32. $x^2 \equiv a \bmod p$

20191583 김태균

10/10

$Z_{13}^*$ $1^2 \to a=1$ $2^2 \to a=4$ $3^2 \to a=9$ $4^2 \to a=3$ $5^2 \to a=12$ $6^2 \to a=10$

$\frac{p-1}{2}=6$ The number of QR is 6

QR: 1, 3, 4, 9, 10, 12

QNR: 2, 5, 6, 7, 8, 11

$Z_{17}^*$ $\frac{17-1}{2}=8$ The number of QR is 8

$1^2 \to a=1$ $2^2 \to a=4$ $3^2 \to a=9$ $4^2 \to a=16$ $5^2 \to a=8$ $6^2 \to a=2$ $7^2 \to a=15$ $8^2 \to a=13$

QR: 1, 2, 4, 8, 9, 13, 15, 16

QNR: 3, 5, 6, 7, 10, 11, 12, 14

$Z_{23}^*$ $\frac{23-1}{2}=11$ The number of QR is 11

$1^2 \to a=1$ $2^2 \to a=4$ $3^2 \to a=9$ $4^2 \to a=16$ $5^2 \to a=2$ $6^2 \to a=13$ $7^2 \to a=3$ $8^2 \to a=18$

$9^2 \to a=12$ $10^2 \to a=8$ $11^2 \to a=6$

QR: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18

QNR: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22

33 a. $x^2 \equiv 4 \bmod 7$

Euler's criterion $4^{(7-1)/2} \equiv 1 \bmod 7$ so 4 is QR

$p=4k+3$ $k=1$ $7=4+3$

$x \equiv 4^{(7+1)/4} \bmod 7$, $x \equiv -4^{(7+1)/4} \bmod 7$ $x=\pm 2$

$\equiv 4^2 \bmod 7$ $\equiv -4^2 \bmod 7$

$=2$ $=-2$

b. $x^2 \equiv 5 \bmod 11$

Euler's criterion $5^{(11-1)/2} \equiv 1 \bmod 11$ So 5 is QR

$p=4k+3$ $k=2$ $11=8+3$

$x \equiv 5^{(11+1)/4} \bmod 11$, $x \equiv -5^{(11+1)/4} \bmod 11$ $x=\pm 4$

$\equiv 5^3 \bmod 11$ $\equiv -5^3 \bmod 11$

$=4$ $=-4$

c. $x^2 \equiv 7 \bmod 13$

7 is QNR (solved it #32), so there is no answer to this question

d. $x^2 \equiv 12 \bmod 17$

12 is QNR (solved it #32). so there is no answer to this question

34. a. $x^2 \equiv 4 \bmod 14$ $\quad 14 = 2 \times 7$

$x^2 \equiv 4 \bmod 2 \equiv 0 \bmod 2$ $\quad x^2 \equiv 4 \bmod 7$ $\quad$ 4 is QR

$x \equiv \pm 0 \bmod 2$ $\quad x \equiv \pm 4^{(P+1)/4} \bmod 7 = \pm 2 \bmod 7$

we can make 4 simultaneous equation

$x = +0 \bmod 2 \quad x = +2 \bmod 7 \rightarrow x = 2$

$x = +0 \bmod 2 \quad x = -2 \bmod 7 \rightarrow x = 12$ $\quad$ So $x = 2$ and $x = 12$

$x = -0 \bmod 2 \quad x = +2 \bmod 7 \rightarrow x = 2$

$x = -0 \bmod 2 \quad x = -2 \bmod 7 \rightarrow x = 12$

b. $x^2 = 5 \bmod 10$ $\quad 10 = 2 \times 5$

$x^2 \equiv 5 \bmod 2$ $\quad x^2 \equiv 5 \bmod 5 \equiv 0 \bmod 5$

$x \equiv \pm 1 \bmod 2$ $\quad x \equiv \pm 0 \bmod 5$

we can make 4 simultaneous equation

$x = +1 \bmod 2 \quad x = +0 \bmod 5 \rightarrow x = 5$

$x = +1 \bmod 2 \quad x = -0 \bmod 5 \rightarrow x = 5$ $\quad$ So $x = 5$

$x = -1 \bmod 2 \quad x = +0 \bmod 5 \rightarrow x = 5$

$x = -1 \bmod 2 \quad x = -0 \bmod 5 \rightarrow x = 5$

c. $x^2 \equiv 7 \bmod 33$ $\quad 33 = 3 \times 11$

$x^2 \equiv 7 \bmod 3 = 1 \bmod 3$ $\quad x^2 \equiv 7 \bmod 11$ $\quad 7^{(11-1)/2} \equiv -1 \bmod 11$ so 7 is QNR

$x \equiv \pm 1 \bmod 3$ $\quad \Rightarrow$ no solution $\quad$ QR: 1, 3, 4, 5, 9

$x^2 \equiv 7 \bmod 11$ has no solution. so $x^2 = 7 \bmod 33$ has no solution

d. $x^2 \equiv 12 \bmod 34$ $\quad 34 = 2 \times 17$

$x^2 \equiv 12 \bmod 2 \equiv 0 \bmod 2$ $\quad x^2 \equiv 12 \bmod 17$ $\quad 12^{(17-1)/2} \equiv -1 \bmod 17$ So 12 is QNR

$x^2 \equiv \pm 0 \bmod 2$ $\quad \Rightarrow$ no solution $\quad$ QR: 1, 2, 4, 8, 9, 13, 15, 16

$x^2 \equiv 12 \bmod 17$ has no solution. so $x^2 \equiv 12 \bmod 34$ has no solution

36. $G = \langle Z_{19}^*, \times \rangle$

a. $\phi(19) = 18$

b. $ord(1): \{1\} = 1$,

when a and n are positive integers that are relatively prime, $a^{\phi(n)} \equiv 1 \bmod n$

So Compute Euler's totient function $\phi(19) = 18$. Factorize 18 to find its division 1, 2, 3, 6, 9, 18.

For each division, check the smallest $k$ such that $a^k \equiv 1 \bmod 19$

$2^{18} \equiv 1 \bmod 19$ $\quad ord(2) = 18$, $\quad 3^{18} \equiv 1 \bmod 19$ $\quad ord(3) = 18$, $\quad 4^9 \equiv 1 \bmod 19$ $\quad ord(4) = 9$, $\quad 5^9 \equiv 1 \bmod 19$ $\quad ord(5) = 9$

$6^9 \equiv 1 \bmod 19$ $\quad ord(6) = 9$, $\quad 7^3 \equiv 1 \bmod 19$ $\quad ord(7) = 3$, $\quad 8^6 \equiv 1 \bmod 19$ $\quad ord(8) = 6$, $\quad 9^9 \equiv 1 \bmod 19$ $\quad ord(9) = 9$

$10^{18} \equiv 1 \bmod 19$ $\quad ord(10) = 18$ $\quad 11^3 \equiv 1 \bmod 19$ $\quad ord(11) = 3$ $\quad 12^6 \equiv 1 \bmod 19$ $\quad ord(12) = 6$ $\quad 13^{18} \equiv 1 \bmod 19$ $\quad ord(13) = 18$

$14^{18} \equiv 1 \bmod 19$ $\quad ord(14) = 18$ $\quad 15^{18} \equiv 1 \bmod 19$ $\quad ord(15) = 18$ $\quad 16^9 \equiv 1 \bmod 19$ $\quad ord(16) = 9$ $\quad 17^9 \equiv 1 \bmod 19$ $\quad ord(17) = 9$

$18^2 \equiv 1 \bmod 19$ $\quad ord(18) = 2$

36. C. A primitive root is an element in a given modular group $Z_{n}^{*}$, that can generate all the elements of the group.

So num of primitive root is $\phi(\phi(19)) = \phi(18) = \phi(2\times 3^2) = 1\times(3^2-3^1) = 6$

d. when $ord(a)=18$, a is primitive group. We find ord at #36-b

2, 3, 10, 13, 14, 15 are primitive roots in the group

e. Since 19 is a prime, $Z_{19}^{*}$ forms a cyclic group. A cyclic group is a group where all elements can be generated by a single element, known as a primitive root.

A primitive root g is an element that can generate all elements of the group

If $g=2$ is a primitive root, it means that $2^k$ mod 19 can generate all elements of $Z_{19}^{*}$.

$2^1:2$, $2^2:4$ $2^3:8$ $2^4:16$ $2^5:13$ $2^6:7$ $2^7:14$ $2^8:9$ $2^9:18$ $2^{10}:17$

$2^{11}:15$ $2^{12}:11$ $2^{13}:3$ $2^{14}:6$ $2^{15}:12$ $2^{16}:5$ $2^{17}:10$ $2^{18}:1$

f. when we express $L_g(x)$, $L_g(x)$ represents how many times the base g must be exponentiated to become x. In orther words, it denotes the smallest exponent k such that $g^k \equiv x$ mod 19.

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $L_2(x)$ | 18 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |
| $L_3(x)$ | 18 | 7 | 1 | 14 | 4 | 8 | 6 | 3 | 2 | 11 | 12 | 15 | 17 | 13 | 5 | 10 | 16 | 9 |
| $L_{10}(x)$ | 18 | 17 | 5 | 16 | 2 | 4 | 12 | 15 | 10 | 1 | 6 | 3 | 13 | 11 | 7 | 14 | 8 | 9 |
| $L_{13}(x)$ | 18 | 11 | 17 | 4 | 14 | 10 | 12 | 15 | 16 | 7 | 6 | 3 | 1 | 5 | 13 | 8 | 2 | 9 |
| $L_{14}(x)$ | 18 | 13 | 7 | 8 | 10 | 2 | 6 | 3 | 14 | 5 | 12 | 15 | 11 | 1 | 17 | 16 | 4 | 9 |
| $L_{15}(x)$ | 18 | 5 | 11 | 10 | 8 | 16 | 12 | 15 | 4 | 13 | 6 | 3 | 7 | 17 | 1 | 2 | 14 | 9 |

37. a. $x^5 \equiv 11 \mod 17$

① Choose a primitive root. when $G=\langle Z_{17}^{*}, x\rangle$, 3, 5, 6, 7, 10, 11, 12, 14 are primitive root.

we can choose any primitive root, so I choose 3.

② Create a discrete Logarithm table for $g=3$

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $L_3(x)$ | 16 | 14 | 1 | 12 | 5 | 15 | 11 | 10 | 2 | 3 | 7 | 13 | 4 | 9 | 6 | 8 |

③ Apply the discrete Logarithm Function. $\phi(17)=16$, $L_3(11)=7$

$L_3(x^5) \equiv L_3(11) \mod 16 \quad \rightarrow 5\times L_3(x) \equiv 7 \mod 16$

④ Solve the transformed congruence equation

Because of $\gcd(5,16)=1$, this equation has a unique solution

$L_3(x) = 5^{-1}\times 7 \mod 16 = 13\times 7 \mod 16 = 11 \mod 16$

When $L_3(x)=11$, $x=7$

37. b. $2x^{11} \equiv 22 \mod 19 \rightarrow 2x^{11} \equiv 3 \mod 19$

① choose a primitive root when $G = \langle \mathbb{Z}_n^*, \times \rangle$, 2, 3, 10, 13, 14, 15 are primitive root

we can chose any primitive root, so I choose 2.

② Create a discrete Logarithm table for $g=2$

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $L_2(x)$ | 18 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |

③ Apply the discrete Logarithm Function $\phi(n)=18$. $L_2(2)=1$, $L_2(3)=13$

$L_2(2x^{11}) \equiv L_2(3) \mod 18 \rightarrow L_2(2) + 11 \times L_2(x) \equiv L_2(3) \mod 18$

$\rightarrow 1 + 11 \times L_2(x) \equiv 13 \mod 18 \rightarrow 11 \times L_2(x) \equiv 12 \mod 18$

④ Solve the transformed congruence equation

Because of $\gcd(11, 18) = 1$. this equation has a unique solution

$L_2(x) \equiv 11^{-1} \times 12 \mod 18 \equiv 5 \times 12 \mod 18 = 6 \mod 18$

When $L_2(x) = 6$ $\quad x = 7$

c. The discrete logarithm is typically used to solve equations of the form $g^k \equiv x \mod n$,

The equation $5x^{12} + 6x \equiv 8 \mod 23$ involves multiple terms with different exponents of $x$

The discrete logarithm method does not direct apply to such composite equations with multiple terms and exponents

So $5x^{12} + 6x \equiv 8 \mod 23$ is difficult to solve using the discrete logarithm method.

Scanned with CamScanner