2MMC10 Cryptology – Fall 2015

September 10, 2015

Finite Fields (continued)

Recap:

Definition (field)**.** A set K is a *field* with respect to $+$ and $\cdot$, denoted $(K, +, \cdot)$, if

i) $(K, +)$ is an abelian group (closure, associativity, identity, inverse, commutative),

ii) $(K^*, \cdot)$ is and abelian group, where $K^* = K \setminus \{0\}$, and

iii) the distributive law holds in K, i.e.,
$a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in K$

Example (GF(4))**.** Let's inspect GF(4) $= (\{■, ●, ★, ▲\}, +, \cdot)$:

+	■	●	★	▲
■	■	●	★	▲
●	●	■	▲	★
★	★	▲	■	●
▲	▲	★	●	■

·	●	★	▲
●	●	★	▲
★	★	▲	●
▲	▲	●	★

We have an identity and an inverse for each $+$ and $\cdot$; both operations are commutative; we have closure under both operations; we have associativity:

▲ + (★ + ●) = ▲ + ▲ = ■
(▲ + ★) + ● = ● + ● = ■

■, ●, ★, and ▲ are not convenient for the representation of field elements, we want something that allows us to compute $+$ and $\cdot$ easily.

Last time, we figured out that we can use $\mathbb{Z}/_{p\mathbb{Z}}$ to represent the elements of the prime subfield of a field K and that K is a vector space over the prime field. So let's write

$$\mathrm{GF}(4) = \left(\left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\}, +, \cdot\right) = (\{0, 1, a, a+1\}, +, \cdot).$$

Use the basis vectors $\alpha_1 = \begin{pmatrix}0\\1\end{pmatrix}$ and $\alpha_2 = \begin{pmatrix}1\\0\end{pmatrix}$ or 1 and a in order to represent each element:

$$\begin{pmatrix}0\\0\end{pmatrix} = 0 \cdot \alpha_2 + 0 \cdot \alpha_1 \quad \longmapsto \quad 0 \cdot a + 0 \cdot 1 = 0$$
$$\begin{pmatrix}0\\1\end{pmatrix} = 0 \cdot \alpha_2 + 1 \cdot \alpha_1 \quad \longmapsto \quad 0 \cdot a + 1 \cdot 1 = 1$$
$$\begin{pmatrix}1\\0\end{pmatrix} = 1 \cdot \alpha_2 + 0 \cdot \alpha_1 \quad \longmapsto \quad 1 \cdot a + 0 \cdot 1 = a$$
$$\begin{pmatrix}1\\1\end{pmatrix} = 1 \cdot \alpha_2 + 1 \cdot \alpha_1 \quad \longmapsto \quad 1 \cdot a + 1 \cdot 1 = a + 1$$

This allows us to compute the addition table:

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

$\cdot$	1	a	$a+1$
1	1	a	$a+1$
a	a	$a+1$	1
$a+1$	$a+1$	1	a

But the vector space does not help as with the multiplication table – because there is no vector-vector multiplication.

Let's try another field GF(8) with $8 = 2^3$ elements, thus a basis $\alpha_1 = 1$, $\alpha_2 = a$, $\alpha_3 = b$. If we use $a^2 = 1$, we run into the same problems as before; choosing $a^2 = a + 1$ constructs the same field as before — no connection with b. So let's try $a^2 = b$; then $a \cdot (a+1) = a^2 + a = b + a$. Again several options for $a \cdot b$. Obviously one can not choose $a \cdot b = a$, b, or $b + a$. Choosing $a \cdot b = 1$ gives $(a+1)(b+a+1) = a \cdot b + a^2 + a + b + a + 1 = 1 + b + b + 1 = 0$ — which is not possible in a field. Similarly $a \cdot b = a + b + 1$ is excluded by $(a+1) \cdot (b+1) = a \cdot b + a + b + 1 = a + b + 1 + a + b + 1 = 0$. Try $a \cdot b = a + 1$:

- $a \cdot (b + 1) = a \cdot b + a = a + 1 + a = 1$;
- $a \cdot (b + a) = a \cdot b + a^2 = (a + 1) + b$;
- $a \cdot (b + a + 1) = \cdots = a + 1 + b + a = b + 1$;
- $(a + 1)^2 = a^2 + 1 = b + 1$;
- $(a + 1)b = a \cdot b + b = (a + 1) + b$;
- $(a + 1)(b + 1) = a \cdot b + a + b + 1 = (a + 1) + a + b + 1 = b$;
- $(a + 1)(b + a) = a \cdot b + a^2 + b + a = (a + 1) + b + b + a = 1$;
- $b^2 = a^2 \cdot b = a \cdot (a \cdot b) = a \cdot (a + 1) = a^2 + a = b + a$;
- $(b + 1)(b + a) = b^2 + ba + b + a = (b + a) + (a + 1) + b + a = a + 1$
- $\ldots$

$\cdot$	1	a	$a+1$	b	$b+1$	$b+a$	$b+a+1$
1	1	a	$a+1$	b	$b+1$	$b+a$	$b+a+1$
a	a	b	$b+a$	$a+1$	1	$b+a+1$	$b+1$
$a+1$	$a+1$	$b+a$	$b+1$	$a+b+1$	b	1	a
b	b	$a+1$	$a+b+1$	$b+a$	a	$b+1$	1
$b+1$	$b+1$	1	b	a	$b+a+1$	$a+1$	$b+a$
$b+a$	$b+a$	$b+a+1$	1	$b+1$	$a+1$	a	b
$b+a+1$	$b+a+1$	$b+1$	a	1	$b+a$	b	$a+1$

How can we get this "automatically"?
How do we compute $a \cdot b = c$ without a lookup table?

The ides is to use a polynomial ring to represent the field elements. A polynomial ring also spans a vector space – but in contrast to the vector space, the multiplication of polynomials is well defined.

Polynomial ring over field K

$$K[x] = \left\{ \sum_{i=1}^{n} a_i x^i \mid n \in \mathbb{N}, a_i \in K \right\}. \quad f \in K[x],\ f = \sum f_i x_i.$$

Let n be the largest integer with $f_n \neq 0$ then $\deg(f) = n$, leading coefficient $\mathrm{LC}(f) = f_n$, leading term $\mathrm{LT}(f) = f_n x^n$.

Definition (irreducible)**.** A polynomial $f \in K[x]$ is called *irreducible* if $\deg(f) \geq 1$ and it cannot be written as a product of polynomials of lower degree over the same field, i.e., if $u(x)/f(x)$ then $u(x) \in K$ or $u(x) = f(x)$.
Otherwise f is *reducible*. Note that this depends on the field K.

Example.

- $x^2 - 1 = (x+1)(x-1)$ is reducible in $\mathbb{R}[x]$.
- $x^4 + 2x + 1 = (x^2+1)^2$ in $\mathbb{R}[x]$ has no roots but is reducible.
- $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but reducible in $\mathbb{C}[x]$ by $(x-i)(x+i)$.
- $x^3 + 6x^2 + 4$ is irreducible in $\mathbb{Z}/_{7\mathbb{Z}}$.

The main choice we made in constructing GF(8) was how to write $a \cdot b$ in terms of the other elements; $b = a^2$ and so the question was how to represent $a \cdot b = a^3$ in terms of 1, a, and a^2. We chose $a^3 = a+1$ and then all operations followed by using this equality. This polynomial, a^3+a+1 does not factor over GF(2); other choices we considered, e.g., a^3+1 do factor and it was exactly by considering these factors, e.g., $(a+1)$ and (a^2+a+1) that we derived contradictions, e.g., $(a+1)\cdot(a^2+a+1) = a^3+1 = 0$ (using $a^3 = 1$). In the end we worked in $\mathrm{GF}(2)[a]/_{(a^3+a+1)\mathrm{GF}(2)[a]}$ — the polynomial ring over GF(2) modulo the irreducible polynomial a^3+a+1.

Example. Compute $a \cdot (a^2+a)$ and $(a+1)\cdot(a^2+a)$ in GF(8) using the irred. polynomial a^3+a+1:

$$a \cdot (a^2+a) = a^3 + a^2 \qquad\qquad (a+1)\cdot(a^2+a) = a^3 + a$$

$$\begin{array}{r|r} & 1 \\ \hline a^3+a+1 & a^3+a^2 \\ & -(a^3+a+1) \\ \cline{2-2} & a^2+a+1 \end{array} \qquad\qquad \begin{array}{r|r} & 1 \\ \hline a^3+a+1 & a^3+a \\ & -(a^3+a+1) \\ \cline{2-2} & 1 \end{array}$$

In general, this construction gives a finite field:
Let f be a monic irreducible polynomial of degree n over $\mathrm{GF}(p)$. We define addition and multiplication on

$$\mathrm{GF}(p)[x]/_{f(x)\mathrm{GF}(p)[x]} = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in \mathrm{GF}(p) \right\}$$

as addition and multiplication in $\mathrm{GF}(p)[x]$ followed by reduction modulo $f(x)$.
The additive structure forms a group; this matches the vectorspace construction using basis 1, x, x^2, ..., x^{n-1}. Multiplication of two elements gives a polynomial of degree $< n$ (after reduction), associativity and commutativity are inherited from $\mathrm{GF}(p)[x]$, the neutral element is 1 — so the question is whether every element $\neq 0$ is invertible.

Let $g = \sum_{i=0}^{n-1} g_i x^i \in \mathrm{GF}(p)[x]/_{f(x)\mathrm{GF}(p)[x]}$. Since f is irreducible, $\gcd(f,g) = 1$ and XGCD computes polynomials h and l with $1 = g \cdot h + f \cdot l$, thus $h \equiv g^{-1} \mod f$. This procedure works for any g — so the multiplicative structure forms a group, too. The distributive laws hold as in $\mathrm{GF}(p)[x]$ — so we have a field with p^n elements, as soon as we have an irreducible polynomial of degree n over $\mathrm{GF}(p)$.

Example. The polynomial $f = x^3 + x^2 + 1$ is irreducible over the field $\mathbb{F}_2$.
What is the inverse of $x^2 + 1$ over $\mathbb{F}_2$ modulo f?

$$
\begin{array}{rr}
 & x + 1 \\
\cline{2-2}
x^2 + 1 \big) & x^3 + x^2 + 1 \\
 - & (x^3 + x) \\
\cline{2-2}
 & x^2 + x + 1 \\
 - & (x^2 + 1) \\
\cline{2-2}
 & x
\end{array}
$$

$$x^3 + x^2 + 1 = (x^2 + 1)(x + 1) + x$$

$$(x^3 + x^2 + 1) + (x^2 + 1)(x + 1) = x$$

$$
\begin{array}{rr}
 & x \\
\cline{2-2}
x \big) & x^2 + 1 \\
 - & x^2 \\
\cline{2-2}
 & 1
\end{array}
$$

$$x^2 + 1 = x \cdot x + 1$$

$$x^2 + 1 + x \cdot x = 1$$

$$1 = (x^3 + x^2 + 1) \cdot ? + (x^2 + 1) \cdot ?$$

$$
\begin{aligned}
1 &= (x^2 + 1) + x \cdot x \\
&= (x^2 + 1) + \left[(x^3 + x^2 + 1) + (x^2 + 1)(x + 1)\right] x \\
&= (x^2 + 1) + (x^3 + x^2 + 1)\ x + (x^2 + 1)(x + 1)\ x \\
&= (x^3 + x^2 + 1)\ x + (x^2 + 1) + (x^2 + 1)(x + 1)\ x \\
&= (x^3 + x^2 + 1)\ x + (x^2 + 1)\,[1 + (x + 1)\ x] \\
&= (x^3 + x^2 + 1)\ x + (x^2 + 1)(x^2 + x + 1)
\end{aligned}
$$

$$(x^2 + 1)(x^2 + x + 1) = x^4 + x^3 + x + +1$$

$$
\begin{array}{rr}
 & x \\
\cline{2-2}
x^3 + x^2 + 1 \big) & x^4 + x^3 + x + 1 \\
 & (x^4 + x^3 + x) \\
\cline{2-2}
 & 1
\end{array}
$$

Alternative approach:
We know that $a^{p^n} = a$ and $a^{p^n - 1} = 1$ for $a \in \mathrm{GF}(p^n)$ (Lagrange's Theorem).
Thus $a \cdot a^{p^n - 2} = a^{p^n - 1} = 1$.
So we can compute the inverse of $(x^2 + 1)$ as $(x^2 + 1)^6$ in GF(8):

$$
\begin{aligned}
(x^2 + 1)^6 &= (x^2 + 1)^4\ (x^2 + 1)^2 \\
&= \left((x^2 + 1)^2\right)^2\ (x^2 + 1)^2 \\
&= (x^4 + 1)^2\ (x^4 + 1) \\
&= (x^8 + 1)\ (x^4 + 1) \\
&= x^{12} + x^8 + x^4 + 1
\end{aligned}
$$

$$
\begin{array}{rr}
 & x^9 + x^8 + x^7 + x^4 + x^3 + x^2 + x \\
\cline{2-2}
x^3 + x^2 + 1 \big) & x^{12} + x^8 + x^4 + 1 \\
 & - \quad (x^{12} + x^{11} + x^9) \\
\cline{2-2}
 & x^{11} + x^9 + x^8 + x^4 + 1 \\
 & - \qquad (x^{11} + x^{10} + x^8) \\
\cline{2-2}
 & \cdots \\
 & x^2 + x + 1
\end{array}
$$

How do we find irreducible polynomials?
Pick a random polynomial and check if it is irreducible using "Rabin's test of irreducibility" (or a computer algebra system of your choice).