

Irreducible polynomials over finite fields.

Prop Let $f \in \mathbb{F}_p[x]$ be irred of deg m . Then

(a) $f \mid x^{p^n} - x$

(b) f is separable

(c) Given an integer $n \geq 1$, $f \mid x^{p^n} - x \iff f$ has a root in $\mathbb{F}_{p^n} \iff m \mid n$.

Pf Begin with (c). Take α a root of f in the splitting field \mathbb{F}_p .

Since f irred, $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ has degree m , so $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^m}$.

Now $\mathbb{F}_{p^n} \cong \mathbb{F}_{p^m}$ iff $m \mid n$, so get second equivalence.

By irreducibility of f , $f \mid \gcd(f, x^{p^n} - x) \iff \deg(\gcd(f, x^{p^n} - x)) > 0$
and this degree = # roots of f in \mathbb{F}_{p^n} .

(a) & (b) follow easily. \square

Note In fact, ~~some~~ irred $f \in \mathbb{F}_q[x]$ are always separable.

Hence inseparability is only a phenomenon in infinite fields of char p .

Let $N_m := \{f \in \mathbb{F}_p[x] \mid f \text{ is monic irred of degree } m\}$

$$\#N_m = |N_m|.$$

Thm For $n \geq 1$, $\sum_{m \mid n} m N_m = p^n$.

Pf We have $x^{p^n} - x = \prod_{m \mid n} \prod_{f \in N_m} f$ b/c the monic ^{irred} divisors of $x^{p^n} - x$ are exactly

this collection of f by (c) above. Computing degrees on both sides (and $f \in N_m$ has deg m) gives the thm. \square

e.g. $N_1 = p$ so $p^2 = 2N_2 + N_1 = 2N_2 + p \Rightarrow N_2 = \frac{1}{2}(p^2 - p)$.

Sim, $N_4 = \frac{1}{4}(p^4 - p^2)$.

Recall $\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ (-1)^s & \text{if } n=p_1 \cdots p_s, p_i \text{ distinct primes} \\ 0 & \text{o/w} \end{cases}$

Thm (Möbius inversion formula) For $f, g: \mathbb{Z}^+ \rightarrow A$, A an Abelian gp, and $g(n) = \sum_{m|n} f(m)$, we have $f(n) = \sum_{m|n} \mu(m)g(n/m)$

(where operation on A is $+$).

Thm $N_n = \frac{1}{n} \sum_{m|n} \mu(m) p^{n/m}$.

Pf Let $f(n) = nN_n$. Then $g(n) = \sum_{m|n} f(m) = \sum_{m|n} mN_m = p^n$.

By Möbius inversion, $nN_n = \sum_{m|n} \mu(m)g(n/m) = \sum_{m|n} \mu(m)p^{n/m}$. \square

e.g. $N_4 = \frac{1}{4} (\mu(1)p^{4/1} + \mu(2)p^{4/2} + \mu(4)p^{4/4})$
 $= \frac{1}{4} (p^4 - p^2)$.

Further directions:

- Irred factors of mod p reduction of \mathbb{F}_d
- Berlekamp's algorithm: When is $f \in \mathbb{F}_p[x]$ irreducible
- Number theory: K/\mathbb{Q} finite, $\mathcal{O}_K \subseteq K$ ring of integers, $\mathcal{O}_K/m \cong \mathbb{F}_2$

Reading

- Matrix groups $\mathbb{F}_q \rightsquigarrow$ finite simple groups
- Coding theory: error correcting codes
- Cryptography via elliptic curves over finite fields

Combinatorics $\binom{n}{k}_q := \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}$

$q \rightarrow 1: \binom{n}{k}$
 $q = p^n: \#k\text{-dim subspaces of } \mathbb{F}_q^n$ } Field with one element \mathbb{F}_1

Aside on Möbius inversion

Suppose $f, g: \mathbb{Z}^+ \rightarrow (A, +)$ for A an Abelian group.

~~Then~~ If $g(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{m|n} \mu(m) g(n/m)$

Pf We have

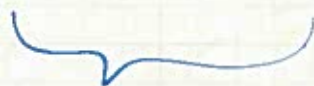
$$\sum_{d|n} \mu(d) g(n/d) = \sum_{d|n} \mu(n/d) g(d)$$

$$= \sum_{d|n} \mu(n/d) \left(\sum_{d_1|d} f(d_1) \right)$$

$$= \sum_{d_1|n} f(d_1) \left(\sum_{d_1|d|n} \mu(n/d) \right)$$

$$= \sum_{d_1|n} f(d_1) \left(\sum_{d_2|m} \mu(m/d_2) \right)$$

$$\text{where } m = \frac{n}{d_1}, d_2 = \frac{d}{d_1}$$



$$= \begin{cases} 1 & \text{for } m=1; \text{ i.e. } d_1=n \\ 0 & \text{otherwise} \end{cases}$$

$$= f(n).$$

