

# Class Notes

## Tuesday, September 5, 2006

### Irreducibility (contd.)

We have a fast deterministic test for irreducibility of polynomials over finite fields. How do we find an irreducible polynomial of given degree  $n$  over  $\mathbb{F}_q$ ? There is no deterministic polynomial time algorithm to do this. There is a probabilistic algorithm.

### Algorithm

Pick a monic polynomial  $f(x) \in \mathbb{F}_q[x]$  of degree  $n$  at random. Test for irreducibility. Repeat until you find an irreducible polynomial.

The algorithm is based on the following theorem.

### Theorem 1.

$$\lim_{q^n \rightarrow \infty} \frac{\#\{\text{monic irreducible polynomials of degree } n \text{ over } \mathbb{F}_q\}}{q^n} = \frac{1}{n}.$$

From this theorem we conclude that the probability of failure after  $k$  tries is  $(1 - \frac{1}{n})^k \rightarrow 0$  as  $k \rightarrow \infty$

*Proof.* Let  $a_d = \#\text{monic irreducible polynomials of deg } n \text{ over } \mathbb{F}_q$ .

### Claim 2.

$$\sum_{d|n} da_d = q^n$$

To prove this note that an irreducible polynomial of degree  $d|n$  divides  $x^{q^n} - x$  because its roots generate  $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ . Conversely an irreducible factor of  $x^{q^n} - x$  has roots in  $\mathbb{F}_{q^n}$ . So  $x^{q^n} - x = \text{product of all irreducible polynomials of deg } d|n$ .

### Möbius Inversion Formula

$$\begin{aligned} \mu(n) &= 0, & \text{if } n \text{ is not square free} \\ &= (-1)^r, & \text{if } n = p_1 \dots p_r \text{ distinct primes} \\ &= 1, & n = 1. \end{aligned}$$

If  $x_n, y_n$  where  $n \geq 1$  are such that  $\sum_{d|n} dx_d = y_n$  then

$$x_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \frac{y_d}{n}$$

Applying the inversion formula to Claim 2 we have

$$\begin{aligned}
a_n &= \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \\
&= \frac{q^n}{n} + \frac{1}{n} \sum_{d|n, d < n} \mu\left(\frac{n}{d}\right) q^d \\
\Rightarrow \frac{a_n}{q^n} &= \frac{1}{n} + \frac{1}{n} \sum_{d|n, d < n} \mu\left(\frac{n}{d}\right) q^{d-n}
\end{aligned}$$

The last term  $\rightarrow 0$  as  $q^n \rightarrow \infty$ . □

This theorem is the function field version of the Prime Number Theorem.

$$\frac{\#\{\text{primes} \leq x\}}{x} \sim \frac{1}{\log x}.$$

**Theorem 3 (Shoup).** *If we can factor cyclotomic polynomials deterministically in polynomial time over  $\mathbb{F}_q$  then we can construct irreducible polynomials of given deg  $n$  in polynomial time over  $\mathbb{F}_q$ .*

## Factoring Polynomials over $\mathbb{F}_q$

**Theorem 4.** *There exist a polynomial time probabilistic algorithm for factoring polynomials in  $\mathbb{F}_q[x]$ .*

### First Step

We first remove repeated factors. Let  $f(x) = a_0x^n + \dots + a_n \in \mathbb{F}_q[x]$  and  $f'(x) = na_0x^{n-1} + \dots + a_{n-1}$  be its formal derivative. If  $f' \equiv 0$  then  $f(x) = g(x)^p$  for some  $g(x) \in \mathbb{F}_q[x]$  where  $p = \text{char } \mathbb{F}_q$ . In this case factoring  $f$  reduces to factoring  $g$ .

$f'(x) \equiv 0 \Rightarrow a_i = 0$  if  $p$  does not divide  $n - i$ . Hence,

$$\begin{aligned}
f(x) &= \sum_{p|n-i} a_i x^{n-i} \\
&= \sum_{p|n-i} a_i \left(x^{\frac{n-i}{p}}\right)^p \\
&= \sum_{p|n-i} b_i^p \left(x^{\frac{n-i}{p}}\right)^p \quad \text{where } b_i = a_i^{p^{m-1}} \text{ and } q = p^m \\
&= \left(\sum_{p|n-i} b_i x^{\frac{n-i}{p}}\right)^p
\end{aligned}$$

If  $f$  has no multiple roots then  $\text{gcd}(f, f') = 1$ . On the other hand if  $f(x)$  has a multiple root then it may be factored as

$$f = \frac{f}{(f, f')} (f, f').$$

If  $f(x)$  has a root  $\alpha$  of multiplicity  $k$  then  $(x - \alpha)^k | f(x)$ . This implies  $f'(x)$  has a root of multiplicity  $\geq (k - 1)$ . Now  $(f, f')$  has a root of multiplicity  $\geq k - 1$  and  $\leq k$  at  $\alpha$ . If  $p$  does not divide  $k$  then  $(f, f')$  has a root of multiplicity  $k - 1$  at  $\alpha$  and  $f/(f, f')$  has a simple root

at  $\alpha$ . We thus have a fast deterministic algorithm which given  $f$  produces a polynomial  $h$  which is square free and has the same irreducible factors as  $f$ . From now on we will assume that  $f(x) \in \mathbb{F}_q[x]$  is a squarefree polynomial. That is,  $f(x) = g_1(x) \dots g_r(x)$  where the  $g_i$  are distinct irreducible polynomials.