Finite Fields and Discrete Logs

Prof. Weibel
Math 348
Spring 2008

A *finite field* $\mathbb{F}_q$ is a finite set of q elements, including 0 and 1, in which you can add and subtract, multiply and divide (except for division by 0). A more formal definition is given in section 19.1 of Garrett. The basic examples are the fields $\mathbb{F}_p = \mathbb{Z}/p$ where p is a prime number. Some fundamental facts (see sections 7.8, 17.6, 26.1, 27.1 and 29.5):

(1) the size is a power of a prime number $q = p^n$, and $\mathbb{Z}/p$ is contained in $\mathbb{F}_q$. In fact, $\mathbb{F}_q$ is an n-dimensional vector space over $\mathbb{Z}/p$;
(2) Any two finite fields with q elements are isomorphic after relabelling;
(3) there is an element ζ such that every element of $\mathbb{F}_q$ is on the list:

$$0, 1, \zeta, \zeta^2, \zeta^3, ..., \zeta^{q-2}.$$

Such an element is called a *primitive root* of $\mathbb{F}_q$. In fact there are $\varphi(q-1)$ different choices of a primitive root, including $\zeta^{-1} = \zeta^{q-2}$.
(4) for an $x \neq 0$ in $\mathbb{F}_q$ there is a unique ℓ ($0 \leq \ell \leq q-2$) so that $x = \zeta^\ell$; ℓ is called the *discrete logarithm* of x base ζ and often written $\log_\zeta(x)$. Since $\zeta^a \zeta^b = \zeta^{a+b}$ we have $\log(xy) = \log(x) + \log(y) \pmod{q-1}$.
(5) Every element x satisfies $x^{q-1} = 1$. Note that the multiplicative inverse of $x = \zeta^\ell$ is $x^{-1} = \zeta^{q-1-\ell}$.

Primitive roots in $\mathbb{Z}/p$. For $p < 100$, all primitive roots are listed in Table 3 on page 511. For $p = 5$ we choose $\zeta = 2$ and note that $\{0, 1, 2, 2^2 = -1, 2^3 = 3\}$ is $\mathbb{Z}/5$. For $p = 7$, 2 is not a primitive root but $\zeta = 3$ and $\zeta = 5 = 3^{-1}$ are: the elements of $\mathbb{Z}/7$ are: $\{0, 1, 3, 3^2 = 2, 3^3 = -1, 3^4 = 4, 3^5 = 5\}$.

The field $\mathbb{F}_4$. A basis for this vector space is $\{t, 1\}$. Thus the elements of this field are elements $at + b$ where $a, b \in \mathbb{Z}/2$. We multiply them as polynomials and then apply the rewriting rule $t^2 = t + 1$. Here t is a primitive root, and $t^3 = t \cdot t^2 = t(t+1) = t^2 + t = 1$. Formally, this construction is written as $\mathbb{F}_4 = \mathbb{Z}/2[t]/(t^2 = t + 1)$.

The field $\mathbb{F}_{16}$. A basis for this vector space is $\{x^3, x^2, x, 1\}$ and it is convenient to represent an element $a_1x^3 + a_2x^2 + a_3x + a_4$ as a binary string (a_1, a_0, a_3, a_4) or as a hexadecimal digit (0,1,...,9,A,B,C,D,E,F).

Here $x = (0010)$ is a primitive root and the powers of x are: $x^2 = (0100)$, $x^3 = (1000)$, $x^4 = (0011)$, $x^5 = (0110)$, $x^6 = (1100) =$'C', $x^7 = (1011) =$'B', $x^8 = (0101)$, $x^9 = (1010) =$'A', $x^{10} = (0111)$, $x^{11} = (1110) =$'E', $x^{12} = (1111) =$'F', $x^{13} = (1101) =$'D' and $x^{-1} = x^{14} = (1001)$. (Of course $x^{15} = 1$.)

Incidentally, if we set t equal to $x^5 = x^2 + x = (0110)$ then $t^2 = t + 1$ because $x^{10} = x^2 + x + 1$. It follows that the subspace with basis $\{t, 1\}$ is the field $\mathbb{F}_4$.