L09

Tuesday, August 9, 2022 9:45 AM

What about $GF(p^m)$ where $m \geq 2$?

We need new tools.

* Polynomials over $GF(p)$ ($GF(p)$ is well-defined already)

* $GF(p)[x]$ is the $\boxed{\underline{\text{set}}}$ of all <u>finite degree</u> polynomial

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n$$

where $a_0, \cdots, a_n \in GF(p)$

(implicitly, all the multiplication and summation is also defined in $GF(p)$)

E.g. $(1+x^2) \in GF(2)[x]$

$(x+x^2) \in GF(2)[x]$

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

$(1+x)+(x+x^2)$
$= 1+x \in GF(2)[x]$

* Sometimes we write it as $F_p[x]$

---

* A <u>monic polynomial</u> is a polynomial with the leading coefficien $a_n = 1$

E.g. $2x+1 \in GF(3)[x]$ is NOT <u>monic.</u>
E.g. all polynomials in $F_2[x]$ is monic

* The degree of a non-zero polynomial $f(x)$, denoted by $\deg(f(x))$, is the index of the leading coefficient.

* The degree of zero-polynomial, by definition, is $-\infty$. i.e. $\deg(0) = -\infty$

* A polynomial $s(x) \in F_p[x]$ is <u>divisible</u> by $r(x) \in F_p[x]$ (or equivalently $r(x)$ is a factor of $s(x)$) if there

$r(x)$ is a factor of $s(x)$) if there exists $a(x) \in \mathbb{F}_p[x]$ such that

$$s(x) = r(x) \cdot a(x)$$

* The <u>greatest common divisor</u> (g.c.d) of $s(x), r(x)$ (denoted by $\gcd(s(x), r(x))$) is the <u>monic</u> polynomial of largest degree that divides both $r(x)$ and $s(x)$

Corollary: $\gcd(s(x), r(x))$ is <u>unique</u>

* Polynomial Division / Modulo

For every pair of polynomials $c(x), d(x) \in \mathbb{F}_p[x]$, with $d(x) \neq 0$, there is a unique pair of polynomials there is a unique pair of polynomials

$Q(x)$: the <u>quotient</u> polynomial

$R(x)$: the remainder polynomial

such that

① $C(x) = Q(x) \cdot d(x) + R(x)$

② $\deg(R(x)) < \deg(d(x))$

* $Q(x)$ and $R(x)$ can be found by long division

E.g. $C(x) = 2x^3 + x + 1$

$d(x) = x^2 + x$

```
              2 , 1
        ____________________
1, 1, 0 | 2 , 0 , 1 , 1
          2   2   2
        ____________________
              1 , 2 , 1
              1 , 1 . 0
        ____________________
```

1.1

$\Rightarrow$ $Q(x) = (2x+1)$ $\quad R(x) = x+1$

* We sometimes write

$$\boxed{R(x) = c(x) \bmod d(x)}$$

* A monic polynomial is <u>irreducible</u> if it cannot be factored as a product of lower degree polynomials

E.g. $x^2+x+1 \in F_2[x]$ is irreducible.

pf: $\because \deg(x^2+x+1) = 2$

plugging in $x=0$ $f(x)=1$

$x=1$ $f(x)=1$

$\Rightarrow$ Irreducible.

E.g. $x^2+x+1 \in GF_3[x]$ is reducible

pf: $x=1$, $f(x)=0$.

pf: $x=1$, $f(x)=0$.

$$\Rightarrow f(x) = (x-1)(x-1)$$
$$= (x+2)(x+2)$$

* Whether a polynomial is reducible or not is dependent on which field it is defined.

* Q: How to check whether a polynomial is reducible / irreducible?

E.g. $x^4+x^3+x^2+x+1 \in F_2[x]$, Is it reducible?

E.g. $x^6+x^4+x^3+x^2+1 \in F_2[x]$, Is it reducible?

Solution #1: Try all smaller degree nonzero polynomials and see whether any of them is a factor. E.g. #1 has $2^4-1 = 15$ choices. E.g. #2 has $2^6-1=63$ choices.

Solution #2: Try all smaller degree <u>irreducible polynomials</u>. I.e. ~~keep~~ keep a list of smaller) degree irreducible polynomial.

Rabin's Test of irreducibility

Solution #3: $f(x) \in \mathbb{F}_q[x]$ has degree m.

$f(x)$ is <u>irreducible</u> if and only if

$$\gcd\left(f(x), x^{p^{\left(\frac{m}{m_i}\right)}} - x\right) = 1 \text{ for}$$

all prime factors m_i of m.

For example if $m = 6$ then

$m_1 = 2$, $m_2 = 3$

If $m = 4$, $m_1 = 2$.

One can see that method 3 is much faster

Theorem Very difficult to prove.

$\boxed{\text{Theorem}}$ difficult to prove.

For any $m \geq 1$, we can always find at least one irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ with degree m

---

* Construction of $GF(p^m)$ where $m \geq 2$.

* For any irreducible $g(x)$ of degree m, define

$$F = \{ f(x) \in GF(p)[x] : \exists\, c(x) \in GF(p)[x] \text{ such that } f(x) = c(x) \bmod g(x) \}$$

* Claim: F is a finite field under the operation

$a(x) + b(x) = a(x) \boxplus b(x) \mod g(x)$

$a(x) \circledast b(x) = a(x) \boxdot b(x) \mod g(x).$

proof: ① Finiteness? We have exactly p^m different elements in F

② "+" Associativity:

$(a(x)+b(x))+c(x)$

$= a(x)+(b(x)+c(x))$

$= a(x) \boxplus b(x) \boxplus c(x) \mod g(x)$

Identity 0. choose the zero-polynomial

Inverse: $a_0 + a_1 x^1 + \cdots + a_{m-1} x^{m-1}$

$\longrightarrow -a_0 - a_1 x^1 - \cdots - a_{m-1} x^{m-1}$

Commutativity.

4 • 4 $\boxed{\text{over } F\setminus\{0\}}$

We need

$a(x) \in F\setminus\{0\}$

$b(x) \in F\setminus\{0\}$

$a(x) \circ b(x) = a(x) \boxdot b(x) \mod g(x)$

$\neq 0.$

That's why we need $\boxed{\text{irreducibility}}$

E.g. $2 \bmod 6 = 2$ | $2 \bmod 5 = 2$

$3 \bmod 6 = 3$ | $3 \bmod 5 = 3$

$(2\cdot 3) \bmod 6 = 0$ | $2\cdot 3 \bmod 5 = 1$

Associativity

Identity, choose 1 ($\deg = 0$) as the identity.

Inverse: any $a(x) \in F_p[x]$

how to find $b(x) \in F_p[x]$

how to find $b(x) \in F_p[x]$

such that

$$a(x) \cdot b(x) = a(x) \boxdot b(x) \mod g(x)$$
$$= 1$$

Q: Is it always possible ?

Ans: Yes, always possible.

$1, a(x), (a(x))^2, (a(x))^3, \ldots$

because we modulo $g(x)$, eventually it will repeat

$$a(x)^{m_1} = a(x)^{m_2} \quad \text{where} \quad m_1 < m_2$$

$$a(x)^{m_1} \cdot a(x)^{m_2 - m_1}$$

$$= \left(a(x)^{\boxdot m_1} \mod g(x)\right) \cdot \left(a(x)^{\boxdot m_2 - m_1} \mod g(x)\right)$$

$$= a(x)^{\boxdot m_2} \mod g(x) = a(x)^{\boxdot m_1} \mod g(x)$$

$\Rightarrow \boxed{} = 1$

$\Rightarrow a(x)^{m_1} = 1$ for some m_1

$\Rightarrow \underline{a(x)^{m_1 - 1} = a^{-1}(x)}$ the inverse.

* The operators $+$ and $\cdot$ distribute.

---

* This modulo (irreducible) $g(x)$ of degree m field is called $GF(p^m)$

* It seems that different irreducible $g(x)$ will result in different $GF(p^m)$

Advanced theorem The resulting $GF(p^m)$ are all isomorphic to each other regardless how we choose the irregular $g(x)$ of deg. m.

* Since irreducible $g(x)$ of degree m always exists for all p, m.

$GF(p^m)$ always exists for all p, m.