

**Lecture Notes from
August 31, 2006**

This course will discuss efficient ways to do computations over finite fields. First, we will search for efficient ways to factor polynomials over finite fields. There is a probabilistic polynomial time algorithm for this, as we'll see. Second, we'll discuss computations involving discrete logarithms. That is, suppose $h \in \langle g \rangle$, find n such that $h = g^n$. As of the first class day, there is no polynomial time algorithm for this problem. It is possible that there is no such algorithm. Third, we will look at primality testing for integers. There is a deterministic polynomial time algorithm for this problem, and it is essentially a finite field algorithm. It starts with a ring depending of the number to be tested, which is a field if and only if the number is prime.

For every prime number p and positive integer n , there exists a field with p^n elements, and any two such fields are isomorphic. \mathbb{F}_{p^n} denotes "the" finite field with p^n elements. When $n = 1$, we have $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. One way of describing \mathbb{F}_{p^n} is as the splitting field of $x^{p^n} - x$ in the algebraic closure of \mathbb{F}_p . This is unsatisfactory, however, since this does not show how to compute the algebraic closure. A better way is to choose an irreducible $f(x) \in \mathbb{F}_p[x]$ of degree n and think of \mathbb{F}_{p^n} as $\mathbb{F}_p[x]/(f(x))$. This is better since we may describe each element in this field as $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ for $a_i \in \mathbb{F}_p$. But, we have a new problem on our hands: Given p and n , find an irreducible polynomial of degree n in $\mathbb{F}_p[x]$. We would like the fastest possible procedure for this, i.e. one that is polynomial in $n \log p$. Indeed, we cannot do better than $n \log p$, since for $f(x) = f_0 + f_1x + \dots + f_nx^n$ we would need $\log p$ digits just to describe each f_i .

Example 1 (Easy) If $n = 2$ and $p \equiv 3 \pmod{4}$, then $f(x) = x^2 + 1$ is good.

Example 2 (Hard) Same $n = 2$ but with $p \equiv 1 \pmod{4}$.

How likely is a polynomial of degree n picked at random irreducible? Over \mathbb{F}_p , the probability is $1/n$. So, our algorithm is simple: pick a random polynomial of degree n , and test whether it is irreducible. If it is, great. If not, pick another.

Now, suppose you are lucky and find two irreducible polynomials $f(x)$ and $g(x)$ of degree n . Then $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$. A natural question to ask is, what is the isomorphism? There is a deterministic polynomial time algorithm for finding this; so now that we know the ending, we'll move along

to the next example.

We know that $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$ is a cyclic group of order $q - 1$, but what is the generator? One algorithm to find it is to pick $g \in \mathbb{F}_q^\times$ at random, and check if $g^{(q-1)/l} \neq 1$ for all primes $l|(q-1)$. It is clear that this is a necessary and sufficient condition for g to generate \mathbb{F}_q^\times . This is not hard to do provided we have a factorization of $q - 1$. (If we know the factorization, then this is a probabilistic polynomial time algorithm for finding the generator.) The number of generators is $\phi(q-1)$, so the probability that an element chosen at random is a generator is $\phi(q-1)/q-1$. This algorithm is efficient for small q , but for large q , we'd like to have a smaller set from which to search for our generator, as opposed to picking from all of \mathbb{F}_q^\times . Under the generalized Riemann Hypothesis, there is a g such that $2 < g < (\log p)^2$ which is a primitive root mod p . It may be $(\log p)^3$, or something close to that, but the point is that it is very specific. So, we have a deterministic algorithm if we pick sequentially, but we must assume the generalized Riemann Hypothesis.

Example 3 Look at $\mathbb{F}_{p^p} = \mathbb{F}_p[x]/(x^p - x - 1)$. $\mathbb{F}_{p^p}^\times$ has $p^p - 1$ elements, and $p^p - 1 = (p - 1)\frac{p^p-1}{p-1}$. We have an exact sequence:

$$1 \longrightarrow \mathbb{F}_p^\times \longrightarrow \mathbb{F}_{p^p}^\times \longrightarrow G \longrightarrow 1.$$

$\text{Ker } N_{\mathbb{F}_{p^p}/\mathbb{F}_p}$ is a subgroup of $\mathbb{F}_{p^p}^\times$ of order $\frac{p^p-1}{p-1}$ splitting the exact sequence.

Conjecture: The image of x in $\mathbb{F}_p[x]/(x^p - x - 1)$ has order $\frac{p^p-1}{p-1}$. (Only been checked for primes less than 20.)