

MATH 470: Communications and Cryptography**Homework 8***Due date: 25 October 2023**Name: Huy Lai*

Problem 1. This exercise asks you to use the index calculus to solve a discrete logarithm problem. Let $p = 19079$ and $g = 17$

Subproblem 1. Verify that $g^i \bmod p$ is 5-smooth for each of the values $i = 3030, i = 6892$ and $i = 18312$.

Solution:

Calculate $g^i \bmod p$

1. For $i = 3030$

$$\begin{aligned} g^{3030} \bmod p &\equiv 17^{3030} \bmod p \\ &\equiv 14580 \bmod p \end{aligned}$$

$$14580 = 2^2 \cdot 3^6 \cdot 5^1$$

2. For $i = 6892$

$$\begin{aligned} g^{6892} \bmod p &\equiv 17^{6892} \bmod p \\ &\equiv 18432 \bmod p \end{aligned}$$

$$18432 = 2^{11} \cdot 3^2$$

3. For $i = 18312$

$$\begin{aligned} g^{18312} \bmod p &\equiv 17^{18312} \bmod p \\ &\equiv 6000 \bmod p \end{aligned}$$

$$6000 = 2^4 \cdot 3^1 \cdot 5^3$$

Subproblem 2. Use your computations in (a) and linear algebra to compute the discrete logarithms $\log_g(2)$, $\log_g(3)$ and $\log_g(5)$.

Solution:

The discrete logs are as follows

$$\begin{aligned}
 \log_g(g^{3030}) &\equiv \log_p(2^2 \cdot 3^6 \cdot 5^1) \pmod{p} \\
 3030 \log_g(g) &\equiv 2 \log_g(2) + 6 \log_g(3) + \log_g(5) \pmod{p} \\
 3030 &\equiv 2 \log_g(2) + 6 \log_g(3) + \log_g(5) \pmod{p} \\
 \log_g(g^{6892}) &\equiv \log_p(2^{11} \cdot 3^2) \pmod{p} \\
 6892 \log_g(g) &\equiv 11 \log_g(2) + 2 \log_g(3) \pmod{p} \\
 6892 &\equiv 11 \log_g(2) + 2 \log_g(3) \pmod{p} \\
 \log_g(g^{18312}) &\equiv \log_p(2^4 \cdot 3^1 \cdot 5^3) \pmod{p} \\
 18312 \log_g(g) &\equiv 4 \log_g(2) + 1 \log_g(3) + 3 \log_g(5) \pmod{p} \\
 18312 &\equiv 4 \log_g(2) + 1 \log_g(3) + 3 \log_g(5) \pmod{p}
 \end{aligned}$$

Converting these congruences to matrixes is as follows:

$$\begin{bmatrix} 2 & 6 & 1 \\ 11 & 2 & 0 \\ 4 & 1 & 3 \end{bmatrix} \begin{bmatrix} \log_g(2) \\ \log_g(3) \\ \log_g(5) \end{bmatrix} \equiv \begin{bmatrix} 3030 \\ 6892 \\ 18312 \end{bmatrix} \pmod{p}$$

We use the note that $p - 1 = 2 \cdot 9539$ and solve this linear system by splitting it $\pmod{2}$ and $\pmod{9539}$

Calculating $\pmod{2}$

$$\left[\begin{array}{ccc|c} 2 & 6 & 1 & 3030 \\ 11 & 2 & 0 & 6892 \\ 4 & 1 & 3 & 18312 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array} \right] \pmod{2}$$

From this we get that

$$(x_2, x_3, x_5) \equiv (0, 0, 0) \pmod{2}$$

$$\begin{array}{l}
\text{Calculating mod 9539} \\
\left[\begin{array}{ccc|c} 2 & 6 & 1 & 3030 \\ 11 & 2 & 0 & 6892 \\ 4 & 1 & 3 & 18312 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 2 & 6 & 1 & 3030 \\ 11 & 2 & 0 & 6892 \\ 4 & 1 & 3 & 8773 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 1 & 8672 & 0 & 7564 \\ 1 & 2385 & 7155 & 4578 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 0 & 6287 & 2384 & 2986 \\ 1 & 2385 & 7155 & 4578 \end{array} \right] \equiv \\
\left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 0 & 6287 & 2384 & 2986 \\ 0 & 2382 & 2385 & 3063 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 0 & 1523 & 7153 & 6399 \\ 0 & 2382 & 2385 & 3063 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 0 & 1 & 8980 & 7564 \\ 0 & 1 & 5203 & 7558 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 0 & 1 & 8980 & 7564 \\ 0 & 0 & 5762 & 9533 \end{array} \right] \equiv \\
\left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 0 & 1 & 8980 & 7564 \\ 0 & 0 & 1 & 7463 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 3 & 4770 & 1515 \\ 0 & 1 & 0 & 1299 \\ 0 & 0 & 1 & 7463 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 3 & 0 & 1515 \\ 0 & 1 & 0 & 1299 \\ 0 & 0 & 1 & 7463 \end{array} \right] \equiv \left[\begin{array}{ccc|c} 1 & 0 & 0 & 8195 \\ 0 & 1 & 0 & 1299 \\ 0 & 0 & 1 & 7463 \end{array} \right]
\end{array}$$

From this we get

$$(x_2, x_3, x_5) \equiv (8195, 1299, 7463) \pmod{9539}$$

Using the Chinese Remainder Theorem to combine these results:

$$(x_2, x_3, x_5) \equiv (17734, 10838, 17002) \pmod{p}$$

Subproblem 3. Verify that $19 \cdot 17^{-12400} \pmod{p}$ is 5-smooth.

Solution:

We compute

$$\begin{aligned}
19 \cdot 17^{-12400} &\equiv 19 \cdot (17^{-1})^{12400} \pmod{p} \\
&\equiv 19 \cdot (11223)^{12400} \pmod{p} \\
&\equiv 19 \cdot 5041 \pmod{p} \\
&\equiv 384 \pmod{p} \\
&\equiv 2^7 \cdot 3 \pmod{p}
\end{aligned}$$

This number is 5-smooth

Subproblem 4. Use the values from (b) and the computation in (c) to solve the discrete logarithm problem

$$17^x \equiv 19 \pmod{p}$$

Solution:

From part (c) we know that $19 \equiv 17^{12400} \cdot (2^7 \cdot 3) \pmod{p}$

Using the discrete logs we calculated in part (b) we can substitute 2 and 3 as follows

$$19 \equiv 17^{12400} \cdot (g^{17734})^7 \cdot (g^{10838})^1 \pmod{p}$$

$$19 \equiv 17^{147376} \pmod{p}$$

Note that $147376 \equiv 13830 \pmod{p-1}$

$$x = 13800$$

Problem 2. Use the Tonelli-Shanks algorithm to compute a square root of 6 modulo 97 (note 97 is prime).

Solution:

$$6^{\frac{p-1}{2}} \equiv 6^{48} \equiv 1 \pmod{97}, \text{ therefore 6 is a quadratic residue } \pmod{97}$$

$$p - 1 = 96 = 2^5 \cdot 3 \rightarrow k = 5, Q = 3$$

Let $z = 5$ which is a non-quadratic residue $\pmod{97}$

Square root 6:

$$6^3 \not\equiv 1 \pmod{97}$$

$$i = 1: 6^{2^1 \cdot 3} \equiv -1 \pmod{97}$$

$$a' \equiv 6 \cdot 5^{2^{5-1}-1} \equiv 6 \cdot 5^{2^3} \equiv 36 \pmod{97}$$

$$R = 91$$

$$\text{Return: } 91 \cdot 5^{-2^{5-1}-2} \equiv 91 \cdot 5^{-2^2} \equiv 54 \pmod{97}$$

Square root 36 (Recursion 1):

$$36^3 \not\equiv 1 \pmod{97}$$

$$i = 0: 36^{2^1 \cdot 3} \equiv -1 \pmod{97}$$

$$a' \equiv 36 \cdot 5^{2^{5-0}-1} \equiv 36 \cdot 5^{2^4} \equiv 36 \pmod{97}$$

$$R = 61$$

$$\text{Return: } 61 \cdot 5^{-2^{5-0}-2} \equiv 61 \cdot 5^{-2^3} \equiv 91 \pmod{97}$$

Square root 35 (Recursion 2):

$$35^3 \equiv 1 \pmod{97}$$

$$\text{Return: } 35^2 \equiv 61 \pmod{97}$$

54 is a square root of 6 modulo 97.

Problem 3. Using the fact that $2021 = 43 \cdot 47$ and that 43 and 47 are both primes, use the Tonelli-Shanks algorithm and the Chinese remainder theorem to compute a square root of $6 \pmod{2021}$.

Solution:

Using the Tonelli-Shanks algorithm, we get that

$$36^2 \equiv 6 \pmod{43}$$

$$37^2 \equiv 6 \pmod{47}$$

Calculate the modular inverses of 43 and 47 modulo each other

$$43^{-1} \equiv 35 \pmod{47}$$

$$47^{-1} \equiv 11 \pmod{43}$$

Next we use the Chinese Remainder Theorem to calculate

$$x \equiv 36 \pmod{43}$$

$$x \equiv 37 \pmod{47}$$

From the first equivalence: $x = 43y + 36, y \in \mathbb{Z}$

$$43y + 36 \equiv 37 \pmod{47}$$

$$43y \equiv 1 \pmod{47}$$

$$y \equiv 35 \pmod{47}$$

$$x = 43(35) + 36 = 1541$$

Therefore, 1541 is a square root of $6 \pmod{2021}$

This can be verified by calculating that $1541^2 \equiv 6 \pmod{2021}$

Problem 4. Prove or disprove the following statement:

Let $N = pq$ where p, q are distinct odd primes. If a, b are integers such that $a^2 \equiv b^2 \pmod{N}$ and $a \not\equiv \pm b \pmod{N}$, then $\gcd(a - b, N)$ or $\gcd(a + b, N)$ gives a nontrivial factor N .

Solution:

This statement is true and the proof is as follows

Proof. First we rewrite the given congruence $a^2 \equiv b^2 \pmod{N}$ as

$$(a - b)(a + b) \equiv 0 \pmod{N}$$

By proposition, this implies that $N = pq \mid (a - b)(a + b)$

Since $p \mid N$, by proposition 1.4(a) and proposition 1.19, $p \mid (a - b) \vee p \mid (a + b)$.

However, since $a \not\equiv \pm b \pmod{N}$, $a + b \not\equiv 0 \pmod{N}$ and $a - b \not\equiv 0 \pmod{N}$.

This means that neither $a - b$ nor $a + b$ is divisible by both p and q .

So one of $a - b$ or $a + b$ is divisible by p but not by q , which means that $\gcd(a + b, N) = p$ or $\gcd(a - b, N) = p$ \square

Problem 5. Read Example 3.69 in the textbook. Explain why $(-1)^{\text{dlog}_g(h)} = \left(\frac{h}{p}\right)$

Solution:

If $\log_g(h) \equiv 0 \pmod{2}$, then $(-1)^{\log_g(h)} = 1$

If $\log_g(h) \equiv 1 \pmod{2}$, then $(-1)^{\log_g(h)} = -1$

By proposition 3.61 we know that $h = g^{\log_g(h)}$ is a quadratic residue if and only if $\log_g(h) \equiv 0 \pmod{2}$ and that $h = g^{\log_g(h)}$ is a non-quadratic residue if $\log_g(h) \equiv 1 \pmod{2}$

By definition of the Legendre Symbol, $\left(\frac{h}{p}\right) = -1$ if h is a non-quadratic residue modulo p and $\left(\frac{h}{p}\right) = 1$ if h is.

From this the Legendre Symbol determines if $\log_g(h)$ is odd or even and we get the relationship described.

The example 3.69 goes on to elaborate how because of this result, the 0-th bit of the discrete logarithm is insecure.

What this means that $\left(\frac{h}{g}\right)$ can predict if the 0-th bit is 0 or 1.

Problem 6. Let p be an odd prime, let $g \in \mathbb{F}_p^*$ be a primitive root, and let $h \in \mathbb{F}_p^*$. Write $p - 1 = 2^s m$ with m odd and $s \geq 1$, and write the binary expansion of $\log_g(h)$ as

$$\log_g(h) = \epsilon_0 + 2\epsilon_1 + 4\epsilon_2 + 8\epsilon_3 + \cdots \quad \text{with} \quad \epsilon_0, \epsilon_1, \dots \in \{0, 1\}$$

Give an algorithm that generalizes Example 3.69 and allows you to rapidly compute $\epsilon_0, \epsilon_1, \dots, \epsilon_{s-1}$, thereby proving that the first s bits of the discrete logarithm are insecure. You may assume that you have a fast algorithm to compute square roots in \mathbb{F}_p^* , as provided for example by Exercise 3.39(a) if $p \equiv 3 \pmod{4}$. (Hint. Use Example 3.69 to compute the 0th bit, take the square root of either h or $g^{-1}h$, and repeat.)