Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 15, 2023

What we have seen last time

- Primality testing
- Modular exponential
- Primitive roots

Today's topics

- Discrete logarithm
- Some cryptography
- Primitive root theorem

Discrete logarithm

Definition 15.1

Let m be a modulus. Then a ***primitive root modulo*** m is an element a in $\Phi(m)$ such that the dynamic of $\boxed{\cdot a \pmod{m}}$ consists of only one circle. Namely, any element of $\Phi(m)$ can be expressed as a power of a modulo m. $\Phi(m) = \{a^i \bmod m \mid i \in \mathbb{Z}\}$

When a primitive root g modulo m exists, we have an *isomorphism* (two-way translation):

add → mult

$\bar{0} \to 1$

$$\begin{aligned} \exp_{g \pmod{m}} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m) \\ \bar{x} &\longmapsto g^x \pmod{m}. \end{aligned}$$

CAN go back! "discrete logarithm"

Discrete logarithm

Question (Discrete logarithm)

Fix the modulus m *and a primitive root* $g \in \Phi(m)$*. For a given* $a \in \Phi(m)$*, find an integer* x *such that* $\bar{x} \in \mathbb{Z}/\varphi(m)$

$$a \equiv g^x \pmod{m}.$$

Unlike the modular exponential problems, for which we have effective algorithm, there is no way to compute discrete logarithm effectively in general. Trial Exp Method : $O(\varphi(m) \log m)$

Discrete logarithm

But in special cases, discrete logarithm can be not that difficult.

Question (Pohlig-Hellman algorithm)

Fix the modulus m and a primitive root $g \in \Phi(m)$. Suppose $\varphi(m) = p^e$. For a given $a \in \Phi(m)$, find an integer x such that

$$a \equiv g^x \pmod{m}.$$

p is small << m
prime

Discrete logarithm

$\varphi(m) = p^e \qquad g^{p^e} \equiv 1 \bmod m \qquad \gamma^p \equiv 1 \bmod m \qquad \ell(\gamma) = p$

First compute $\gamma \equiv g^{p^{e-1}} \pmod{m}$. Starting with $x_0 = 0$, repeat the following steps for $k = 0, \cdots, e-1$:

1. compute $a_k \equiv (g^{-x_k} a)^{p^{e-1-k}} \pmod{m}$.
2. Solve the discrete logarithm $\gamma^{d_k} \equiv a_k \pmod{m}$. ⇐ trial Exp Method ($\because p$ is small)
3. Let x_{k+1} be $x_k + p^k d_k$.

Then x_e is an answer to our discrete logarithm problem.

Example 15.2

Solving $3^x \equiv 2 \pmod{17}$.

$3^0 \quad 3^1 \quad 3^2 \quad 3^{2^2} \quad 3^{2^3} \quad 3^{2^4}$

$1 \to 3 \to 9 \to -4 \to -1 \to 1$

$p=2$ $\qquad 3^8$

First, $\varphi(17) = 2^4$. We then have $\gamma \equiv 3^{2^{4-1}} \equiv -1 \pmod{17}$.

$1 \to 2 \to 4 \to -1 \to 1$

1. $x_0 = 0$. Then $a_0 \equiv (3^{-0}2)^{2^{4-1-0}} \overset{2^8}{\equiv} 1 \equiv \gamma^0 \pmod{17}$. Hence,
   $x_1 = x_0 + 2^0 d_0 = 0 + 1 \cdot 0 = 0$
2. $a_1 \equiv (3^{-x_1}2)^{2^{4-1-1}} \equiv (3^{-0}2)^{2^{4-1-1}} \overset{2^4}{\equiv} -1 \equiv \gamma^1 \pmod{17}$. Hence,
   $x_2 = x_1 + 2^1 d_1 = 0 + 2 \cdot 1 = 2$

   $3^4 \equiv -4 \qquad 2^2 \equiv 4$

   $3^{-4} \cdot 2^2 \equiv -1$
3. $a_2 \equiv (3^{-x_2}2)^{2^{4-1-2}} \equiv (3^{-2}2)^{2^{4-1-2}} \overset{3^{-4}2^2}{\equiv} -1 \equiv \gamma^1 \pmod{17}$. Hence,
   $x_3 = x_2 + 2^2 d_2 = 2 + 4 \cdot 1 = 6$

   $3^6 = 3^2 \cdot 3^4 = 9 \cdot (-4) = -2$
4. $a_3 \equiv (3^{-x_3}2)^{2^{4-1-3}} \equiv (3^{-6}2)^{2^{4-1-3}} \overset{3^{-6}2}{\equiv} -1 \equiv \gamma^1 \pmod{17}$. Hence,
   $x_4 = x_3 + 2^3 d_3 = 6 + 8 \cdot 1 = 14$

   $3^{-6} \cdot 2 \equiv (-2)^{-1} \cdot 2 = -1$

$3^{14} = 3^8 \cdot 3^4 \cdot 3^2 = (-1) \cdot (-4) \cdot 9 \equiv 2 \bmod 17.$

Apply to cryptography

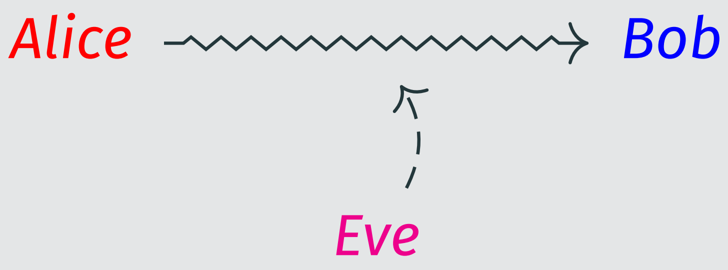
Discrete Logarithm is Hard!

Apply to cryptography

We may use the difficulty of discrete logarithms to encrypt communication.

Question (Public key system, Diffie-Helman key exchange)

Alice wants to encrypt a message so that **only** *Bob can decrypt it, not Eve.*



Apply to cryptography

1. Alice chooses a large ($\sim 2^{2048}$) prime p such that $\varphi(\varphi(p))$ also has a large prime factor, and finds a primitive root g modulo p. Publishes (p, g), which is the ***public key***. $\# \cdot\cdot = \varphi(\varphi(p))$
2. Alice chooses a ***private key*** a and computes $A := g^a \pmod{p}$. Bob chooses a ***private key*** b and computes $B := g^b \pmod{p}$.

$$\begin{tikzcd} \text{Alice} \arrow[r, rightsquigarrow, bend left, "A"] & \text{Bob} \arrow[l, rightsquigarrow, bend left, "B"] \end{tikzcd}$$

Then they exchange A and B (through any channel, probably intercepted by Eve).

Apply to cryptography

$A \equiv g^a$ $B \equiv g^b$ $A^b \equiv g^{ab}$ $B^a \equiv g^{ba}$

3. Alice computes $B^a \pmod{p}$ and Bob computes $A^b \pmod{p}$, both are $\equiv g^{ab} \pmod{p}$. This is their common secret key S.
4. Now Alice and Bob can encrypt their communication using the secret key S.
5. Eve may know (p, g, A, B). Can Eve find out what S is? This is very hard since finding a (resp. b) from A (resp. B) is difficult.

discrete log !

Apply to cryptography

Some remarks:

$\varphi(2q) = q-1$

- A ***Sophie Germain prime*** is a prime q such that $p := 2q + 1$ is also a prime. Note that $\varphi(p) = 2q$. Hence, when q is large, p would be a safe prime for the public key system.
- The primality testing is fast, so generating a public key wouldn't cost too much time.
- Alice needs to compute $g^a \pmod{p}$ and $B^a \pmod{p}$, while Bob needs to compute $g^b \pmod{p}$ and $A^b \pmod{p}$. These are modular exponential problems, and we can solve them effectively using binary exponentiation algorithms.

Primitive root theorem

Primitive root theorem

Theorem 15.3 (Gauss)

If p is prime, then $\Phi(p)$ contains exactly $\varphi(\varphi(p))$ primitive roots.

Example 15.4 $\varphi(7) = 7-1 = 6$ $\Phi(6) = \{1, 5\}$

For the prime 7, we have $\varphi(\varphi(7)) = \varphi(6) = 2$. Indeed, we have exactly two primitive roots 3 and 5.

3: $1 \to 3 \to 2 \to 6 \to 4 \to 5 \to 1$ pr ✓ $1 \to 2 \to 4 \to 1$ ✗

5: $1 \to 5 \to 4 \to 6 \to 2 \to 3 \to 1$ pr ✓ $1 \to 4 \to 2 \to 1$ ✗

$1 \to 6 \to 1$ ✗

Proof. For $a \in \Phi(p)$, theorem 13.11 tells us the dynamic of $\boxed{\cdot a \pmod{p}}$ consists of cycles of the same length $\ell(a)$. Let $c(a)$ be the number of cycles. Then we have

$$c(a) \cdot \ell(a) = \varphi(p) = p - 1.$$

In particular, $\ell(a) \mid p - 1$.

Conversly, for each divisor ℓ of $p - 1$, define

$$\Phi_\ell(p) := \{a \in \Phi(p) \mid \ell(a) = \ell\}.$$

In particular, $\Phi_{p-1}(p) = \{\text{primitive roots}\}$.

$\# \Phi_{p-1}(p) = \varphi(p-1)$ WTS: $\# \Phi_\ell(p) = \varphi(\ell)$

Proof of the theorem

Proof. We want to show: each $\Phi_\ell(p)$ is nonempty.

1. For distinct divisors $\ell_1 \neq \ell_2$ of $p-1$, we necessarily have $\Phi_{\ell_1}(p) \cap \Phi_{\ell_1}(p) = \varnothing$. Therefore,
$$p - 1 = |\Phi(p)| = \sum_{\ell \mid p-1} |\Phi_\ell(p)|.$$
2. We will show that
$$\sum_{\ell \mid p-1} \varphi(\ell) = p - 1.$$
3. But for each divisor ℓ of $p-1$, we will see that
$$|\Phi_\ell(p)| \leqslant \varphi(\ell).$$
4. Hence, combining 1–3, we must have $|\Phi_\ell(p)| = \varphi(\ell) > 0$. $\square$

After Class Work

After Class Work

Exercise 15.1

Alice wants to encrypt communication with Bob using Diffie-Helman key exchange. Suppose the public key is $(467, 2)$.

If the private keys of Alice and Bob are $a = 22$ and $b = 33$ respectively. What are A, B and the secret key S?

Exercise 15.2

Is there any primitive root modulo 8?