Discrete Logarithm(s) (DLs)

- Fix a prime p. Let a, b be nonzero integers (mod p). The problem of finding x such that $a^x \equiv b \pmod{p}$ is called the discrete logarithm problem. Suppose that n is the smallest integer such that $a^n \equiv 1 \pmod{p}$, i.e., $n = ord_p(a)$. By assuming $0 \le x < n$, we denote $x = L_a(b)$, and call it the discrete log of b w.r.t. a (mod p).

- Ex: $p=11$, $a=2$, $b=9$, then $x=L_2(9)=6$

- In the RSA algorithms, the difficulty of factoring a large integer yields good cryptosystems
- In the ElGamal method, the difficulty of solving the discrete logarithm problem yields good cryptosystems
- Given p, a, b, solve $a^x \equiv b \pmod{p}$
- a is suggested to be a primitive root mod p

Here is an example using a nonprime modulus, $n = 9$. Here $\phi(n) = 6$ and $a = 2$ is a primitive root. We compute the various powers of a and find

$$\begin{array}{ll} 2^0 = 1 & 2^4 \equiv 7 \pmod 9 \\ 2^1 = 2 & 2^5 \equiv 5 \pmod 9 \\ 2^2 = 4 & 2^6 \equiv 1 \pmod 9 \\ 2^3 = 8 & \end{array}$$

This gives us the following table of the numbers with given discrete logarithms (mod 9) for the root $a = 2$:

Logarithm	0	1	2	3	4	5
Number	1	2	4	8	7	5

To make it easy to obtain the discrete logarithms of a given number, we rearrange the table:

Number	1	2	4	5	7	8
Logarithm	0	1	2	5	4	3

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Algorithm 4.2.1 (Shanks' baby-step giant-step algorithm). This algorithm computes the discrete logarithm x of y to the base a, modulo n, such that $y = a^x \pmod{n}$:

[1] (Initialization) Computes $s = \lfloor \sqrt{n} \rfloor$.

[2] (Computing the baby step) Compute the first sequence (list), denoted by S, of pairs (ya^r, r), $r = 0, 1, 2, 3, \cdots, s-1$:

$$S = \{(y, 0), (ya, 1), (ya^2, 2), (ya^3, 3), \cdots, (ya^{s-1}, s-1) \bmod n\} \tag{4.1}$$

and sort S by ya^r, the first element of the pairs in S.

[3] (Computing the giant step) Compute the second sequence (list), denoted by T, of pairs (a^{ts}, ts), $t = 1, 2, 3, \cdots, s$:

$$T = \{(a^s, 1), (a^{2s}, 2), (a^{3s}, 3), \cdots, (a^{s^2}, s) \bmod n\} \tag{4.2}$$

and sort T by a^{ts}, the first element of the pairs in T.

[4] (Searching, comparing and computing) Search both lists S and T for a match $ya^r = a^{ts}$ with ya^r in S and a^{ts} in T, then compute $x = ts - r$. This x is the required value of $\log_a y \pmod{n}$.

Example 4.2.1. Suppose we wish to compute the discrete logarithm

$$x = \log_2 6 \bmod 19$$

such that $6 = 2^x \bmod 19$. According to Algorithm 4.2.1, we perform the following computations:

[1] $y = 6$, $a = 2$ and $n = 19$, $s = \lfloor \sqrt{19} \rfloor = 4$.

[2] Computing the baby step:

$$\begin{aligned} S &= \{(y,0),(ya,1),(ya^2,2),(ya^3,3) \mod 19\} \\ &= \{(6,0),(6\cdot 2,1),(6\cdot 2^2,2),(6\cdot 2^3,3) \bmod \ 19\} \\ &= \{(6,0),(12,1),(5,2),(10,3)\} \\ &= \{(5,2),(6,0),(10,3),(12,1)\}. \end{aligned}$$

[3] Computing the giant step:

$$\begin{aligned} T &= \{(a^s,s),(a^{2s},2s),(a^{3s},3s),(a^{4s},4s) \bmod \ 19\} \\ &= \{(2^4,4),(2^8,8),(2^{12},12),(2^{16},16) \mod 19\} \\ &= \{(16,4),(9,8),(11,12),(5,16)\} \\ &= \{(5,16),(9,8),(11,12),(16,4)\} \end{aligned}$$

[4] Matching and computing: The number 5 is the common value of the first element in pairs of both lists S and T with $r = 2$ and $st = 16$, so $x = st - r = 16 - 2 = 14$. That is, $\log_2 6 \pmod{19} = 14$, or equivalently, $2^{14} \pmod{19} = 6$.