Building Finite Fields through Counting

$\mathbb{F}_q$: field with q elements

Clear ! $q = p^n$, $p \in \mathbb{P}$.

Does $\mathbb{F}_q$ exist ?

$q = p$! $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ unique .

Method 1. $f(x) = x^q - x \in \mathbb{F}_p[x]$.

$\gcd(f(x), f'(x)) = \gcd(x^q - x, -1) = 1 \Rightarrow f(x)$ separable

F = splitting field of $f(x)$ over $\mathbb{F}_p$.

Freshman's dream $\Rightarrow \{$roots of $f(x)$ in $F\} \subseteq F$ is a field $\Rightarrow |F| = q$.

Method 2. Given $q = p^n$, find an irreducible $P \in \mathbb{F}_p[x]$ of degree n and take $F = \mathbb{F}_p[x]/(P(x))$. Then $[F : \mathbb{F}_p] = n$ and $|F| = q$.

Existence of f: Let

$$\mathcal{N} := \{ f \in \mathbb{F}_p[x] : f \text{ monic} \},$$

$$\mathcal{P} := \{ P \in \mathbb{F}_p[x] : P \text{ monic, irreducible} \}.$$

Put $F_n = \prod_{\substack{f \in \mathcal{N} \\ \deg f = n}} f$. Then $\deg F_n = n p^n$.

Claim: $$\frac{F_n}{F_{n-1}^p} = \prod_{\substack{P \in \mathcal{P} \\ \deg P \mid n}} P.$$

Pf. Let $P \in \mathcal{P}$ with $\deg P = d$. Then $\forall k \in \mathbb{N}$,

$$\#\{f \in \mathcal{N} : \deg f = n \text{ and } p^k \mid f\} = \lfloor p^{n-kd} \rfloor .$$

So, $\nu_p(F_n) = \sum_{1 \leq k \leq n/d} \lfloor p^{n-kd} \rfloor$.

Similarly, $\nu_p(F_{n-1}^p) = p \cdot \nu_p(F_{n-1}) = \sum_{1 \leq k \leq n/d} p \lfloor p^{n-1-kd} \rfloor$.

So $\nu_p\left(\frac{F_n}{F_{n-1}^p}\right) = \nu_p(F_n) - \nu_p(F_{n-1}^p) = \sum_{1 \leq k \leq n/d} \left(\lfloor p^{n-kd} \rfloor - p \lfloor p^{n-1-kd} \rfloor \right)$.

$1 \leq k < n/d$: $\lfloor p^{n-kd} \rfloor - p \lfloor p^{n-1-kd} \rfloor = 0$.

$\Rightarrow d \nmid n$: $\nu_p\left(\frac{F_n}{F_{n-1}^p}\right) = 0$.

$d \mid n$: $\lfloor p^{n-kd} \rfloor - p \lfloor p^{n-1-kd} \rfloor = 1$ for $k = n/d$.

$\Rightarrow d \mid n$: $\nu_p\left(\frac{F_n}{F_{n-1}^p}\right) = 1$. $\square$

Now we have

$$\deg\left(\frac{F_n}{F_{n-1}^p}\right) = \deg\Big(\prod_{\substack{p \in \mathcal{P} \\ \deg p = n}} p\Big) + \deg\Big(\prod_{\substack{p \in \mathcal{P} \\ \deg p \mid n,\ \deg p < n}} p\Big)$$

$$\|$$

$$n p^n - p(n-1) p^{n-1} = p^n$$

Note that

$$\deg\Big(\prod_{\substack{p \in \mathcal{P} \\ \deg p \mid n,\ \deg p < n}} p\Big) \leq \sum_{\substack{d \mid n \\ d < n}} \#\{f \in \mathcal{N} : \deg f = d\} \cdot d$$

$$\leq \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} d \cdot p^d$$

$$\leq \left\lfloor \frac{n}{2} \right\rfloor \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} p^d$$

$$= \left\lfloor \frac{n}{2} \right\rfloor \cdot \frac{p\left(p^{\lfloor \frac{n}{2} \rfloor} - 1\right)}{p-1}$$

$$< 2 \left\lfloor \frac{n}{2} \right\rfloor p^{\lfloor \frac{n}{2} \rfloor} \leq p^{2\lfloor \frac{n}{2} \rfloor} \leq p^n .$$

Thus, $\deg\left(\prod_{\substack{P\in\mathcal{P}\\ \deg P=n}} P\right) > 0$. Hence, $\exists\, P\in\mathcal{P}$ with $\deg P = n$. $\square$

Remarks. 1. $p^n = \sum_{d\mid n} d\cdot \#\{P\in\mathcal{P} : \deg P = d\}$.

Möbius inversion $\Rightarrow$ $\#\{P\in\mathcal{P} : \deg P = n\} = \frac{1}{n}\sum_{d\mid n}\mu\left(\frac{n}{d}\right)p^d$.

2. $\dfrac{F_n}{F_{n-1}^p} = \prod_{\substack{P\in\mathcal{P}\\ \deg P\mid n}} P = x^{p^n} - x$.

Mersenne Primes & Lucas-Lehmer Primality Test

$q = M_p = 2^p - 1$, $p\in\mathbb{P}$.

Suppose $p\geq 3$. Then $q\equiv 1 \pmod 3$ and $q\equiv -1 \pmod 8$.

Consider $R_q = (\mathbb{Z}/q\mathbb{Z})[\sqrt{3}]$. $\alpha = a + b\sqrt{3}$, $a, b \in \mathbb{Z}/q\mathbb{Z}$.

Reciprocity for Jacobi symbol : $\left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) = -1 \Rightarrow 3 \notin (\mathbb{Z}/q\mathbb{Z})^{\times 2}$.

($\exists$ prime $r \mid q$, s.t. $3 \notin (\mathbb{Z}/r\mathbb{Z})^{\times 2}$)

Can define conjugate of α : $\bar{\alpha} := a - b\sqrt{3} \in R_q$.

$\alpha, \beta \in R_q$: $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$, $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$, $\overline{\alpha^{-1}} = \bar{\alpha}^{-1}$ $(\alpha \in R_q^{\times})$.

$$\omega = 2 + \sqrt{3}, \quad \bar{\omega} = \omega^{-1} = 2 - \sqrt{3}.$$

$q \in \mathbb{P} \Rightarrow \left(\frac{2}{q}\right) = 1 \Rightarrow 2 \in \mathbb{F}_q^{\times 2} = (\mathbb{Z}/q\mathbb{Z})^{\times 2}$.

Freshman's dream : $q \in \mathbb{P} \Rightarrow$

$$\begin{aligned}(a + b\sqrt{3})^q &= a^q + (b\sqrt{3})^q \\ &= a + b \cdot 3^{\frac{q-1}{2}} \cdot \sqrt{3} \\ &= a + b\left(\frac{3}{q}\right)\sqrt{3} \\ &= a - b\sqrt{3} \\ &= \overline{a + b\sqrt{3}}.\end{aligned}$$

Prop. $q = M_p = 2^p - 1$ $(p \geq 3)$ is prime $\Leftrightarrow \omega^{\frac{q+1}{2}} = -1$ in R_q.

$\mathbb{F}_q(\sqrt{3})$
$\parallel$

Pf. ($\Rightarrow$) Suppose q is prime. Let $\alpha = \dfrac{1+\sqrt{3}}{\sqrt{2}} \in K_q = \mathbb{F}_q[\sqrt{3}]$.

$\alpha^2 = \omega$. So $\omega^{\frac{q+1}{2}} = \alpha^{q+1} = \alpha \cdot \alpha^q = \alpha\bar{\alpha} = \dfrac{1+\sqrt{3}}{\sqrt{2}} \cdot \dfrac{1-\sqrt{3}}{\sqrt{2}} = -1$.

($\Leftarrow$) Suppose $\omega^{\frac{q+1}{2}} = -1$ in K_q. Let r be any (odd) prime divisor of q s.t. $3 \notin \mathbb{F}_r^{\times 2}$, and take $K = \mathbb{F}_r[\sqrt{3}] \cong \mathbb{F}_{r^2}$. Then $\omega \in K^\times$ with $\mathrm{ord}(\omega) = q+1$. So by Lagrange's thm, $q+1 \mid |K^\times| = r^2 - 1$. But $r > \sqrt{q}$. Hence $q = r$ is prime. $\square$

Now we prove LLT, one of the primality test used by GIMPS.

Thm (Lucas-Lehmer Primality Test) Define $S_0 = 4$ and $S_m = S_{m-1}^2 - 2$ for $m \geq 1$. Then $q = M_p = 2^p - 1$ ($p \geq 3$) is prime $\Leftrightarrow q \mid S_{p-2}$.

Rmk: $S_m = \omega^{2^m} + \overline{\omega}^{2^m} \in \mathbb{N}$, $m \geq 0$.

Pf. ($\Rightarrow$) Suppose q is prime. By Prop, $\omega^{2^{p-1}} = \omega^{\frac{q+1}{2}} = -1$ and

$\overline{\omega}^{2^{p-1}} = \overline{\omega^{2^{p-1}}} = -1$ in $K_q = \mathbb{F}_q[\sqrt{3}]$. So $S_{p-1} = -2$. Thus $S_{p-2}^2 = 0$

in K_q. In particular, $q \mid S_{p-2}$.

($\Leftarrow$) Suppose $q \mid S_{p-2}$. Then $\omega^{2^{p-2}} = -\overline{\omega}^{2^{p-2}}$ in K_q. It follows

that $\omega^{\frac{q+1}{2}} = \omega^{2^{p-1}} = -\omega^{2^{p-1}}\overline{\omega}^{2^{p-1}} = -1$ in K_q. By Prop,

q is prime. $\square$