定義：$n \geq 1$ について，$\zeta_n = \exp(2\pi\sqrt{-1}/n) \in \mathbb{C}$ は 1 の原始 n 乗根（i.e, n 乗してはじめて 1 になる）の 1 つであるが，$\Phi_n(x) = \prod_{1\leq k\leq n, \gcd(n,k)=1}(x - \zeta_n^k) \in \mathbb{Z}[x]$ を円分多項式という．

注：$\Phi_n(x) \in \mathbb{Z}[x]$ であることは，$x^n - 1 = \prod_{d|n} \Phi_d(x)$ から帰納的に従う．

補題：p を $m \neq n$ をどちらも割らない素数とする．$\Phi_m(x)$ と $\Phi_n(x)$ は $\mathbb{F}_p[x]$ で互いに素．

証明：$\mathbb{Z}[x]$ で $x^a - 1$ を $x^b - 1$ で割った余りは $x^c - 1$ であることを注意する（ここで c は a を b で割った余り）．よって $d = \gcd(m, n)$ とすると，$\mathbb{F}_p[x]$ で $\gcd(x^n - 1, x^m - 1) = x^d - 1$ である．

$kd = n$ とする．$h(x) = (x^n - 1)/(x^d - 1) = 1 + x^d + \cdots + x^{(k-1)d}$ について，$(x^n - 1) = h(x)(x^d - 1)$ となることを注意する．$h(x)$ を $x^d - 1$ で割った余りは k で，これは $\mathbb{F}_p$ で非ゼロなので，$\mathbb{F}_p[x]$ で $\gcd(h(x), x^d - 1) = 1$．$d < n$ と注より $\Phi_n(x)|h(x)$ なので，$\gcd(\Phi_n(x), x^d - 1) = 1$．$\gcd(\Phi_n(x), \Phi_m(x))|(x^d - 1)$ なので，$\gcd(\Phi_n(x), \Phi_m(x)) = 1$.

系：p を n を割らない素数とし，$\mathbb{F}_p \subseteq L$ を体拡大とする．$\theta \in L$ が $\Phi_n(\theta) = 0$ であれば，θ は 1 の原始 n 乗根である．

定理：p を n を割らない素数とし，$f(x)$ を $\Phi_n(x)$ の $\mathbb{F}_p[x]$ における既約因子の 1 つとする．このとき $\deg f(x) = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}([p])$ である（特に，既約因子の選び方に依らない）．

証明：$L = \mathbb{F}_p[x]/(f(x))$ とする．$\theta = [x]$ が 1 の原始 n 乗根であることより，$\iota : \mathrm{Gal}(L/\mathbb{F}_p) \to (\mathbb{Z}/n\mathbb{Z})^\times, \sigma \mapsto d(\sigma)$ は単射群準同型である（ここで $d(\sigma)$ は $\theta^{d(\sigma)} = \sigma(\theta)$ で定まる）．一方で，$\mathrm{Gal}(L/\mathbb{F}_p)$ は Frobenius 写像 σ_L で生成されるのであった．$\iota(\sigma_L) = [p]$ を注意する．

系：p を素数とする．任意の $e \geq 1$ について，位数 p^e の有限体が存在する．

証明：前の系で $n = p^e - 1$ とすると，$\mathbb{F}_p[x]$ における既約 e 次多項式が得られる．

命題：$Q(x) = \mathrm{Irr}(\mathbb{Q}; \zeta_n) \in \mathbb{Z}[x]$ とする（Gauss の補題より $\mathbb{Z}[x]$ に属する）．p を n を割らない素数とし，$f(x)$ を $Q(x)$ の $\mathbb{F}_p[x]$ における既約因子の 1 つとし，$L = \mathbb{F}_p[x]/(f(x))$ とする．環準同型写像 $\varphi : \mathbb{Z}[\zeta_n] \to L$ であって，$\varphi(\zeta_n) = \theta(:= [x])$ となるものが存在する．

証明：$L = \mathbb{F}_p[x]/(f(x)) = \mathbb{Z}[x]/(p, f(x))$ より従う（環同型 $R/(I + J) \cong (R/I)/((I + J)/I)$ で同一視している）．$\mathbb{Z}[\zeta_n] \cong \mathbb{Z}[x]/(Q(x))$ と $(Q(x)) \subseteq (p, f(x))$ に注意する（ちなみに実際には $\subsetneq$）．

系：上の命題において，単射群準同型 $\mathrm{Gal}(L/\mathbb{F}_p) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ が存在する．

証明：θ は 1 の原始 n 乗根だったから，$\sigma \in \mathrm{Gal}(L/\mathbb{F}_p)$ は，$\sigma(\theta) = \theta^{d(\sigma)}$ なる $d = d(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ によって決まる．$f(\theta^d) = 0$ から $Q(\zeta_n^d) = 0$ である．よって $\sigma'(\zeta_n) = \zeta_n^d$ で定まる $\sigma' \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ を対応させることができる．

定理：円分多項式 $\Phi_n(x)$ は $\mathbb{Q}[x]$ で既約である．

証明：p を n を割らない素数とする．これまで同様 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ を $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群と同一視したとき，系によって $[p] \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ が分かる．よって $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$ である．

おまけ：16 人で麻雀大会を行う（4 人でするゲームならば何でもよい）．1 回戦に 4 組が同時にゲームを行い，計 5 回戦する．どの 1 人も他の 15 人と丁度 1 回ずつ対戦するような対戦表を作れ．

（解答）$|K|=4$ となる体 $K=\mathbb{F}_4$ について，平面 $\mathbb{F}_4^2$ は 16 個の点からなる．これらの点を 16 人とそれぞれ対応させる．$\mathbb{F}_4^2$ の直線は 4 つの点からなり，指定された傾きを持つ直線は 4 本存在する．原点を通る直線は $(16-1)/(4-1)=5$ 本あるので，傾きは 5 種類ある．傾きごとに直線上の 4 点（=4 人）が対戦するようにすれば，題意の対戦表を構成できる．

以下，もう少し具体的に計算していこう．まずは $\mathbb{F}_4$ を構成する必要がある．そのために $|K|=2$ となる体 $K=\mathbb{F}_2$ の構成を思い出す．$\mathbb{F}_2=\{\overline{0},\overline{1}\}$ で，$\overline{0}=$ 偶数, $\overline{1}=$ 奇数 と思えるような演算法則に従う（たとえば $\overline{1}+\overline{1}=\overline{0}$ である）．次に $\mathbb{R}$ から $\mathbb{C}$ を構成するように，$\mathbb{F}_2$ に「虚数」を添加して $\mathbb{F}_4$ を構成する（ただし $\mathbb{F}_2$ では $-\overline{1}=\overline{1}$ なので、$i^2=-\overline{1}$ となる i は存在することに注意）．天下り的だが，$\mathbb{F}_4=\{a+b\omega \mid a,b\in\mathbb{F}_2\}$ として $\omega^2=\omega+\overline{1}$ なる法則に従うとすればよい．たとえば

$$(\overline{1}+\omega)^2=\overline{1}^2+\overline{1}\omega+\overline{1}\omega+\omega^2=\overline{1}+(\overline{1}+\overline{1})\omega+(\omega+\overline{1})=\omega$$

のように計算できる．傾きは $\overline{0},\overline{1},\omega,\overline{1}+\omega,\infty$ であり，

- $\{L_y^0:=\{(\overline{0},y),(\overline{1},y),(\omega,y),(\overline{1}+\omega,y)\} \mid y\in\mathbb{F}_4\}$ が傾き 0 の 4 本の直線
- $\{L_x^\infty:=\{(x,\overline{0}),(x,\overline{1}),(x,\omega),(x,\overline{1}+\omega)\} \mid x\in\mathbb{F}_4\}$ が傾き ∞ の 4 本の直線
- $\{(\overline{0},\overline{0}),(\overline{1},\overline{1}),(\omega,\omega),(\overline{1}+\omega,\overline{1}+\omega)\}$, $\{(\overline{1},\overline{0}),(\overline{0},\overline{1}),(\overline{1}+\omega,\omega),(\omega,\overline{1}+\omega)\}$, $\{(\omega,\overline{0}),(\overline{1}+\omega,\overline{1}),(\overline{0},\omega),(\overline{1},\overline{1}+\omega)\}$, $\{(\overline{1}+\omega,\overline{0}),(\omega,\overline{1}),(\overline{1},\omega),(\overline{0},\overline{1}+\omega)\}$ が傾き 1 の 4 本の直線
- $\{(\overline{0},\overline{0}),(\overline{1},\omega),(\omega,\overline{1}+\omega),(\overline{1}+\omega,\overline{1})\}$, $\{(\overline{1},\overline{0}),(\overline{0},\omega),(\overline{1}+\omega,\overline{1}+\omega),(\omega,\overline{1})\}$, $\{(\omega,\overline{0}),(\overline{1}+\omega,\omega),(\overline{0},\overline{1}+\omega),(\overline{1},\overline{1})\}$, $\{(\overline{1}+\omega,\overline{0}),(\omega,\omega),(\overline{1},\overline{1}+\omega),(\overline{0},\overline{1})\}$, が傾き ω の 4 本の直線である
- $\{(\overline{0},\overline{0}),(\overline{1},\overline{1}+\omega),(\omega,\overline{1}),(\overline{1}+\omega,\omega)\}$, $\{(\overline{1},\overline{0}),(\overline{0},\overline{1}+\omega),(\overline{1}+\omega,\overline{1}),(\omega,\omega)\}$, $\{(\omega,\overline{0}),(\overline{1}+\omega,\overline{1}+\omega),(\overline{0},\overline{1}),(\overline{1},\omega)\}$, $\{(\overline{1}+\omega,\overline{0}),(\omega,\overline{1}+\omega),(\overline{1},\overline{1}),(\overline{0},\omega)\}$ が傾き $\overline{1}+\omega$ の 4 本の直線

となっている．以上より，$\mathbb{F}_4^2$ の点 $(\overline{0},\overline{0}),(\overline{0},\overline{1}),(\overline{0},\omega),(\overline{0},\overline{1}+\omega),(\overline{1},\overline{0}),(\overline{1},\overline{1}),(\overline{1},\omega),(\overline{1},\overline{1}+\omega),(\omega,\overline{0}),(\omega,\overline{1}),(\omega,\omega),(\omega,\overline{1}+\omega),(\overline{1}+\omega,\overline{0}),(\overline{1}+\omega,\overline{1}),(\overline{1}+\omega,\omega),(\overline{1}+\omega,\overline{1}+\omega)$ をこの順に A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P とすると，題意の対戦表は以下のようになる．

1 回戦 (A,E,I,M),(B,F,J,N),(C,G,K,O),(D,H,L,P)
2 回戦 (A,B,C,D),(E,F,G,H),(I,J,K,L),(M,N,O,P)
3 回戦 (A,F,K,P),(E,B,O,L),(I,N,C,H),(M,J,G,D)
4 回戦 (A,G,L,N),(E,C,P,J),(I,O,D,F),(M,K,H,B)
5 回戦 (A,H,J,O),(E,D,N,K),(I,P,B,G),(M,L,F,C)

（コメント）以上の論理で重要なのは $\mathbb{F}_4$ の存在である．$|K|=n$ となる体は $n=p^e$ のように，n が素数べきの場合にのみ存在することが知られている（ガロア体，有限体）．よってこの構成法は，麻雀以外にも，たとえば 3 人, 5 人, 7 人, 8 人, 9 人でするゲームに適用できる．6 人でするゲームには適用できないが，その場合，そもそもこのような対戦表が存在しないことを証明できる．