Date: Mar 27 Made by Eric

In this note, n is always a natural number, and $\mathbb{Z}_n$ is always a ring, containing congruence classes of $\equiv_n$, or the cosets of $\mathbb{Z}/n\mathbb{Z}$ if you wish

In this note, p_i is always a prime for each $i \in \mathbb{Z}$

Definitions

Definition 1. *Let $a \in \mathbb{Z}$*

a is a ***primitive root*** *of U_n if U_n is cyclic and $[a]$ is a generator of U_n*

Theorems

Theorem 1. *Let p be a prime*

U_p is cyclic

Proof. Notice $\mathbb{Z}_p$ is a field, so U_p is cyclic follows the following stronger result

We now prove every finite multiplicative subgroup of a field is cyclic

Let G be a multiplicative subgroup of a field $\mathbb{F}$

Because the multiplication of $\mathbb{F}$ is commutative, so G is abelian

By the fundamental theorem of finitely generated abelian group, we write $G \simeq H_1 \times \cdots \times H_k$, where $\forall i : 1 \leq i \leq k, \exists c_i \in \mathbb{N}, |H_i| = p_i^{c_i}$,

We now prove $\forall i : 1 \leq i \leq k, H_i \simeq \mathbb{Z}_{p_i^{c_i}}$

Assume $H_i \not\simeq \mathbb{Z}_{p_i^{c_i}}$

Say, $H_i \simeq \mathbb{Z}_{p_i^{d_1}} \times \cdots \times \mathbb{Z}_{p_i^{d_j}}$, where $\sum_{n=1}^{j} d_n = c_i$

Consider the polynomial $x^{(p_i^{c_i-1})} - 1 \in \mathbb{F}[x]$

Because that $\forall 1 \leq n \leq j, d_n < c_i$, so we know $\forall 1 \leq n \leq j, p_i^{d_n} | p_i^{c_i-1}$

Then we see every element in G that can be precisely represented by $(0, \ldots, r, \ldots, 0)$, where r is in the i-th slot, is a root of $x^{(p_i^{c_i-1})} - 1$

So there are $|H_i| = p_i^{c_i} > p_i^{c_i-1} = deg(x^{(p_i^{c_i-1})} - 1)$ number amount of roots CaC (done)

$G \simeq \mathbb{Z}_{p_1^{c_1}} \times \cdots \times \mathbb{Z}_{p_k^{d_k}} \simeq \mathbb{Z}_{p_1^{c_1} \cdots p_k^{c_k}}$ (done)

■

Lemma 2. *Let g be a primitive root of U_p*

Either g is a primitive root of U_{p^2}, or g have the order $p-1$ in U_{p^2}

Proof. Let d be the order of g in U_{p^2}

$g^d \equiv_{p^2} 1 \implies g^d \equiv_p 1 \implies |U_p|$ divides $d \implies p-1|d$

By Theorem of Lagrange, d divides $|U_{p^2}| = \varphi(p^2) = (p-1)p$

$p-1|d$ and $d|(p-1)p \implies d = p-1$ or $d = (p-1)p$

Notice that if $d = (p-1)p$, then g is a primitive root of U_{p^2}

■

Theorem 3. *Let p be a prime bigger than 2 and let $e > 1$*

U_{p^e} is cyclic

Proof. Let g be a primitive root of U_p

We prove by induction on e

Base step: between g and $g+p$, at least one of them is a primitive root of U_{p^2}

Assume both g and $g+p$ are not primitive root of U_{p^2}

Notice $g+p \equiv_p g$, so we know $g+p$ is also a primitive root of U_p

Then by Lemma 2, $g+p$ have the order $p-1$ in U_{p^2}

Expand $(g+p)^{p-1}$ in U_p^2, then we will have the following, where the dots can be divided by p^2

$(g+p)^{p-1} \equiv_{p^2} g^{p-1} + g^{p-2}p(p-1) + \cdots \equiv_{p^2} 1 + g^{p-2}p(p-1)$

Notice $g \in U_p$ and $p-1 \in U_p$

So $g^{p-2}(p-1) \not\equiv_p 0$

Then $g^{p-2}p(p-1) \not\equiv_{p^2} 0$

So $(g+p)^{p-1} \equiv_{p^2} 1 + g^{p-2}p(p-1) \not\equiv_{p^2} 1$ CaC to $g+p$ have the order $p-1$ in U_{p^2}

Induction step: h is a primitive root of $U_{p^c} \implies h$ is a primitive root of $U_{p^{c+1}}$

Let d be the order of h in $U_{p^{c+1}}$

By Theorem of Lagrange, we know d divides $|U_{p^{c+1}}| = p^c(p-1)$

Then we know $h^d \equiv_{p^{c+1}} 1 \implies h^d \equiv_{p^c} 1 \implies |U_{p^c}|$ divides $d \implies p^{c-1}(p-1)|d$

So either $d = p^c(p-1)$ or $d = p^{c-1}(p-1)$

Notice if $d = p^c(p-1)$, then h is a primitive root of $U_{p^{c+1}}$

Assume $d = p^{c-1}(p-1)$

Notice $p^{c-2}(p-1) = |U_{p^{c-1}}|$

So $h^{p^{c-2}(p-1)} \equiv_{p^{c-1}} 1$

Then we know $h^{p^{c-2}(p-1)} = 1 + kp^{c-1}, \exists k \in \mathbb{Z}$

Be aware that p do not divides k, otherwise $h^{p^{c-2}(p-1)} \equiv_{p^c} 1$ CaC to that h is a primitive root of U_{p^c}

Because $c > 2$, so we can deduce $\forall n > 3, p^{c+1}|(p^{c-1})^n$, which help us deduce the following

$h^d = h^{p^{c-1}(p-1)} = (h^{p^{c-2}(p-1)})^p = (1+kp^{c-1})^p \equiv_{p^{c+1}} 1+\binom{p}{1}kp^{c-1}+\binom{p}{2}k^2p^{2c-2}+\cdots \equiv_{p^{c+1}} 1 + kp^c + (p-1)k^2p^{2c-1}$

Because $c > 2$, so $p^{c+1}|p^{2c-1}$, which give us $h^d \equiv_{p^{c+1}} 1 + kp^c$

Because p do not divides k, so $h^d \equiv_{p^{c+1}} 1 + kp^c \not\equiv_{p^{c+1}}$ CaC

$\blacksquare$

Theorem 4. *Let $e \in \mathbb{N}$*

$$U_{2^e} \text{ is cyclic if and only if } e = 1 \text{ or } e = 2$$

Proof. It is computationally verifiable that U_{2^e} is cyclic when $e = 1$ or $e = 2$

Let $e > 2$

We now prove $\forall a \in U_{2^e}, a^{2^{e-2}} \equiv_{2^e} 1$ by induction, so that no element in U_{2^e} have the order $|U_{2^e}| = 2^{e-1}$

$$\text{Base step: } \forall a \in U_8, a^2 \equiv_8 1$$

This is also computationally verifiable

Induction step: $c > 2$ and $\forall a \in U_{2^c}, a^{2^{c-2}} \equiv_{2^c} 1 \implies \forall a \in U_{2^{c+1}}, a^{2^{c-1}} \equiv_{2^{c+1}} 1$

Let $a \in U_{2^{c+1}}$

Notice $U_{2^c} = U_{2^{c+1}}$, so $a \in U_{2^c}$

Then by $a^{2^{c-2}} \equiv_{2^c} 1$, we can write $a^{2^{c-2}} = 1 + k2^c, \exists k \in \mathbb{Z}$

Fix k and we see

$a^{2^{c-1}} = (a^{2^{c-2}})^2 = (1+k2^c)^2 = 1 + k2^{c+1} + k^2 2^{2c} \equiv_{2^{c+1}} 1$ (done) ∎

Theorem 5. *Let $n = rs$ where r and s are coprime and greater than 2*

$$U_n \textit{ is not cyclic}$$

Proof. Let p be any odd prime

Notice that $\varphi(p^e) = p^{e-1}(p-1)$ is even

This show us that any number x greater than 2 satisfy that $2|\varphi(x)$

So $2|\varphi(n)$ and $2|\varphi(r)$ and $2|\varphi(s)$

Let $i = \frac{\varphi(n)}{2} = \frac{\varphi(r)\varphi(s)}{2} = \frac{\varphi(r)}{2}\varphi(s) = \varphi(r)\frac{\varphi(s)}{2}$

We now prove $\forall a \in U_n, a^i \equiv_n 1$, then no element of U_n is a primitive root

Let $a \in U_n$

$gcd(a,n) = 1 \implies gcd(a,r) = 1$ and $gcd(a,s) = 1 \implies a \in U_r$ and $a \in U_s$

$a^i \equiv_s a^{\frac{\varphi(r)}{2}\varphi(s)} \equiv_s (a^{\varphi(s)})^{\frac{\varphi(r)}{2}} \equiv_s 1^{\frac{\varphi(r)}{2}} \equiv_s 1$

$a^i \equiv_r a^{\frac{\varphi(s)}{2}\varphi(r)} \equiv_r (a^{\varphi(r)})^{\frac{\varphi(s)}{2}} \equiv_r 1^{\frac{\varphi(s)}{2}} \equiv_r 1$

$s|a^i - 1$ and $r|a^i - 1$

Then $gcd(r,s) = 1$ give us $rs = n|a^i - 1$

So $a^i \equiv_n 1$ (done)

∎

Theorem 6. ***(The Result of This Research)*** *Let $e \in \mathbb{N}$*

U_n is cyclic if and only if $n = 2$ or 4 or p^e or $2p^e$, for some odd prime p

Proof. $(\longleftarrow)$

U_n is cyclic when $n = 2$ or 4 or p^e have already been proven by Theorem 3 and 4

We only have to prove U_{2p^e} is cyclic

Let g be a primitive root of U_{p^e}

Because p^e is odd, so only one of g and $g + p^e$ is odd

Let h be the odd g or the odd $g + p^e$

Be aware that h is a primitive root of U_{p^e}

We now prove h is a primitive root of U_{2p^e}

Notice that h is odd and $h \equiv_{p^e} 1 \implies gcd(h, p^e) = 1$ give us $gcd(h, 2p^e) = 1$, so $h \in U_{2p^e}$

Let i be the order of h in U_{2p^e}

Notice $|U_{2p^e}| = \varphi(2p^e) = p^{e-1}(p-1) = \varphi(p^e)$, so $i|\varphi(p^e)$

$h^i \equiv_{2p^e} 1 \implies h^i \equiv_{p^e} 1$

Because h is a primitive root of U_{p^e}, so we know $p^{e-1}(p-1) = \varphi(p^e)|i$

Then $i = \varphi(p^e) = \varphi(2p^e)$ (done)

$(\longrightarrow)$

Case: 2 appears over twice in the prime factorization of n

Assume 2 appears over twice in the prime factorization of n

Either n is a power of 2, or n contain other primes which are greater than 2

If the former is the case, then by Theorem 4, there is a contradiction. If the latter is the case, then we can easily use Theorem 5 to cause a contradiction CaC

Case: 2 appears only once in the prime factorization of n

Assume there are two distinct non-two primes $p_1^{c_1}, p_2^{c_2}$ appear in the prime factorization

By Theorem 5, $gcd(p_1^{c_1}, \frac{n}{p_1^{c_1}}) = 1$ and $p_1^{c_1} > 2$ and $\frac{n}{p_1^{c_1}} \geq 2p_2^{c_2} > 2$ CaC

Case: 2 does not appear in the prime factorization of n

Assume there are two distinct non-two primes $p_1^{c_1}, p_2^{c_2}$ appear in the prime factorization

By Theorem 5, $gcd(p_1^{c_1}, \frac{n}{p_1^{c_1}}) = 1$ and $p_1^{c_1} > 2$ and $\frac{n}{p_1^{c_1}} \geq p_2^{c_2} > 2$ CaC

∎

Summary

1. If p is an odd prime and g is a primitive root $(\textbf{mod } p)$, then either g or $g+p$ is a primitive root $(\textbf{mod } p^e)$ for all $e \in \mathbb{N}$

2. If p is an odd prime and g is a primitive root $(\textbf{ mod } p^e)$, then the odd one between g or $g+p^e$ is a primitive root $(\textbf{ mod } 2p^e)$

3. If $e \geq 3$ then $U_{2^e} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$, where $(1,0) \mapsto -1$ and $(0,1) \mapsto 3$

4. $n = p_1^{c_1} \cdots p_k^{c_k} \implies U_n \simeq U_{p_1^{c_1}} \times \cdots \times U_{p_k^{c_k}}$

Exercises

6.12

Let $e \geq 3$

Show that in U_{2^e}, the elements of order 2 are $2^{e-1} \pm 1$ and -1

Proof. It is computationally verifiable that $2^{e-1} \pm 1$ and -1 are of order 2

Let $a \in U_{2^e}$ be an element of order 2^e

$a^2 \equiv_{2^e} 1 \implies 2^e | (a-1)(a+1)$ **(i)**

Because $a \in U_{2^e}$, we know a is odd, then we know both $a-1$ and $a+1$ are even, then by **(i)** , we know $2^{e-1} | a-1$ and $2^{e-1} | a+1$

Also, there is the possibility that $a = \pm 1$, which satisfy $a^2 \equiv_{2^e} 1$. We only have to notice that 1 have order 1

∎

6.14

Find an integer which is a primitive root mod $(2 * 3^e)$ for all $e \geq 1$

Find an integer which is a primitive root mod $(2 * 7^e)$ for all $e \geq 1$

Proof. 5 is a primitive root mod $(2 * 3^e)$

3 is a primitive root mod $(2 * 7^e)$

∎

6.15

Solve the congruence $x^6 \equiv_{23} 4$

Proof. 2 is a primitive root of U_{23}, and $|U_{23}| = 22$

$4 \equiv_{23} 2^2$

Write $[x] = [2^a]$

$x^6 \equiv_{23} 4 \implies 2^{6a} \equiv_{23} 2^2 \implies 22|6a-2 \implies a = 11m+4 \implies [x] = [2^4]$ or $[x] = [2^15] \implies [x] = [16]$ or $[x] = [7]$

■

6.16

Solve the congruence $x^4 \equiv_{99} 4$

Proof. $x^4 \equiv_{99} 4 \iff x^4 \equiv_{11} 4$ and $x^4 \equiv_9 4$

2 is a primitive root of U_{11} and $4 \equiv_{11} 2^2$

Write $x = 2^a$

$2^{4a} \equiv_{11} 2^2 \implies \varphi(11) = 10|4a-2 \implies a = 5m+3, \exists m \in \mathbb{Z} \implies x = 11n+8$ or $x = 11n+3, \exists n \in \mathbb{Z}$

Write $x = 2^b$

2 is a primitive root of U_9 and $4 \equiv_9 2^2$

$2^{4b} \equiv_9 2^2 \implies \varphi(9) = 6|4b-2 \implies b = 3m+2, \exists m \in \mathbb{Z} \implies x = 9n+4$ or $x = 9n+5, \exists n \in \mathbb{Z}$

Then by Chinese Remainder Theorem, we have $[x] = [(-4)*9+2*11]$ or $[(-4)*9+7*11]$ or $[4*9+2*11]$ or $[4*9+7*11]$ ■

6.17

Solve the congruence $x^{11} \equiv_{32} 7$

Proof. Notice $U_{32} = \{\pm 5^i | 0 \leq i < 8\}$

And notice $7 \equiv_{32} -5^2$

Write $x = \pm 5^i$

$\pm 5^{11i} \equiv_{32} -5^2 \implies \pm 5^{11i} \equiv_4 -25 \equiv_4 -1$

Because $5^{11i} \equiv_4 1$, so $x = -5^i$

$-5^{11i} \equiv_{32} -5^2 \implies 5^{11i} \equiv_{32} 5^2$

By direct computation, we see that in U_{32}, $ord(5) = 8$

Then $8|11i - 2$

Then $i = 8n + 6, \exists n \in \mathbb{Z}$

Then $x \equiv_{32} -5^i \equiv_{32} -5^6 \equiv_{32} -9$ ■

6.22

(i) Show that if p is prime, then $(p-2)! \equiv_p 1$

(ii) Show that if p is an odd prime, then $(p-3)! \equiv_p \frac{p-1}{2}$

Proof. **(i)**

We show that in U_p, 1 and $p-1$ are the only two element that is the inverse of itself, so in the set $\{2, \ldots, p-2\}$, we can find pairs of two distinct element being inverse of each other, then we see $(p-2)! \equiv_p 1$

Notice $\mathbb{Z}_p$ is a field

Let $g(x) \in \mathbb{Z}_p[x]$ be defined by $g(x) = x^2 - 1$

Let $a \in U_p$

If the inverse of a is a itself, then $g(a) = 0$

Notice $deg(g) = 2$ and $g(1) = 0$ and $g(p-1) = 0$

So no other element $a \neq 1 \neq p-1$ satisfy $g(a) = 0$

(ii)

Notice $\mathbb{Z}_p$ is a field, so division is doable in $\mathbb{Z}_p$

$[(p-3)!] = [(p-2)!][p-2]^{-1} = [-2]^{-1}$

Notice $[\frac{p-1}{2}][-2] = [1]$

So $[(p-3)!] = [-2]^{-1} = [\frac{p-1}{2}]$

Then $(p-3)! \equiv_p \frac{p-1}{2}$

■

6.25

Find all the primitive roots for U_{18} **(i)** and U_{27} **(ii)**

Proof. **(i)**

Notice $18 = 2 * 3^2$

So we first find the primitive root of U_9, by first finding the primitive root for U_3

2 is a primitive for U_3

$|U_9| = 6$ and $2^2 \equiv_{18} 4$ and $2^3 \equiv_{18} -1 \implies 2$ is a primitive root of U_9

Then $11 = 2 + 9$ is a primitive root of U_{18}

Because $U_{18} \simeq \mathbb{Z}_6$, so we know 11^5 is another primitive root for U_{18}, which is 5

(ii)

Notice $27 = 3^3$

Because 2 is a primitive root of U_9, we know 2 is a primitive root of U_{27}

Notice $U_{27} \simeq \mathbb{Z}_{18}$

Then we know $2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$ are also primitive root of U_{27}

They are respectively $5, 20, 23, 11, 14$

■