Date: Mar 27 Made by Eric

Definitions and Theorems

Theorem 1. *Let p be prime, and let $f(x) = a_d x^d + \cdots + a_1 x + a_0$ be a polynomial with integer coeffiicients, where $a_i \not\equiv_p 0$ for some i*

The congruence $f(x) \equiv_p 0$ is satisfied by at most d congruence classes $[x] \in \mathbb{Z}_p$

Proof. ■

Theorem 2. ***(Fermat's Little Theorem)*** *Let p be a prime*

$$\forall a \in \mathbb{N}, a^{p-1} \equiv_p 1$$

Proof. We now prove the non-zero elements of $\mathbb{Z}_p$ constitute a group

Notice $\mathbb{Z}_p$ is a field, so $\forall a, b \neq 0 \in \mathbb{Z}_p, ab \neq 0$

$\forall a \in \mathbb{Z}_p, 1a = a$

Because p is a prime, so $\forall a \in \mathbb{Z}_p, gcd(a, p) = 1$

Then $\forall a \in \mathbb{Z}_p, \exists \alpha, \beta \in \mathbb{Z}, \alpha a + \beta p = 1$

Pick the α that satisfy $\alpha a + \beta p = 1$

We see $\alpha a \equiv_p 1$

Then α (you can choose to use the remainder of α divided by p, instead of α) is the inverse of a (done)

This group G is of order $p - 1$

So $\forall a \in G, a^{p-1} = e = 1$

■

Theorem 3. *Every finite multiplicative group of some field is cyclic*

Proof. Let G be a finite multiplicative group of some field $\mathbb{F}$

G is abelian, since it is a multiplicative subgroup of $\mathbb{F}$

So by Fundamental Theorem of Finitely Generated Abelian Group, we have $G = \mathbb{Z}_{p_1^{c_1}} \times \mathbb{Z}_{p_2^{c_2}} \times \cdots \times \mathbb{Z}_{p_s^{cs}}$

We prove by induction

$$\text{Base step: } |G| = p^n \implies G \text{ is cyclic}$$

Assume G is not cyclic

So $\forall a \in G, ord(a) < |G|$, and $ord(a)$ divides $|G| = p^n$

This give us $\forall a \in G, ord(a)|p^{n-1}$

Then every element of G satisfy the equation $a^{p^{n-1}} = e$, where e is the unity of the field $\mathbb{F}$.

This CaC, since the equation $a^{p^{n-1}}$ can have at most p^{n-1} roots

Induction step: $|G| = nr$, where $gcd(n,r) = 1$

We see $G = (\mathbb{Z}_{p_1^{c_1}} \times \cdots \times \mathbb{Z}_{p_u^{c_u}}) \times (\mathbb{Z}_{p_{u+1}^{c_{u+1}}} \times \cdots \times \mathbb{Z}_{p_s^{c_s}})$

The product of the generator of $\mathbb{Z}_{p_1^{c_1}} \times \cdots \times \mathbb{Z}_{p_u^{c_u}}$ and the generator of $\mathbb{Z}_{p_{u+1}^{c_{u+1}}} \times \cdots \times \mathbb{Z}_{p_s^{c_s}}$ is a generator of G

■

Exercises

Example 4.9

Solve $2x \equiv_{5^i} 3$, for each $i \in \mathbb{N}$

Proof. We first prove $2x \equiv_{5^i} 3 \implies 2x \equiv_{5^{i-1}} 3$

$5^i|2x - 3 \implies 5^{i-1}|2x - 3$

Solve $2x \equiv_5 3$, we have $x \equiv_5 4$ **(i=1) done**

Let $2y \equiv_{25} 3$, we know $2y \equiv_5 3$, so we know $y \equiv_5 4$

Write $y = 5k + 4$

$2y - 3 = 10k + 5$ and $2y \equiv_{25} 3 \implies 25|10k + 5 \implies k = 2, 7, 12, \cdots \implies k \equiv_5 2$

So $y \equiv_{25} 14$ **(i=2) done**

Let $2x \equiv_{125} 3$, we know $2x \equiv_{25} 3$

So we know $x \equiv_{25} 14$

Write $x = 25m + 14$

$2x - 3 = 50m + 25$ and $2x \equiv_{125} 3 \implies 125|50m + 25 \implies m = 2, 12, 22, \cdots \implies x \equiv_{125} 64$ **(i=3) done**

UNFINISHED ■

4.15

Find the solutions of $f(x) = x^3 + 4x^2 + 19x + 1 \equiv_{5^2} 0$

Proof. $f(x) \equiv_{25} 0$ only if $f(x) \equiv_5 0$

We first solve $f(x) \equiv_5 0$

$0 \equiv_5 x^3+4x^2+19x+1 \equiv_5 x^3-x^2-x+1 \equiv_5 (x-1)(x^2-1) \equiv_5 (x-1)^2(x+1)$

$\mathbb{Z}_5$ is a field, so either $x - 1 \equiv_5 0$ or $x + 1 \equiv_5 0$

Then $x \equiv_5 1$ or -1

case: $x \equiv_5 1$

We write $x = 5k + 1, \exists k \in \mathbb{Z}$

$0 \equiv_{25} f(x) = (5k + 1)^3 + 4(5k + 1)^2 + 19(5k + 1) + 1$

$\equiv_{25} (15k + 1) + 4(10k + 1) + 19(5k + 1) + 1$

$\equiv_{25} 170k + 25 \equiv_{25} 20k$

$20k \equiv_{25} 0 \iff 4k \equiv_5 0 \iff 5|k$

Because $x = 5k + 1$, so $x \equiv_{25} 1$

case: $x \equiv_5 -1$

We write $x = 5m - 1, \exists m \in \mathbb{Z}$

$0 \equiv_{25} f(x) = (5m - 1)^3 + 4(5m - 1)^2 + 19(5m - 1) + 1$

$\equiv_{25} (15m - 1) + 4(-10m + 1) + 19(5m - 1) + 1$

$\equiv_{25} 70m - 15 \equiv_{25} 20m - 15$

$20m \equiv_{25} 15 \iff 4m \equiv_5 3 \iff m \equiv_5 2$

Let $m = 5n + 2, \exists n \in \mathbb{Z}$

$x = 5m - 1 = 5(5n + 2) - 1 = 25n + 9 \equiv_{25} 9$

■

4.18

Let p and q be two primes, and $\Phi(x) = 1 + x + \cdots + x^{q-1}$ Show

$$\begin{gathered} p = q \implies \Phi(x) \equiv_p 0 \text{ have one congruence solution} \\ p \equiv_q 1 \implies \Phi(x) \equiv_p 0 \text{ have } q-1 \text{ congruence solutions} \\ p > q \text{ and } p \not\equiv_q 1 \implies \Phi(x) \equiv_p 0 \text{ have no solution} \end{gathered}$$

Proof. $\Phi(x) \equiv_p 0$ only if $(x-1)\Phi(x) \equiv_p 0$

Notice $(x-1)\Phi(x) = x^q - 1$

So $\Phi(x) \equiv_p 0$ only if $x^q - 1 \equiv_p 0$

In each case, we first solve $x^q \equiv_p 1$, then we

Case: $p = q$

Because $x^{p-1} \equiv_p 1$, by Fermat's little Theorem

$x^p \equiv_p 1 \implies x \equiv_p 1$

Then $\Phi(x) = 1 + x + \cdots + x^{q-1} \equiv_p q = p \equiv_p 0$

So the only solution is $x \equiv_p 1$

Case $p \equiv_q 1$

Let G be the multiplicative subgroup of $\mathbb{Z}_p$

Clearly, $|G| = p - 1$

$x^q \equiv_p 1 \iff ord(x) = q$

By Theorem 2, we know $G \simeq \mathbb{Z}_{p-1}$

$p \equiv_q 1 \implies q|p-1$

We see in $\mathbb{Z}_{p-1}$, there are elements $x = 0, \frac{p-1}{q}, \frac{2(p-1)}{q}, \ldots, \frac{(q-1)(p-1)}{q}$ satisfy $ord(x) = q$

So there are q elements satisfy $ord(x) = q$, that is $x^q \equiv_p 1$

Yet we notice if $x = 0$ in $\mathbb{Z}_{p-1} \simeq G$, $x = 1 \in \mathbb{N}$

Yet $x = 1$ is clearly not a solution of $\Phi(x) \equiv_p 0$, by direct computation, but a byproduct of multiplying $x - 1$ with $\Phi(x)$

So there are $q - 1$ elements, eg, congruence classes satisfy $\Phi(x) \equiv_p 0$

Case: $p > q$ and $p \not\equiv_q 1$

Let G be the multiplicative subgroup of $\mathbb{Z}_p$

Clearly, $|G| = p - 1$

$x^q \equiv_p 1 \iff ord(x) = q$

Yet $p \not\equiv_q 1$ give us $q \not| p - 1 = |G|$, so no element x is of the order q $\blacksquare$