \frac{1}{(k+1)\log(k+1)}\right| \le \sum_{k=2}^{n}\left(\frac{1}{k} - \frac{1}{k+1}\right) = O(1),$$

O resultado segue do lema anterior, já que $\sum\limits_{k=2}^{n} \frac{1}{(k+1)\log(k+1)} = \log\log n + O(1)$. □

Observação 3.26. *Não é difícil mostrar que a prova acima fornece um termo de erro do tipo $c+O(\frac{1}{\log n})$ (em lugar de $O(1)$) para uma certa constante c (a constante de Mertens), que vale aproximadamente*

$$0,2614972128476427837554268386\ldots.$$

Deixamos os detalhes como exercício para o leitor. É possível provar que a constante de Mertens c é igual a $\gamma + \sum\limits_{p \text{ primo}} (\log(1-\frac{1}{p}) + \frac{1}{p})$, onde γ é a constante de Euler-Mascheroni.

É possível obter estimativas mais precisas para o termo de erro. Landau, por exemplo, provou em [12] que é possível trocar o termo de erro $O(\frac{1}{\log n})$ por $O(\exp(-(\log n)^{1/14}))$, e Vinogradov ([25]) provou que é possível trocar o termo de erro por $O(\exp(-a(\log n)^{3/5}(\log\log n)^{-1/5}))$, para alguma constante positiva a.

Mais recentemente, Diamond e Pintz ([4]) provaram que o erro $\sum\limits_{\substack{p \text{ primo}\\ p\le n}} \frac{1}{p} - \log\log n - c$ troca de sinal infinitas vezes. Mais precisamente, $n^{1/2}\log n(\sum\limits_{\substack{p \text{ primo}\\ p\le n}} \frac{1}{p} - \log\log n - c)$ atinge valores positivos e negativos de módulos arbitrariamente grandes.

Um outro resultado importante, que será usado nas seções seguintes, é

Proposição 3.27. $\sum\limits_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

DEMONSTRAÇÃO: No plano complexo, temos

$$\operatorname{sen} z = z\prod_{k=1}^{\infty}\left(1 - \frac{z^2}{\pi^2 k^2}\right).$$

Assumindo esta fórmula, vejamos como terminar a prova. O coeficiente de z^3 neste produto é $-\sum_{k=1}^{\infty} \frac{1}{\pi^2k^2}$, mas como

$$\operatorname{sen} z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \cdots$$

concluímos que $\sum_{k=1}^{\infty} \frac{1}{\pi^2k^2} = \frac{1}{3!}$, donde o resultado segue.

Para provar a fórmula acima, basta fazê-lo para z real, uma vez que o resultado geral segue por continuação analítica. Note que para todo $k \ge 1$, $\operatorname{sen}((2k+1)y)$ pode ser escrito como $P_k(\operatorname{sen} y)$, onde P_k é um polinômio de grau $2k+1$ (e coeficiente líder $(-4)^k$). De fato, $\operatorname{sen} y = \operatorname{sen} y$, $\operatorname{sen}(3y) = 3\operatorname{sen} y - 4\operatorname{sen}^3(y)$ e, para todo $k \ge 1$,

$$\begin{aligned}
P_{k+1}(\operatorname{sen} y) + P_{k-1}(\operatorname{sen} y) &= \operatorname{sen}((2k+3)y) + \operatorname{sen}((2k-1)y)\\
&= \operatorname{sen}((2k+1)y + 2y) + \operatorname{sen}((2k+1)y - 2y)\\
&= 2\operatorname{sen}((2k+1)y)\cos(2y)\\
&= 2P_k(\operatorname{sen} y)(1 - 2\operatorname{sen}^2(y)),
\end{aligned}$$

o que implica o resultado por indução, com $P_{k+1}(t) = 2(1-2t^2)P_k(t) - P_{k-1}(t)$. As raízes de $P_k(t)$ são os $2k+1$ números $\operatorname{sen}(\pi r/(2k+1))$, onde r é inteiro com $-k \le r \le k$. Assim, temos

$$\begin{aligned}\operatorname{sen}((2k+1)y) &= (-4)^k \operatorname{sen} y \prod_{1\le r\le k}\Big(\operatorname{sen}^2 y - \operatorname{sen}^2\Big(\frac{\pi r}{2k+1}\Big)\Big)\\ &= c_k \operatorname{sen} y \prod_{1\le r\le k}\Big(1 - \frac{\operatorname{sen}^2 y}{\operatorname{sen}^2(\frac{\pi r}{2k+1})}\Big)\end{aligned}$$

para alguma constante c_k. Como $\lim\limits_{y\to 0} \frac{\operatorname{sen}((2k+1)y)}{\operatorname{sen} y} = 2k+1$, temos que $c_k = 2k+1$. Fazendo agora $y = x/(2k+1)$, temos

$$\operatorname{sen} x = (2k+1)\operatorname{sen}\Big(\frac{x}{2k+1}\Big) \prod_{1\le r\le k}\Big(1 - \frac{\operatorname{sen}^2(\frac{x}{2k+1})}{\operatorname{sen}^2(\frac{\pi r}{2k+1})}\Big).$$

Como $2t/\pi \le \operatorname{sen} t \le t$ para todo t entre 0 e $\pi/2$, temos, para todo x real e $1 \le r \le k$,

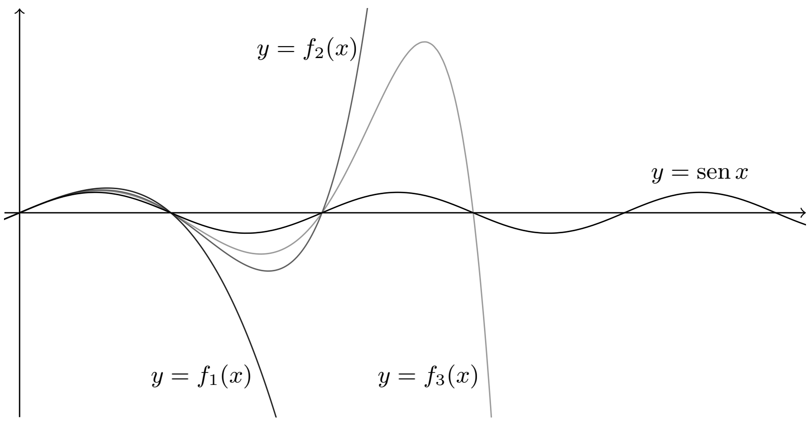
$$\frac{2r}{2k+1} \le \operatorname{sen}\Big(\frac{\pi r}{2k+1}\Big) \le \frac{\pi r}{2k+1} \implies 1 - \frac{x^2}{4r^2} \le 1 - \frac{\operatorname{sen}^2(\frac{x}{2k+1})}{\operatorname{sen}^2(\frac{\pi r}{2k+1})} \le 1.$$

Assim, o produto converge uniformemente em compactos, e podemos passar ao limite $k \to \infty$ termo a termo, obtendo a fórmula

$$\operatorname{sen} x = x \prod_{r\ge 1}\Big(1 - \frac{x^2}{\pi^2 r^2}\Big).$$

□

No seguinte desenho se ilustram os gráficos $y = f_k(x)$, dos primeiros três termos da sequência $f_k(x) := x \prod\limits_{1\le r\le k}\Big(1 - \frac{x^2}{\pi^2 r^2}\Big)$ que converge em compactos à função $\operatorname{sen} x$.



Problemas Propostos

3.20. *Seja* $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ *a* função zeta de Riemann. *Mostrar usando a proposição anterior que* $\zeta(4) = \frac{\pi^4}{90}$.

3.21. *Mostrar indutivamente que* $\frac{\zeta(2k)}{\pi^{2k}}$ *é sempre racional.*

3.22 (Frações egípcias)**.** *Uma fração egípcia é uma fração da forma* $\frac{1}{n}$*, onde* n *é um inteiro positivo (parece que os egípcios não gostavam de frações com numerador maior que* 1*). Prove que todo racional positivo pode ser escrito como soma de frações egípcias distintas.*

3.23. *(a) Dados inteiros* $b \geq 2$ *e* a*, com* $0 \leq a \leq b-1$*, seja* $X_{a,b}$ *o conjunto dos inteiros positivos* n *em cuja representação na base* b *o algarismo* a *não aparece. Prove que* $\sum_{n \in X_{a,b}} \frac{1}{n}$ *converge.*

(b) Prove que qualquer sequência finita de dígitos aparece como uma sequência de dígitos consecutivos na representação decimal de infinitos números primos.

3.4 A Função φ de Euler

As seguintes proposições mostram algumas estimativas da função φ de Euler.

Proposição 3.28. $\sum_{k=1}^{n} \varphi(k) = \frac{3n^2}{\pi^2} + O(n \log n)$.

Demonstração: Observemos que pela fórmula de inversão de Möbius (teorema 3.9) e o lema 1.77 temos $\varphi(k) = \sum_{d \mid k} \mu(d) \frac{k}{d}$, logo

$$\begin{aligned}\sum_{k=1}^{n} \varphi(k) &= \sum_{k=1}^{n} \sum_{d \mid k} \mu(d) \cdot \frac{k}{d} = \sum_{d=1}^{n} \sum_{\substack{d \mid k \\ 1 \leq k \leq n}} \mu(d) \cdot \frac{k}{d} \\ &= \sum_{d=1}^{n} \mu(d) \sum_{r=1}^{\lfloor \frac{n}{d} \rfloor} r = \sum_{d=1}^{n} \mu(d) \frac{\lfloor \frac{n}{d} \rfloor (\lfloor \frac{n}{d} \rfloor + 1)}{2}\end{aligned}$$

onde fizemos a substituição $r = \frac{k}{d} \leq \frac{n}{d}$. Por outro lado,

$$\Big\lfloor \frac{n}{d} \Big\rfloor \Big(\Big\lfloor \frac{n}{d} \Big\rfloor + 1 \Big) = \Big(\frac{n}{d} \Big)^2 + O\Big(\frac{n}{d}\Big)$$

e $\sum\limits_{k > n} \frac{1}{k^2} = O(\int_n^\infty \frac{dx}{x^2}) = O(\frac{1}{n})$, logo $\sum\limits_{d > n} \frac{\mu(d)}{d^2} = O(\frac{1}{n})$ e assim

$$\sum_{k=1}^{n} \varphi(k) = \frac{n^2}{2} \sum_{d=1}^{n} \frac{\mu(d)}{d^2} + O\Big(n \sum_{d=1}^{n} \frac{1}{d} \Big) = \frac{n^2}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(n \log n).$$

Além disso, note que para todo $\alpha > 1$ temos que

$$\sum_{m=1}^{\infty} \frac{1}{m^\alpha} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^\alpha} = \sum_{k=1}^{\infty} \frac{\sum_{d \mid k} \mu(d)}{k^\alpha} = 1.$$

Em particular $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = (\sum_{d=1}^{\infty} \frac{1}{d^2})^{-1} = \frac{6}{\pi^2}$ pela proposição 3.27, assim substituindo este valor na expressão acima temos o resultado desejado.

□

Observemos que a proposição anterior mostra que a "probabilidade" de que dois números naturais sejam primos entre si, ou seja,

$$\lim_{N \to \infty} \frac{1}{N^2} \#\{(m,n) \in \mathbb{N}^2 \mid 1 \leq n, m \leq N \text{ e } \operatorname{mdc}(m,n) = 1\}$$

é igual a $\frac{6}{\pi^2} \approx 60{,}79\%$. Este resultado pode ser generalizado da seguinte forma:

Proposição 3.29. *Dados $k \geq 2$ um inteiro e $x \in (0, +\infty)$, sejam*

$$X = \{(m_1, m_2, \ldots, m_k) \in \mathbb{N}^k \mid \operatorname{mdc}(m_1, m_2, \ldots, m_k) = 1\} \text{ e}$$

$$f(x) = \#\{(m_1, m_2, \ldots, m_k) \in X \mid 1 \leq m_1, m_2, \ldots, m_k \leq x\}.$$

Seja ainda ζ a função zeta de Riemann dada por $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$. Então, para $k = 2$, $f(x) = \frac{x^2}{\zeta(2)} + O(x \log x)$ e, para $k > 2$, $f(x) = \frac{x^k}{\zeta(k)} + O(x^{k-1})$.

Em particular, $\lim\limits_{x \to +\infty} \frac{f(x)}{x^k} = \frac{1}{\zeta(k)}$. Em outras palavras, a "probabilidade" de termos $\operatorname{mdc}(m_1, m_2, \ldots, m_k) = 1$, para $m_1, m_2, \ldots, m_k \in \mathbb{N}$ é $\frac{1}{\zeta(k)}$.

Demonstração: Temos $f(x) = 0$ para todo $x \in (0, 1)$, e, para todo $x \in (0, +\infty)$, $\sum_{d \geq 1} f(x/d) = \lfloor x \rfloor^k$, pois cada um dos $\lfloor x \rfloor^k$ pontos inteiros $(m_1, m_2, \ldots, m_k) \in [1, \lfloor x \rfloor]^k$ se escreve de maneira única como $d.(r_1, r_2, ..., r_k)$, onde d (que é igual a $\operatorname{mdc}(m_1, m_2, ..., m_k)$) é um inteiro positivo e $\operatorname{mdc}(r_1, r_2, \ldots, r_k) = 1$, com $(r_1, r_2, \ldots, r_k) \in [1, \lfloor x/d \rfloor]^k$.

Portanto, pela segunda fórmula de inversão de Möbius, temos $f(x) = \sum_{d \geq 1} \mu(d) \lfloor x/d \rfloor^k = \sum_{d=1}^{\lfloor x \rfloor} \mu(d) \lfloor x/d \rfloor^k$.

Como $\lfloor x/d \rfloor^k = x^k/d^k + O(x^{k-1}/d^{k-1})$, temos

$$f(x) = \sum_{d=1}^{\lfloor x \rfloor} \mu(d) \Big(\frac{x}{d}\Big)^k + O\Big(\sum_{d=1}^{\lfloor x \rfloor} \frac{x^{k-1}}{d^{k-1}}\Big) = \sum_{d=1}^{\lfloor x \rfloor} \mu(d) \Big(\frac{x}{d}\Big)^k + O\Big(\sum_{d=1}^{\lfloor x \rfloor} \frac{x^{k-1}}{d^{k-1}}\Big) =$$
$$= x^k \sum_{d=1}^{\infty} \frac{\mu(d)}{d^k} + O\Big(x^{k-1} . \sum_{d=1}^{\lfloor x \rfloor} \frac{1}{d^{k-1}}\Big) = \frac{x^k}{\zeta(k)} + O\Big(x^{k-1} . \sum_{d=1}^{\lfloor x \rfloor} \frac{1}{d^{k-1}}\Big),$$

o que implica o resultado desejado. □

Proposição 3.30. $\sum_{k=1}^{n} \frac{\varphi(k)}{k} = \frac{6n}{\pi^2} + O(\log n)$.

Demonstração: Como na proposição anterior, $\varphi(k) = \sum_{d \mid k} \mu(d) \frac{k}{d}$ e portanto

$$\sum_{k=1}^{n} \frac{\varphi(k)}{k} = \sum_{k=1}^{n} \sum_{d \mid k} \frac{\mu(d)}{d} = \sum_{d=1}^{n} \Big\lfloor \frac{n}{d} \Big\rfloor \cdot \frac{\mu(d)}{d}$$
$$= n \sum_{d=1}^{n} \frac{\mu(d)}{d^2} + O\Big(\sum_{d=1}^{n} \frac{1}{d}\Big) = \frac{6}{\pi^2} n + O(\log n).$$

□

Proposição 3.31. $0 < \liminf\limits_{n \to \infty} \frac{\varphi(n) \log \log n}{n} < +\infty$.

Demonstração: Seja p_i o i-ésimo número primo. Se n tem k fatores distintos, então $n > n_k$ onde $n_k = p_1 \cdot p_2 \cdots p_k$ é o produto dos k primeiros números primos. Assim,

$$\frac{\varphi(n)}{n} = \prod_{\substack{p \text{ primo} \\ p \mid n}} \left(1 - \frac{1}{p}\right) \geq \prod_{1 \leq i \leq k} \left(1 - \frac{1}{p_i}\right) = \frac{\varphi(n_k)}{n_k},$$

logo $\frac{\varphi(n)\log\log n}{n} \geq \frac{\varphi(n_k)\log\log n_k}{n_k}$. Basta mostrar que $\liminf\limits_{k\to\infty} \frac{\varphi(n_k)\log\log n_k}{n_k} \in (0,\infty)$, mas

$$\log \frac{\varphi(n_k)\log\log n_k}{n_k} = \sum_{j=1}^{k} \log\left(1-\frac{1}{p_j}\right) + \log\log\log n_k.$$

Como $\log\bigl(1-\frac{1}{p_j}\bigr) = -\frac{1}{p_j} + O(\frac{1}{p_j^2})$, pela proposição 3.25 obtemos

$$\sum_{j=1}^{k} \log\Bigl(1-\frac{1}{p_j}\Bigr) = -\sum_{j=1}^{k} \frac{1}{p_j} + O(1) = -\log\log p_k + O(1).$$

Mas pelo corolário 3.17, temos que $k \leq p_k \leq Ck\log k$ para algum C, o que implica $\log\log p_k = \log\log k + O(1)$. Desta maneira, para mostrar que $\liminf\limits_{k\to\infty} \frac{\varphi(n_k)\log\log n_k}{n_k} \in (0,\infty)$, basta verificar que

$$\limsup_{k\to\infty}(\log\log k - \log\log\log n_k) = 0.$$

Temos que $n_k = \prod_{j=1}^{k} p_k \leq (Ck\log k)^k$, donde

$$\log n_k \leq k(\log k + \log(C\log k)) < 2k\log k \quad \text{para } k \text{ grande},$$

e assim $\log\log n_k < \log k + \log\log k + \log 2$. Portanto

$$\limsup_{k\to\infty}(\log\log k - \log\log\log n_k) \geq 0.$$

Por outro lado, certamente temos $n_k > 2^k$, logo $\log n_k > k\log 2$, $\log\log n_k > \log k + \log\log 2$, e assim

$$\limsup_{k\to\infty}(\log\log k - \log\log\log n_k) \leq 0.$$

Logo este $\limsup$ é zero, completando a prova. □

Observação 3.32. *É possível provar que* $\liminf\limits_{n\to\infty} \frac{\varphi(n)\log\log n}{n} = e^{-\gamma}$.

Observe que outro tipo de estimativa trivial pode ser obtida do fato que $\varphi(p) = p-1$, para todo p primo, assim fica claro que $\limsup\limits_{n\to\infty} \frac{\varphi(n)}{n} = 1$.

Resumindo os vários tipos de resultados que obtivemos sobre $\varphi(n)$ dizemos que a ordem média de $\varphi(n)$ é $\frac{6n}{\pi^2}$, a ordem máxima de $\varphi(n)$ é n e a ordem mínima de $\varphi(n)$ é $\frac{e^{-\gamma}n}{\log\log n}$.

Problemas Propostos

3.24. *Prove que se a parte real de α é maior ou igual a 2 então*

$$\sum_{m=1}^{\infty} \frac{\varphi(m)}{m^\alpha} = \sum_{m=1}^{\infty} \frac{1}{m^{\alpha-1}} \Bigg/ \sum_{m=1}^{\infty} \frac{1}{m^\alpha}.$$

3.25 (Sierpiński)**.** *Mostrar que o conjunto*

$$\Bigl\{\frac{\varphi(n+1)}{n} \Bigm| n \in \mathbb{N}\Bigr\}$$

é denso em $[0,1]$, isto é, que , para todo $a \in [0,1]$ e todo $\epsilon > 0$, existe um inteiro positivo n tal que $\left|\frac{\varphi(n)}{n} - a\right| < \epsilon$.

3.26 (Schinzel)**.** *Mostrar que o conjunto*

$$\Big\{\frac{\varphi(n+1)}{\varphi(n)}\;\Big|\;n\in\mathbb{N}\Big\}$$

é denso no conjunto dos números reais positivos.

3.27. *Mostar que para todo $\alpha\le 1$ e $n\gg 0$*

$$\sum_{k=1}^{n}\frac{\varphi(k)}{k^{\alpha}}=\frac{6}{\pi^2(2-\alpha)}n^{2-\alpha}+O(n^{1-\alpha}\log n).$$

3.28. *Mostrar que*

$$\sum_{k=1}^{n}\frac{\varphi(k)}{k^2}=\frac{6}{\pi^2}\log n+C+O\Big(\frac{\log n}{n}\Big),$$

onde $C=\frac{6\gamma}{\pi^2}-\sum_{d\ge 1}\frac{\mu(d)\log d}{d^2}$.

3.5 A Função σ

Lembramos que $\sigma(n)=\sum_{d|n}d$ é uma função multiplicativa. Assim, se $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ é a fatoração canônica de n, então

$$\sigma(n)=\prod_{j=1}^{k}(1+p_j+\cdots+p_j^{\alpha_j})=\prod_{j=1}^{k}\frac{p_j^{\alpha_j+1}-1}{p_j-1}=\prod_{j=1}^{k}p_j^{\alpha_j}\left(1+\frac{1-p_j^{-\alpha_j}}{p_j-1}\right)$$

donde $n\prod_{j=1}^{k}(1+\frac{1}{p_j})\le\sigma(n)<n\prod_{j=1}^{k}\frac{p_j}{p_j-1}$. Usando a fórmula de $\varphi(n)$ temos que

$$\prod_{j=1}^{k}\Big(1-\frac{1}{p_j^2}\Big)\le\frac{\varphi(n)\sigma(n)}{n^2}<1,$$

mas

$$\prod_{p\text{ primo}}\frac{1}{1-\frac{1}{p^2}}=\prod_{p\text{ primo}}\Big(1+\frac{1}{p^2}+\frac{1}{p^4}+\frac{1}{p^6}+\cdots\Big)=\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2}{6}$$

já que expandindo o produto, cada natural k aparece exatamente uma vez pelo teorema fundamental da aritmética. Logo temos que $\frac{6}{\pi^2}<\frac{\varphi(n)\sigma(n)}{n^2}<1$ para todo $n>1$. Juntamente com a proposição 3.31 isso implica a

Proposição 3.33. $\limsup\limits_{n\to\infty}\frac{\sigma(n)}{n\log\log n}\in(0,\infty)$. *Naturalmente, se n é primo, $\sigma(n)=n+1$, donde* $\liminf\limits_{n\to\infty}\frac{\sigma(n)}{n}=1$.

Observação 3.34. *É possível provar que* $\limsup\limits_{n\to\infty}\frac{\sigma(n)}{n\log\log n}=e^{\gamma}$.

Temos também a

Proposição 3.35. $\sum_{k=1}^{n}\sigma(k)=\frac{\pi^2}{12}n^2+O(n\log n)$

Demonstração: Da definição de σ temos que

$$\begin{aligned}\sum_{k=1}^{n}\sigma(k) &= \sum_{k=1}^{n}\sum_{d|k} d = \sum_{d=1}^{n} d\left\lfloor\frac{n}{d}\right\rfloor\\ &= \sum_{d\geq 1}\sum_{\substack{k\geq 1\\ kd\leq n}} d = \sum_{k\geq 1}\sum_{\substack{d\geq 1\\ kd\leq n}} d = \sum_{k=1}^{n}\frac{\lfloor\frac{n}{k}\rfloor(\lfloor\frac{n}{k}\rfloor+1)}{2}\\ &= \frac{n^2}{2}\sum_{k=1}^{n}\frac{1}{k^2}+O(n\log n)\\ &= \frac{\pi^2}{12}n^2+O(n\log n),\end{aligned}$$

pois $\sum\limits_{k>n}\frac{1}{k^2}=O(\int_n^\infty\frac{dx}{x^2})=O(\frac{1}{n})$ e $\sum\limits_{k\geq 1}\frac{1}{k^2}=\frac{\pi^2}{6}$. □

Proposição 3.36. $\sum\limits_{k=1}^{n}\frac{\sigma(k)}{k}=\frac{\pi^2}{6}n+O(\log n)$.

Demonstração: Observemos que $\frac{\sigma(k)}{k}=\sum_{d|k}\frac{d}{k}=\sum_{d'|k}\frac{1}{d'}$, assim por um procedimento similar ao anterior temos

$$\begin{aligned}\sum_{k=1}^{n}\frac{\sigma(k)}{k} &= \sum_{k=1}^{n}\sum_{d'|k}\frac{1}{d'} = \sum_{d'=1}^{n}\frac{1}{d'}\left\lfloor\frac{n}{d'}\right\rfloor\\ &= n\sum_{d'=1}^{n}\frac{1}{d'^2}+O(\log n)=\frac{\pi^2}{6}n+O(\log n).\end{aligned}$$

□

3.6 Números Livres de Quadrados

Vamos nesta seção a estimar a "probabilidade" de um número natural dado ser livre de quadrados, ou seja, vamos calcular o limite

$$\lim_{n\to\infty}\frac{1}{n}\#\{1\leq k\leq n \mid k \text{ é livre de quadrados}\} = \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}|\mu(k)|.$$

Proposição 3.37. $\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{k=1}^{n}|\mu(k)|=\frac{6}{\pi^2}$.

Demonstração: Seja $g(x)=\lfloor x^2\rfloor$ e $f(x)=\sum_{k\leq x}|\mu(k)|$. Observemos que como um natural n se escreve unicamente como $n=r^2l$ com l livre de quadrados, temos que $\sum_{r\geq 1}f(\frac{x^2}{r^2})=g(x)$. Assim, pela segunda fórmula de inversão de Möbius (teorema 3.12), temos

$$\begin{aligned}f(x^2) &= \sum_{k\leq x}\mu(k)g\Big(\frac{x}{k}\Big)=\sum_{k\leq x}\mu(k)\left\lfloor\frac{x^2}{k^2}\right\rfloor\\ &= \sum_{k\leq x}\frac{\mu(k)x^2}{k^2}+O(x)=\frac{6}{\pi^2}x^2+O(x),\end{aligned}$$

já que $\sum_{k\geq 1}\frac{\mu(k)}{k^2}=6/\pi^2$ (ver a demonstração da proposição 3.28). Se $y=x^2$, temos que $f(y)=\frac{6}{\pi^2}y+O(\sqrt{y})$, o que implica o resultado. □

3.7 As Funções ω e Ω

Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ com $p_1 < p_2 < \cdots < p_k$ primos é a fatoração canônica de n, então $\omega(n) = k$ e $\Omega(n) = \sum_{j=1}^{k} \alpha_j$ são respectivamente o número de fatores primos distintos de n e o número de fatores primos de n com multiplicidade. Vamos provar que, para a "maioria" dos valores de n, $\omega(n)$ e $\Omega(n)$ são da ordem $\log\log n$.

Notemos inicialmente que $\omega(n) \le \Omega(n)$ para todo n e que

$$\Omega(n) = \sum_{k\ge 1} \sum_{\substack{p \text{ primo} \\ p^k \mid n}} 1 \qquad \text{e} \qquad \omega(n) = \sum_{\substack{p \text{ primo} \\ p \mid n}} 1,$$

donde

$$\begin{aligned}
\sum_{r=1}^{n} \Omega(r) - \omega(r) &= \sum_{r=1}^{n} \sum_{k\ge 2} \sum_{\substack{p \text{ primo} \\ p^k \mid r}} 1 = \sum_{k\ge 2} \sum_{p \text{ primo}} \left\lfloor \frac{n}{p^k} \right\rfloor \\
&\le \sum_{p \text{ primo}} \sum_{k\ge 2} \frac{n}{p^k} = \sum_{p \text{ primo}} \frac{n}{p(p-1)} \\
&\le n \sum_{k\ge 2} \Big(\frac{1}{k-1} - \frac{1}{k} \Big) = O(n).
\end{aligned}$$

Para mostrar que $\omega(n)$ é da ordem de $\log\log n$ para a maioria dos n, vamos estimar a soma $\sum_{r=1}^{n} (\omega(r) - \log\log n)^2$. Começamos estimando $\sum_{r=1}^{n} \omega(r)$. Pelo teorema 3.25, temos

$$\sum_{r=1}^{n} \omega(r) = \sum_{\substack{p \text{ primo} \\ p \le n}} \left\lfloor \frac{n}{p} \right\rfloor = n \sum_{\substack{p \text{ primo} \\ p \le n}} \frac{1}{p} + O(n) = n \log\log n + O(n),$$

Vamos agora estimar $\sum_{r=1}^{n} \omega(r)^2$, para isso observemos que

$$\begin{aligned}
\sum_{r=1}^{n} \omega(r)^2 &= \sum_{r=1}^{n} \Big(\sum_{\substack{p \text{ primo} \\ p \mid r}} 1 \Big)^2 \\
&= \sum_{r=1}^{n} \sum_{\substack{p_1, p_2 \text{ primos} \\ p_1 \mid r, p_2 \mid r}} 1 = \sum_{\substack{p \text{ primo} \\ p \le n}} \sum_{\substack{q \text{ primo} \\ q \le n}} \left\lfloor \frac{n}{\operatorname{mmc}(p,q)} \right\rfloor \\
&= \sum_{\substack{p \text{ primo} \\ p \le n}} \left\lfloor \frac{n}{p} \right\rfloor + \sum_{\substack{p,q \text{ primos} \\ p \ne q}} \left\lfloor \frac{n}{pq} \right\rfloor = \sum_{r=1}^{n} \omega(r) + \sum_{\substack{p,q \text{ primos} \\ p \ne q}} \left\lfloor \frac{n}{pq} \right\rfloor.
\end{aligned}$$

Note que $\sum_{\substack{p,q \text{ primos} \\ p \ne q}} \lfloor \frac{n}{pq} \rfloor \le n \Big(\sum_{\substack{p \text{ primo} \\ p \le n}} \frac{1}{p} \Big)^2 = n(\log\log n)^2 + O(n \log\log n)$. Por outro lado,

$$\begin{aligned}
\sum_{\substack{p,q \text{ primos} \\ p \ne q}} \left\lfloor \frac{n}{pq} \right\rfloor &= \sum_{\substack{p,q \text{ primos} \\ p \ne q, pq \le n}} \frac{n}{pq} + O(n) \\
&\ge n \Big(\sum_{\substack{p \text{ primos} \\ p \le \sqrt{n}}} \frac{1}{p} \Big)^2 + O(n) = n(\log\log \sqrt{n} + O(1))^2 + O(n) \\
&= n(\log\log n)^2 + O(n \log\log n).
\end{aligned}$$

Portanto $\sum_{r=1}^{n} \omega(r)^2 = n(\log\log n)^2 + O(n \log\log n)$.

Assim, temos que

$$\begin{aligned}\sum_{r=1}^{n}(\omega(r)-\log\log n)^2 &= \sum_{r=1}^{n}\omega(r)^2 - 2\log\log n\sum_{r=1}^{n}\omega(r) + n(\log\log n)^2\\ &= n(\log\log n)^2 + O(n\log\log n)\\ &\quad - 2\log\log n\cdot\big(n\log\log n + O(n)\big) + n(\log\log n)^2\\ &= O(n\log\log n).\end{aligned}$$

Definição 3.38. *Seja $f, g\colon \mathbb{N}\to\mathbb{R}$. Dizemos que a* ordem normal *de $f(n)$ é $g(n)$ se podemos decompor $\mathbb{N} = A\cup B$ de modo que*

$$\lim_{n\to\infty}\frac{\#\{k\in B\mid k\le n\}}{n} = 0 \qquad e \qquad \lim_{\substack{n\to\infty\\ n\in A}}\frac{f(n)}{g(n)} = 1.$$

Observe que esta partição de $\mathbb{N}$ implica que A contém quase todos os números naturais.

Em particular, dado $\alpha > 0$, $B(n) = \{r\le n \mid |\omega(r)-\log\log n| \ge (\log\log n)^{\frac{1}{2}+\alpha}\}$ é tal que $\#B(n) = O(n/(\log\log n)^{2\alpha})$. Temos assim que a ordem normal de $\omega(n)$ (e de $\Omega(n)$ pois $\sum_{k\le n}|\Omega(k)-\omega(k)| = O(n)$) é $\log\log n$.

Erdős e Kac provaram em [5] que a distribuição de probabilidade de $\frac{\omega(n)-\log\log n}{\sqrt{\log\log n}}$, $n\in\mathbb{N}$, é a distribuição normal usual. Mais precisamente, dados $a, b\in\mathbb{R}$ com $a<b$, temos

$$\lim_{n\to\infty}\frac{1}{n}\#\left\{k\le n\mid a\le\frac{\omega(k)-\log\log k}{\sqrt{\log\log k}}\le b\right\} = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-t^2/2}dt.$$

3.8 A Função Número de Divisores $d(n)$

A função $d(n) = \sum_{d\mid n}1$ tem um comportamento bastante irregular. Temos que $d(p) = 2$ para todo primo p, donde $\liminf_{n\to\infty} d(n) = 2$. Por outro lado podemos estimar a ordem máxima de $d(n)$.

Proposição 3.39. *Se $\epsilon > 0$ então*

$$\lim_{n\to\infty}\frac{d(n)}{2^{(1+\epsilon)\log n/\log\log n}} = 0 \qquad e \qquad \limsup_{n\to\infty}\frac{d(n)}{2^{(1-\epsilon)\log n/\log\log n}} = +\infty.$$

Demonstração: Para a primeira afirmação, basta mostrar que

$$\log d(n)\le(1+\epsilon')\frac{\log 2\log n}{\log\log n}$$

para algum ϵ' tal que $0<\epsilon'<\epsilon$. Para isto, considere a fatoração canônica em primos $n{=}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, de modo que $d(n){=}\prod_{i=1}^{k}(1{+}\alpha_i)$. Temos

$$\log d(n) = \sum_{i=1}^{k}\log(1+\alpha_i) \qquad \text{e} \qquad \log n = \sum_{i=1}^{k}\alpha_i\log p_i.$$

Seja $\delta > 0$. Dividimos em dois casos: primeiro, se $p_i\ge(\log n)^{1-\delta}$, temos $\log p_i\ge(1-\delta)\log\log n$, e como $2^{\alpha_i}\ge 1+\alpha_i \iff \alpha_i\log 2\ge\log(1+\alpha_i)$,

$$\log(1+\alpha_i)\le\alpha_i\log 2\le(1-\delta)^{-1}\frac{\log 2\cdot\alpha_i\log p_i}{\log\log n}.$$

Segundo, se $p_i < (\log n)^{1-\delta}$, como $2^{\alpha_i} \le n \implies \alpha_i \le \log n / \log 2 \implies \log(1+\alpha_i) \le 2 \log\log n$ para $n \gg 0$, temos

$$\sum_{p_i < (\log n)^{1-\delta}} \log(1+\alpha_i) \le 2(\log n)^{1-\delta} \log\log n = o\left(\frac{\log n}{\log\log n}\right).$$

Somando sobre todos os primos, temos portanto

$$\begin{aligned}
\log d(n) &= \sum_{1\le i\le k} \log(1+\alpha_i) \\
&\le (1-\delta)^{-1} \frac{\log 2 \cdot \sum_{1\le i\le k} \alpha_i \log p_i}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right) \\
&\le \big((1-\delta)^{-1} + \delta\big) \frac{\log 2 \cdot \log n}{\log\log n},
\end{aligned}$$

o que implica nossa afirmação para $n \gg 0$ e δ suficientemente pequeno.

Para a segunda afirmação, considere o produto $n_k = p_1 p_2 \cdots p_k$ dos k primeiros primos. Basta mostrar que

$$\log d(n_k) - (1-\epsilon) \frac{\log 2 \log n_k}{\log\log n_k} \to \infty$$

quando $k \to \infty$. Temos $d(n_k) = 2^k$ donde $\log d(n_k) = k \log 2$. Por outro lado, pelo corolário 3.17, temos

$$\log n_k = \sum_{j=1}^{k} \log p_j = \sum_{j=1}^{k} \log O(j \log j) = k \log k + O(k \log\log k)$$

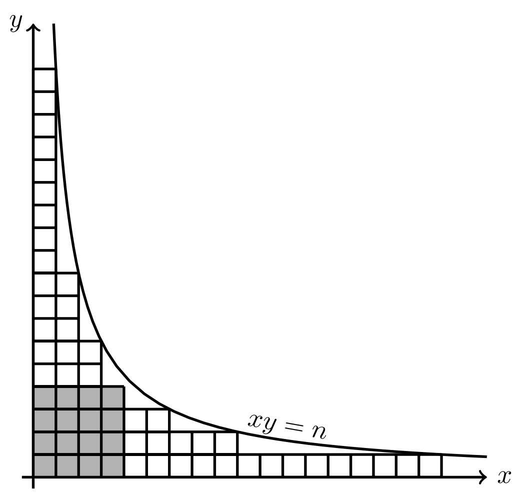
de modo que $\log n_k = \big(1 + o(1)\big) k \log k$, $\log\log n_k = \big(1+o(1)\big) \log k$ e assim $\frac{\log n_k}{\log\log n_k} = \big(1+o(1)\big)k$, o que implica o resultado. □

Vamos agora calcular a ordem média de $d(n)$.

Proposição 3.40. $\frac{1}{n}\sum_{k=1}^{n} d(k) = \log n + 2\gamma - 1 + O\big(\frac{1}{\sqrt{n}}\big)$ *onde γ é a constante de Euler-Mascheroni*

Demonstração: Temos

$$\sum_{k=1}^{n} d(k) = \sum_{k=1}^{n} \sum_{d\mid k} 1 = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor = n \sum_{d=1}^{n} \frac{1}{d} + O(n) = n \log n + O(n).$$



Podemos estimar o termo de erro de forma mais precisa, contando os pontos de coordenadas inteiras sob o gráfico de $y = n/x$, conforme a figura:

$$\begin{aligned}
\sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor &= \#\{(x,y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid xy \le n\} \\
&= \#\{(x,y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid x \le \sqrt{n}, xy \le n\} \\
&\quad + \#\{(x,y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid y \le \sqrt{n}, xy \le n\} \\
&\quad - \#\{(x,y) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \mid x \le \sqrt{n}, y \le \sqrt{n}\} \\
&= 2 \sum_{d=1}^{\lfloor \sqrt{n} \rfloor} \left\lfloor \frac{n}{d} \right\rfloor - \lfloor \sqrt{n} \rfloor^2 = 2\Big(n \sum_{d=1}^{\lfloor \sqrt{n} \rfloor} \frac{1}{d} + O(\sqrt{n})\Big) - \Big(\sqrt{n} + O(1)\Big)^2 \\
&= 2n\Big(\log \sqrt{n} + \gamma + O\Big(\frac{1}{\sqrt{n}}\Big)\Big) - n + O(\sqrt{n}) \\
&= n \log n + (2\gamma - 1)n + O(\sqrt{n})
\end{aligned}$$

utilizando a estimativa mais precisa $\sum_{1 \le j \le n} \frac{1}{j} = \log n + \gamma + O(\frac{1}{n})$. □

Observação 3.41. *É possível dar estimativas mais precisas para o termo de erro nesta proposição. Seja* $\Delta(n) := \sum_{k=1}^{n} d(k) - n(\log n + 2\gamma - 1)$. *A proposição anterior (que é devida a Dirichlet) diz que* $\Delta(n) = O(n^{1/2})$. *O problema dos divisores de Dirichlet consiste em determinar o menor* $\theta \in \mathbb{R}$ *tal que* $\Delta(n) = O(n^{\theta+\varepsilon}), \forall \varepsilon > 0$. *Hardy provou em [7] que* $\theta \ge \frac{1}{4}$: *de fato, ele mostrou que existe* $c > 0$ *tal que, para certos valores arbitrariamente grandes de* n, $\Delta(n) > cn^{1/4}$, *e, para outros valores arbitrariamente grandes de* n, $\Delta(n) < -cn^{1/4}$. *Por outro lado, Huxley provou em [11] que* $\theta \le \frac{131}{416} = 0{,}31490384615384615384615\ldots$. *Conjetura-se que* $\theta = 1/4$.

Finalmente, para quase todo $n \in \mathbb{N}$, $\omega(n)$ e $\Omega(n)$ são da ordem de $\log \log n$ pela seção anterior, donde, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ é a fatoração canônica de n,

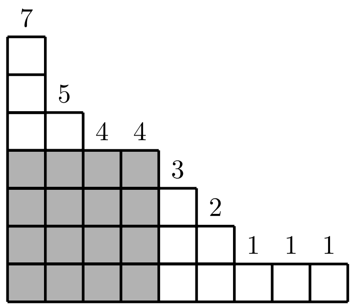
$$2^{\omega(n)} = 2^k \le \prod_{j=1}^{k} (1 + \alpha_j) = d(n) \le \prod_{j=1}^{k} 2^{\alpha_j} = 2^{\Omega(n)}.$$

Assim, $\log d(n)$ é da ordem de $\log 2 \cdot \log \log n$ para quase todo n, ou seja, $d(n) = (\log n)^{\log 2} \ll \log n$ para quase todo n, apesar de a ordem média de $d(n)$ ser $\log n$. Isso se deve ao fato de, para alguns poucos valores de n, $d(n)$ ser muito maior que $\log n$, lembrando que a ordem máxima de $d(n)$ é $2^{(1+o(1)) \log n / \log \log n} \gg \log n$, para todo $n \in \mathbb{N}$. De fato, Ramanujam mostrou que, para $r \ge 1$, esse efeito faz com que $\sum_{k=1}^{n} (d(k))^r$ seja da ordem $C(r) n (\log n)^{2^r - 1}$ para uma certa constante $C(r) \in (0, \infty)$.

3.9 A Função Número de Partições $p(n)$

Uma *partição* de um inteiro positivo n é uma forma de escrever n como soma de inteiros positivos, não importando a ordem. Assim, podemos identificar uma partição de n com um vetor $(a_1, a_2, \ldots, a_k)$, onde $k, a_1, a_2, \ldots, a_k$ são inteiros positivos, $a_1 \ge a_2 \ge \cdots \ge a_k$ e $a_1 + a_2 + \cdots + a_k = n$. Para cada inteiro positivo n, denotamos por $p(n)$ o número de partições distintas de n. Por exemplo, como as formas de escrever 6 como soma de inteiros positivos são $6 = 5+1 = 4+2 = 4+1+1 = 3+3 = 3+2+1 = 3+1+1+1 = 2+2+2 = 2+2+1+1 = 2+1+1+1+1 = 1+1+1+1+1+1$, temos $p(6) = 11$.

Uma partição pode ser representada por uma pilha de quadradinhos onde a altura de cada coluna da pilha é monótona não crescente da esquerda para a direita. Uma convenção é de que as alturas das colunas são os inteiros $a_1 \geq a_2 \geq \cdots \geq a_k$. Na figura mostramos a partição $7+5+4+4+3+2+1+1+1$ de 28.



Não é muito fácil estimar com precisão a ordem de magnitude da função $p(n)$. Começamos mostrando as seguintes estimativas elementares, análogas às estimativas mostradas em [10]:

Proposição 3.42. $2^{\lfloor\sqrt{2n}\rfloor-2} \leq p(n) \leq \lfloor\sqrt{n}\rfloor n^{2\lfloor\sqrt{n}\rfloor}, \forall n \geq 1.$

DEMONSTRAÇÃO: Essas desigualdades são claramente válidas para $n=1$. Vamos supor a partir de agora que $n>1$. A primeira desigualdade pode ser mostrada considerando as partições obtidas da seguinte forma: Escolhemos k um número natural tal que $1+2+\cdots+k+(k+1) \leq n$ (para isto basta tomar $k=\lfloor\sqrt{2n}\rfloor-2$ para $n \geq 2$). Para cada conjunto $A=\{a_1,a_2,\dots,a_r\} \subset \{1,2,\dots,k\}$, podemos associar a partição

$$n = a_1+a_2+\cdots+a_r+(n-a_1-a_2-\cdots-a_r).$$

Note que $n-(a_1+a_2+\cdots+a_r) \geq n-(1+2+\cdots+k) \geq k+1$ é o maior termo da partição, o que mostra que, para $n \geq 3$, a subconjuntos distintos de $\{1,2,\dots,k\}$ correspondem partições distintas, e como há $2^k = 2^{\lfloor\sqrt{2n}\rfloor-2}$ subconjuntos de $\{1,2,\dots,k\}$, segue que $p(n) \geq 2^{\lfloor\sqrt{2n}\rfloor-2}$ para $n \geq 2$, e a primeira desigualdade está provada.

Já para a segunda desigualdade, a cada partição $\pi=(a_1,a_2,\dots,a_k)$ de n, com $a_1 \geq a_2 \geq \cdots \geq a_k$, associamos o maior inteiro positivo $q=q(\pi)$ tal que $a_q \geq q$. Em outras palavras, $q(\pi)$ é o lado do maior quadrado contido no diagrama da partição: no exemplo da figura anterior, $q(\pi)=4$ (e o quadrado está sombreado). Note que $q(\pi)^2 \leq n$. Assim, há $\lfloor\sqrt{n}\rfloor$ possibilidades para $q(\pi)$.

Por outro lado, uma vez determinado $q(\pi)$, temos que $a_1,\dots,a_{q(\pi)} \geq q(\pi)$ satisfazem as desigualdades $0 \leq a_i < n, \forall i \leq q(\pi)$, que têm (esquecendo o fato de que os a_i estão em ordem decrescente) no máximo $n^{q(\pi)} \leq n^{\lfloor\sqrt{n}\rfloor}$ soluções (pois há no máximo n possibilidades para cada a_i). Além disso, como $a_j \leq q(\pi), \forall j > q(\pi)$, os a_j, para $j > q(\pi)$ estão unicamente determinados pelos números $b_i, 1 \leq i \leq q(\pi)$ dados por $b_i = |\{j > q(\pi); a_j \geq i\}|, 1 \leq i \leq q(\pi)$, os quais satisfazem $\sum\limits_{i \leq q(\pi)} b_i = \sum\limits_{j > q(\pi)} a_j < n$, e assim, como antes, há no máximo $n^{q(\pi)} \leq n^{\lfloor\sqrt{n}\rfloor}$ possibilidades para os $b_i, 1 \leq i \leq q(\pi)$ e portanto para os $a_j, j > q(\pi)$. Assim, temos

$$p(n) \leq \sum_{1 \leq q \leq \lfloor\sqrt{n}\rfloor} (n^q)^2 \leq \lfloor\sqrt{n}\rfloor (n^{\lfloor\sqrt{n}\rfloor})^2 = \lfloor\sqrt{n}\rfloor \cdot n^{2\lfloor\sqrt{n}\rfloor}.$$

$\square$

Para estimativas um pouco mais precisas, vamos usar a *função geratriz* de $p(n)$. Note que $p(n)$ é o número de soluções $(m_1, m_2, m_3, \dots)$ com os m_k inteiros não negativos de $\sum_{k\geq 1} km_k = n$. Assim, convencionando $p(0) = 1$, temos a igualdade seguinte:

$$\sum_{n\geq 0} p(n)x^n = \prod_{k\geq 1}\Big(\sum_{m\geq 0} x^{km}\Big) = \prod_{k\geq 1}\Big(\frac{1}{1-x^k}\Big).$$

A igualdade em princípio é formal mas a estimativa acima garante a convergência se $|x| < 1$. Assim, para todo $N \in \mathbb{N}$, e todo $x \in [0, 1)$,

$$\sum_{n\geq 0}^{N} p(n)x^n \leq \prod_{k=1}^{N}\Big(\sum_{m\geq 0} x^{km}\Big) = \prod_{k=1}^{N}\Big(\frac{1}{1-x^k}\Big).$$

Usaremos esses fatos para provar o seguinte

Teorema 3.43. *Para todo $N \in \mathbb{N}$, temos $p(N) \leq e^{\pi\sqrt{2N/3}}$. Além disso,* $\lim\limits_{n\to+\infty} \frac{\log p(n)}{\sqrt{n}} = \pi\sqrt{\frac{2}{3}}$.

Demonstração: Da discussão anterior, temos que, para todo $x > 0$,

$$p(N)x^N \leq \sum_{n\geq 0}^{N} p(n)x^n \leq \prod_{k\geq 1}^{N}\Big(\frac{1}{1-x^k}\Big) \leq \prod_{k\geq 1}\Big(\frac{1}{1-x^k}\Big).$$

Tomando $x{=}e^{-\varepsilon}$, com $\varepsilon > 0$, obtemos $p(N)e^{-\varepsilon N}{\leq} \prod\limits_{k\geq 1}(\frac{1}{1-e^{-\varepsilon k}})$, donde $\log p(N) - \varepsilon N \leq \sum\limits_{k\geq 1} -\log(1-e^{-\varepsilon k})$. Temos que $\varepsilon \sum\limits_{k\geq 1} -\log(1-e^{-\varepsilon k})$ é a soma inferior de Riemann associada à partição $\{0, \varepsilon, 2\varepsilon, 3\varepsilon, \dots\}$ para a integral $\int_0^\infty -\log(1-e^{-t})dt = \frac{\pi^2}{6}$ (essa última igualdade segue de

$$\begin{aligned}\int_0^\infty -\log(1-e^{-t})dt &= \int_0^\infty \Big(\sum_{n\geq 1} e^{-nt}/n\Big)dt \\ &= \sum_{n\geq 1}\frac{1}{n}\int_0^\infty e^{-nt}dt = \sum_{n\geq 1}\frac{1}{n^2} = \frac{\pi^2}{6},\end{aligned}$$

sendo a troca da ordem da soma e da integral justificada pelo fato de os termos serem todos positivos), e logo $\varepsilon \sum\limits_{k\geq 1} -\log(1-e^{-\varepsilon k}) \leq \frac{\pi^2}{6}$.

Assim, $\log p(N) - \varepsilon N \leq \sum\limits_{k\geq 1} -\log(1-e^{-\varepsilon k}) \leq \frac{\pi^2}{6\varepsilon}$, donde $\log p(N) \leq \varepsilon N + \frac{\pi^2}{6\varepsilon}$, para todo $\varepsilon > 0$. Escolhendo $\varepsilon = \frac{\pi}{\sqrt{6N}}$, obtemos

$$\log p(N) \leq 2\pi\sqrt{\frac{N}{6}} = \pi\sqrt{\frac{2N}{3}},$$

o que prova a primeira parte do teorema.

Da estimativa da proposição 3.42 (ou da primeira parte do teorema) e da discussão sobre a função geratriz de $p(n)$ segue que, $\forall x{\in}[0,1)$, a série $\sum\limits_{n\geq 0} p(n)x^n$ converge e vale a igualdade $\sum\limits_{n\geq 0} p(n)x^n = \prod\limits_{k\geq 1}(\frac{1}{1-x^k})$. Vamos tomar $x = e^{-\varepsilon}$, onde $\varepsilon = \frac{\pi}{\sqrt{6m}}$ ($m \gg 1$ vai ser escolhido posteriormente). Temos $\log \prod\limits_{k\geq 1}(\frac{1}{1-e^{-\varepsilon k}}) =$

$\sum\limits_{k\geq 1} -\log(1-e^{-\varepsilon k}) \leq \frac{\pi^2}{6\varepsilon}$, como acima, e, por outro lado, como $\varepsilon \sum\limits_{k\geq 1} -\log(1-e^{-\varepsilon k})$ é a soma superior de Riemann associada à partição $\{\varepsilon, 2\varepsilon, 3\varepsilon, \dots\}$ para a integral

$$\int_\varepsilon^\infty -\log(1-e^{-t})dt = \frac{\pi^2}{6} - O(\varepsilon \log \varepsilon^{-1}),$$

temos

$$\log \prod_{k\geq 1} \left(\frac{1}{1-e^{-\varepsilon k}}\right) = \frac{\pi^2}{6\varepsilon} - O(\log \varepsilon^{-1}) = \pi\sqrt{\frac{m}{6}} - O(\log m),$$

e portanto $\sum\limits_{n\geq 0} p(n)x^n = \exp\bigl(\pi\sqrt{\frac{m}{6}} - O(\log m)\bigr)$.

Por outro lado, temos, para cada $n \in \mathbb{N}$,

$$\begin{aligned} p(n)x^n &= p(n)\exp(-\varepsilon n) \leq \exp\bigl(-\varepsilon n + \pi\sqrt{2n/3}\bigr) \\ &= \exp\Bigl(\pi\Bigl(-\frac{n}{\sqrt{6m}} + \sqrt{2n/3}\Bigr)\Bigr) = \exp\Bigl(\frac{\pi}{\sqrt{6m}}\Bigl(2\sqrt{mn} - n\Bigr)\Bigr) \\ &= \exp\Bigl(\frac{\pi}{\sqrt{6m}}\bigl(m - (\sqrt{n} - \sqrt{m})^2\bigr)\Bigr). \end{aligned}$$

Tomando $m = N - N^{5/6}$ e $n = N + k$, $k \geq 0$,

$$\sqrt{n} - \sqrt{m} = \frac{n-m}{\sqrt{n}+\sqrt{m}} > \frac{N^{5/6}+k}{2\sqrt{N+k}} > \frac{N^{1/3}}{2} + \frac{1}{3}\sqrt{\frac{k}{N}},$$

e logo

$$\begin{aligned} p(n)x^n &\leq \exp\left(\frac{\pi}{\sqrt{6m}}\left(m - \left(\frac{N^{1/3}}{2} + \frac{1}{3}\sqrt{\frac{k}{N}}\right)^2\right)\right) \\ &< \exp\left(\frac{\pi}{\sqrt{6m}}\left(m - \left(\frac{N^{2/3}}{4} + \frac{k}{9N}\right)\right)\right). \end{aligned}$$

Assim,

$$\begin{aligned} \sum_{n\geq N} p(n)x^n &< \exp\left(\pi\sqrt{\frac{m}{6}}\right)\exp\left(-\frac{\pi m^{1/6}}{4\sqrt{6}}\right)\sum_{k\geq 0}\exp\left(-\frac{\pi k}{9N\sqrt{6m}}\right) \\ &= O\left(\exp\left(\pi\sqrt{\frac{m}{6}}\right)\exp\left(-\frac{\pi m^{1/6}}{4\sqrt{6}}\right)N\sqrt{m}\right) \\ &= o\left(\exp\left(\pi\sqrt{\frac{m}{6}} - \frac{\pi m^{1/6}}{10}\right)\right). \end{aligned}$$

Analogamente, se $n \leq N - 2N^{5/6} = m - N^{5/6}$,

$$\sqrt{m} - \sqrt{n} = \frac{m-n}{\sqrt{n}+\sqrt{m}} > \frac{N^{5/6}}{2\sqrt{N}} = \frac{N^{1/3}}{2} > \frac{m^{1/3}}{2},$$

donde

$$p(n)x^n \leq \exp\left(\frac{\pi}{\sqrt{6m}}\left(m - \frac{m^{2/3}}{4}\right)\right) = \exp\left(\pi\sqrt{\frac{m}{6}}\right)\exp\left(-\frac{\pi m^{1/6}}{4\sqrt{6}}\right).$$

Assim,

$$\begin{aligned} \sum_{n\leq N-2N^{5/6}} p(n)x^n &< N\exp\left(\pi\sqrt{\frac{m}{6}}\right)\exp\Bigl(-\frac{\pi m^{1/6}}{4\sqrt{6}}\Bigr) \\ &= o\left(\exp\left(\pi\sqrt{\frac{m}{6}} - \frac{\pi m^{1/6}}{10}\right)\right). \end{aligned}$$

Portanto, como $\sum_{n\ge 0} p(n)x^n = \exp(\pi\sqrt{\frac{m}{6}} - O(\log m))$, temos

$$\sum_{n\ge N} p(n)x^n = o\Big(\sum_{n\ge 0} p(n)x^n\Big), \quad \sum_{n\le N-2N^{5/6}} p(n)x^n = o\Big(\sum_{n\ge 0} p(n)x^n\Big),$$

donde $\sum_{n=N-2N^{5/6}}^{N-1} p(n)x^n > \frac{1}{2}\sum_{n\ge 0} p(n)x^n$, e portanto existe k com

$$N - 2N^{5/6} \le k \le N-1, \qquad p(k)x^k > \frac{1}{4N^{5/6}}\sum_{n\ge 0} p(n)x^n,$$

donde

$$\begin{aligned}\log p(k) - \frac{k\pi}{\sqrt{6m}} &= \log p(k) + k\log x\\ &> \log\sum_{n\ge 0} p(n)x^n - \log(4N^{5/6}) = \pi\sqrt{\frac{m}{6}} - O(\log m),\end{aligned}$$

e portanto

$$\begin{aligned}\log p(k) &> \pi\sqrt{\frac{m}{6}} - O(\log m) + \frac{k\pi}{\sqrt{6m}}\\ &= \pi\sqrt{\frac{m}{6}} - O(\log m) + \big(m - O(m^{5/6})\big)\frac{\pi}{\sqrt{6m}}\\ &= \pi\sqrt{\frac{2m}{3}} - O(m^{1/3}).\end{aligned}$$

Como $p(n)$ é crescente,

$$\log p(N) \ge \log p(k) > \pi\sqrt{\frac{2m}{3}} - O\big(m^{1/3}\big) = \pi\sqrt{\frac{2N}{3}} - O\big(N^{1/3}\big).$$

Junto com a estimativa da primeira parte do teorema, isto implica a segunda afirmação do teorema.

□

Com métodos mais sofisticados, Hardy e Ramanujan provaram em [9] que $\lim_{n\to\infty} 4n\sqrt{3}\cdot p(n)\exp(-\pi\sqrt{2n/3}) = 1$.

Posteriormente, Rademacher provou em [18] um resultado ainda mais preciso, que fornece, para cada inteiro positivo n, uma série que converge a $p(n)$. Para cada inteiro positivo k, seja

$$A_k(n) = \sum_{\substack{1\le h\le k\\ \mathrm{mdc}(h,k)=1}} \exp\left(\pi i s(h,k) - 2\pi i\frac{nh}{k}\right)$$

onde

$$s(h,k) = \sum_{j=1}^{k-1} \frac{j}{k}\left(\left\{\frac{hj}{k}\right\} - \frac{1}{2}\right)$$

(lembre que $\{x\} = x - \lfloor x\rfloor$). Então

$$p(n) = \frac{1}{\pi\sqrt{2}}\sum_{k=1}^{\infty} A_k(n)\sqrt{k}\frac{d}{dn}\left(\frac{\sinh\left(\pi\sqrt{\frac{2}{3}(n-1/24)}/k\right)}{\sqrt{n-1/24}}\right).$$

Aqui a notação $\frac{d}{dn}$ significa derivada em relação a n, considerando a expressão acima definida para todo número real $n \geq 1$. Estimativas cuidadosas mostram que este resultado implica que, para todo $n \geq 576$, $p(n)$ é o inteiro mais próximo a

$$\frac{1}{2\pi\sqrt{2}} \sum_{k=1}^{\lfloor 2\sqrt{n}/3 \rfloor} A_k(n)\sqrt{k}\frac{d}{dn}\left(\frac{\exp\left(\pi\sqrt{\frac{2}{3}(n-1/24)}/k\right)}{\sqrt{n-1/24}}\right).$$

É possível mostrar que o erro da aproximação acima de $p(n)$ é $O(n^{-3/8})$ (veja o capítulo 14 de [19]).

3.10 A Função Custo Aritmético $\tau(n)$

O custo de um número inteiro é definido como o número mínimo de operações aritméticas necessárias para obter esse inteiro a partir de 1. Mais precisamente, dado $k \in \mathbb{N}$, definimos $\tau(k)$ como o menor $m \in \mathbb{N}$ para o qual existe uma sequência $(s_0, s_1, \dots, s_m)$ onde $s_0 = 1$, $s_m = k$ e para cada $l \geq 1$, existem i, j com $0 \leq i, j < l$ com $s_l = s_i * s_j$, onde $* \in \{+, -, \cdot\}$. Essa função tem um papel importante em [24], e também é estudada em [13]. Esta seção é baseada em [15].

Não é difícil ver que $|\tau(n) - \tau(-n)| \leq 2$ para todo $n \in \mathbb{Z}$. Vamos nos restringir ao caso $n \in \mathbb{N}$, e queremos dar estimativas assintóticas para $\tau(n)$, $n \in \mathbb{N}$.

Proposição 3.44. $\log_2 \log_2 n + 1 \leq \tau(n) \leq 2\log_2 n$.

DEMONSTRAÇÃO: Dada a sequência $(s_0, \dots, s_m)$ como na definição de $\tau(n)$ temos que $s_k \leq 2^{2^{k-1}}$ para todo $k \geq 1$, de fato, isso segue por indução de $s_k \leq \max\{2s, s^2\}$, onde $s = \max\{|s_j| : j < k\}$. Por outro lado, como $\tau(2n) \leq \tau(n) + 1$ e $\tau(2n + 1) \leq \tau(n) + 2$ para todo $n \in \mathbb{N}$, por indução segue que $\tau(n) \leq 2\log_2 n$ para todo $n \geq 1$, assim temos a segunda desigualdade. A primeira desigualdade não pode ser melhorada para todo $n \in \mathbb{N}$ grande já que $\tau(2^{2^k}) = k + 1$ para todo $k \in \mathbb{N}$. □

Vamos provar que $\tau(n) > \frac{\log n}{\log\log n}$ para quase todo $n \in \mathbb{N}$. Mas precisamente, temos

Teorema 3.45. *Dado $\epsilon > 0$ temos que*

1. $\tau(n) \geq \frac{\log n}{\log\log n} + (1-\epsilon)\frac{\log n \cdot \log\log\log n}{(\log\log n)^2}$ *para quase todo* $n \in \mathbb{N}$
2. $\tau(n) \leq \frac{\log n}{\log\log n} + (3+\epsilon)\frac{\log n \cdot \log\log\log n}{(\log\log n)^2}$ *para* $n \in \mathbb{N}$ *suficientemente grande.*

Na verdade o mesmo resultado vale se tivéssemos um número arbitrário de operações binárias, incluindo $+, \cdot$. Vamos dividir a prova do teorema acima nos seguintes resultados

Proposição 3.46. *Suponha que temos s operações binárias na definição de τ. Então $N(k) = \#\{n \in \mathbb{N} \mid \tau(n) \leq k\}$ satisfaz $N(k) \leq A^k \cdot k^k$, para uma certa constante $A = A(s) > 0$.*

DEMONSTRAÇÃO: Seja $\Lambda = \{*_1, \dots, *_s\}$ o conjunto de operações. Se $\tau(n) = k$ então existe $(s_0, \dots, s_k)$ com $s_0 = 1$, $s_k = n$, e para cada $l \geq 1$ existem $t_l \leq s$, i_l, j_l com $0 \leq i_l, j_l < l$ tais que $s_l = s_{i_l} *_{t_l} s_{j_l}$. Devemos ter $\{i_1, j_1, i_2, j_2, \dots, i_k, j_k\} = \{0, 1, \dots, k-1\}$, se não teríamos criado um s_i desnecessário, e logo $\tau(n) < k$. Além disso, se $(r_1, \dots, r_{2k}) = (i_1, j_1, \dots, i_k, j_k)$, podemos supor que existe uma sequência $1 \leq l_1 < l_2 < \dots < l_k \leq 2k$ tal que $r_{l_i} = i - 1$, para $1 \leq i \leq k$. De fato, se $P(j) = \min\{i \mid r_i = j\}$ podemos supor sem perda de generalidade que $P(0) < P(1) < \cdots < P(k-1)$, já que caso contrário, se $P(j) > P(j+1)$, então s_j não é usado para criar s_{j+1}, e portanto s_{j+1} pode ser criado antes de s_j. Assim, escolhendo $(s_0, s_1, \dots, s_k)$ com $M = \max\{m \geq 1 \mid P(j) < P(j+1), \forall j < m\}$ máximo, devemos ter $M = k-1$, pois, caso contrário, $P(M) > P(M+1)$ e, trocando as posições de s_{M+1} e s_M, aumentaríamos o valor de M, o que é uma contradição. Podemos então tomar $l_i = P(i)$, para $0 \leq i \leq k-1$.

Seja $N'(k) = \#\{n \in \mathbb{N} \mid \tau(n) = k\}$. Pelos argumentos acima, segue que $N'(k) \leq s^k N''(k)$, onde

$$N''(k) = \#\left\{(r_1, \dots, r_{2k}) \left| \begin{array}{l} r_i \in \{0, 1, \dots, k-1\} \text{ e existe uma sequência} \\ 1 \leq l_1 < \cdots < l_k \leq 2k \text{ com } r_{l_j} = j-1 \text{ para} \\ j = 1, \dots k \end{array} \right.\right\}$$

Por outro lado, $N''(k) \leq \binom{2k}{k} k^k < 2^{2k} \cdot k^k = (4k)^k$, donde $N'(k) \leq (4sk)^k$. Portanto $N(k) \leq \sum_{r=0}^{k} N'(r) \leq (4s+1)^k \cdot k^k$. $\square$

Corolário 3.47. *Dado $\epsilon > 0$, temos, para quase todo $n \in \mathbb{N}$, $\tau(n) \geq f(n)$ onde*

$$f(n) = \frac{\log n}{\log\log n} + (1-\epsilon)\frac{\log n \cdot \log\log\log n}{(\log\log n)^2}$$

Demonstração: Vamos estimar $B(n) = \#\{k \leq n \mid \tau(k) \leq f(k)\}$. Se $k \in B(n)$ então $\tau(k) \leq f(k) \leq f(n)$, e, pela proposição acima, temos no máximo $N(f(n)) \leq (Af(n))^{f(n)}$ naturais k com essa propriedade, onde $A = 4s+1$, mas então para n grande, $\#B(n)$ é menor ou igual a

$$\begin{aligned}
&(Af(n))^{f(n)} = \exp\big(f(n)\log(Af(n))\big) \\
&< \exp\left(f(n)\log\left(\frac{\log n}{(\log\log n)^{1-\epsilon/2}}\right)\right) \\
&= \exp\left(\frac{\log n}{\log\log n}\Big(1 + \frac{(1-\epsilon)\log\log\log n}{\log\log n}\Big) \times\right. \\
&\qquad \left.\times \Big(\log\log n - \big(1-\frac{\epsilon}{2}\big)\log\log\log n\Big)\right) \\
&\leq \exp\left(\log n - \frac{\epsilon}{2}\frac{\log n \cdot \log\log\log n}{\log\log n}\right) \\
&= n \cdot \exp\left(-\frac{\epsilon}{2}\frac{\log n \cdot \log\log\log n}{\log\log n}\right) = o(n).
\end{aligned}$$

$\square$

Se tivermos operações p-árias em vez de operações binárias ($p \geq 2$) temos um resultado análogo trocando $N(k) \leq A^k \cdot k^k$ por $N(k) \leq A^k \cdot k^{(p-1)k}$ no enunciado da proposição 3.46 e $f(n)$ por $\frac{f(n)}{p-1}$ no corolário.

Vamos agora obter a estimativa superior do teorema, usando somente as operações $+$ e $\cdot$.

Proposição 3.48. *Dado $\epsilon > 0$, temos, para n suficientemente grande, $\tau(n) \leq g(n)$ onde*

$$g(n) = \frac{\log n}{\log\log n} + (3+\epsilon)\frac{\log n \cdot \log\log\log n}{(\log\log n)^2}.$$

Demonstração: Sejam $B = \lfloor \frac{\log n}{(\log\log n)^3} \rfloor$ e $C = B^k$, onde $k = \lfloor \log\log n \rfloor$. Nos cálculos a seguir vamos omitir as partes inteiras. Tome

$$\begin{array}{cccc}
s_0 = 1, & s_1 = 2, & \dots & s_{B-2} = B-1, \\
s_{B-1} = B, & s_B = 2B, & \dots & s_{2B-3} = (B-1)B \\
 & & \vdots & \\
s_{(k-1)(B-1)} = B^{k-1}, & s_{(k-1)(B-1)+1} = 2B^{k-1} & \dots & s_{k(B-1)-1} = (B-1)B^{k-1} \\
s_{k(B-1)} = B^k & & &
\end{array}$$

Considere agora a representação de n na base C, isto é

$$\begin{aligned}
n &= a_0 + a_1 C + \cdots + a_r C^r, \quad 0 \le a_i \le C-1, \\
r &= \left\lfloor \frac{\log n}{\log C} \right\rfloor \sim \frac{\log n}{(\log\log n)^2},
\end{aligned}$$

e as representações dos a_i na base B

$$a_i = b_{i1} + b_{i2}B + \cdots + b_{ik}B^{k-1} \text{ onde } 0 \le b_{ij} \le B-1.$$

Observe agora que já construímos os números $b_{ij}B^{j-1}$ e logo podemos construir cada a_i fazendo $k-1$ somas. Como temos $r+1$ coeficientes a_i, gastamos no total $(k-1)(r+1)$ operações para gerar todos os a_i. Uma vez gerados os a_i, podemos gerar n com os seguintes $2r$ passos:

$$\begin{aligned}
a_r &\to a_r C \\
&\to a_r C + a_{r-1} \\
&\to (a_r C + a_{r-1})C \to \cdots \\
&\to a_r C^r + \cdots + a_1 C + a_0 = N.
\end{aligned}$$

O número total de passos que usamos é no máximo $k(B-1) + (k-1)(r-1) + 2r$, assim

$$\begin{aligned}
\tau(n) &\le k(B-1) + (k-1)(r-1) + 2r = rk + O\left(\frac{\log n}{(\log\log n)^2}\right) \\
&= \left\lfloor \frac{\log n}{\log C} \right\rfloor \cdot \frac{\log C}{\log B} + O\left(\frac{\log n}{(\log\log n)^2}\right) \\
&= \frac{\log n}{\log B} + O\left(\frac{\log n}{(\log\log n)^2}\right) \\
&= \frac{\log n}{\log\log n - 3\log\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right) \\
&= \frac{\log n}{\log\log n} + \frac{3\log n \cdot \log\log\log n}{(\log\log n)^2} + O\left(\frac{\log n}{(\log\log n)^2}\right) < g(n).
\end{aligned}$$

$\square$

Usando a prova acima, podemos trocar $g(n)$ por $\frac{g(n)}{p-1}$ se tivermos o produto binário e a soma p-ária $\oplus(x_1, x_2, \dots, x_p) = x_1 + \cdots + x_p$.

Vamos agora considerar o caso em que temos apenas a operação soma: dado $n \in \mathbb{N}_{>0}$, definimos

$$\tau_+(n) = \min\left\{ m \in \mathbb{N} \,\middle|\, \begin{array}{l} \exists (s_0, \dots, s_m) \text{ com } s_0 = 1, s_m = n \text{ e, para cada} \\ l \ge 1, \text{ existem } i, j \text{ com } 0 \le i, j < l \text{ e } s_l = s_i + s_j \end{array} \right\}$$

Nesse caso podemos provar o seguinte resultado devido a Erdős

Teorema 3.49. $\lim\limits_{n\to\infty} \frac{\tau_+(n)}{\log_2 n} = 1.$

DEMONSTRAÇÃO: Se $(s_0, \ldots, s_m)$ é uma sequência como na definição de $\tau_+(n)$ então $s_j \leq 2^j$ para todo $j \leq m$. Em particular, se $m = \tau_+(n)$, temos $n = s_m \leq 2^m = 2^{\tau_+(n)}$ donde $\tau_+(n) \geq \log_2 n$ para todo $n \in \mathbb{N}_{>0}$. Dado $n \in \mathbb{N}^*$, fixamos $k = k(n) \geq 1$ e começamos gerando os números

$$s_0 = 1, s_1 = 2, s_2 = 3, \ldots, s_{2^k-1} = 2^k.$$

Escrevemos agora n na base $B = 2^k$

$$n = a_0 + a_1 B + \cdots + a_r B^r$$

onde

$$r = \left\lfloor \frac{\log n}{\log B} \right\rfloor \qquad \text{e} \qquad 0 \leq a_j \leq B-1, \quad \forall j \leq r.$$

Observemos que os a_j já foram gerados, assim fazemos agora

$$\begin{array}{lll} s_{2^k}{=}a_r + a_r{=}2a_r, & s_{2^k+1}{=}2a_r + 2a_r{=}4a_r, \quad \ldots & s_{2^k+k-1}{=}2^k a_r{=}Ba_r \\ s_{2^k+k}{=}Ba_r + a_{r-1}, & s_{2^k+k+1}{=}2(Ba_r + a_{r-1}), \quad \ldots & s_{2^k+2k}{=}B^2 a_r + Ba_{r-1} \\ & \qquad\qquad\qquad\qquad\quad \vdots & \\ & \multicolumn{2}{r}{s_{2^k-1+(k+1)r}{=}B^r a_r + B^{r-1} a_{r-1} + \cdots + Ba_1 + a_0{=}n} \end{array}$$

Temos

$$2^k - 1 + (k+1)r \leq 2^k + \frac{(k+1)\log n}{k \log 2} = \log_2 n + 2^k + \frac{\log_2 n}{k}.$$

Escolhendo $k = \lceil \log_2(\frac{\log n}{(\log\log n)^2}) \rceil = \lceil \log_2 \log n - 2\log_2 \log\log n \rceil$, temos que

$$\tau_+(n) \leq (1 + o(1)) \log_2 n$$

o que prova o resultado. □

Problemas Propostos

3.29. *Mostrar que para todo $n \gg 0$*

$$\sum_{k=1}^{n} \frac{\sigma(k)}{k} = \frac{\pi^2 n}{6} + O(n \log n).$$

3.30. *Mostrar que para todo $\alpha \leq 0$ e $n \gg 0$*

$$\sum_{k=1}^{n} \frac{d(k)}{k^\alpha} = \frac{1}{(1-\alpha)} n^{1-\alpha} \log n + \frac{\pi^4}{36} + O(n^{1-\alpha}).$$

3.31. *Mostrar que*

$$\sum_{k=1}^{n} \frac{d(k)}{k} = \frac{1}{2} \log^2 n + 2\log n + O(1).$$

3.32. *Prove que, para todo inteiro positivo n, existem exatamente 2^{n-1} vetores $(a_1, a_2, \ldots, a_k)$, onde $k, a_1, a_2, \ldots, a_k$ são inteiros positivos e $a_1 + a_2 + \cdots + a_k = n$.*

3.33. *Seja P_n o conjunto das partições de n. Dada $\pi = (a_1, a_2, \dots a_r) \in P_n$, definimos $a(\pi) = |\{j \le r | a_j = 1\}|$, o número de termos iguais a 1 na partição π e $b(\pi) = |\{a_1, a_2, \dots, a_r\}|$, o número de termos distintos na partição π.*

Prove que, para todo $n \in \mathbb{N}$, $\sum_{\pi \in P_n} a(\pi) = \sum_{\pi \in P_n} b(\pi)$.

3.34. *Prove que, para todo $n \ge 1$,*

$$n \cdot p(n) = \sum_{\ell k \le n} \ell \cdot p(n - \ell k) = \sum_{v=1}^{n} \sigma(v) p(n - v).$$

(Sugestão: use a função geratriz de $p(n)$.)

3.35 (OIbM1994). *Demostrar que todo número natural $n \le 2^{1\,000\,000}$ pode ser obtido a partir de 1 fazendo menos do que $1\,100\,000$ de somas, isto é, existe uma sequência finita de números naturais tais que*

$$x_0, x_1, \dots, x_k$$

com $k \le 1\,100\,000$, tais que $x_0 = 1$, $x_k = n$, e para cada $i = 1, 2, \dots, k$, existem r, s, com $0 \le r, s < i$ e $x_i = x_r + x_s$.

3.36 (OBM2009). *Para n inteiro positivo seja $f(n)$ o número de produtos de inteiros maiores que 1 cujo resultado é no máximo n, isto é, $f(n)$ é o número de k-uplas $(a_1, a_2, \dots, a_k)$ onde k é algum natural, $a_i \ge 2$ é inteiro para todo i e $a_1 \cdot a_2 \cdot \dots \cdot a_k \le n$ (contando a 0-upla vazia $()$, cujo produto dos termos é 1).*

Assim, por exemplo, $f(1) = 1$, por causa da 0-upla $()$ e $f(6) = 9$, por causa da 0-upla $()$, das 1-uplas $(2), (3), (4), (5)$ e (6) e das 2-uplas $(2, 2), (2, 3)$ e $(3, 2)$.

Seja $\alpha > 1$ tal que $\sum_{m=1}^{\infty} \frac{1}{m^\alpha} = 2$.

a) Prove que existe uma constante $K > 0$ tal que $f(n) \le K \cdot n^\alpha$ para todo inteiro positivo n.

b) Prove que existe uma constante $c > 0$ tal que $f(n) \ge c \cdot n^\alpha$ para todo inteiro positivo n.

Bibliografia

[1] J. H. Conway e R. K. Guy, *The Book of Numbers*, Springer-Verlag (1996).

[2] S. C. Coutinho, *Números inteiros e criptografia RSA*, Coleção Computação e Matemática, SBM e IMPA (2000).

[3] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arithmetica 2: 23–46 (1936).

[4] H. G. Diamond, J. Pintz, *Oscillation of Mertens' product formula* Journal de théorie des nombres de Bordeaux 21, no. 3 (2009), 523–533.

[5] P. Erdős e M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. 62 (1940), 738–742.

[6] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete mathematics*, segunda edição, Addison-Wesley (1994).

[7] Hardy, G. H., *On Dirichlet's Divisor Problem*, Proc. London Math. Soc.(2) 15 (1917), 1–25.

[8] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers*, quinta edição, Oxford University Press (1979).

[9] G. H. Hardy e S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. 17 (1918), 75–115.

[10] L. K. Hua, *Introduction to number theory*, Springer-Verlag (1982).

[11] M. N. Huxley, *Exponential Sums and Lattice Points III*, Proc. London Math. Soc.(3) 87 (2003), 591–609.

[12] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner (1909). Reprinted: Chelsea (1953).

[13] W. de Melo e B. F. Svaiter, *The cost of computing integers*, Proc. AMS 124 (1996), no. 5, 1377–1378.

[14] C. G. Moreira, *O teorema de Ramsey*, Revista Eureka! 6, 23–29.

[15] C. G. Moreira, *On asymptotic estimates for arithmetic cost fuction*, Proc. AMS 125 (1997), 347–353.

[16] A. Politi, J. C. F. Matthews, J. L. O'Brien, *Shor's Quantum Factoring Algorithm on a Photonic Chip*, Science 4 September 2009: Vol. 325. no. 5945, p. 1221.

[17] D. H. J. Polymath, *Deterministic methods to find primes*, preprint, http://polymathprojects.files.wordpress.com/2010/07/polymath.pdf; veja também http://polymathprojects.org/2009/08/09/research-thread-ii-deterministic-way-to-find-primes/ e http://michaelnielsen.org/polymath1/index.php? title=Finding_primes

[18] H. Rademacher, *On the partition function p(n)*, Proc. London Math. Soc. (2) 43 (1937), 241–254.

[19] H. Rademacher, *Topics in analytic number theory*, Grundlehren der mathematischen Wissenschaften 169, Springer-Verlag (1973).

[20] P. Ribenboim, *Selling primes*, Math. Mag. 68 (1995), 175–182. Traduzido como *Vendendo primos*, Rev. Mat. Univ. 22/23 (1997), 1–13.

[21] J.P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) 40 (2003), no. 4, 429–440.

[22] A. Shen e N. K. Vereshchagin, *Basic Set Theory*, AMS, 2002.

[23] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. 26 (5), 1484-1509 (1997). Também em arXiv:quant-ph/9508027v2.

[24] M. Shub e S. Smale, *On the intractability of Hilbert's Nullstellesatz and algebraic version of "$NP = P$"*, Duke Math J. 81 (1995), 47–54.

[25] A. I. Vinogradov *On the remainder in Merten's formula* (Russian), Dokl. Akad. Nauk SSSR 148 (1963), 262–263.