

Algorithms for Finite Fields

Notes for October 5, 2006

Primitive Roots

An element $g \in \mathbb{F}_q^*$ is called a *primitive root* if $\langle g \rangle = \mathbb{F}_q^*$.

How many primitive roots are there? $\varphi(q-1)$.

If you pick $g \in \mathbb{F}_q^*$ at random, then g is a primitive root with probability

$$\frac{\varphi(q-1)}{q-1} = \prod_{l|q-1, l \text{ prime}} (1 - 1/l) \gg 1/\log q.$$

So there are many primitive roots.

How can we test if g is a primitive root? g is a primitive root $\Leftrightarrow g^{\frac{q-1}{l}} \neq 1 \forall l|q-1, l \text{ prime}$.

This is easy to do, *provided* we know the prime factors of $q-1$.

To construct finite fields, we construct $\mathbb{F}_q = \mathbb{F}_p[x]/(f(x))$.

A polynomial $f(x)$ is primitive if $f(x) \in \mathbb{F}_p[x]$ is irreducible and $\langle x \rangle = (\mathbb{F}_p[x]/(f(x)))^*$.

Example: $\mathbb{F}_{p^p} = \mathbb{F}_p[x]/(x^p - x + g)$, where g is a primitive root *mod* p .

Conjecture: $x^p - x + g$ is primitive.

This is equivalent to the root of $x^p - x + 1$ having order $\frac{p^p-1}{p-1}$.

We know this element has order $\gg (5.9)^p$.

To see this: $\bar{x}^p = \bar{x} - 1$, so induction implies $\bar{x}^{p^k} = \bar{x} - k$.

So if $n = \sum n_k p^k$, then $\bar{x}^n = \prod (\bar{x} - k)^{n_k}$.

If $\sum n_k < p$, then we get distinct elements of $\mathbb{F}_p[x]/(x^p - x + 1)$, at least 2^p of them. So the order is at least 2^p , and getting to $(5.9)^p$ is another technique.

Example: $p = 2$, $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$. This case can be extended to all fields with 2^{2^n} elements by a construction of Wiedemann.

Theorem. For $n \geq 0$, define $\alpha_0 = 1$, and α_n to be a root of $x^2 + \alpha_{n-1}x + 1 = 0$. Then $\mathbb{F}_{2^{2^n}} = \mathbb{F}_2(\alpha_n)$.

Lemma. If $a \in \mathbb{F}_{2^m}$, then $x^2 + x + a$ is irreducible in $\mathbb{F}_{2^m}[x] \Leftrightarrow \text{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(a) = 1$.

Proof. Consider $\varphi : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ where $x \mapsto x^2 + x$. φ is \mathbb{F}_2 -linear and $\ker \varphi = \mathbb{F}_2$, so $\text{Im} \varphi$ is of codimension 1 in \mathbb{F}_{2^m} .

On the other hand, $Im\phi \subseteq ker(Tr_{\mathbb{F}_{2^m}/\mathbb{F}_2})$ because $Tr(x^2 + x) = Tr(x^2) + Tr(x) = 2Tr(x) = 0$ (since x^2 and x are conjugates).

Since Tr is non-trivial (an algebra fact), we get $Im(\phi) = ker(Tr)$.

Since quadratics are irreducible when they don't have roots, we get the lemma. \square

So now back to the Theorem:

Proof of Theorem. $\frac{1}{\alpha_{n-1}^2}(x^2 + \alpha_{n-1}x + 1) = (\frac{x}{\alpha_{n-1}})^2 + (\frac{x}{\alpha_{n-1}}) + \frac{1}{\alpha_{n-1}^2}$.

We need to prove that $Tr(\frac{1}{\alpha_{n-1}^2}) = 1$.

We prove this by induction.

$$\begin{aligned} Tr(\frac{1}{\alpha_{n-1}^2}) &= Tr(\frac{1}{\alpha_{n-1}}) \text{ since they are conjugates} \\ &= Tr(\alpha_{n-1} + \alpha_{n-2}) \text{ since } \alpha_{n-1}^2 + \alpha_{n-2}\alpha_{n-1} + 1 = 0 \Rightarrow \alpha_{n-1} + \alpha_{n-2} + 1/\alpha_{n-1} = 0 \\ &= Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_2}(\alpha_{n-1}) + Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_2}(\alpha_{n-2}) \end{aligned}$$

Now

$$Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_2}(\alpha_{n-2}) = Tr_{\mathbb{F}_{2^{2n-2}}/\mathbb{F}_2}(Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_{2^{2n-2}}}(\alpha_{n-2})) = 0,$$

since

$$Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_{2^{2n-2}}}(\alpha_{n-2}) = \alpha_{n-2} + \alpha_{n-2} = 0$$

since $\alpha_{n-2} \in \mathbb{F}_{2^{2n-2}}$.

And

$$Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_2}(\alpha_{n-1}) = Tr_{\mathbb{F}_{2^{2n-2}}/\mathbb{F}_2}(Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_{2^{2n-2}}}(\alpha_{n-1})).$$

But α_{n-1} is a root of $x^2 + \alpha_{n-2}x + 1$ over $\mathbb{F}_{2^{2n-2}}$, we get

$$Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_{2^{2n-2}}}(\alpha_{n-1}) = \alpha_{n-2},$$

so $Tr_{\mathbb{F}_{2^{2n-1}}/\mathbb{F}_2}(\alpha_{n-1}) = 1$ by induction. \square

We will now use the notation $q = 2^{2^{n-1}}$. So $\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha)$, where $\alpha = \alpha_n$. Every element of \mathbb{F}_{q^2} is of the form $u + v\alpha$, $u, v \in \mathbb{F}_q$. Arithmetic is

$$(u_1 + v_1\alpha)(u_2 + v_2\alpha) = (u_1u_2 + v_1v_2) + (u_1v_2 + u_2v_1 + \alpha_{n-1}v_1v_2)\alpha.$$

So to do multiplication in \mathbb{F}_{q^2} , one must do multiplication in \mathbb{F}_q , so it's recursive and can be very efficient in larger fields.

Conjecture. $\alpha_n\alpha_{n-1}\cdots\alpha_1$ is a primitive root for $\mathbb{F}_{2^{2^n}}$ for all n .

($\Leftrightarrow \alpha_n$ has order $q + 1$, i.e. $2^{2^{n-1}} + 1 \nmid n$)

Note that $q^2 - 1 = (q - 1)(q + 1)$ and that $q^2 - 1 = \#\mathbb{F}_{q^2}^*$, $q - 1 = \#\mathbb{F}_q^*$, and $q + 1 = \#\{x \in \mathbb{F}_{q^2}^* \mid N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x) = 1\}$. On the other hand, $\alpha^2 + \alpha_{n-1}\alpha + 1 = 0$, so $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 1$. So the conjecture is that α is a generator of the subgroup of norm 1 elements of \mathbb{F}_{q^2} .

The conjecture is known for $n \leq 11$. The hard part is factoring $F_n = 2^{2^n} + 1$.

Question: Give a lower bound to the order of α_n .

A good lower bound combined with the partial factorizations of \mathbb{F}_n 's might allow us to check the conjecture for a few more values of n .