FINITE FIELDS (CONTINUED): HOW TO CONSTRUCT

MATH 195

[For more on finite fields, consult the treatise by Lidl and Neiddereiter entitled *Finite Fields.*]

In our dictionary,

$$\mathbb{F}_p[X]/(f) = \{g : g = 0 \text{ or } \deg g < \deg f\}$$

with usual adiition and multiplication modulo f corresponds to

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$$

with addition and multiplication modulo n.

For example, if $f(X) = X^8 + X^4 + X^3 + X + 1$ and $b = 00010000 = X^4 \in \mathbb{F}_2[X]/(f)$, then $b^2 = X^8 = X^4 + X^3 + X + 1 = 00011011$ by doing long division and reducing modulo f.

Note that for any prime p and polynomial $f \in \mathbb{F}_p[X]$, there is a map

$$\begin{gathered} \mathbb{F}_p[X] \to \mathbb{F}_p[X]/(f) \\ g \mapsto g \bmod f \end{gathered}$$

preserving addition and multiplication, analogous to the map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Also, g and h have the same image if and only if they have the same remainder upon division by f, which is to say f divides $g - h$.

Our motivation to study these algebraic objects was to construct finite fields. Recall that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime. Analogously, $\mathbb{F}_p[X]/(f)$ is a field if and only f is irreducible.

Recall that every finite field k has $\#k = p^n = q$, a prime power number of elements. Counting, we see that $\#\mathbb{F}_p[X]/(f) = p^{\deg f}$, since we have representatives $c_{n-1}c_{n-2}\dots c_1c_0$ if $\deg f = n$.

Conclusion: To construct a finite field of p^n elements, it suffices to find a (monic) *irreducible* polynomial $f \in \mathbb{F}_p[X]$ of degree n:

$$f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0,\ a_i \in \mathbb{F}_p.$$

The field is then $\mathbb{F}_p[X]/(f)$.

This requires storage $n\lceil \log p/\log 2\rceil \sim \log q/\log 2$, which is much better than keeping track of tables, which we saw required storage space $2q^2(\log q)/(\log 2)$!

Example. For $p = 2$, $n = 3$, we have two choices for f: $X^3 + X + 1$ and $X^3 + X^2 + 1$. So one model for $\mathbb{F}_8$ is

$$\mathbb{F}_2[X]/(X^3 + X + 1)$$

and another is

$$\mathbb{F}_2[X]/(X^3 + X^2 + 1).$$

This is some of the material covered March 19–21, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

Even though the addition structure is the same in the field, when multiplying we reduce modulo different f. These are, by the theorem, isomorphic as fields, meaning that there is a way of matching up the elements so that the multiplication corresponds.

It suffices to find one such polynomial, therefore. Given a prime number p and a positive integer n, how do we quickly produce a monic irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n? Just as in the case of the integers, random searching is enough:

(1) Pick a random f of degree n, monic, in $\mathbb{F}_p[X]$.
(2) Test f for irreducibility, and iterate until answer is "yes".

We need to discuss how fast this algorithm is (what is the analogy of the prime number theorem for $\mathbb{F}_p[X]$?) and give a fast algorithm to test a polynomial for irreducibility.

We let

$$a_n(p) = \#\{f \in \mathbb{F}_p[X] : f \text{ monic, irreducible, } \deg f = n\}.$$

The probability of "yes" in (2) above is $a_n(p)/p^n$.

From unique factorization in $\mathbb{F}_p[X]$ one can dedcue: for all $n \geq 1$, $\sum_{d|n} d a_d(p) = p^n$. From this, we can obtain the closed formula:

$$a_n(p) = \frac{1}{n}\sum_{d|n} \mu(d) p^{n/d}$$

where $\mu(d)$ is defined by

$$\mu(d) = \begin{cases} 0, & d \text{ is divisible by the square of a prime number;} \\ (-1)^r, & d \text{ is the product of } r \text{ distinct prime numbers.} \end{cases}$$

Example. For example, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, and so on. Therefore

$$a_{45}(p) = \frac{1}{45}(p^{45} - p^{15} - p^9 + p^3).$$

For our purposes, we have the estimate from before:

$$\frac{p^n - 2p^{\lfloor n/2 \rfloor}}{n} < a_n(p) \leq \frac{p^n}{n}.$$

Therefore

$$\frac{1}{n} - 2\frac{p^{-n/2}}{n} < \frac{a_n(p)}{p^n} \leq \frac{1}{n}.$$

Hence $a_n(p)/p^n \approx 1/n$. A random polynomial monic of degree n is irreducible with probability $\sim 1/n$, independent of p. Recall that a random positive integer near x is prime with probability $\sim 1/\log x$: the degree of a polynomial corresponds roughly to the logarithm of an integer.

We have the following remarkable theorem:

Theorem. *In $\mathbb{F}_p[X]$, one has*

$$X^{p^n} - X = \prod_{\substack{g \in \mathbb{F}_p[X] \\ g \text{ monic, irreducible} \\ (\deg g) | n}} g$$

for all $n \geq 1$.

Note, the relation

$$\sum_{d|n} d a_d(p) = p^n$$

expresses that the degrees of the LHS and RHS are the same.

If k is a finite field, $\#k = q$, then we see from the multiplicative structure of k that $\alpha^q = \alpha$. Recall that if $k = \mathbb{F}_p$, where p is prime, then by Fermat's little theorem, for all $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$. Similarly, we will see that $k = \mathbb{F}_p[X]/(g)$, where g is irreducible, with $q = p^{\deg g}$, has the property that for all polynomials f,

$$f^{p^{\deg g}} \equiv f \pmod{g}.$$

As a consequence, take $f = X$: then

$$g \mid (X^{p^{\deg g}} - X).$$

By induction, we see that $\alpha = \alpha^q = (\alpha^q)^q = \alpha^{q^2} = \cdots = \alpha^{q^i}$, so in fact

$$f^{p^{i \deg g}} \equiv f \pmod{g}.$$

This shows that if $\deg g \mid n$, then

$$g \mid (X^{p^n} - X)$$

in $\mathbb{F}_p[X]$.

Now we can prove the theorem:

Proof. Since we have unique factorization in $\mathbb{F}_p[X]$, $X^{p^n} - X$ can be written as the product of irreducible factors. Therefore for each g which is monic, irreducible, with $\deg g \mid n$, we know that $g \mid X^{p^n} - X$, so all of those g occur, hence

$$X^{p^n} - X = h \prod_{\substack{g \\ \deg g | n}} g.$$

We would like to show that h is trivial.

But from the relation

$$\sum_{d|n} d a_d(p) = p^n$$

we count degrees on both sides and see that $\deg h = 0$, so h is constant, but since both sides are monic, $h = 1$. □

Testing for Irreducibility

Given $f \in \mathbb{F}_p[X]$, monic of degree $n \geq 1$, how can we tell whether f is irreducible? We see from the above that one necessary condition is: $X^{p^n} \equiv X \pmod{f}$. This is something that can easily be tested. If no, then the polynomial is *not* irreducible. If yes, then $f \mid (X^{p^n} - X)$ so f is a subproduct of $\prod_g g$ as above so each irreducible factor of f occurs only *once* in f and has degree dividing n.

We therefore have the following:

Theorem. *Let $f \in \mathbb{F}_p[X]$ be monic of degree $n \geq 1$.*

(a) *Suppose first n is a power of a prime number $n = r^t$, $t \geq 1$. Then: f is irreducible if and only if*

$$X^{p^n} \equiv X \pmod{f} \text{ and } X^{p^{n/r}} = X^{p^{r^{t-1}}} \not\equiv X \pmod{f}.$$

(b) *For general n: f is irreducible if and only if*

$$X^{p^n} \equiv X \pmod{f}$$

and for each $r \mid n$ prime,

$$X^{p^{n/r}} - X \in (\mathbb{F}_p[X]/(f))^*,$$

i.e. the element $X^{p^{n/r}} - X$ is a unit modulo f.

Proof. It is clear from the above that if f is irreducible, then we have conditions (a) and (b), respectively.

Now suppose that we have the condition in (a). We see that every irreducible factor g must have degree dividing $n = r^t$, so in particular unless $g = f$ its degree must be strictly smaller, hence divide r^{t-1}. Therefore $X^{p^{r^{t-1}}} \equiv X \pmod{f}$, which is a contradiction.

For (b), let g be an irreducible factor of f. We will show that $g = f$. Suppose otherwise: then again since $\deg g \mid \deg f$ we may assume that there is a prime factor r such that it divides $\deg f = n$ to a higher power than $\deg g$; in particular, by adding degrees, we see that $X^{p^{n/r}} \equiv X \pmod{g}$ and $g \mid f$, so $g \mid \gcd(X^{p^{n/r}} - X, f) = 1$, a contradiction. □

A word on computational complexity: by using repeated squarings as in the case of $\mathbb{Z}/n\mathbb{Z}$, we may obtain the time for this algorithm (which requires only powerings and computing gcd) as $cn(\log p)^3$. However, if you take advantage of the freshperson's dream, and use the fact that pth power can be represented as a linear map (and hence a matrix), we can compute this in $n(\log p)$ steps: in particular, we see that $X^{p^n} \equiv X \pmod{f}$ if and only if the matrix representing the pth power Frobenius has nth power the identity.

An Aside

We now sketch

$$\sum_{d \mid n} d a_d(p) = p^n$$

very briefly! We have the following equalities:

$$\begin{aligned} Z(t) &= \sum_{\substack{h \in \mathbb{F}_p[X] \\ h \text{ monic}}} t^{\deg h} = \prod_{\substack{f \text{ monic} \\ \text{irreducible}}} \frac{1}{1 - t^{\deg f}} \\ &= \sum_{n=0}^{\infty} p^n t^n = \frac{1}{1 - pt} = \prod_{d=1}^{\infty} \frac{1}{(1 - t^d)^{a_d(p)}}. \end{aligned}$$

Now we apply the logarithmic derivative: to a power series $P(t)$, we have $\lambda(P) = P'/P$: we get

$$\lambda(1/(1 - pt)) = -\lambda(1 - pt) = \frac{tp}{1 - tp} = \sum_{n=1}^{\infty} p^n t^n$$

and this is equal to

$$\lambda(\prod (1 - t^d)^{-a_d(p)}) = \sum_d a_d(p) \frac{dt^d}{1 - t^d} = \sum_d \sum_{m=1}^{\infty} d a_d(p) t^{md}.$$

Now compare coefficients at t^n.