암호학기초 HW#4 20191629 이주헌

Chapter 9

32. Find all QRs and QNRs in $\mathbb{Z}_{13}^*$, $\mathbb{Z}_{17}^*$, and $\mathbb{Z}_{23}^*$.

For $\mathbb{Z}_p^*$, if $a^{(p-1)/2} \equiv 1 \pmod p$ then a is a QR,
if $a^{(p-1)/2} \equiv -1 \pmod p$ then a is a QNR.

i) For $\mathbb{Z}_{13}^*$, QR = { 1, 3, 4, 9, 10, 12 } ; QNR = { 2, 5, 6, 7, 8, 11 }.

ii) For $\mathbb{Z}_{17}^*$, QR = { 1, 2, 4, 8, 9, 13, 15, 16 } ; QNR = { 3, 5, 6, 7, 10, 11, 12, 14 }.

iii) For $\mathbb{Z}_{23}^*$, 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. Using quadratic residues, solve the following congruences.

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

$4 \in QR(\mathbb{Z}_7^*)$, $7 = 4\times1+3 \Rightarrow$ special case.
$x = 4^{(7+1)/4} \bmod 7$ or $-4^{(7+1)/4} \bmod 7 = \boxed{2, \text{ or } -2}$.

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

$5 \in QR(\mathbb{Z}_{11}^*)$, $11 = 4\times2+3 \Rightarrow$ special case.
$x = 5^{(11+1)/4} \bmod 11$ or $-5^{(11+1)/4} \bmod 11 = \boxed{4 \text{ or } -4}$

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

$7 \notin QR(\mathbb{Z}_{13}^*)$. $\Rightarrow$ No solution.

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

$12 \notin QR(\mathbb{Z}_{17}^*)$ $\Rightarrow$ No solution.

34. Using quadratic residues, solve the following congruences.

a. $x^2 \equiv 4 \bmod 14$.

$14 = 2\times7 \Rightarrow p_1 = 2,\ p_2 = 7$.
$x^2 \equiv 4 \bmod 2$, $x^2 \equiv 4 \bmod 7$.

$$\left.\begin{array}{ll} \text{i) } x \equiv +0 \bmod 2, & x \equiv +2 \bmod 7 \\ \text{ii) } x \equiv +0 \bmod 2, & x \equiv -2 \bmod 7 \\ \text{iii) } x \equiv -0 \bmod 2, & x \equiv +2 \bmod 7 \\ \text{iv) } x \equiv -0 \bmod 2, & x \equiv -2 \bmod 7 \end{array}\right\} x = 2 \text{ or } 12$$

b. $x^2 \equiv 5 \bmod 10$.

$10 = 2\times5 \Rightarrow p_1 = 2,\ p_2 = 5$.
$x^2 \equiv 5 \bmod 2$, $x^2 \equiv 5 \bmod 5$

$$\left.\begin{array}{ll} \text{i) } x \equiv +1 \bmod 2, & x \equiv +0 \bmod 5 \\ \text{ii) } x \equiv +1 \bmod 2, & x \equiv -0 \bmod 5 \\ \text{iii) } x \equiv -1 \bmod 2, & x \equiv +0 \bmod 5 \\ \text{iv) } x \equiv -1 \bmod 2, & x \equiv -0 \bmod 5 \end{array}\right\} x = 5.$$

c. $x^2 \equiv 7 \bmod 33$

$33 = 3 \times 11. \Rightarrow p_1 = 3,\ p_2 = 11.$

$x^2 \equiv 7 \bmod 3,\ \underbrace{x^2 \equiv 7 \bmod 11.}_{\text{no solution.}}$

No solution.

d. $x^2 \equiv 12 \bmod 34$

$34 = 2 \times 17 \Rightarrow p_1 = 2,\ p_2 = 17.$

$x^2 \equiv 12 \bmod 2,\ \underbrace{x^2 \equiv 12 \bmod 17.}_{\text{no solution.}}$

No solution.

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

a. The order of the group is $\phi(19) = 18$.

b. ord(1) = 1, ord(2) = 18, ord(3) = 18, ord(4) = 9, ord(5) = 9, ord(6) = 9,
ord(7) = 3, ord(8) = 6, ord(9) = 9, ord(10) = 18, ord(11) = 3, ord(12) = 6,
ord(13) = 18, ord(14) = 18, ord(15) = 18, ord(16) = 9, ord(17) = 9, ord(18) = 2.

c. The number of primitive roots is $\phi(\phi(19)) = \phi(18) = 6$.

d. The primitive roots are 2, 3, 10, 13, 14, 15.

e. Trying $g = 2$ as the generator seed...

$2 \to 4 \to 8 \to 16 \to 13 \to 7 \to 14 \to 9 \to 18 \to 17 \to 15 \to 11$
$\to 3 \to 6 \to 12 \to 5 \to 10 \to 1 \to 2 \to \cdots$

Therefore this group is cyclic.

f. Table of discrete logarithms:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9
3	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9
10	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9
13	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9
14	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9
15	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

37. Using the properties of discrete logarithms, show how to solve the following congruences.

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

Using 3 as the base of the discrete logarithm,

$L_3(x^5) \equiv L_3(11) \mod 16$

$L_3(11) = 7$ for $\langle \mathbb{Z}_{17}^*, \times \rangle$, and $L_3(x^5) = 5L_3(x)$.

$5L_3(x) \equiv 7 \mod 16.$

$L_3(x) \equiv 5^{-1} \times 7 \mod 16. \equiv 11 \mod 16 \rightarrow 11.$

From the logarithm table, $L_3(7) = 11. \Rightarrow \boxed{x = 11}$

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

Using 2 as the base of the discrete logarithm,

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

$L_2(2) = 1$, $L_2(3) = 13$ for $\langle \mathbb{Z}_{19}^*, \times \rangle$ and $L_2(2x^{11}) = L_2(2) + 11 \times L_2(x)$.

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

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

From the logarithm table, $L_2(7) = 6. \Rightarrow \boxed{x = 7}$

c. $5x^{12} + 6x \equiv 8 \mod 23.$

There is no property of discrete logarithm that isolates $L_k(x)$ from the original equation.

In order to get the solution (or verify its non-existance), one needs to numerically verify.

To do that, compute $5x^{12} + 6x$ for all $x \in \{1, \cdots, 22\}$.