

Introduction to Modern Cryptography

Benny Chor

Finite Fields: $GF(p)$ and $GF(p^k)$

Lecture 3 Part b

School of Computer Science
Tel-Aviv University

November 3rd, 2009

Cyclic Groups

- **Claim:** Let G be a group, and a an element of order n . The set $\langle a \rangle = \{0, a, \dots, a^{n-1}\}$ is a **subgroup** of G .
- a is called the **generator** of $\langle a \rangle$.
- By Lagrange theorem, for every $a \in G$, the **order** of a **divides** $|G|$.
- Fermat's "little" theorem: For every $a \in \{1, \dots, p-1\}$, $a^{p-1} \bmod p = 1$ (why does this hold?).
- If G is generated by some a then G is called **cyclic**, and a is called a **primitive element** of G .

Fields – Reminder

A field is a commutative ring with identity where each **non-zero** element has a **multiplicative inverse**:

$$\forall a \neq 0 \in F \exists c \in F, a \cdot c = 1.$$

The multiplicative inverse of a is also denoted a^{-1} .

Equivalently, $(F, +)$ is a commutative (additive) group, and $(F \setminus \{0\}, \cdot)$ is a commutative (multiplicative) group.

Finite Fields

Definition: A field $(F, +, \cdot)$ is called a **finite field** if the set F is **finite**.

Example: As we already saw, Z_p denotes the set $\{0, 1, \dots, p-1\}$, where we define $+$ and \cdot as addition and multiplication modulo p , respectively.

It is not hard to prove that $(Z_p, +, \cdot)$ is a field iff p is a **prime**. (try this!)

It is also possible to show that for any prime, p , $(Z_p, +, \cdot)$ is the **only** finite field with p elements. This means that any finite field with that many elements is essentially $(Z_p, +, \cdot)$ (up to changing names).

Question: Are there any finite fields except $(Z_p, +, \cdot)$?

The Characteristic of Finite Fields

Let $(F, +, \cdot)$ be a finite field.

There must be a positive integer, n , such that $1 + 1 + \dots + 1$ (n times) equals 0.

The minimal such n is called the **characteristic** of F , $\text{char}(F)$.

Theorem: For any finite field F , $\text{char}(F)$ is a **prime** number.

Galois Fields $GF(p^k)$

Theorem: For every prime power p^k ($k = 1, 2, \dots$) there is a **unique** finite field with p^k elements (unique up to renaming). These fields are denoted by $GF(p^k)$. There are **no finite fields** with **other** cardinalities.



Évariste Galois (1811-1832)

(<http://www.wqsb.qc.ca/philemon/pmessier/mathematicians.htm>)

Remarks:

1. For $F = GF(p^k)$, $\text{char}(F) = p$.
2. We will shortly see how $GF(p^k)$ (for $k > 1$) is represented and implemented. Recall it is **not** the same as Z_{p^k} !

The Multiplicative Group of $GF(p^k)$

- For a field F , we denote by F^* the set of all non zero elements in F .
- Recall that F^* is an Abelian group with respect to the field's multiplication.
- In the case that $F = GF(p^k)$ is finite, F^* has $q = p^k - 1$ elements.
- By Lagrange, for every $a \in F^*$, the order of a divides q .
- Furthermore, if $ord_{F^*}(a) = \ell$ and $a^j = 1$, then ℓ divides j .

Roots of Univariate Polynomials over Fields

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \dots + a_1x + a_0$ be a polynomial of degree n in one variable x over a field F (namely $a_n, a_{n-1}, \dots, a_1, a_0 \in F$).

Theorem: The equation $f(x) = 0$ has **at most** n solutions in F . Such solution is called a **root** of $f(x)$.

We will employ this theorem, together with the last two assertions from the last slide, to show the following:

Primitive Elements in $GF^*(p^k)$

Theorem: Let $F = GF(p^k)$ be a finite field. Then the multiplicative group $GF^*(p^k)$ is **cyclic**. This means there is an element $g \in GF^*(p^k)$ such that the powers $g, g^2, g^3, \dots, g^{p^k-1}$ are all different, and thus they span all of $GF^*(p^k)$.

Remark 1: Such element g is called a **primitive element** of $GF^*(p^k)$.

Remark 2: This theorem does not hold in general for **infinite fields**. Consider, for example, \mathbb{Q}, \mathbb{R} , or \mathbb{C} .

Remark 3: Such primitive elements will be useful in Diffie-Hellman key exchange.

Primitive Elements in $GF^*(p^k)$: Proof ¹

Suppose, by way of contradiction, that $GF^*(p^k)$ is **not cyclic**. Let g be an element of **maximal order** in $GF^*(p^k)$, denote $ord(g) = k$ (by assumption, $k < p^k - 1$).

It is not possible that for every a , $ord(a) | k$, because then the polynomial $x^k - 1$ would have more than k roots.

So there must be another element, h ($h \neq g$) such that $ord(h) \nmid k$.

By raising to appropriate power, we have, without loss of generality, $ord(h) = p_i^\ell$ for some prime p_i , and furthermore $p_i^\ell \nmid k$ yet $p_i^{\ell-1} | k$ (**think why this holds**).

Thus the **least common multiple** of k and p_i^ℓ equals $\text{lcm}(k, p_i^\ell) = kp$. Denote this number by m .

¹thanks to Nir Bitansky for this elegant proof

Primitive Elements in $GF^*(p^k)$: Proof (cont.) ²

We have $\text{ord}(g) = k$, $\text{ord}(h) = p_i^\ell$, and $m = \text{lcm}(k, p_i^\ell) = kp_i$.

Take the field element gh . What is its order, $t = \text{ord}(gh)$?

Certainly $t \mid kp_i$, because $(gh)^{kp_i} = g^{kp_i} h^{kp_i} = 1$ ($h^{kp_i} = 1$ because p_i^ℓ divides kp_i and $\text{ord}(h) = p_i^\ell$).

Suppose $t < kp_i$. Let $k = Np_i^{\ell-1}$. Since $t \mid kp_i$, either $t \mid Np_i^{\ell-1} = k$ or $t \mid Sp_i^\ell$ where S is a **proper factor** of N . In the first case, $1 = (gh)^k = g^k h^k = h^k$, implying $\text{ord}(h) \mid k$, contradicting the choice of h . In the second case, $1 = (gh)^{Sp_i^\ell} = g^{Sp_i^\ell} h^{Sp_i^\ell} = g^{Sp_i^\ell}$. But then, since $\text{ord}(g) = k$, we must have $k \mid Sp_i^\ell$, contradiction.

So we must have $t = kp_i$. But then $t = \text{ord}(gh) > k$, contradicting the **maximality** of $k = \text{ord}(g)$. ♠

²continued thanks to Nir Bitansky for this elegant proof

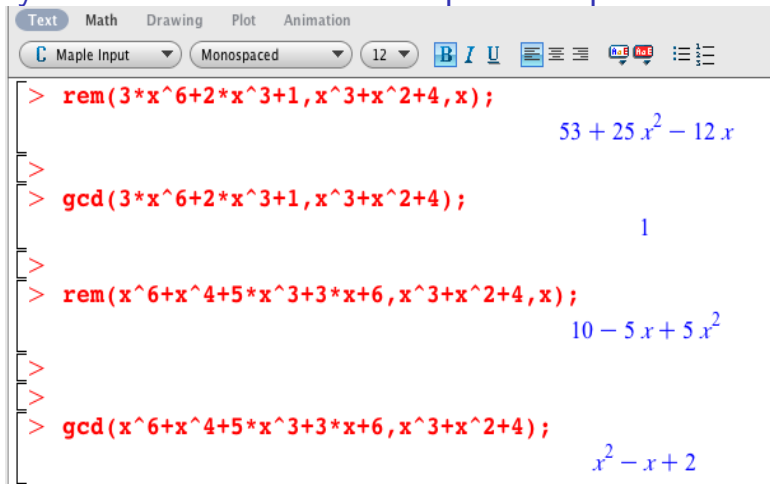
Polynomial Remainders

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \dots + a_1x + a_0$
 $g(x) = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + b_{m-2} \cdot x^{m-2} + \dots + b_1x + b_0$ be two polynomials in one variable x over a field F such that $m \leq n$.

Theorem: There is a unique polynomial $r(x)$ of degree **smaller than** m , and another unique polynomial, $h(x)$, both over F , such that $f(x) = h(x) \cdot g(x) + r(x)$.

The polynomial $r(x)$ is called the **remainder** of $f(x)$ modulo $g(x)$.

Polynomial Remainders: A Maple Example



The screenshot shows the Maple software interface with a menu bar (Text, Math, Drawing, Plot, Animation) and a toolbar (Maple Input, Monospaced, font size 12, Bold, Italic, Underline, and other icons). The command window contains the following input and output:

```
> rem(3*x^6+2*x^3+1, x^3+x^2+4, x);  
53 + 25 x^2 - 12 x  
  
>  
> gcd(3*x^6+2*x^3+1, x^3+x^2+4);  
1  
  
>  
> rem(x^6+x^4+5*x^3+3*x+6, x^3+x^2+4, x);  
10 - 5 x + 5 x^2  
  
>  
>  
> gcd(x^6+x^4+5*x^3+3*x+6, x^3+x^2+4);  
x^2 - x + 2
```

The remainder is 0 (the zero polynomial) iff $g(x) \mid f(x)$. But if this is not the case, the remainder may be of degree $m - 1$, while $f(x)$ and $g(x)$ may or may not be relatively prime.

Polynomials over Finite Fields

Polynomial equations and factorizations over finite fields can be quite different than their rationals/reals counterparts.

Examples from a Maple session:

```
> factor(x^6-1); # over the rationals/reals
(x-1)(x+1)(x^2+x+1)(x^2-x+1)
> p:=7;
p:=7
> f := modp1(ConvertIn(x^6-1,x),p);
f := (x^6 + 6) mod 7
>
> modp1(Factors(f),p)[2]; # list of factors and their multiplicities over GF(7)
[[ (x+5) mod 7, 1], [(x+6) mod 7, 1], [(x+2) mod 7, 1], [(x+1) mod 7, 1], [(x+4) mod 7, 1], [(x+3) mod 7, 1]]
> p:=2;
p:=2
> g := modp1(ConvertIn(x^6-1,x),p);
g := (x^6 + 1) mod 2
> modp1(Factors(g),p)[2]; # list of factors and their multiplicities over GF(2)
[[ (x+1) mod 2, 2], [(x^2+x+1) mod 2, 2]]
```

Over $GF(7)$, $x^6 - 1$ has **six linear factors** (btw, is this a coincidence?), while over $GF(2)$ the factorization is the same as over the rationals (given that $-1 = 1$).

Irreducible Polynomials

A polynomial is **irreducible** over $GF(p)$ if it does not factor in $GF(p)$. Otherwise, it is called **reducible**.

Maple example:

```
> p:=2;
                                     p:=2
> f := modp1(ConvertIn(x^5+x^3+1,x),p);
                                     f:=(x^5+x^3+1) mod 2
> modp1(Factors(f),p)[2]; # list of factors and their multiplicities over GF(2)
                                     [[(x^5+x^3+1) mod 2, 1]]
> p:=5;
                                     p:=5
> g := modp1(ConvertIn(x^5+x^3+1,x),p);
                                     g:=(x^5+x^3+1) mod 5
> modp1(Factors(g),p)[2]; # list of factors and their multiplicities over GF(5)
                                     [[(x^2+2.x+3) mod 5, 1], [(x^3+3.x^2+2.x+2) mod 5, 1]]
```

$x^5 + x^3 + 1$ is irreducible over $GF(2)$, but reducible over $GF(5)$.

Implementing $GF(p^k)$ Arithmetic

Theorem: Let $f(x)$ be an **irreducible** polynomial of degree k over $GF(p)$.

The arithmetic of the finite field $GF(p^k)$ can be realized by the set of polynomials over $GF(p)$ whose degree is at most $k - 1$, where addition and multiplication are done **modulo** $f(x)$.

Comment: For every p, k there are irreducible polynomials of degree k over $GF(p)$. Furthermore, such polynomial can be found **efficiently** (random polynomial time in $\log p$ and k).

Example: Implementing $GF(2^5)$

By the theorem, the finite field $GF(2^5)$ can be realized as the set of degree 4 polynomials over Z_2 , with addition and multiplication done modulo the irreducible polynomial $f(x) = x^5 + x^3 + 1$.

Remark: $f(x) = x^5 + x^3 + 1$ is **not** the only irreducible polynomial over Z_2 . But it does not matter which (irreducible) one we take – they all give the **same** object, $GF(2^5)$.

The coefficients of polynomials over Z_2 are 0 or 1. So a degree $k - 1$ polynomial can be written down by k bits. For example, with $k = 5$:

- $x^3 + x + 1$ is represented by $(0, 1, 0, 1, 1)$
- $x^4 + x^3 + x + 1$ is represented by $(1, 1, 0, 1, 1)$

Implementing Addition in $GF(p^k)$

In fields of characteristic 2, $1 + 1 = 0$, so addition corresponds to bit-wise XOR.

For example, $(x^3 + x + 1) + (x^4 + x^3 + x + 1)$ corresponds to

$$(0, 1, 0, 1, 1) \oplus (1, 1, 0, 1, 1),$$

which equals $(1, 0, 0, 0, 0)$, so

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

For fields of larger characteristic $p > 2$, the procedure is the same, only instead of XOR we do $\text{mod } p$ addition.

Implementing Multiplication in $GF(p^k)$

Multiplication has two stages. First stage is polynomial multiplication, which results in a polynomial of degree (at most) $2k - 2$. The second stage is computing the remainder of this polynomial modulo the defining, irreducible polynomial of degree k , $f(x)$, doing the computation mod p .

Maple example, in $GF(2^5)$, with $f(x) = x^5 + x^3 + 1$:

```
> p(x) := expand((x^3+x+1)*(x^4+x^3+x+1));  
                                     p(x) := x^7 + x^6 + 3x^4 + 2x^3 + x^5 + x^2 + 2x + 1  
>  
> rem(p(x), x^5+x^3+1, x) mod 2;  
                                     1 + x  
_
```

So $(0, 1, 0, 1, 1) \cdot (1, 1, 0, 1, 1)$ equals $(0, 0, 0, 1, 1)$.

For **small** size finite field, a lookup table is the most efficient method for implementing multiplication.

Example: Implementing $GF(2^5)$ with Maple

Again, we take the irreducible polynomial $f(x) = x^5 + x^3 + 1$.

```
> G32:=GF(2,5,x^5+x^3+1);  
      G32:=Z2[x] /<(x^5 + x^3 + 1)>  
> a:=G32[ConvertIn](x); # slightly cumbersome notation  
      a:=x mod 2  
> b:=G32[^^](a,8): # raising to power 8  
> c:=G32[^^](a,9): # colon after statement supresses  
      printing  
> G32[ConvertOut](b); # back to regular representation  
      x^4 + x^3 + x  
> G32[ConvertOut](c);  
      x^4 + x^3 + x^2 + 1  
> d:=G32[ConvertIn](x^3+x+1);  
      d:=(x^3 + x + 1) mod 2  
> e:=G32[^^](d,8):  
> G32[ConvertOut](e);  
      x^2 + x + 1
```

More Operations in $GF(p^k)$ with Maple

We continuing the previous slide, with the finite field $GF(2^5)$ represented using the irreducible polynomial $f(x) = x^5 + x^3 + 1$. We now check whether elements are **primitive**, namely if they are generators of the **multiplicative group** $GF^*(2^5)$.

```
> e:=G32[``^``](d,31);  
> G32[ConvertOut](e);  
1  
> G32[isPrimitiveElement](a);  
true  
> G32[isPrimitiveElement](b);  
true  
> G32[isPrimitiveElement](c);  
true  
> G32[isPrimitiveElement](d);  
true  
> G32[isPrimitiveElement](e);  
false
```

Theorem: For any prime p , the multiplicative group Z_p^* is **cyclic**.