II Colóquio de Matemática do Centro Oeste
07-11/11/2011

Introdução à Teoria dos Números e Criptografia

José Gilvan de Oliveira, Elisabete Sousa Freitas

Sumário

Capítulo 1

Introdução

A crescente necessidade de segurança nas diversas comunicações atuais, por exemplo, comunicações bancárias para transferência eletrônicas de valores, comunicações entre filiais de uma empresa, assinaturas e autenticações digitais, e até mesmo comunicações pessoais via a rede internet (senhas e partilhas de senhas), tem enfatizado o papel de destaque da área da matemática chamada criptografia.

A criptografia consiste dos conceitos e técnicas usados para a transmissão segura de dados e de informações sigilosas através de canais monitorados por terceiros. Esta área obteve uma profunda evolução a partir de 1976 com a introdução, por W. Diffie e M. E. Hellman, da técnica chamada criptografia da chave pública.

Nosso objetivo é apresentar dois importantes sistemas de criptografia de chave pública usados atualmente. O sistema RSA, assim chamado devido as iniciais dos nomes dos seus autores Rivest, Shamir e Adleman, está baseado na dificuldade computacional de fatoração de números inteiros com fatores primos grandes, com mais de cem dígitos. O sistema ECC, assim chamado devido as iniciais em inglês de criptografia de curvas elípticas, foi desenvolvido em 1985 independentemente por N. Koblitz e V. Miller, inspirado no uso de curvas elípticas para implementação de algoritmos de fatoração de números inteiros, por H. W. Lenstra, e usa uma interessante propriedade das curvas elípticas que será abordada posteriormente.

Os principais tópicos que serão abordados neste minicurso são: propriedades dos números inteiros, congruência módulo n, grupos e a função ϕ de Euler, corpos finitos, plano projetivo, curvas elípticas, os sistemas RSA e ECC de criptografia e criptoanálise. Isto será feito em sintonia com alguns conceitos apresentados em disciplinas do curso de graduação em matemática tais como: grupos, anéis, corpos, espaços vetoriais, etc. Assim, queremos destacar a importância desses assuntos com aplicações diretas no nosso cotidiano.

Dado a restrição de tempo o assunto é apresentado de forma breve e em alguns tópicos de forma superficial. Esperamos que o leitor sinta-se estimulado a procurar nas referências apresentadas um maior aprofundamento sobre o assunto.

Capítulo 2

Números Inteiros

Neste capítulo vamos considerar o conjunto $\mathbb{Z}$ dos números inteiros como um conjunto já conhecido do leitor com relação aos seus elementos, a ordem $\leq$, as suas operações de multiplicação $\cdot$ e adição $+$, e a existência da função injetiva $s : \mathbb{N} \to \mathbb{N}$, definida no conjunto dos números inteiros não-negativos $\mathbb{N}$, que associa a cada $n \in \mathbb{N}$ o seu sucessor $s(n) = n + 1$. O conjunto imagem da função s é o conjunto dos números inteiros positivos $\mathbb{N}\backslash\{0\}$.

Observação 1 *Princípio da Boa Ordem. Todo subconjunto não-vazio X do conjunto $\mathbb{N}$ dos números inteiros não-negativos tem um menor elemento, isto é, existe $m_0 \in X$ tal que $m_0 \leq x$ para todo $x \in X$.*

Observação 2 *Princípio de Indução. Seja X um subconjunto de $\mathbb{N}$ tal que:*

1. *$n_0 \in X$;*
2. *Se $n \geq n_0$ pertence a X então $n + 1$ também pertence a X.*
   Então X contém todos os números inteiros $m \geq n_0$.

1 Propriedades

A *função módulo* (ou *valor absoluto*) $|\cdot| : \mathbb{Z} \to \mathbb{N}$ é definida por $|m| = m$ se m é não-negativo ($n \geq 0$) e $|m| = -m$ se m é negativo ($m < 0$).

Proposição 3 *Divisão Euclidiana. Dados inteiros $m, n \in \mathbb{Z}$, $m \neq 0$, existem $q, r \in \mathbb{Z}$, $0 \leq r < |m|$, unicamente determinados, tais que $n = qm + r$.*

Prova. Vamos considerar inicialmente m positivo. O conjunto $X = \{n - jm;\ j \in \mathbb{Z},\ jm \leq n\}$ está contido em $\mathbb{N}$ e não é vazio pois $n = n - 0.m$ pertence a X, se $n \geq 0$, e $n - nm = n(1 - m)$ pertence a X, se $n \leq 0$. Pelo princípio da boa ordem existe r o menor elemento de X e portanto $n = qm + r$ para algum inteiro q. Além disso, pela minimalidade do inteiro r, temos $0 \leq r = n - qm \leq m$ e claramente r e q são unicamente determinados. Finalmente, se m é negativo então o seu simétrico $-m$ é positivo e pelo caso anterior existem q e r tais que $n = q(-m) + r$, com $0 \leq r < -m = |m|$. Assim basta observar que $n = (-q)m + r$. $\triangle$

Nas condições da proposição anterior, se o inteiro r, chamado *resto* da divisão de n por m, é zero então dizemos que n é *múltiplo* de m e que m *divide* n. Notação: $m|n$. Por exemplo os números inteiros $-1,\ 1,\ -m,\ m$ são divisores do inteiro não-nulo m. No caso em que estes são todos os divisores de $m \neq 0$, no total de quatro divisores, dizemos que m é *primo*. Equivalentemente, m é *primo* se, para $a,\ b$ inteiros, vale: $m|ab \Rightarrow m|a$ ou $m|b$. Como pode ser facilmente verificado, os números $2,\ 3,\ 5$ são os três menores números primos positivos.

Exercício 4 *Calcule o resto da divisão euclidiana de n por m nos seguintes casos:*

i) $m = 3$ *e* $n = j^2$, $j = 1, 2, 4, 5, 7, 8$.

ii) $m = 5$ *e* $n = j^4$, $j = 1, 2, 3, 4, 6, 7, 8, 9$.

iii) Considerando os resultados obtidos nos itens anteriores, conjecture a validade de um resultado geral para $m = p$ *e* $n = j^{p-1}$, $j = 1, 2, \ldots, p-1$, *onde* p *é um número inteiro primo positivo.*

Exercício 5 *Mostre que se um número inteiro positivo n divide $(n-1)! = 1.2.\ldots.(n-1)$, o fatorial de $n-1$, então ele é primo. Veremos posteriormente que vale a recíproca desse resultado (16).*

Um método para se obter os números primos é o chamado *Crivo de Eratóstenes* descrito a seguir. Dados os números inteiros positivos em ordem crescente, o menor número primo é 2. Elimina-se todos os múltiplos de 2 maiores do que 2. O próximo número não eliminado, no caso 3, é primo. Elimina-se em seguida todos os múltiplos desse número maiores do que ele. Repetindo-se o processo sucessivamente, os números não eliminados maiores que 1 são números primos. Como exemplo, usando o crivo de Eratóstenes na tabela a seguir, podemos verificar que os números primos positivos menores do que 100 são os seguintes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Crivo de Eratóstenes até 100.

1	2	3	$\not{4}$	5	$\not{6}$	7	$\not{8}$	$\not{9}$	$\not{10}$
11	$\not{12}$	13	$\not{14}$	$\not{15}$	$\not{16}$	17	$\not{18}$	19	$\not{20}$
$\not{21}$	$\not{22}$	23	$\not{24}$	$\not{25}$	$\not{26}$	$\not{27}$	$\not{28}$	29	$\not{30}$
31	$\not{32}$	$\not{33}$	$\not{34}$	$\not{35}$	$\not{36}$	37	$\not{38}$	$\not{39}$	$\not{40}$
41	$\not{42}$	43	$\not{44}$	$\not{45}$	$\not{46}$	47	$\not{48}$	$\not{49}$	$\not{50}$
$\not{51}$	$\not{52}$	53	$\not{54}$	$\not{55}$	$\not{56}$	$\not{57}$	$\not{58}$	59	$\not{60}$
61	$\not{62}$	$\not{63}$	$\not{64}$	$\not{65}$	$\not{66}$	67	$\not{68}$	$\not{69}$	$\not{70}$
71	$\not{72}$	73	$\not{74}$	$\not{75}$	$\not{76}$	$\not{77}$	$\not{78}$	79	$\not{80}$
$\not{81}$	$\not{82}$	83	$\not{84}$	$\not{85}$	$\not{86}$	$\not{87}$	$\not{88}$	89	$\not{90}$
$\not{91}$	$\not{92}$	$\not{93}$	$\not{94}$	$\not{95}$	$\not{96}$	97	$\not{98}$	$\not{99}$	$\not{100}$

Proposição 6 *O conjunto dos números inteiros primos é infinito.*

Prova. Se $p_1,\ p_2, \ldots,\ p_n$ representam os n primeiros números primos positivos então $m = 1 + p_1.p_2.\ldots.p_n$ ou é primo ou possui um fator primo positivo diferente de todos os n primeiros, já que nenhum deles é divisor de m. $\triangle$

O maior primo conhecido até hoje é o número $2^{43112609} - 1$, obtido em agosto de 2008. Ele tem 12978189 dígitos (http://primes.utm.edu). O crivo de Eratóstenes não é prático para obtenção de números primos grandes. Para termos uma idéia dessa limitação, mencionamos o seguinte exemplo. O primo $2^{44497}-1$ obtido em 1979 tem 13.395 dígitos. Com o uso do crivo de Eratóstenes para verificar que ele é de fato primo, considerando-se os cálculos efetuados em um computador com capacidade de operar um milhão de multiplicações por segundo, seriam necessários 10^{6684} anos para conclusão da tarefa ([2], p. 160). Como provar que um dado número é ou não primo? A *Eletronic Frontier Foundation* oferece prêmios de 250 mil dólares para a obteção do primeiro número primo com um bilhão de dígitos decimais (https://www.eff.org/awards/coop).

Observação 7 *Existência de desertos de números primos. Para cada inteiro $m > 1$ existe uma sequência de m números inteiros consecutivos que não são primos. De fato, representando por $m!$ o* fatorial *de m, isto é, o produto de todos os números inteiros positivos menores ou igual a m, vemos que a seguinte sequência, com m elementos consecutivos,*

$$2 + (m+1)!,\ 3 + (m+1)!, \ldots,\ m + 1 + (m+1)!,$$

não contém primos, pois $j < j + (m+1)!$ e j divide $j + (m+1)!$, para cada inteiro $j = 2,\ 3,\ \ldots,\ m+1$.

Apesar da especial particularidade da distribuiçao dos números primos visto na abservação anterior, não é conhecido (mas conjectura-se que sim) se existem infinitos números *primos gêmeos*, que são os pares de números primos da forma p e $p + 2$. Por exemplo, conforme observa-se usando o crivo de Eratóstenes, existem sete pares de primos gêmeos menores do que 100, que são os seguintes: (3, 5), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), e (71, 73).

A questão da determinação de todos os números primos, isto é, qual é a função que, para cada inteiro positivo n, associa o n-ésimo número primo, é considerado um dos grandes problemas da teoria dos números. Como aplicação do Teorema de Wilson (16), exibiremos no exemplo (17) uma função com imagem exatamente o conjunto de todos os números inteiros primos positivos, mas com domínio

$\mathbb{Z}^+ \times \mathbb{Z}^+$. Esta questão está relacionada com a famosa *Hipótese de Riemann*, que é considerada por alguns matemáticos de destaque, o maior problema não resolvido da matemática. A Hipótese de Riemann é um dos seis problemas do milênio e a sua solução será recompensada com um prêmio de um milhão de dólares, pelo Clay Mathematics Institute (http://www.claymath.org/). O mais recente problema do milênio resolvido foi a conjectura de Poincaré, por Grigori Perelman em 2003. Com recurso dos modernos computadores, a hipótese de Riemann foi verificada para os primeiros dez trilhões de valores. In 1973, Pierre Deligne, ganhador da medalha fields em 1978, provou que a hipótese de Riemann é válida para variedades algébricas sobre corpos finitos (Conjectura de Weil).

Exercício 8 *Sejam a, m e n inteiros positivos, com n ímpar. Justifique as igualdades abaixo e encontre condições nos números inteiros a, m e n para que $a^m - 1$ e $a^n + 1$ sejam números primos.*

i) $a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots + a + 1)$.

ii) $a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1)$.

2 Congruência Módulo n

As operações de adição e multiplicação no conjunto dos números inteiros são os pilares da estrutura algébrica desse conjunto infinito. Do ponto de vista computacional, entretanto, trabalhamos com conjunto finitos. Nesta seção vamos introduzir uma estrutura aditiva e multiplicativa em especiais conjuntos finitos.

Fixado um inteiro positivo n, os possíveis restos da divisão euclidiana de números inteiros por n são $0,\ 1, \ldots,\ n-1$. Dizemos que os números inteiros a e b são *congruentes módulo n* se eles têm o mesmo resto da divisão euclidiana por n, isto é, se $b - a$ é um múltiplo de n. Neste caso escrevemos $a \equiv b \ mod\ n$, ou simplesmente $a \equiv b$ se o inteiro n já está subentendido.

Para cada inteiro a, o conjunto de todos os números inteiros congruentes a a módulo n, representado por $\bar{a}$, é chamado a *classe de equivalência* de a. A congruência módulo n é uma *relação de equivalência* no sentido que $a \equiv a$, se $a \equiv b$ então $b \equiv a$, e se $a \equiv b$ e $b \equiv c$ então $a \equiv c$, para todos números inteiros $a,\ b,\ c$. Isto permite decompor o conjunto dos números inteiros como união finita disjunta de todas as classes de equivalências. O conjunto dessas classes de equivalência tem n elementos e é representado por $\mathbb{Z}_n$, isto é, o conjunto $\mathbb{Z}_n$ é dado por $\mathbb{Z}_n = \{\bar{0},\ \bar{1},\ \ldots,\ \overline{n-1}\}$. Se um dado $\mathbb{Z}_n$ está fixado de forma que não há dúvida sobre os seus elementos então, por comodidade, também representamos os elementos de $\mathbb{Z}_n$ sem o emprego das barras superiores, isto é, $\mathbb{Z}_n = \{0,\ 1,\ \ldots,\ n-1\}$.

Exercício 9 *No conjunto $\mathbb{R}$ dos números reais considere a seguinte relação: dados $a,\ b \in \mathbb{R}$ tem-se $a \sim b$ se, e somente se, $a - b$ é um número inteiro. Verifique que $\sim$ é de fato uma relação de equivalência e proponha um modelo geométrico, identificando $\mathbb{R}$ com uma reta, para o conjunto das classes de equivalências distintas dessa relação. Se o leitor conseguiu entender o caso anterior então considere um problema análogo para o plano $\mathbb{R}^2$.*

No conjunto das classes de equivalências módulo n introduzimos duas operações da seguinte maneira. Dados $\bar{a}, \bar{b} \in \mathbb{Z}_n$ definimos $\bar{a} + \bar{b} = \overline{a+b}$ e $\bar{a} \cdot \bar{b} = \overline{ab}$. Estas operações de adição e multiplicação, respectivamente, estão bem definidas no sentido que não dependem dos representantes a e b.

Observação 10 *As operações de $\mathbb{Z}_n$ acima possuem as seguintes propriedades:*

i) Associativa: $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$ *e* $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$;

ii) Existência de elemento neutro: $\bar{a} + \bar{0} = \bar{a}$ *e* $\bar{a} \cdot \bar{1} = \bar{a}$;

iii) Existência de elemento inverso: $\bar{a} + \overline{(-a)} = \bar{0}$;

iv) Comutativa: $\bar{a} + \bar{b} = \bar{b} + \bar{a}$ *e* $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$;

v) Distributiva: $(\bar{a}+\bar{b})\cdot\bar{c}=\bar{a}\cdot\bar{c}+(\bar{b}\cdot\bar{c})$;
para todos $a,\ b,\ c\in\mathbb{Z}$.

Como consequência das propriedades acima serem satisfeitas, o conjunto $\mathbb{Z}_n$ ou, nas mesmas condições, qualquer conjunto A com operações de adição e multiplicação, é chamado *anel comutativo com unidade*. Com as suas operações usuais o conjunto dos números inteiros também é um anel comutativo com unidade já que estas mesmas propriedades também são satisfeitas.

Cada subconjunto não-vazio I de um anel comutativo que é fechado em relação à adição de elementos de I e é fechado em relação à multiplicação de elementos de I por elementos do anel é chamado *ideal*. Isto significa que, se I é um subconjunto não-vazio de um anel A então I é um ideal de A se as duas condições seguintes são satisfeitas:

i) $a,\ b\in I \implies a+b\ \in I$,

ii) $a\in A,\ b\in I \implies ab\ \in I$.

Por exemplo, dados elementos $a_1,\ a_2,\ldots,\ a_j$, de um anel comutativo A então o conjunto $a_1A+a_2A+\cdots+a_jA$, formado por todas as somas dos múltiplos em A dos elementos $a_1,\ a_2,\ldots,\ a_j$, é um ideal de A. Em particular, para cada número inteiro a, o conjunto $a\mathbb{Z}=\{aj:\ j\in\mathbb{Z}\}$ é um ideal de $\mathbb{Z}$. De fato, conforme veremos a seguir, cada ideal do anel dos números inteiros é da forma $a\mathbb{Z}$, para algum $a\in\mathbb{Z}$. O conjunto $\mathbb{Z}_n$ é também chamado o *anel quociente* do anel $\mathbb{Z}$ pelo ideal $n\mathbb{Z}$ *gerado* por n.

Proposição 11 *Se I é um ideal de $\mathbb{Z}$ então existe $a\in\mathbb{Z}$ tal que $I=a\mathbb{Z}$.*

Prova. O conjunto I é não-vazio por hipótese. Se $I=\{0\}$ então $a=0$. Se $I\neq\{0\}$ seja então $m\in I\backslash\{0\}$. Como $(-1)m$ é produto de um elemento do anel por um elemento do ideal, segue da definição de ideal que $-m\in I$. Portanto não é vazio o conjunto interseção X do ideal I com o conjunto dos números inteiros positivos e, pela Observação 1, ele tem um menor elemento, digamos $a\in X$. Segue da definição de ideal que $a\mathbb{Z}$ é um subconjunto de I. Para mostrar a outra inclusão consideremos um elemento qualquer n do ideal I. Pela Proposição 3 existem inteiros q e r tais que $n=qa+r$, com $0\leq r<a$. Consequentemente $r=n-qa$ pertence ao ideal I pois n e $-qa$ pertencem I. Como a é o menor elemento de X e $r<a$ devemos ter $r=0$, isto é, $n=qa$. Concluimos assim que $I=a\mathbb{Z}$. $\triangle$

Exemplo 12 *Tabelas das operações em* $\mathbb{Z}_2=\{0,1\}$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Exemplo 13 *Tabelas das operações em* $\mathbb{Z}_4=\{-1,\ 0,\ 1,\ 2\}$:

$+$	-1	0	1	2
-1	2	-1	0	1
0	-1	0	1	2
1	0	1	2	-1
2	1	2	-1	0

$\cdot$	-1	0	1	2
-1	1	0	-1	2
0	0	0	0	0
1	-1	0	1	2
2	2	0	2	0

Na tabela acima encontramos uma profunda diferença entre o anel dos números inteiros e o anel $\mathbb{Z}_4$. Com efeito, em $\mathbb{Z}_4$ existe elemento não-nulo cujo quadrado é nulo. Mais geralmente, se $n > 3$ não é primo então o anel $\mathbb{Z}_n$ possui *divisores de zero*, ou seja, existem elementos não nulos em $\mathbb{Z}_n$ cujo produto é nulo.

Em contraste com o caso anterior, se p é um primo então o anel $\mathbb{Z}_p$ não possui divisores de zero. Mais ainda, conforme veremos a seguir, cada elemento não-nulo tem inverso com relação à operação de multiplicação. Um anel comutativo com unidade onde todo elemento não-nulo possui inverso é chamado *corpo*. Os conjuntos dos números racionais $\mathbb{Q}$, dos números reais $\mathbb{R}$, e dos números complexos $\mathbb{C}$, com as suas operações usuais, são exemplos de corpos com uma infinidade de elementos.

Proposição 14 *O anel $\mathbb{Z}_p$ é um corpo se p é um número primo.*

Prova. Resta apenas mostrar que se $a \in \mathbb{Z}_p$ não é nulo então existe $b \in \mathbb{Z}_p$ tal que $ab = 1$. Seja α um número inteiro representante da classe de equivalência de a. O conjunto $J = \alpha\mathbb{Z} + p\mathbb{Z}$, cujos elementos são da forma $\alpha m + pn$, onde m e n são inteiros, é um ideal de $\mathbb{Z}$ e contém o ideal $p\mathbb{Z}$ propriamente, pois α não é um múltiplo de p. Pela Proposição 11 existem inteiros β e γ tais que $k = \alpha\beta + p\gamma$ e $J = k\mathbb{Z}$. Como $p \in J$ e $k \notin p\mathbb{Z}$ segue daí que 1 pertence ao ideal J e consequentemente $J = \mathbb{Z}$. Em particular a classe de equivalência b de β satisfaz a igualdade procurada. $\triangle$

Como consequência desse resultado podemos provar duas importantes identidades envolvendo números primos.

Corolário 15 *Pequeno Teorema de Fermat. Se p é um número inteiro primo então $a^p = a$, para cada elemento a do corpo $\mathbb{Z}_p$.*

Prova. Seja a um elemento não-nulo do corpo $\mathbb{Z}_p$. Nestas condições, a função que a cada elemento não-nulo x de $\mathbb{Z}_p$ associa o elemento não-nulo ax é uma bijeção em $\mathbb{Z}_p\backslash\{0\}$. Considerando o produto de todos os elementos não-nulos do corpo de duas formas convenientes, uma no domínio e outra na imagem da função, obtemos a igualdade

$$(p-1)! \;=\; a^{p-1}(p-1)!,$$

onde $(p-1)! = 1.2\ldots(p-1)$ representa o fatorial de $p-1$. Como $\mathbb{Z}_p$ é um corpo, a igualdade do corolário está provada. $\triangle$

Corolário 16 *Teorema de Wilson. Se p é um número inteiro primo então $(p-1)! = -1$ em $\mathbb{Z}_p$.*

Prova. A igualdade é imediata no caso $p = 2$. Assim vamos considerar $p \geq 3$ primo. Como $\mathbb{Z}_p$ é um corpo, as únicas soluções da equação $x^2 - 1 = 0$ são apenas 1 e -1. Em outras palavras, os únicos elementos de $\mathbb{Z}_p$ com a propriedade de ser igual ao seu inverso multiplicativo são 1 e -1. A igualdade do corolário segue então, já que $p \geq 3$ é impar, agrupando-se no produto $(p-1)!$ cada elemento com o seu respectivo inverso multiplicativo. $\triangle$

Como uma interessante aplicação do Teorema de Wilson, vamos apresentar uma função com domínio $\mathbb{Z}^+ \times \mathbb{Z}^+$ e com conjunto imagem exatamente o conjunto de todos os números inteiros primos positivos.

Exemplo 17 *Seja f a função que a cada par $(x,\ y)$, de números inteiros positivos, associa o inteiro positivo*

$$f(x,\ y) = 2 + (y-1)(|\alpha| - \alpha)/2,$$

onde $\alpha = \beta^2 - 1$ *e* $\beta = x(1+y)-(y!+1)$. *Vamos mostrar que a imagem de* f *é o conjunto dos números primos positivos. Consideremos inicialmente* p *destes primos. Então, pelo teorema de Wilson, o primo* p *divide* $(p-1)!+1$. *Concluimos assim que o par* $(((p-1)!+1)/p,\ p-1)$ *pertence ao domínio e que a sua imagem é* p, *pois neste caso* $\beta = 0$. *Mais geralmente, se* $\beta = 0$, *para algum par* $(x,\ y)$ *no domínio da função, então segue da igualdade* $x(1+y) = (y!+1)$ *que* $1+y$ *é primo (5)*. Neste caso temos que $f(x,\ y) = y+1$ é primo. Finalmente, se $\beta \neq 0$, para algum par $(x,\ y)$ no domínio da função, então $f(x,\ y) = 2$ é primo.

Os números primos estão intimamente ligado aos números inteiros como um todo. Em um certo sentido, que será esclarecido no teorema seguinte, os números primos geram todos os números inteiros. Este fato por si só já seria suficiente para justificar uma atenção especial aos números primos.

Teorema 18 *Teorema Fundamental da Aritmética. Todo número inteiro diferente de* 0 *e de* ± 1 *é igual ao produto de números primos. Além disso o produto é único a menos de sinal e de ordem dos fatores.*

Prova. O resultado é claramente válido para números primos. A prova será feita por indução. Consideremos então $n > 2$ um número inteiro qualquer tal que cada inteiro m, $2 < m < n$, é produto de primos. Como podemos nos restringir ao caso que n não é primo, isto assegura a existência de algum ideal J de $\mathbb{Z}$ tal que $n\mathbb{Z} \subsetneq J \subsetneq \mathbb{Z}$. Nestas condições, segue da Proposição 11 que existe algum inteiro $1 < a < n$ tal que $J = a\mathbb{Z}$. Daí, como $n \in J$, existe algum inteiro $1 < b < n$ tal que $n = ab$. Pela hipótese de indução a e b são produto de números primos. Consequentemente $n = ab$ é também o produto de números primos. Concluimos por induçao que todos os números maiores do que 1 é produto de primos. A prova da unicidades da fatoração é deixada como exercício. $\triangle$

3 Máximo Divisor Comum e Equações Diofantinas Lineares

Segue do teorema acima que dados inteiros $m > 1$ e $n > 1$ existem números primos distintos $p_1,\ p_2,\ \ldots,\ p_r$ tais que $m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$ e $n = p_1^{f_1} \cdot p_2^{f_2} \cdots p_r^{f_r}$, onde $e_1,\ e_2,\ \ldots,\ e_r$ e $f_1,\ f_2,\ \ldots,\ f_r$ são inteiros não-negativos. É claro então que cada inteiro da forma $p_1^{j_1} \cdot p_2^{j_2} \cdots p_r^{j_r}$ é divisor simultaneamente de m e n se cada inteiro j_i satisfaz as desigualdades $0 \leq j_i \leq \min\{e_{j_i},\ f_{j_i}\}$, onde $\min\{e_{j_i},\ f_{j_i}\}$ é o menor elemento do conjunto $\{e_{j_i},\ f_{j_i}\}$. O *máximo divisor comum* de m e n, representado por $mdc\{m,\ n\}$, é aquele entre esses divisores onde cada j_i nestas condições é tomado o maior possível, isto é,

$$mdc\{m,\ n\} = p_1^{j_1} \cdot p_2^{j_2} \cdots p_r^{j_r},$$

onde $j_i = \min\{e_{j_i},\ f_{j_i}\}$ para cada i. Se a e b são inteiros diferente de zero então definimos $mdc\{0,\ a\} = |a|$ e $mdc\{a,\ b\} = mdc\{|a|,\ |b|\}$. Quando $mdc\{a,\ b\} = 1$ os inteiros a e b são *primos entre si.*

Proposição 19 *Identidade de Bézout. Dados números inteiros* a *e* b, *não simultaneamente nulos, existem números inteiros* α *e* β *tais que* $mdc\{a,\ b\} = a\alpha + b\beta$.

Prova. Os ideais $a\mathbb{Z}$ e $b\mathbb{Z}$, gerados por a e b respectivamente, estão contidos no ideal $a\mathbb{Z}+b\mathbb{Z}$ e este, por sua vez, está contido no ideal gerado por $mdc\{a,\ b\}$. O resultado segue então da observação que o ideal $a\mathbb{Z} + b\mathbb{Z}$ é principal e que de fato vale a igualdade $a\mathbb{Z} + b\mathbb{Z} = mdc\{a,\ b\}\mathbb{Z}$. $\triangle$

Uma equação algébrica na qual todos os coeficientes são números inteiros é chamada *equação diofantina.* A proposição anterior assegura a existência de solução, no conjunto dos números inteiros, para a equação diofantina linear $ax + by = c$, no caso $c = mdc\{a,\ b\}$. A existência ou não de soluções dessa equação diofantina no conjunto dos números inteiros é descrita completamente no próximo resultado.

Proposição 20 *Sejam a e b números inteiros não simultaneamente nulos. Dado $c \in \mathbb{Z}$ a equação*

$$ax + by = c$$

tem solução no conjunto dos números inteiros se, e somente se, c é um múltiplo de $d = mdc\{a,\ b\}$. Além disso, se $(\alpha_0,\ \beta_0)$ é uma tal solução então qualquer outra solução da equação é dada por $(\alpha_t,\ \beta_t)$, onde $\alpha_t = \alpha_o + b't$, $\beta_t = \beta_0 - a't$, $a = a'd$, $b = b'd$ e $t \in \mathbb{Z}$.

Prova. A primeira afirmação é consequência do fato que a equação $ax + by = c$ tem solução em $\mathbb{Z}$ se, e somente se, c pertence ao ideal $a\mathbb{Z} + b\mathbb{Z}$ gerado por a e b, o qual já sabemos ser igual ao ideal $d\mathbb{Z}$ gerado pelo máximo divisor comum de a e b. Finalmente, se $(\alpha_0,\ \beta_0)$ e $(\alpha',\ \beta')$ são soluções da equação diofantina $ax + by = c$ então $(\alpha' - \alpha_0,\ \beta' - \beta_0)$ é solução da equação $ax + by = 0$. O resultado segue do teorema fundamental da aritmética [Teorema (18)]. $\triangle$

Se a e b são números inteiros primos entre si então a equação diofantina $ax + by = c$ tem solução em $\mathbb{Z}$, qualquer que seja o inteiro c. Um problema interessante é procurar soluções dessa equação no conjunto $\mathbb{N}$, dos números inteiros não-negativos.

Exercício 21 *Determine todos os números inteiros positivos l para os quais a equação $4x + 7y = l$ não admite solução em $\mathbb{N}$.*

O cálculo do máximo divisor comum de dois inteiros pode ser efetuado a partir da divisão euclidiana. Na elaboração de um algoritmo para esse fim vamos usar a propriedade do máximo divisor comum destacada na próxima proposição.

Proposição 22 *Se a, b e q são números inteiros não nulos então*

$$mdc\{a,\ b\} = mdc\{a - qb,\ b\}.$$

Prova. A partir da definição de $mdc\{a,\ b\}$, basta observar que os seguintas conjuntos são iguais: $a\mathbb{Z} + b\mathbb{Z} = (a - qb)\mathbb{Z} + b\mathbb{Z}$. $\triangle$

Dados inteiros não nulos a e b, usando sucessivamente a proposição anterior, vamos apresentar a seguir um algoritmo para determinar inteiros α e β tais que $a\alpha + b\beta = mdc\{a,\ b\}$. Na tabela abaixo, os inteiros r_i, q_i, α_i e β_i, em cada linha i, são tais que $r_{i-1} = q_i r_i + r_{i+1}$ representa a divisão euclidiana de r_{i-1} por r_i com quociente q_i e resto r_{i+1}. Além disso, os elementos α_i e β_i das duas últimas colunas satisfazem a igualdade $r_i = a\alpha_i + b\beta_i$. Por conveniência, também definimos: $r_{-1} = a$, $r_0 = b$, $\alpha_{-1} = 1$, $\alpha_0 = 0$, $\beta_{-1} = 0$ e $\beta_0 = 1$.

Observação 23 *Algoritmo da Divisão Euclidiana Estendido. Nas condições acima temos:*

Restos	*Quocientes*	α	β
a	$*$	1	0
b	$*$	0	1
r_1	q_1	α_1	β_1
r_2	q_2	α_2	β_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{j-2}	q_{j-2}	α_{j-2}	β_{j-2}
r_{j-1}	q_{j-1}	α_{j-1}	β_{j-1}
r_j	q_j	α_j	β_j
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$mdc\{a,\ b\} = r_k > 0$	q_k	α_k	β_k
$r_{k+1} = 0$			

Nestas condições, para cada número inteiro positivo j tal que r_j é positivo, podemos verificar que r_j é dado por

$$r_j = a(\alpha_{j-2} - q_j\alpha_{j-1}) + b(\beta_{j-2} - q_j\beta_{j-1}).$$

Isto nos leva a conclusão que $mdc\{a,\ b\} = r_k$, onde k é o índice tal que $r_k > 0$ e $r_{k+1} = 0$, e também que os números inteiros α_j e β_j são dados respectivamente por

$$\alpha_j = \alpha_{j-2} - q_j\alpha_{j-1}$$

e

$$\beta_j = \beta_{j-2} - q_j\beta_{j-1}.$$

Em particular, observamos que esses números inteiros, além do quociente na própria linha, dependem apenas dos correspondentes inteiros nas duas linhas anteriores. A partir dessas informações podemos, de forma prática, obter a identidade de Bézout (19). Para isto, representando o número inteiro $a\alpha + b\beta$ por $[\alpha : \beta]$, definimos as seguintes operações nos pares $[\alpha : \beta]$ dos números inteiros α e β:

$$[\alpha : \beta] + [\alpha' : \beta'] = [\alpha + \alpha' : \beta + \beta']$$

e

$$q[\alpha : \beta] = [q\alpha : q\beta],\ q \in \mathbb{Z}.$$

Com essa notação, o correspondente par $[\alpha_j : \beta_j]$ é dado por

$$[\alpha_j : \beta_j] = [\alpha_{j-2} : \beta_{j-2}] - q_j[\alpha_{j-1} : \beta_{j-1}].$$

Exemplo 24 *Neste exemplo, usando o algoritmo da divisão euclidiana estendido, calcularemos o máximo divisor comum d de* 588 *e* 420 *e determinaremos inteiros* α *e* β *tais que* $d = 588\alpha + 420\beta$. *Usando secessivamente a divisão euclidiana temos:* $588 = 1 \cdot 420 + 168$, $420 = 2 \cdot 168 + 84$ *e* $168 = 2 \cdot 84$. *Então, como o resto nesta última divisão é zero, concluimos que* $mdc\{588,\ 420\} = 84$. *Além disso, colocando estas informações na tabela abaixo e seguindo o algoritmo da divisão euclidiana estendido temos* $\alpha_2 = -2$ *e* $\beta_2 = 3$. *Outros inteiros claramente podem ser obtidos, por exemplo os inteiros* $\alpha_j = -2 + 420j/84$ *e* $\beta_j = 3 - 588j/84$, *com* $j \in \mathbb{Z}$. *Estes são todos os inteiros possíveis, de acordo com a Proposição (20).*

Restos	*Quocientes*	$[\alpha \ : \ \beta]$
$a = 588$	$*$	$[1 \ : \ 0]$
$b = 420$	$*$	$[0 \ : \ 1]$
168	1	$[1 \ : \ -1]$
84	2	$[-2 \ : \ 3]$
0	2	$[5 \ : \ -7]$

Usando o procedimento descrito no algoritmo da divisão euclidiana estendido (23), vamos ignorar os números inteiros a e b e tomar, em cada etapa j, o inteiro q_j como sendo igual a -1 para obter uma importante consequência desse algoritmo. Nestas condições os valores da segunda coordenada de $[\alpha_j, \ \beta_j]$, para $j \geq -1$ (ou da primeira coordenada para $j \geq 0$), definem a clássica *sequência de Fibonacci*: 0, 1, 1, 2, 3, 5, 8, 13, ..., onde cada elemento F_j da sequência, a partir do terceiro termo, é a soma dos dois elementos anteriores, isto é, $F_j = F_{j-1} + F_{j-2}$, $j \geq 2$. Encontramos diversas aplicações dessa sequência na natureza. Ela está presente na árvore genealógica de zangões, na distribuição das sementes na flor do girassol, na forma de caracóis, entre tantas outras aplicações.

Proposição 25 *Para cada inteiro positivo j, o número de Fibonacci F_{j+1} satisfaz a igualdade $F_{j+1} = \sum_{i=0}^{j} \binom{j-i}{i}$, onde convencionamos $\binom{n}{l} = 0$ se $n < l$.*

Prova. Dados n e k inteiros positivos com $k \leq n$, temos a chamada *Fórmula de Pascal*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},$$

a qual segue das seguintes igualdades:

$$\begin{aligned}
\tbinom{n}{k} &= \tfrac{n!}{k!\ (n-k)!} = \tfrac{(n-1)!\ n}{k!\ (n-k)!} \\
&= \tfrac{(n-1)!\ (n-k)}{k!\ (n-k)!} + \tfrac{(n-1)!\ k}{k!\ (n-k)!} \\
&= \tfrac{(n-1)!}{k!\ (n-1-k)!} + \tfrac{(n-1)!}{(k-1)!\ (n-k)!} \\
&= \tbinom{n-1}{k} + \tbinom{n-1}{k-1}.
\end{aligned}$$

A prova da proposição será feita por indução matemática no inteiro positivo j. O resultado é claramente válido para $j = 1$. Se ele é também válido para os inteiros menores do que $j > 1$ então, pela Fórmula de Pascal, temos

$$\begin{aligned}
\textstyle\sum_{i=0}^{j} \tbinom{j-i}{i} &= \textstyle\sum_{i=0}^{j} (\tbinom{j-i-1}{i} + \tbinom{j-i-1}{i-1}) \\
&= \textstyle\sum_{i=0}^{j-1} \tbinom{j-1-i}{i} + \sum_{i-1=0}^{j-2} \tbinom{j-2-(i-1)}{i-1}) \\
&= F_{j-1} + F_{j-2} = F_j.
\end{aligned}$$

O resultado segue então do princípio de indução matemática. $\triangle$

Exercício 26 *Quantos coelhos podem ser gerados em um ano, a partir de um casal de coelhos recém-nascidos, se a reprodução de um casal de coelhos adultos é de um novo casal a cada mês, e se cada casal recém-nascido começa a reproduzir com dois meses de vida?*

Exercício 27 *Dados j e k inteiros positivos, mostre que os números de Fibonacci satisfazem as seguintes igualdades:*

i) $\sum_{i=0}^{j} F_i = F_{j+2} - 1$.

ii) $F_{j+k} = F_j F_{k+1} + F_{j-1} F_k$.

Uma interessante aplicação na matemática dos números de Fibonacci é a sua relação com a clássica razão áurea. Dizemos que um segmento de reta de comprimento a está dividido em *média e extrema razão* quando ele está dividido em duas partes de forma que o quociente do comprimento b da maior delas pelo comprimento a do segmento original é igual ao quociente do comprimento c da menor parte pelo comprimento b, isto é, $b/a = c/b$, onde $a = b + c$. Considerando o caso em que $c = 1$ temos que b satisfaz a relação $b^2 = b + 1$. A raíz real positiva $\rho = (1 + \sqrt{5})/2$ da equação $x^2 = x + 1$ é chamada *razão áurea*.

Exercício 28 *Mostre que em um triângulo isósceles com medida dos ângulos da base* $72°$*, a bissetriz interna de um desses ângulos divide o lado oposto em média e extrema razão.*

Exercício 29

i) Se $a > b$ *são números reais tais que* $(a+b)/a = a/b$ *então mostre que quaisquer três números sucessivos da sequência abaixo também estão nessa mesma proporção:*

$$a + b,\ a,\ b,\ a - b,\ 2b - a,\ 2a - 3b,\ 5b - 3a,\ 5a - 8b,\ \ldots$$

ii) Justifique geometricamente a construção dessa sequência e perceba a existência de uma relação com a sequência de Fibonacci.

Exercício 30 (*) *Mostre que* $F_j = (\rho^j - \rho^{-j})/\sqrt{5}$*, onde* ρ *é a razão áurea.*
Sugestão: Use o método de frações parciais, no conjunto dos números reais, após provar a identidade

$$\sum_{j \geq 0} F_j\, z^j = z/(1 - z - z^2).$$

Exercício 31 *Identidade de Cassini (1680) Mostre que os números de Fibonacci satisfazem a seguinte igualdade* $F_{n+1}F_{n-1} - F_n^2 = (-1)^n,\ n > 0$.

4 Semigrupos Numéricos

No exercício 21 procuramos todos os números inteiros l para os quais a equação diofantina $4x + 7y = l$ não admite solução em $\mathbb{N}$. Neste caso, o maior inteiro com essa propriedade é 17 e os demais inteiros são exatamente 1, 2, 3, 5, 6, 9, 10, 13. Este é um caso particular, para apenas duas variáveis, resolvido por J. J. Sylvester em 1882, do clássico *Problema de Frobenius* que trataremos nesta seção.

Sejam m e n inteiros primos entre si, com $2 \leq m < n$. Nestas condições já sabemos que a equação diofantina

$$nx + my = l \tag{2.1}$$

tem solução no conjunto dos números inteiros, qualquer que seja o número inteiro l, já que, sendo m e n primos entre si, o ideal de $\mathbb{Z}$ gerado por estes inteiros é todo o anel $\mathbb{Z}$.

Proposição 32 *Dado um número inteiro* l*, existe uma única solução da equação (2.1) na faixa* $[0,\, m) \times \mathbb{Z}$.

Prova. Como m e n são primos entre si, segue da proposição (20) que existe uma solução $(x_0,\, y_0) \in \mathbb{Z}^2$ da equação (2.1). Pela divisão euclidiana existem inteiros q e r, com $0 \leq r < m$, tais que $x_0 = qm+r$. Daí $\ell = nx_0+my_0 = nr+m(y_0+nq)$ e, portanto, $(r,\, y_0+qn)$ é uma solução da equação (2.1) nas condições estabelecidas. Além disso, se $(r,\, s)$ e $(r',\, s')$ são duas dessas soluções então $n(r-r') = m(s'-s)$. Daí m divide a diferença $r-r'$, pois m e n são primos entre si, o que implica que r e r' são iguais, dado que ambos são números inteiros não negativos menores do que m. Retornando a igualdade $n(r-r') = m(s'-s)$, concluímos também que s e s' são iguais e assim temos que nossa solução é única na faixa $[0,\, m) \times \mathbb{Z}$. $\triangle$

Vamos modificar ligeiramente nosso interesse, passando a procurar soluções $(x_0,\, y_0)$ da família de equações diofantinas $nx + my = l$, $l \in \mathbb{Z}$, com ambas coordenadas x_0 e y_0 no conjunto $\mathbb{N}$ dos números inteiros não-negativos.

Seja L o conjunto dos números inteiros ℓ tais que a equação diofantina (2.1) não tem solução com as duas coordenadas em $\mathbb{N}$. Seja N o complementar de L em $\mathbb{N}$, isto é, os elementos de N são os números inteiros não-negativos da forma $nx + my$, com x e y em $\mathbb{N}$. No caso particular do exercício (21), com $m = 4$ e $n = 7$, os correspondentes conjuntos L e N nesse caso são $\{1, 2, 3, 5, 6, 9, 10, 13, 17\}$ e $\{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, \dots\}$, respectivamente. É importante destacar a propriedade que a soma de dois elementos de N é também um elemento de N, ou seja, o conjunto N é fechado com relação a operação de adição. Uma completa descrição do conjunto L está dada no próximo teorema.

Teorema 33 *J.J. Sylvester [1882] Sejam m e n números inteiros primos entre si, com $2 \leq m < n$. Neste caso os elementos do conjunto L são dados por:*

$$n(m-1-i) + m(-1-j),$$

onde i e j são números inteiros satisfazendo $0 \leq i \leq m-2$, $0 \leq j \leq n-2$ e $ni+mj < (m-1)(n-1)-1$. Em particular, L tem $(m-1)(n-1)/2$ elementos e o maior deles é $(m-1)(n-1)-1$. Mais ainda, um inteiro ℓ pertence a L se, e somente se, $(m-1)(n-1)-1-\ell$ não pertence a L.

Prova. No plano cartesiano $\mathbb{R}^2$, a família de equações diofantinas (2.1), com $\ell \in \mathbb{Z}$, representa uma família de retas paralelas, onde cada elemento da família tem coeficiente angular $-n/m$. Como as interseções com os eixos coordenados da reta da família para ℓ igual a mn são os pontos $(m,\, 0)$ e $(0,\, n)$, segue da proposição (32) que o intervalo $[mn,\, \infty)$ e o conjunto L são disjuntos, ou seja $[mn,\, \infty) \subset N$. Mais ainda, pelas condições em m e n e também pela proposição (32), o maior elemento de L é $(m-1)(n-1)-1$, obtido tomando-se o ponto $(m-1,\, -1)$ na família de retas, pois, pela definição de L, respectivamente, $m-1$ e -1 são os maiores valores possíveis para as coordenadas x e y na faixa $[0,\, m) \times \mathbb{Z}$, considerada na proposição (32).

Para determinar os demais elementos do conjunto L, observamos inicialmente que nos pontos $(m-1,\, 0)$ e $(0,\, n-1)$ obtemos respectivamente os inteiros $n(m-1)$ e $m(n-1)$, que são maiores do que o maior elemento de L. Assim podemos nos restringir ao retângulo $[0,\, m-2] \times [0,\, n-2]$. Para um ponto $(i,\, j)$ nesse retângulo, temos que $ni + mj \in N$ é menor do que $(m-1)(n-1)-1$ se, e somente se, no ponto $(m-1-i,\, -1-j)$ da faixa $[0,\, m) \times \mathbb{Z}$ obtemos o elemento $(m-1)(n-1)-1-(ni+mj) \in L$. Segue então que os números inteiros do intervalo $[0,\, (m-1)(n-1)-1]$ estão agrupados aos pares $(\ell,\, (m-1)(n-1)-1-\ell)$ de forma que $\ell \in L$ se, e somente se, $(m-1)(n-1)-1-\ell \notin L$. Consequentemente a cardinalidade dos conjuntos L e $N \cap [0,\, (m-1)(n-1)-1]$ é $(m-1)(n-1)/2$. $\triangle$

Vamos estudar a seguir uma generalização dos conceitos considerados nas duas últimas seções. Dados números inteiros positivos $a_1,\, a_2,\, \dots,\, a_r$ primos entre si, isto é, o máximo divisor comum $mdc\{a_1,\, a_2,\, \dots,\, a_r\}$ desses números é 1, ou ainda, o ideal $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_r\mathbb{Z}$ gerado por esses números inteiros é o próprio anel $\mathbb{Z}$, então a equação diofantina linear

$$a_1x_1 \;+\; a_2x_2 \;+\; \dots \;+\; a_rx_r \;=\; \ell, \tag{2.2}$$

tem solução no conjunto $\mathbb{Z}$ dos números inteiros, qualquer que seja o número inteiro ℓ. Nestas condições, como já vimos analogamente para o caso $r = 2$, existe um número inteiro positivo c tal que, para qualquer número inteiro $\ell \geq c$, esta equação também tem solução no conjunto $\mathbb{N}$ dos números inteiros não-negativos. O clássico *Problema de Frobenius* procura uma forma fechada, a partir dos números $a_1, a_2, \ldots, a_r$, para o maior inteiro ℓ para o qual a equação (2.2) *não* tem solução no conjunto $\mathbb{N}$. A solução desse problema no caso $r = 2$ é $\ell = (a_1 - 1)(a_2 - 1) - 1$ de acordo com o Teorema (33). O problema de Frobenius para o caso $r = 3$ já foi, e continua sendo, fonte de uma vasta publicação científica.

É claro que se a equação (2.2) tem solução em $\mathbb{N}$ quando $\ell = \ell'$ e $\ell = \ell''$ então ela também tem solução em $\mathbb{N}$ quando $\ell = \ell' + \ell''$. Esta propriedade, juntamente com o fato mencionado no parágrafo anterior da existência do número inteiro c naquelas condições, motivam a seguinte definição. Um subconjunto N dos números inteiros não-negativos é um *semigrupo numérico* se ele é fechado em relação a adição, isto é $N + N \subseteq N$, e se $L = \mathbb{N}\backslash N$, o complementar de N em $\mathbb{N}$, é um conjunto com uma quantidade finita de elementos. A cardinalidade g do conjunto $L = \{\ell_1 < \ell_2 < \cdots < \ell_g\}$ é o *gênero* de $N = \{0 = n_0 < n_1 < \ldots\}$ e cada número inteiro $\ell_i \in L$ (respectivamente $n_j \in N$) é uma *lacuna* (respectivamente *não-lacuna*) do semigrupo numérico N. O menor elemento positivo n_1 é chamado a *multiplicidade* de N. Para cada número inteiro $g \geq 0$ representamos por η_g a quantidade de semigrupos numéricos de gênero g.

Exemplo 34 *Os semigrupos numéricos de gênero até 3 são os seguintes:*

i) $\mathbb{N}$ *e* $\eta_0 = 1$*;*

ii) $\mathbb{N}\backslash\{1\}$ *e* $\eta_1 = 1$*;*

iii) $\mathbb{N}\backslash\{1, 2\}$, $\mathbb{N}\backslash\{1, 3\}$ *e* $\eta_2 = 2$*;*

iv) $\mathbb{N}\backslash\{1, 2, 3\}$, $\mathbb{N}\backslash\{1, 2, 4\}$, $\mathbb{N}\backslash\{1, 2, 5\}$, $\mathbb{N}\backslash\{1, 3, 5\}$ *e* $\eta_3 = 4$.

Exercício 35 *Determine quantos e quais são todos os semigrupos numéricos de gênero* 4.

Observação 36 *Se N é um semigrupo numérico de gênero g então existem números inteiros positivos $a_1, a_2, \ldots, a_r$, primos entre si, tais que cada elemento n de N é escrito da forma $n = a_1m_1 + a_2m_2 + \cdots + a_rm_r$, onde cada m_i é um número inteiro não-negativo; isto é, para cada $\ell \in N$ a equação diofantina (2.2) tem solução em $\mathbb{N}$. Nestas condições escrevemos $N = a_1\mathbb{N} + a_2\mathbb{N} + \cdots + a_r\mathbb{N}$.*

Segue da definição de semigrupo numérico de gênero g que os seguintes números inteiros positivos $\ell_g - n_{(\ell_g - g)}$, $\ell_g - n_{(\ell_g - g - 1)}$, $\ldots, \ell_g - n_0$, no total de $\ell_g - g + 1$ elementos, pertencem ao conjunto L, o qual tem g elementos. Portanto a maior lacuna ℓ_g é limitada superiormente por $2g - 1$, isto é, $\ell_g \leq 2g - 1$. Um semigrupo numérico de gênero g é *simétrico* quando ocorre a igualdade $\ell_g = 2g - 1$. Neste caso o conjunto de lacunas é dado por

$$L = \{\ell_g - n_{(\ell_g - g)}, \ \ell_g - n_{(\ell_g - g - 1)}, \ \ldots, \ell_g - n_0\},$$

e tem a interessante propriedade de simetria: para cada número inteiro ℓ, tem-se $\ell \in L$ se, e somente se, $\ell_g - \ell \notin L$. No teorema (33) mostramos que os semigrupos numéricos $m\mathbb{N} + n\mathbb{N}$, onde m e n são números inteiros positivos primos entre si, são semigrupos simétricos.

Sobre a quantidade η_g de semigrupos numéricos de gênero g, analisando os valores para $g \leq 50$, M. Brás-Amorós conjecturou que eles têm um comportamento assintótico semelhantes ao dos números de Fibonacci. Mais precisamente ela fez a seguinte conjectura:

Conjectura 37 *M. Brás-Amorós [2008]*

i) $\eta_g \geq \eta_{g-1} + \eta_{g-2}$, $g \geq 2$,

ii) $\lim_{g\to\infty}(\eta_{g-1} + \eta_{g-2})/\eta_g = 1$,

iii) $\lim_{g\to\infty} \eta_g/\eta_{g-1} = \rho$, *onde* ρ *é a razão áurea.*

Em 2009 ela obteve as seguintes cotas para o número η_g de semigrupos numéricos de gênero g: $2F_g \leq \eta_g \leq 1 + 3\ 2^{g-3}$. Em 2010, Y. Zhao observou que o item (ii) da conjectura de Brás-Amorós decorre facilmente do item (iii) [Exercício (40)] e fez a seguinte conjectura:

Conjectura 38 *Y. Zhao [2010]* $\lim_{g\to\infty} \eta_g \rho^{-g} < \infty$.

Essa surpreendente relação da quantidade de semigrupos numéricos com os números de Fibonacci está confirmada de forma precisa na seguinte proposição.

Proposição 39 *Y. Zhao [2010] Para cada número inteiro positivo g, a quantidade de semigrupos numéricos de gênero g com a maior lacuna menor do que o dobro da multiplicidade é o número de Fibonacci* F_{g+1}.

Prova. Seja m um número inteiro positivo. Vamos contar inicialmente o número de semigrupos numéricos de gênero g tal que $\ell_g < 2m$. Podemos verificar que qualquer tal semigrupo numérico é dado por

$$\{0\} \cup \{m\} \cup S \cup [2m,\ \infty) \cap \mathbb{N},$$

onde o subconjunto $S \subset [m+1,\ m-1] \cap \mathbb{N}$ tem cardinalidade $|S| = 2m-2-g$. Assim, nestas condições, temos exatamente $\binom{m-1}{2m-2-g}$ tais semigrupos. Pela proposição (25), o resultado segue considerando-se a soma de todas as multiplicidades menores do que g, isto é, $\sum_{m=1}^{g} \binom{m-1}{2m-2-g} = \sum_{m}^{g} \binom{g-(g-m+1)}{g-m+1} = F_{g+1}$. $\triangle$

Exercício 40 *Mostre que o item (iii) na conjectura de Brás-Amorós (37)* implica o item (ii).

Exercício 41 *(**) R.-O.Buchweitz [1980] Existe um semigrupo numérico de gênero* $g = 16$ *com a cardinalidade do conjunto* $L + L$ *maior do que* $3g - 3$.
Aviso: Existem $\eta_{16} = 4.806$ *semigrupos numéricos de gênero* $g = 16$.

Exercício 42 *(**) Mostre que se* $g \leq 15$ *então, para qualquer semigrupo numérico de gênero g, o conjunto* $L + L$ *tem no máximo* $3g - 3$ *elementos.*

Exercício 43 *(**) G. Oliveira [1989] Mostre que se N é um semigrupo numérico de gênero g com multiplicidade* $m \geq 3$ *então ele é simétrico se, e somente se,* $|nL| = (2n-1)(g-1)$ *para todo número inteiro* $n \geq 2$, *onde nL representa o conjunto de todas as somas de n lacunas de N.*

Exercício 44 *(**) Mostre que* $\eta_{50} = 101.090.300.128$.

5 Grupos e a Função ϕ de Euler

Consideremos o produto cartesiano $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ com as operações de adição e multiplicação componente à componente dos correspondentes anéis. Nestas condições obtemos um outro anel chamado *produto direto* dos anéis $\mathbb{Z}_{m_1}, \ \ldots, \ \mathbb{Z}_{m_r}$. A função $\psi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, definida de maneira que cada componente da imagem de cada número inteiro n é a classe de equivalência de n no correspondente anel, é um *homomorfismo de anéis*, isto significa que a função ψ é compatível com as operações de adição e multiplicação dos anéis. Mais precisamente, dados números inteiros quaisquer a e b tem-se $\psi(a+b) = \psi(a) + \psi(b)$ e $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$. O conjunto de todos os elementos de $\mathbb{Z}$ cuja imagem é o elemento neutro da adição do produto direto é um ideal de $\mathbb{Z}$, chamado *núcleo* do homomorfismo ψ.

Teorema 45 *Teorema Chinês dos Restos. Se* $mdc\{m_i, \ m_j\} = 1$, $i \neq j$, *então a função* ψ *é sobrejetiva.*

Prova. É fácil verificar que o ideal de $\mathbb{Z}$ gerado por $m_1 m_2 \ldots m_r$ está contido no núcleo do homomorfismo ψ. Estes conjuntos são na verdade iguais já que por hipótese os inteiros m_i e m_j, $i \neq j$, são primos entre si. Como a função ψ é um homomorfismo as imagens das $m_1 m_2 \ldots m_r$ diferentes classes de equivalência do anel quociente $\mathbb{Z}/(m_1 m_2 \ldots m_r)\mathbb{Z}$ são todas distintas. Por outro lado o número de elementos do anel $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ é exatamente $m_1 m_2 \ldots m_r$. Portanto a função ψ é sobrejetiva. $\triangle$

Exemplo 46 *Determinar o inteiro* n *entre* 0 *e* 64 *que tem resto* 3 *e* 6 *quando dividido por* 5 *e* 13*, respectivamente.*

Podemos listar, como na tabela abaixo, todos os inteiros entre 0 e 64. O número procurado encontra-se na quarta linha e sétima coluna, isto é, $n = 58$. Será que o leitor consegue justificar a construção da tabela e a afirmação feita sobre o inteiro n?

$\mathbb{Z}_5 \times \mathbb{Z}_{13}$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	40	15	55	30	5	45	20	60	35	10	50	25
1	26	1	41	16	56	31	6	46	21	61	36	11	51
2	52	27	2	42	17	57	32	7	47	22	62	37	12
3	13	53	28	3	43	18	58	33	8	48	23	63	38
4	39	14	54	29	4	44	19	59	34	9	49	24	64

Uma interessante aplicação prática do teorema chinês dos restos é a partilha de senhas.

Exercício 47 *Prove que se* $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ *é uma sequência ascendente de ideais de* $\mathbb{Z}$ *então ela é finita, isto é, existe algum inteiro* j *tal que* $I_j = I_{j+i}$*, para todo número inteiro* i *positivo.*

Um conjunto com uma operação satisfazendo as três primeiras condições da Observação 10 é chamado *grupo*. Se a quarta condição também é satisfeita então o grupo é dito *abeliano* (ou *comutativo*). A *ordem* de um grupo é a quantidade de elementos do grupo. Por exemplo, considerando a operação de adição, o anel $\mathbb{Z}_n$ é um grupo abeliano de ordem n. Segue da Proposição 14 que se p é um número primo então $\mathbb{Z}_p \backslash \{0\}$ tem $p-1$ elementos e, com a operação de multiplicação, é um grupo abeliano. Este é um caso particular do resultado abaixo.

Proposição 48 *O conjunto* $U_n = \{\bar{a} \in \mathbb{Z}_n : mdc\{a,\ n\} = 1\}$ *é um grupo multiplicativo abeliano.*

Prova. Pelo Teorema Fundamental da Aritmética se $\bar{a}$ e $\bar{b}$ são elementos de U_n então $\bar{a}\bar{b}$ pertence a U_n. Daí, como $\mathbb{Z}_n$ é um anel, é suficiente mostrar que cada elemento de U_n tem inverso. Seja então $\bar{a} \in U_n$. Segue da definição de U_n e da Proposição 23 que existem inteiros r e s tais que $ra + sn = 1$. Consequentemente, considerando as classes de equivalências, temos $\bar{r}\bar{a} = \bar{1}$, ou seja, $\bar{r}$ é o inverso de $\bar{a}$. $\triangle$

A *função* ϕ *de Euler* é a função $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ que associa a cada inteiro positivo n o número $\phi(n)$ de inteiros j entre 1 e n tais que j e n são primos entre si, isto é, $\phi(n) = |\{j : 1 \leq j \leq n,\ mdc\{j,\ n\} = 1\}|$. Por exemplo temos $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$ e $\phi(4) = 2$. Segue da proposição anterior que $\phi(n)$ é a ordem do grupo multiplicativo U_n, $n \geq 2$. Se a fatoração de $n > 1$ é dada, então $\phi(n)$ pode ser calculado explicitamente conforme a próxima proposição.

Proposição 49 *Se* $e_1,\ e_2,\ \ldots,\ e_r$ *são inteiros positivos e* $p_1,\ p_2,\ \ldots,\ p_r$ *são primos distintos então*

$$\phi(p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}) = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_r}).$$

Prova. Sejam a e b inteiros positivos primos entre si. Para cada inteiro n, $1 \leq n \leq ab$, tem-se $mdc\{n,\ ab\} = 1$ se, e somente se, $mdc\{r,\ a\} = 1$ e $mdc\{s,\ b\} = 1$, onde $0 < r < a$, $0 < s < b$ e os inteiros $n - r$, $n - s$ são múltiplos de a e b, respectivamente. Portanto segue da definição da função de Euler que $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. Podemos concluir por indução que $\phi(p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}) = \phi(p_1^{e_1}) \cdot \phi(p_2^{e_2}) \cdots \phi(p_r^{e_r})$. Para calcular $\phi(p_j^{e_j})$ basta observar que os inteiros entre 1 e $p_j^{e_j}$ que têm algum fator primo p_j são exatamente os inteiros mp_j, onde $1 \leq m \leq p_j^{e_j - 1}$. Daí $\phi(p_j^{e_j}) = p_j^{e_j} - p_j^{e_j - 1}$. $\triangle$

Já vimos anteriormente que um grupo é um conjunto com uma operação satisfazendo as três primeiras condições da Observação 10. Se um subconjunto H de um grupo G é também um grupo com a operação induzida do grupo G então H é chamado um *subgrupo* de G. Isto significa que $H \subset G$ não é vazio e que, se $*$ é a operação do grupo G, então $a * b$ pertence a H para cada par $a,\ b$ de elementos de H, e também que H é um grupo com a operação $*$ restrita ao conjunto H. Cada ideal de um anel é um subgrupo do anel considerado como um grupo aditivo. Outro exemplo de subgrupo de um grupo G é obtido tomando-se um elemento qualquer a do grupo e considerando-se o chamado *subgrupo gerado* por a dado por $< a >= \{a^j :\ j \in \mathbb{Z}\}$.

A *ordem* do elemento a do grupo G é o inteiro $ord\, a = |< a >|$ igual a ordem do subgrupo gerado por ele. Se existe algum elemento $a \in G$ tal que $< a >= G$ dizemos que G é um grupo *cíclico*. No caso de grupo finito, isto significa que existe algum elemento cuja ordem é a ordem do grupo. Veremos posteriormente que o grupo multiplicativo $\mathbb{Z}_p$, p primo, é um grupo cíclico. Mais geralmente, veremos que o grupo multiplicativo $K\backslash\{0\}$ de um corpo finito K é um grupo cíclico (Proposição 53).

Dado um subgrupo H de um grupo abeliano G, definimos uma relação de equivalência $\equiv$ em G da seguinte maneira: se $a, b \in G$ então $a \equiv b$ se, e somente se, $a * b^{-1} \in H$. Para cada elemento a do grupo G, a *classe de equivalência* de a determinada por H, representada por $\bar{a}$, é o conjunto de todos os elementos $b \in G$ tais que a e b são equivalentes.

Como o grupo G considerado acima é abeliano, o conjunto G/H de todas as classes de equivalências determinadas por H também é um grupo abeliano com a operação $\bar{a} * \bar{b} = \overline{(a * b)}$. Ele é chamado o *grupo quociente* do grupo abeliano G pelo subgrupo H. Observamos que no caso em que o grupo G não é abeliano o conjunto das classes de equivalência pode não ser um grupo.

O nosso principal interesse aqui é considerar grupos abelianos com uma quantidade finita de elementos. Dados um grupo abeliano G finito e um subgrupo H de G, cada classe de equivalência determinada por H tem a mesma quantidade $|H|$ de elementos. De fato, dado $a \in G$ a função $f : H \to \bar{a}$, definida por $f(h) = h^{-1} * a$ é uma bijeção. Isto prova, no caso de grupos abelianos, o seguinte teorema.

Teorema 50 *Teorema de Lagrange. Se G é um grupo finito e H é um subgrupo de G então a ordem de H divide a ordem de G.*

Prova. No caso de grupo abeliano a demostração foi feita no comentário que antecede o teorema. Se o grupo não é abeliano, defina a noção de classe lateral à esquerda (ou à direita) e siga, com a devida coerência, como na demonstração do teorema para grupo abeliano. $\triangle$

Corolário 51 *Teorema de Euler. Sejam a e n números inteiros , $n > 0$.*
Se $mdc\{a, n\} = 1$ então

$$a^{\phi(n)} \equiv 1 mod\, n.$$

Prova. Como mdc$\{a, n\} = 1$, a classe $\overline{a}$ em $\mathbb{Z}_n$ pertence ao grupo multiplicativo U_n (proposição 48). Usando o Teorema de Lagrange, concluimos que a ordem de $\overline{a}$, indicada aqui por r, divide a ordem de U_n, que é igual a $\phi(n)$. Logo $\phi(n) = r.k$, para algum número inteiro $k > 0$. Portanto, $(\overline{a})^{\phi(n)} = ((\overline{a})^r)^k = \overline{1}$, o que significa $a^{\phi(n)} \equiv 1 \text{ mod } n$. $\triangle$

Capítulo 3

Corpos Finitos

1 Definições e Exemplos

O *corpo quociente* $\mathbb{Z}_p$ do anel dos números inteiros $\mathbb{Z}$ pelo *ideal* gerado pelo número primo p é um exemplo de um corpo finito com p elementos. Em outras palavras, no conjunto de todos os possíveis restos da divisão de um número inteiro pelo primo p é possível definir operações de adição e de multiplicação de maneira que todo elemento tem simétrico e todo elemento não nulo tem inverso.

Dado um corpo qualquer K, o homomorfismo $\psi : \mathbb{Z} \to K$, do anel dos números inteiros $\mathbb{Z}$ no corpo K, tal que $\psi(1) = 1$, ou é injetivo ou o seu núcleo é o ideal não-nulo gerado por algum número primo, digamos p. No primeiro caso K é um corpo de *característica zero* e no outro K é um corpo de *característica p*. Se K é finito então apenas o segundo caso ocorre e, tomando-se o homomorfismo determinado por ψ no corpo quociente, obtem-se um subcorpo de K isomorfo ao corpo $\mathbb{Z}_p$. Assim, nesse caso, podemos considerar $\mathbb{Z}_p$ como um subcorpo de K e assim K é um espaço vetorial de dimensão finita sobre $\mathbb{Z}_p$.

Veremos a seguir que os possíveis valores do número de elementos de um corpo finito devem ser bem especiais.

Proposição 52 *Se K é um corpo finito de característica p com $q = |K|$ elementos então existe um inteiro positivo m tal que $q = p^m$.*

Prova. Fixada uma base do espaço vetorial K sobre o corpo $\mathbb{Z}_p$, digamos $u_1, ..., u_m$, cada elemento $\alpha \in K$ pode ser escrito de modo único na forma $\alpha = \sum a_j u_j$, onde $a_1, ..., a_m$ são elementos de $\mathbb{Z}_p$. Portanto o número q de elementos de K é p^m. $\triangle$

Veremos posteriormente que a recíproca da proposição acima é verdadeira. O subconjunto $K^* = K\backslash\{0\}$, de um corpo K com p^m elementos, é um grupo multiplicativo e portanto (segue do teorema de Lagrange que) as ordens dos seus elementos são divisores de $p^m - 1$. Veremos a seguir que esse grupo é cíclico, isto é, existe algum elemento de ordem $p^m - 1$ em K^*.

Proposição 53 *Se K é um corpo finito então $K^* = K\backslash\{0\}$ é um grupo cíclico.*

Prova. Segue da proposição anterior que o número de elementos de K é da forma p^m, onde p é um número primo. Para cada inteiro positivo r, seja n_r o número de elementos de ordem r de K^*. Como o grupo multiplicativo K^* tem ordem $p^m - 1$, pelo Teorema de Lagrange (50), o inteiro n_r é nulo quando r não é um divisor de $p^m - 1$. Além disso, se n_r não é nulo e $\alpha \in K^*$ tem ordem r então, para cada inteiro positivo $j \leq r$ que é relativamente primo com r, o elemento α^j também tem ordem r. Portanto no subgrupo gerado por α existem $\phi(r)$ elementos de ordem r, onde ϕ é a função de Euler. Daí $n_r \geq \phi(r)$. O número de raízes de um polinômio de grau t com coeficientes em um corpo é no máximo t, portanto o número de raízes primitivas da unidade de ordem r em K é no máximo $\phi(r)$. Consequentemente se n_r é diferente de zero então $n_r = \phi(r)$. Analisando-se o número de geradores de

todos os possíveis subgrupos de um grupo cíclico de ordem ℓ obtem-se $\sum_{r|\ell}\phi(r)=\ell$. Pela definição de n_r tem-se $\sum_{r|(p^m-1)}n_r=p^m-1$ e portanto, dessas duas últimas igualdades, obtem-se $n_r=\phi(r)$ para cada divisor r de p^m-1. Em particular $n_{(p^m-1)}=\phi(p^m-1)$ é positivo, isto é, existe algum elemento de K^* de ordem p^m-1. Assim o grupo multiplicativo K^* é cíclico. $\triangle$

Exemplo 54 *Os geradores do grupo multiplicativo de* $\mathbb{Z}_5=\{-2,-1,0,1,2\}$, *isto é, do grupo* $\mathbb{Z}_5^*$, *são* 2 *e* $2^3=-2$. *Analogamente, os geradores do grupo multiplicativo de* $\mathbb{Z}_7=\{-3,-2,-1,0,1,2,3\}$ *são* 3 *e* $3^5=-2$, *e os geradores do grupo multiplicativo de* $\mathbb{Z}_{11}=\{-5,-4,-3,-2,-1,0,1,2,3,4,5\}$ *são* -5, $(-5)^3=-4$, $(-5)^7=-3$ *e* $(-5)^9=2$.

Os elementos não nulos de um corpo finito K com $q=p^m$ elementos são as raízes do polinômio $X^{(q-1)}-1$, ou ainda, todos os elementos de K são as raízes do polinômio $f(X)=X^q-X$, o qual não tem raiz múltipla dado que a derivada $f'(X)$ do polinômio $f(X)$ é igual a $qX^{(q-1)}-1$, isto é, $f'(X)=-1$. Assim K é o corpo de decomposição deste polinômio. Desta forma, admitindo-se a existência de um corpo algebricamente fechado com característica p, obtemos a existência de um corpo finito com $q=p^m$ elementos como o corpo de decomposição do polinômio X^q-X. A partir do estudo de polinômios irredutíveis sobre o corpo $\mathbb{Z}_p$, p primo, provaremos posteriormente, de forma alternativa, para cada inteiro positivo m, a existência de um corpo com p^m elementos.

A seguir usamos a teoria de grupos para apresentar uma outra prova do pequeno teorema de Fermat (corolário 15).

Corolário 55 *Pequeno Teorema de Fermat. Se* p *é um número inteiro primo então* $a^p=a$, *para cada elemento* a *do corpo* $\mathbb{Z}_p$.

Prova. Já sabemos que $\mathbb{Z}_p\backslash\{0\}$ é um grupo multiplicativo com $\phi(p)=p-1$ elementos. Pelo Teorema de Lagrange (50) a ordem de cada elemento a de $\mathbb{Z}_p\backslash\{0\}$ é um divisor de $p-1$, portanto $a^{p-1}=1$ em $\mathbb{Z}_p$ e logo $a^p=a$. O resultado é claramente válido se $a=0$. $\triangle$

Segue do Pequeno Teorema de Fermat que se $\alpha^n\not\equiv\alpha\ mod\ n$ para algum número inteiro α então n não é primo.

Corolário 56 *Sejam* K_1 *e* K_2 *corpos finitos de característica* p *com* p^{m_1} *e* p^{m_2} *elementos, respectivamente. O corpo* K_1 *é um subcorpo de* K_2 *se, e somente se,* m_1 *divide* m_2.

Prova. Já sabemos que os corpos K_1 e K_2 são os corpos de decomposição dos polinômios $X^{(p^{m_1})}-X$ e $X^{(p^{m_2})}-X$, respectivamente. Portanto K_1 é um subcorpo de K_2 se, e somente se, $X^{(p^{m_1})}-X$ divide $X^{(p^{m_2})}-X$, isto é, $X^{(p^{m_1}-1)}-1$ divide $X^{(p^{m_2}-1)}-1$. Dados inteiros positivos $a<b$, escrevendo $b=\lambda a+r$, onde λ é um inteiro e $0\leq r<a$, por cálculo direto temos:

$$X^b-1=(X^a-1)(X^{(\lambda-1)a}+...+X^a+1)X^r+(X^r-1).$$

Usando esta identidade com $X=p$, $b=m_2$ e $a=m_1$, e posteriormente com apenas $b=p^{m_2}-1$ e $a=p^{m_1}-1$, e observando que se $0\leq r<m_1$ então $0\leq p^r-1<p^{m_1}-1$, concluimos do algoritmo da divisão que m_1 divide m_2 se, e somente se, $p^{m_1}-1$ divide $p^{m_2}-1$ se, e somente se, $X^{(p^{m_1}-1)}-1$ divide $X^{(p^{m_2}-1)}-1$. $\triangle$

2 Existência de Corpos Finitos

Vimos na seção anterior que a quantidade de elementos de um corpo finito é uma potência de sua característica. Entretanto os únicos exemplos de corpos finitos apresentados até agora são da forma $\mathbb{Z}_p$, onde p é um número primo. Nesta seção vamos provar que para cada número primo p e cada inteiro positivo m existe um corpo com p^m elementos. Isso será feito seguindo a mesma filosofia empregada para obter o corpo $\mathbb{Z}_p$, isto é, como anel quociente de um domínio de integridade conveniente por um ideal maximal.

No exemplo abaixo é apresentado de maneira mais detalhada o método para produzir esses corpos finitos, de característica p, a partir de polinômios irredutíveis sobre o corpo $\mathbb{Z}_p$.

Exemplo 57 *Sejam p um número primo, $\mathbb{Z}_p$ o corpo com p elementos e $f(X)$ um polinômio de grau m, irredutível no anel de polinômios $\mathbb{Z}_p[X]$. O corpo quociente $\mathbb{Z}_p[X]/(f(X))$, do anel $\mathbb{Z}_p[X]$ pelo ideal gerado por $f(X)$, é um corpo de característica p com p^m elementos.*

De acordo com o Exemplo 57 acima a existência de um corpo com p^m elementos depende apenas da existência de um polinômio de grau m irredutível em $\mathbb{Z}_p[X]$.

Teorema 58 *Seja p um número primo. Para cada inteiro positivo m existe um corpo com p^m elementos.*

Prova. Sejam $q = p^m$ e $f(X) = X^q - X$. Pela Proposição 53 os possíveis graus de fatores de $f(X)$, em $\mathbb{Z}_p[X]$, são divisores de m. Seja $f(X) = \prod_{d|m} g_d(X)$ uma fatoração de $f(X)$, onde $g_d(X)$ é o produto dos fatores mônicos de grau d de $f(X)$ irredutíveis em $\mathbb{Z}_p[X]$. Analisando os graus desses polinômios concluimos que $p^m = \sum_{d|m} d\, n_d$, onde n_d é o número de fatores mônicos de $g_d(X)$ irredutíveis em $\mathbb{Z}_p[X]$. Usando a Fórmula de Inversão de Möbius segue a seguinte identidade:

$$m\, n_m = \sum_{d|m} \mu(d) p^{(\frac{m}{d})}, \tag{3.1}$$

onde μ é a função de Möbius definida, no conjunto dos números inteiros positivos, por $\mu(1) = 1$, $\mu(j) = 0$ se na fatoração de j em números primos existe algum com expoente maior do que 1 e $\mu(j) = (-1)^s$ se a fatoração de j tem exatamente s números primos distintos e todos eles com expoente 1. Em particular $n_1 = p$ e $2n_2 = p(p-1)$. Para $m \geq 2$ temos $m\, n_m = \sum_{d|m} \mu(d) p^{(\frac{m}{d})} \geq p^m - (\sum_{j=1}^{[m/2]} p^j) \geq p^{[m/2]}(p^{m-[m/2]} - 2) + 2$, onde $[x]$ é o maior inteiro menor ou igual a x. Assim, concluindo a prova do teorema, temos que n_m é positivo, isto é, existe algum polinômio de grau m irredutível em $\mathbb{Z}_p[X]$. $\triangle$

Exemplo 59 *Seja p um número primo. É claro que para cada $\alpha \in \mathbb{Z}_p$ o polinômio mônico $X - \alpha$ é irredutível em $\mathbb{Z}_p[X]$. Pela equação (3.1) estes são todos os $n_1 = p$ polinômios mônicos de grau um irredutíveis em $\mathbb{Z}_p[X]$.*

Exemplo 60 *a) Pela equação (3.1) existe apenas um polinômio de grau dois mônico e irredutível em $\mathbb{Z}_2[X]$, a saber $X^2 + X + 1$. Usando o Exemplo 57* obtemos um corpo de característica dois com quatro elementos $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, onde $\alpha^2 = \alpha + 1$.

b) Usando o Exemplo 57 obtemos um corpo de característica dois com oito elementos $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$, onde $\alpha^3 = \alpha^2 + 1$ ou $\alpha^3 = \alpha + 1$, conforme a escolha de um dos dois polinômio mônicos irredutíveis em $\mathbb{Z}_2[X]$.

c) Os três polinômios de grau quatro mônicos e irredutíveis em $\mathbb{Z}_2[X]$ são $f_1(X) = X^4 + X^3 + X^2 + X + 1$, $f_2(X) = X^4 + X + 1$ e $f_3(X) = X^4 + X^3 + 1$. Usando o Exemplo 57 obtemos um corpo de característica dois com 16 elementos $\mathbb{F}_{16} = \{\sum_{j=0}^{3} a_j\alpha^j;\ a_j \in \mathbb{Z}_2\}$, onde $f_i(\alpha) = 0$, para algum $i = 1, 2, 3$.

Exemplo 61 *O polinômio $X^2 + X + 2$ é irredutível em $\mathbb{Z}_5[X]$. Pelo Exemplo 57* obtemos um corpo com 25 elementos $\mathbb{F}_{5^2} = \{a + b\alpha;\ a, b \in \mathbb{Z}_5\}$, onde $\alpha^2 = -\alpha - 2$. Afirmamos que α é um gerador do grupo cíclico $\mathbb{F}_{5^2}\backslash\{0\}$. De fato, calculando potências convenientes de α, temos:

$$\alpha^3 = -\alpha^2 - 2\alpha = -\alpha + 2,\ \alpha^6 = (\alpha^3)^2 = \alpha^2 + \alpha - 1 = 2,\ \alpha^{12} = -1,\ \alpha^{24} = 1.$$

A ordem de α é 24 já que as possíveis ordens são divisores de 24 e ela, de acordo com os cálculos acima, não pode ser um divisor de 8. Portanto α é um gerador do grupo $\mathbb{F}_{5^2}\backslash\{0\}$.

Nos corpos de característica positiva o cálculo de potências de binômios, cujos expoentes são potências da característica, torna-se mais simples. Mais precisamente vale a seguinte regra:

Proposição 62 *Se p é primo então p divide $\binom{p}{j}$ para cada $j = 1, ..., p-1$. Em particular, se K é um corpo de característica p e a e b são elementos de K então, para cada inteiro positivo n, tem-se*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Prova. A primeira afirmação segue da hipótese de p ser primo e da definição $\binom{p}{j} = p(p-1)...(p-j+1)/j!$. Usando o desenvolvimento binomial temos $(a+b)^p = a^p + b^p + \sum_{j=1}^{p-1}\binom{p}{j}a^j b^{p-j}$. Pela afirmação anterior temos que $\binom{p}{j}$ é nulo em K, para cada $j = 1, ..., p-1$, e logo $(a+b)^p = a^p + b^p$. Agora admitindo que $(a+b)^{p^{n-1}} = a^{p^{n-1}} + b^{p^{n-1}}$ temos $(a+b)^{p^n} = ((a+b)^{p^{n-1}})^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = a^{p^n} + b^{p^n}$. A conclusão resulta então do princípio de indução. $\triangle$

Seja K um corpo qualquer de característica p. Segue da Proposição 62 que a aplicação $\phi : K \to K$, que associa a cada $\alpha \in K$ o elemento $\phi(\alpha) = \alpha^p$, é um homomorfismo. No caso em que K é finito esta aplicação é um isomorfismo, chamado *isomorfismo de Frobenius*. Se K não é finito então a aplicação ϕ é injetiva mas pode não ser sobrejetiva conforme o exemplo a seguir. Para verificar a injetividade, sejam α e β elementos de K tais que $\alpha^p = \beta^p$. Se α ou β não é nulo então existe γ em K tal que $\gamma^p = 1$, isto é, γ é raiz do polinômio $X^p - 1 \in \mathbb{Z}_p[X]$, e assim γ é algébrico sobre $\mathbb{Z}_p$ e a sua ordem é 1 ou p. Mais ainda, γ é um elemento não nulo de um corpo finito e daí a ordem de γ é um divisor de $p^m - 1$ para algum $m \geq 1$. Portanto $\gamma = 1$ já que p e $p^m - 1$ são relativamente primos.

Exemplo 63 *Seja K um corpo qualquer de característica p e seja X um elemento transcendente sobre K. O homomorfismo injetivo $\psi : K(X) \to K(X)$, $\psi(\alpha) = \alpha^p$, não é sobrejetivo pois $X \notin \psi(K(X))$.*

No exemplo anterior X é a única raiz do polinômio $Y^p - X^p \in K(X^p)[Y]$ e a sua multiplicidade é p. Assim temos um exemplo de um polinômio irredutível com raiz múltipla; de fato, segue da Proposição 62 que $Y^p - X^p = (Y - X)^p$. Este fenômeno não pode ocorrer em corpos finitos ou em corpos com característica zero.

Capítulo 4

Curvas Algébricas

1 Espaços Projetivos

Seja K um corpo. No produto cartesiano K^{n+1} de dimensão $n+1$ definimos uma relação de equivalência entre os elementos não nulos da seguinte forma:

$$\alpha \sim \beta \Leftrightarrow \alpha = \lambda\beta, \text{ para algum } \lambda \in K\backslash\{0\}.$$

O *espaço projetivo* $\mathbb{P}^n = \mathbb{P}^n(K)$ de dimensão n é o conjunto de todas as possíveis classes de equivalência dessa relação. Em outras palavras, $\mathbb{P}^n$ é o conjunto de todas as retas de K^{n+1} que passam pela origem. Dado um ponto não nulo $(a_0, a_1, ..., a_n)$ de K^{n+1} o correspondente ponto do espaço projetivo $\mathbb{P}^n$ é representado em *coordenadas homogênias* por $(a_0 : a_1 : ... : a_n)$. Para cada constante não nula λ observamos que $(a_0 : a_1 : ... : a_n)$ e $(\lambda a_0 : \lambda a_1 : ... : \lambda a_n)$ são representaões em *coordenadas homogênias* de um mesmo ponto de $\mathbb{P}^n$.

Exemplo 64 *A reta projetiva* $\mathbb{P}^1$ *pode ser identificada com a união disjunta* $K \cup \{\infty\}$, *do corpo* K *juntamente com um outro ponto representado por* ∞, *chamado infinito. Mais precisamente, a cada* $a \in K$ *associamos o ponto* $(a : 1)$ *e ao ponto infinito associamos o ponto* $(1 : 0)$, *chamado ponto no infinito.*

Exemplo 65 *O plano projetivo* $\mathbb{P}^2$ *pode ser identificado com a união disjunta* $K^2 \cup K \cup \{\infty\}$, *de* K^2 *com a reta projetiva. Mais precisamente, a cada ponto* $(a, b) \in K^2$ *associamos o ponto* $(a : b : 1)$ *e a cada ponto* $(a : b)$ *da reta projetiva associamos o ponto* $(a : b : 0)$.

2 Curvas Algébricas Planas Projetivas

Dado um polinômio $f(X, Y)$ de grau $d \geq 1$ no anel de polinômios $K[X, Y]$, onde K é um corpo, definimos a *curva algébrica plana afim* C_f sobre K como sendo

$$C_f(K) = \{(x, y) \in K^2 : \ f(x, y) = 0\}.$$

Considerando o polinômio homogêneo $F(X, Y, Z) = Z^d f(X/Z, Y/Z)$ no anel de polinômios $K[X, Y, Z]$, definimos a *curva algébrica plana projetiva* C_F sobre K como sendo

$$C_F(K) = \{(x : y : z) \in \mathbb{P}^2(K) : \ F(x, y, z) = 0\}.$$

Desta forma o ponto (x, y) da curva C_f corresponde ao ponto $(x : y : 1)$ da curva C_F. Se f é irredutível em $K[X, Y]$ então as curvas C_f e C_F são *irredutíveis.* Para cada $\lambda \in K\backslash\{0\}$ é claro que $C_{\lambda f} = C_f$ e $C_{\lambda F} = C_F$. A curva C_F é chamada *reta, cônica, cúbica,* se o grau de F é igual a 1, 2, 3, respectivamente. Um ponto P de uma curva C_F é *singular* se as derivadas de F com relação a X, Y e Z são nulas em P. Se a curva C_F de grau d não tem pontos singulares então o inteiro $g = (d-1)(d-2)/2$ é chamado o *gênero* de C_F.

Exemplo 66 *Dados a, b, c elementos não todos nulos de um corpo K, a curva projetiva $\{(x : y : z);\ ax+by+cz=0\}$ é uma reta em $\mathbb{P}^2$, não tem ponto singular e o seu gênero é zero, enquanto a curva plana projetiva $\{(x : y : z);\ ax^2+bxy+cy^2=0\}$ é uma cônica.*

Se o corpo K é algebricamente fechado temos o resultado seguinte.

Teorema 67 *(Teorema de Bezout) Se C_1 e C_2 são curvas algébricas planas projetivas de graus d_1 e d_2 sem componente comum, então o número de pontos de interseção das curvas, contados com multiplicidades, é o produto d_1d_2.*

Capítulo 5

Curvas Elípticas

1 Definição e Exemplos

A teoria das curvas elípticas é um dos mais belos assuntos da matemática e tem aplicações em diversas áreas, por exemplo em geometria diferencial (superfícies mínimas), teoria dos números (último teorema de Fermat - teorema de Wiles/Taylor), geometria algébrica sobre corpos finitos (teorema de Hasse/Weil - hipótese de Riemann) e criptografia (senhas, autenticações e assinaturas digitais, etc.).

Uma *curva elíptica* é uma curva algébrica não-singular de gênero um (com algum ponto racional). Se o corpo K tem característica diferente de dois e três então uma curva elíptica sobre K pode ser determinada pelo polinômio $f(X,Y) = Y^2 - X^3 - aX - b$ no anel $K[X,Y]$, onde $4a^3 + 27b^2$ não é zero, isto é, a curva elíptica pode ser representada no plano projetivo por

$$C = \{(x : y : z) \in \mathbb{P}^2 : \ y^2z = x^3 + axz^2 + bz^3\}. \tag{5.1}$$

A condição nos coeficientes de f é equivalente a não existência de pontos singulares da curva C_f. O ponto $(0 : 1 : 0)$ é o único ponto da curva elíptica no infinito, ele é um ponto de inflexão e não é ponto singular. Portanto o gênero dessa curva é um.

Exemplo 68 *Algumas representações geométricas de curvas elípticas podem ser encontradas nos endereços:*
http://mathworld.wolfram.com/EllipticCurve.html
http://www.certicom.com/ecc_tutorial/ecc_javaCurve.html.

2 Propriedades

A principal razão para o uso de curvas elípticas em criptografia é a existência de uma estrutura de grupo em tais curvas.

A operação do grupo na curva elíptica (5.1) é definida da seguinte maneira. O ponto no infinito $(0 : 1 : 0)$ é o elemento neutro $\mathcal{O}$ do grupo. Dados pontos P e Q da curva, segue do teorema de Bezout, que existe um "terceiro" ponto na interseção da curva com a reta l_{PQ} determinada por P e Q (Se $P = Q$ então l_{PQ} é a reta tangente à curva em P). O inverso do ponto P, representado por $-P$, é o ponto da curva tal que P, $\mathcal{O}$ e $-P$ são colineares. O ponto $P+Q$ é definido como sendo o ponto da curva tal que P, Q e $-(P+Q)$ são colineares. A curva elíptica (5.1) com esta operação é um grupo abeliano, isto é, $P + Q = Q + P$. Uma visão geométrica da operação do grupo pode ser obtida no seguinte endereço:
www.certicom.com/index.php/21-elliptic-curve-addition-a-geometric-approach.

Observação. Na definição da operação do grupo acima foi usado o teorema de Bezout para garantir a existência do "terceiro" ponto de interseção da reta com a curva elíptica. No caso em que o corpo não é algebricamente fechado isto pode ser contornado por meio da determinação explícita das coordenadas desse "terceiro" ponto de interseção a partir das coordenadas dos outros dois pontos ([1], [4]).

Se a curva elíptica está definida sobre um corpo finito com q elementos então o número N de pontos da curva está controlado de acordo com o resultado seguinte.

Teorema 69 *(Teorema de Hasse) O número N de pontos da curva elíptica sobre $\mathbb{F}_q$ satisfaz* $1 + q - 2\sqrt{q} \leq N \leq 1 + q + 2\sqrt{q}$.

O teorema acima foi generalizado por A. Weil para curvas não singulares sobre o corpo $\mathbb{F}_q$ de gênero $g \geq 1$, (análogo da Hipótese de Riemann Clássica):

$$1 + q - 2g\sqrt{q} \leq N \leq 1 + q + 2g\sqrt{q}.$$

Posteriormente ele foi generalizado por P. Deligne para variedades algébricas sobre corpos finitos (Conjectura de Weil).

Capítulo 6

Criptografia

O primeiro sistema de chave pública foi proposto por Diffie e Helmann em 1976. Anteriormente as comunicações por meio de transmissão de mensagens criptografadas eram feitas com uso das chamadas chaves privadas, ou chaves simétricas. Este processo permite ao usuário com conhecimento da chave do sistema tanto criptografar como decifrar mensagens. Isto por si só já impõe restrições ao conhecimento prévio da chave pelos usuários. Neste caso há necessidade de um encontro pessoal prévio entre os envolvidos na comunicação ou há necessidade de transmissão da chave do sistema por algum outro meio, o que pode tornar o processo mais vulnerável.

O ponto crucial na idéia da chave pública consiste em usar uma função f com a propriedade que seja prático, do ponto de vista computacional, calcular $f(n)$ mas que seja inviável na prática calcular a imagem inversa $f^{-1}(m)$. No caso do sistema de criptografia RSA a chave pública apoia-se na facilidade de se efetuar a multiplicação de números primos e na dificuldade prática de se inverter o processo, ou seja, de fatorar números inteiros. No sistema de criptografia ECC a chave pública apoia-se no chamado problema do logaritmo discreto.

Antes de criptografar uma mensagem sabemos que o texto original deve ser previamente adaptado ao sistema através do qual será feita a sua transmissão. Este procedimento, chamado pré-codificação, usualmente consiste em considerar uma correspondência bijetiva entre o conjunto de todos os possíveis símbolos usados na redação da mensagem, por exemplo, o alfabeto juntamente com acentos e pontuação do idioma utilizado, e um conjunto apropriado de sequências finitas de números. Um exemplo de tal correspondência é dado pelo ASCII, que são as iniciais das palavras em inglês de código padrão americano de intercâmbio de informação, e é bastante usado em computadores. Outros exemplos são EBCDIC (adotado pala IBM), HTML (usado na comunicação via internet) e Unicode (implementado em todos os sistemas operacionais modernos e nas linguagens de computação).

Vamos admitir no que segue que uma pré-codificação já está estabelecida. Isto já ocorre naturalmente quando digitamos um texto a partir de um teclado de um computador e visualizamos o resultado dessa ação projetado no monitor do mesmo. Este também é o caso quando imprimimos um arquivo usando uma das opções possíveis, tais como: pdf, doc, odt, rtf, txt.

1 Criptografia RSA

Vamos apresentar agora o sistema de criptografia RSA. Consideremos que dois usuários desejam combinar, por meio de um canal de comunicação pública, uma chave para comunicação privada entre eles usando o sistema RSA. Para implementar esse sistema de criptografia cada usuário procede como segue. Ele escolhe inicialmente um inteiro $n = pq$, produto de dois números primos distintos p e q, tomados suficientemente grande em relação ao desempenho computacional dos atuais computadores. Em seguida ele escolhe um número e tal que $mdc\{e,\ \phi(n)\} = 1$. A chave pública dele neste caso é o par $(n,\ e)$ e os fatores primos p e q do número n são mantidos em segredo. O procedimento para criptografar um

número a entre 1 e $n-1$, obtendo-se o número $C(a)$ criptografado, consiste em calcular

$$C(a) \equiv a^e \ mod \ n.$$

Para decodificar o número $b = C(a)$, e assim recuperar a mensagem original a enviada, deve-se usar a chave de decodificação $(n,\ d)$, onde o número inteiro d, mantido em segredo, é o inverso de e no grupo $U_{\phi(n)}$, isto é, $ed \equiv 1 \ mod \ \phi(n)$. Portanto os inteiros e e d são dados por $ed - 1 = r\phi(n)$, para algum inteiro r. Mais precisamente, para decodificar $b = C(a)$ calcula-se

$$D(b) \equiv b^d \ mod \ n.$$

Nestas condições, como $D(b) = D(C(a)) = a^{ed} \equiv a(a^{\phi(n)})^r \equiv a \ mod \ n$, a mensagem criptografada a, originalmente enviada, torna-se conhecida após a decodificação da mensagem recebida $b = C(a)$.

Observe que usamos acima o Teorema de Euler, $a^{\phi(n)} \equiv 1 \ mod \ n$, e assim
assumimos que $\text{mdc}\{a, n\} = 1$. Vamos então provar que $a^{ed} \equiv a \ mod \ n$, para qualquer inteiro a.

Nestas condições, sabemos que $ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$ e assim $a^{ed} = a(a^{p-1})^{k(q-1)}$. Daí, usando o Pequeno Teorema de Fermat no caso em que $p \nmid a$, obtemos

$$a^{ed} \equiv a \ mod \ p.$$

Se a é um múltiplo de p então a igualdade acima também vale, pois neste caso $a \equiv 0 \ mod \ p$. Portanto, obtemos $a^{ed} \equiv a \ mod \ p$, para cada inteiro a, e, do mesmo modo, $a^{ed} \equiv a \ mod \ q$. Como $\text{mdc}\{p, q\} = 1$, concluimos que $a^{ed} - a$ é um múltiplo de $n = pq$ e portanto

$$a^{ed} \equiv a \ mod \ n.$$

Observamos que é fácil calcular $\phi(n)$ a partir da fatoração de n, pois $\phi(n) = \phi(pq) = n - p - q + 1$. Por outro lado, conhecendo-se apenas a chave pública $(n,\ e)$ é inviável na prática determinar a chave de decodificação $(n,\ d)$.

Exemplo 70 *Exemplo para fixar idéias.*

João e Maria escolherão uma chave pública (n, e) para trocarem mensagens secretas. Para começar o procedimento a mensagem será representada por uma sequência de inteiros $B_1, B_2, \cdots B_k$, sendo que cada B_i deverá ser menor do que n. A representação de mensagens por números é sempre feita quando usamos o teclado de um computador, onde cada caracter está associado à um número (ASII-code).

Será usado o seguinte ASCII-code para representar as letras do ALFABETO por números, e o espaço entre palavras será indicado por 32:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	96	87	88	89	90

A mensagem "Ola Maria" se transforma no número

797665327765827365

Este número será codificado e enviado para Maria. Maria de posse do número codificado deverá recuperar o número original e desta forma conseguirá ler a mensagem.

Maria escolhe os primos 13 e 17 obtendo $n = p.q = 221$. Para completar a chave pública, como $\phi(n) = 12.17 = 192$, Maria precisa escolher o número e, de tal forma que $\text{mdc}(\phi(n), e) = 1)$, por exemplo $e = 11$.

Pronto, Maria informa a chave pública $(221, 11)$ para João.

João quebra o número em blocos $B_1, B_2, \cdots B_9$, menores do que n e codifica cada bloco:

$$79 - 76 - 65 - 32 - 77 - 65 - 82 - 73 - 65$$

$C(79) = 79^{11} \pmod{221} = 131$
$C(76) = 76^{11} \pmod{221} = 19$
$C(65) = 65^{11} \pmod{221} = 78$
$C(32) = 32^{11} \pmod{221} = 128$
$C(77) = 77^{11} \pmod{221} = 168$
$C(82) = 82^{11} \pmod{221} = 10$
$C(73) = 73^{11} \pmod{221} = 96$

Maria recebe o número $131 - 19 - 78 - 128 - 168 - 78 - 10 - 96 - 78$. Usando o algoritmo Euclidiano estendido, calcula o inverso do número $e = 11$ em $\mathbb{Z}_{221}$e determina $d = 35$.

Agora a chave $(221, 35)$ é usada e Maria recupera o correspondente número original 797665327765827365 e lê "Ola Maria".

Observação 71 *Neste exemplo, onde $n = 221$, fica muito fácil para João determinar p e q e a partir daí determinar $\phi(n) = 12.17 = 192$. Na prática, n é escolhido de tal forma que a decomposição se torne muito difícil. Assim o conhecimento da chave pública não implica no conhecimento da chave de*
decodificação.

Observação 72 *O conhecimento do valor de $\phi(n)$ por qualquer outro método que não seja pela decomposição de n nos levará a descoberta dos primos p e q, conforme nos mostra o exercício abaixo. Assim o cálculo $\phi(n)$ e a decomposição de n são problemas equivalentes.*

Exercício 73 *Suponha n e $\phi(n)$ conhecidos. Determine p e q sabendo que $n = p.q$.*

Exercício 74 *Fatore n, sabendo-se que $n = 3400013$ é igual ao produto de dois primos e que $\phi(n) = 3396288$.*

Exercício 75 *A chave pública utilizada por João para codificar mensagens agora é (10403,8743). Voce recebeu a seguinte mensagem*

$$3148 - 4748 - 7778$$

O que diz esta mensagem?

2 Criptografia de Curvas Elípticas

A idéia da chave pública de Diffie-Helmann, adaptada para curvas elípticas, pode ser assim descrita. Dois usuários A e B, tradicionalmente chamados Alice e Bob respectivamente, desejam combinar por meio de um canal de comunicação pública uma chave para comunicação privada entre eles. Seja $C(\mathbb{F}_q)$ uma curva elíptica sobre o corpo $\mathbb{F}_q$ e seja Q um ponto da curva que ambos publicamente escolheram. Alice então escolhe em segredo um inteiro k_A e calcula o ponto da curva k_AQ. Ela envia ao Bob apenas o ponto obtido, mantendo em sigilo o inteiro escolhido k_A. Analogamente, Bob escolhe em segredo um inteiro k_B, calcula o ponto da curva k_BQ e o envia à Alice, mantendo também em sigilo o inteiro escolhido k_B. A chave comum é o ponto $P = k_Ak_BQ$ que é determinado por Alice multiplicando o

ponto recebido de Bob pelo seu número secreto k_A, enquanto Bob calcula o ponto P multiplicando o ponto recebido de Alice pelo seu número secreto k_B. Uma intrusa que deseja espionar Alice e Bob deveria calcular o ponto P conhecendo apenas os pontos Q, k_AQ k_BQ e não os inteiros k_A e k_B. Este é o chamado Problema de Diffie-Helmann para curvas elípticas.

Admitindo-se que a base de uma linguagem já está mergulhada em uma curva elíptica C_q sobre um corpo $\mathbb{F}_q$, então nas condições acima, se Bob deseja enviar de forma sigilosa uma mensagem M para Alice ele procede da seguinte maneira. Escolhe em segredo um número ℓ e envia o par de pontos $(\ell Q, M + \ell(k_AQ))$. Então para ler a mensagem de Bob recebida Alice subtrai do segundo ponto enviado por Bob o resultado da multiplicação do primeiro ponto por sua chave secreta k_A.

A segurança da criptografia reside no fato de que não se conhece (mesmo para um grupo multiplicativo $\mathbb{F}_q^*$ bem escolhido) um algoritmo "adequado" para obtenção da solução do chamado *problema do logaritmo discreto* de um grupo G com base $g \in G$: dado $g \in G$ encontrar para cada $y \in G$ um elemento $x \in G$ tal que $y = g^x$, caso exista.

É claro que uma vez resolvido o problema do logaritmo discreto automaticamente estará também resolvido o problema de Diffie-Helmann. Existe uma conjectura sobre a recíproca.

3 Criptoanálise

A criptoanálise consiste do estudo de técnicas que permitam revelar mensagens criptografadas. Assim a criptoanálise trabalha no sentido contrário ao da criptografia, investigando vulnerabilidades do sistema na busca de possível quebra de sistemas de criptografia. Por exemplo, no sistema RSA investiga-se eficientes algoritmos de fatoração de números inteiros usando curvas elípticas.

4 Outras Aplicações

- A função $\mathcal{P}$ de Weierstrass:
  http://mathworld.wolfram.com/WeierstrassEllipticFunction.html

- Números congruentes:
  Um número inteiro positivo N é um número congruente ele é a área de um triângulo retângulo cujas medidas dos lados são números racionais. Os inteiros 6 (3-4-5) e 5 (3/2-20/3-41/6) são, mas 1,2,3 e 4 não são, congruentes. Um inteiro positivo N é um número congruente se, e somente se, a curva elíptica $y^2 = x(x - N)(x + N)$ tem algum ponto não trivial, isto é, diferente do ponto no infinito e dos pontos $(0, 0)$ e $(\pm N, o)$.

- Último Teorema de Fermat.
  Gerhard Frey (1985), K. Ribet (1995) (Taniyama conjectura): se $A^p + B^p = C^p$ então o discriminante da curva elíptica $y^2 = x(x - A)(x - B)$ é $-(A^pB^p(A^p + B^p))^2 = -(ABC)^{2p}$ (A. Wiles, R. Taylor (1995): Último teorema de Fermat).

- Curvas elípticas recomendadas USA.
  No Apêndice D do documento FIPS 186-3, june-2009, do NIST (National Institute of Standards and Technology) estão curvas elípticas recomendadas para uso do governo americano em assinaturas digitais, com sugestões de chave privada e corpo de base:
  http://csrc.nist.gov/publications/fips/fips186-3/fips-186-3.pdf

- Desafios premiados:
  O Certicom Elliptic Curve Cryptosystem (ECC) Challenge foi criado visando ampliar o entendimento e a apreciação da dificuldade do problema do logaritmo discreto em curvas elípticas e para

estimular e encorajar pesquisas e análise do nível de segurança da criptografia de curvas elípticas. O desafio está dividido em dois níveis e oferece prêmios a partir de US$ 5,000 até US$ 100,000. http://www.certicom.com/images/pdfs/cert_ecc_challenge.pdf .

Referências Bibliográficas

[1] M. Agrawal, N. Kayal, N. Saxena: *PRIMES is in P*, Annals of Math. 160 (2004), 781-793.

[2] M. W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo: *Elementary Number Theory, Cryptography and Codes*, Universitext, Springer-Verlag, 2009.

[3] D. J. Berstein: *Proving Primality after Agrawal-Kayal-Saxena*, *http : //cr.yp.to/papers.html#aks*

[4] M. Brás-Amorós: *Fibonacci-like behavior of the number of numerical semigroups of a given genus*, Semigroup Forum, 76 (2008), 379-384.

[5] M. Brás-Amorós: *Bounds on the number of numerical semigroups of a given genus*, J. Pure Appl. Algebra, 213 (2009), 997-1001.

[6] C. Cardoso: *Fatoração de números inteiros usando curvas elíticas*, Dissertação de Mestrado - UFMS, 2003.

http://www.dct.ufms.br/mestrado/dissertacoes/2003/celso.pdf

[7] S. C. Coutinho: *Números inteiros e criptografia RSA*, Coleção SCM - IMPA / SBM, 2007.

[8] E. Fischer *The Evolution of Character Codes, 1874-1968*,

www.transbay.net/ enf/ascii/ascii.pdf

[9] R. L. Graham, D. E. Knuth, O. Patashnik: *Concrete Mathematics - A Foundation for Computer Science*, Addison-Wesley Publishing Company, 1994.

[10] J. Hoffstein, J. Pipher, J. H. Silverman: *An Introduction to Mathematical Cryptography*, UTM, Springer, 2008.

[11] M. Jacobson, A. Menezes, A. Stein: *Solving elliptic curves discrete logarithm problems using Weil descent*, Journal of the Ramanujan Mathematical Society, 16 (2001), 231-260.

[12] N. Koblitz: *Algebraic Aspects of Cryptography,* Springer-Verlag, 2004.

[13] N. Koblitz: *A Course in Number Theory and Cryptography,* Springer-Verlag, 1994.

[14] V. Miller: *Uses of elliptic curves in cryptography,* Advances in Cryptography - Crypto'85, Springer-Verlag (1986), 417-426.

[15] E. Strey: *A hipótese de Riemann para curvas algébricas e uma caracterização da curva hermitiana*, Dissertação de Mestrado - PPGMAT/UFES, 2008.

[16] Unicode Consortium: *Unicode 5.2.0,*

www.unicode.org/versions/Unicode5.2.0/

[17] Y. Zhao: *Constructing numerical semigroups of a given genus*, Semigroup Forum, 80 (2010), 242-254.