Discrete logarithm

Definition 4.7.1

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.

Definition 4.7.1

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.

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

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

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

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

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

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

Unlike the modular exponential problems, for which we have effective algorithm, there is no way to compute discrete logarithm effectively in general.

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

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

$p^e = \varphi(m)$

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 $\gamma^{d_k} \equiv a_k \pmod{m}$.
3. Let x_{k+1} be $x_k + p^k d_k$.

Then x_e is an answer to our discrete logarithm problem.

Example 4.7.2

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

Example 4.7.2

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

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

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

Example 4.7.2

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

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

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

Example 4.7.2

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

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

1. $x_0 = 0$. Then $a_0 \equiv (3^{-0}2)^{2^{4-1-0}} \equiv 1 \equiv \gamma^0 \pmod{17}$. Hence, $x_1 = x_0 + 2^0 d_0 = 0$.
2. $a_1 \equiv (3^{-x_1}2)^{2^{4-1-1}} \equiv (3^{-0}2)^{2^{4-1-1}} \equiv -1 \equiv \gamma^1 \pmod{17}$. Hence, $x_2 = x_1 + 2^1 d_1 = 2$.
3. $a_2 \equiv (3^{-x_2}2)^{2^{4-1-2}} \equiv (3^{-2}2)^{2^{4-1-2}} \equiv -1 \equiv \gamma^1 \pmod{17}$. Hence, $x_3 = x_2 + 2^2 d_2 = 6$.

Example 4.7.2

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

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

1. $x_0 = 0$. Then $a_0 \equiv (3^{-0}2)^{2^{4-1-0}} \equiv 1 \equiv \gamma^0 \pmod{17}$. Hence, $x_1 = x_0 + 2^0 d_0 = 0$.
2. $a_1 \equiv (3^{-x_1}2)^{2^{4-1-1}} \equiv (3^{-0}2)^{2^{4-1-1}} \equiv -1 \equiv \gamma^1 \pmod{17}$. Hence, $x_2 = x_1 + 2^1 d_1 = 2$.
3. $a_2 \equiv (3^{-x_2}2)^{2^{4-1-2}} \equiv (3^{-2}2)^{2^{4-1-2}} \equiv -1 \equiv \gamma^1 \pmod{17}$. Hence, $x_3 = x_2 + 2^2 d_2 = 6$.
4. $a_3 \equiv (3^{-x_3}2)^{2^{4-1-3}} \equiv (3^{-6}2)^{2^{4-1-3}} \equiv -1 \equiv \gamma^1 \pmod{17}$. Hence, $x_4 = x_3 + 2^3 d_3 = 14$.

$x \equiv 14 \bmod 17$.