

$$z_3 = (a_3 + b_3) \bmod m_3 = (4 + 0) \bmod 5 = 4$$

$$a + b = (z_1, z_2, z_3) = (2, 1, 4)$$

Pre operáciu  $a - b$  platí

$$a - b = (z'_1, z'_2, z'_3) \bmod m_i \text{ kde } z'_i = (a_i - b_i) \bmod m_i \text{ pre } i = 1, 2, 3, \dots, k$$

$$z'_1 = (a_1 - b_1) \bmod m_1 = (1 - 1) \bmod 3 = 0$$

$$z'_2 = (a_2 - b_2) \bmod m_2 = (3 - 2) \bmod 4 = 1$$

$$z'_3 = (a_3 - b_3) \bmod m_3 = (4 - 0) \bmod 5 = 4$$

$$a - b = (z'_1, z'_2, z'_3) = (0, 1, 4)$$

Pre operáciu  $a \cdot b$  platí

$$a \cdot b = (w_1, w_2, w_3) \text{ kde } w_i = (a_i \cdot b_i) \bmod m_i \text{ pre } i = 1, 2, 3, \dots, k$$

$$w_1 = (a_1 \cdot b_1) \bmod m_1 = (1 \cdot 1) \bmod 3 = 1$$

$$w_2 = (a_2 \cdot b_2) \bmod m_2 = (3 \cdot 2) \bmod 4 = 2$$

$$w_3 = (a_3 \cdot b_3) \bmod m_3 = (4 \cdot 0) \bmod 5 = 0$$

$$a \cdot b = (w_1, w_2, w_3) = (1, 2, 0)$$

## 6.9 Diskrétné logaritmy

**Diskrétné logaritmy** sú základom viacerých algoritmov v kryptografii s verejným kľúčom, napr. algoritmu *Diffie-Hellman*, algoritmu DSA na digitálne podpisy, atď.

Na vysvetlenie pojmu diskrétny logaritmus je potrebné uviesť niekoľko úvodných poznámok.

Z Eulerovej vety (veta 6.9) vyplýva, že pre  $a, n \in \mathbb{N}$ ,  $n > 1$  ak  $\gcd(a, n) = 1$  platí

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

kde  $\phi(n)$  je Eulerova funkcia.

**Veta 6.12.** Ak  $a, n \in \mathbb{N}$  a  $\gcd(a, n) = 1$ , potom existuje aspoň jedno celé kladné číslo  $m$  také, že

$$a^m \equiv 1 \pmod{n}. \quad (6.11)$$

Najmenšie číslo  $m$ , ktoré spĺňa rovnici (6.11) sa označuje viacerými spôsobmi a to:

- stupeň  $a \pmod{n}$ ,
- exponent, pre ktorý  $a$  prináleží  $(\bmod n)$ ,
- dĺžka periód generovanej číslom  $a$ .

### Priklad

Stanovte číslo  $m$  pre  $a=11$  a  $n=19$ .

Pretože  $\gcd(a, n) = \gcd(11, 19) = 1$ , existuje číslo  $m$  také, že  $a^m \equiv 1 \pmod{n}$ .

Mocniny čísla  $a$  vytvárajú postupnosť

$$11^1 \bmod 19 = 11 \bmod 19$$

$$11^2 = 121 \equiv 7 \bmod 19$$

$$11^3 = 1331 \equiv 1 \bmod 19$$

$$11^4 \equiv 11 \bmod 19$$

$$11^5 \equiv 7 \bmod 19$$

$$11^6 \equiv 1 \bmod 19$$

⋮

⋮

Postupnosť mocnín čísla  $a=11$  je periodická a dĺžka periód je rovná najmenšiemu kladnému exponentu  $m$ , pre ktorý platí  $11^m \equiv 1 \pmod{19}$ . V tomto prípade je  $m=3$ .

V Tab. 6.2 sú uvedené všetky mocniny čísel  $a \pmod{19}$  pre  $a < 19$ . Z uvedenej tabuľky vyplývajú tieto závery:

1. všetky postupnosti mocnín  $a \pmod{19}$  bez opakovania končia číslom 1
2. dĺžky postupností mocnín  $a \pmod{19}$  delia  $\phi(19)$ , teda číslo 18 (pretože  $\phi(19)=18$ ). V uvedenom prípade sú dĺžky postupností rovné 1, 3, 6, 9 a 18 a teda uvedené dĺžky delia číslo 18.

Tab. 6.2 Mocniny celých čísel modulo 19

a	a <sup>2</sup>	a <sup>3</sup>	a <sup>4</sup>	a <sup>5</sup>	a <sup>6</sup>	a <sup>7</sup>	a <sup>8</sup>	a <sup>9</sup>	a <sup>10</sup>	a <sup>11</sup>	a <sup>12</sup>	a <sup>13</sup>	a <sup>14</sup>	a <sup>15</sup>	a <sup>16</sup>	a <sup>17</sup>	a <sup>18</sup>
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

**Definícia 6.7.** Číslo  $a \in \mathbb{N}$ , pre ktoré platí, že  $a^m \equiv 1 \pmod{n}$  a zároveň  $m = \phi(n)$  sa nazýva *primitívny koreň n* (primitive root of  $n$ ).

Pre  $n=19$  sú primitívne korene  $a=2, 3, 10, 13, 14$  a  $15$ , pretože pre tieto čísla  $a$  platí  $a^m = a^{\phi(n)} = a^{18} \equiv 1 \pmod{19}$  a neexistuje  $m < 18$ , že  $a^m \equiv 1 \pmod{19}$ .

**Poznámka.** Je potrebné poznamenať, že nie všetky celé čísla majú primitívne korene. Dá sa dokázať, že primitívne korene majú iba celé čísla, ktoré sú z postupnosti  $2, 4, p^\alpha$  a  $2p^\alpha$ , kde  $p$  je prvočíslo a  $\alpha \in \mathbb{N}$ .

**Veta 6.13.** Ak  $p$  je prvočíslo a číslo  $a$  je primitívny koreň prvočísla  $p$ , potom postupnosť  $a \bmod p, a^2 \bmod p, \dots, a^{p-1} \bmod p$  tvoria čísla  $1, 2, 3, \dots, (p-1)$  v určitom poradí.

#### 6.9.1 Logaritmická funkcia

Logaritmická funkcia na množine kladných reálnych čísel je inverznou funkciou exponenciálnej funkcie. Analogická funkcia existuje aj v modulárnej aritmetike.

Najprv však uvedieme stručný prehľad vlastností logaritmickej funkcie, resp. logaritmov.

**Definícia 6.7.** Nech  $y$  je reálne číslo a  $y > 0$ ,  $x$  je kladné reálne číslo a  $x \neq 1$ . Potom číslo  $z$ , pre ktoré platí

$$y = x^z \quad (6.12)$$

sa nazýva **logaritmus** čísla  $y$  pri základe  $x$ .

Výraz (6.12) možno zapísť aj v tvare

$$z = \log_x y \quad \text{alebo} \quad y = x^{\log_x y}$$

Vlastnosti logaritmov možno v stručnej forme zapísť takto.

Nech  $y, z$  sú reálne čísla a  $y > 0$ ,  $z > 0$ ,  $x$  je kladné reálne číslo a  $x \neq 1$ ,  $r$  je kladné reálne číslo, potom platí

$$\begin{aligned} \log_x 1 &= 0 \\ \log_x x &= 1 \\ \log_x(y \cdot z) &= \log_x y + \log_x z \\ \log_x y^r &= r \cdot \log_x y \end{aligned}$$

Prepokladajme, že číslo  $a$  je primitívny koreň prvočísla  $p$ . Z vety 6.11 vyplýva, že postupnosť mocnín  $a, a^2, \dots, a^{p-1}$  v module  $p$ , generuje celé čísla  $1, 2, \dots, (p-1)$  v určitom poradí.

Zároveň platí, že ľubovoľné celé číslo  $b$  možno vyjadriť v tvare

$$b \equiv r \pmod{p}, \text{ kde } 0 \leq r \leq (p-1) \quad (6.13)$$

Z uvedeného vyplýva nasledovné tvrdenie.

**Tvrdenie.** Ak číslo  $a$  je primitívny koreňom prvočísla  $p$ , potom pre ľubovoľné celé číslo  $b$  možno nájsť jediný exponent  $i$  taký, že platí

$$b \equiv a^i \pmod{p} \quad 0 \leq i \leq (p-1)$$

Exponent  $i$  označíme predbežne ako index čísla  $b$  pre základ  $a \pmod{p}$  a vyjadríme ho symbolom  $\text{ind}_{a,p}(b)$ .

V ďalšom postupe ukážeme, že  $\text{ind}_{a,p}(b)$  má podobné vlastnosti ako logaritmická funkcia.

Pre  $\text{ind}_{a,p}(b)$  platí

$$\begin{aligned} \text{ind}_{a,p} 1 &= 0, \text{ pretože } a^0 \pmod{p} = 1 \pmod{p} = 1 \\ \text{ind}_{a,p} a &= 1, \text{ pretože } a^1 \pmod{p} = a \pmod{p} = a \end{aligned}$$

Ked'že platí  $x \equiv a^{\text{ind}_{a,p}(x)} \pmod{p}$   
 $y \equiv a^{\text{ind}_{a,p}(y)} \pmod{p}$   
 $x \cdot y \equiv a^{\text{ind}_{a,p}(xy)} \pmod{p}$ ,

potom

$$a^{\text{ind}_{a,p}(xy)} \pmod{p} = (a^{\text{ind}_{a,p}(x)+\text{ind}_{a,p}(y)}) \pmod{p} \quad (6.14)$$

Uvedený vzťah možno získať aplikovaním pravidiel násobenia v modulárnej aritmetike.

Platí

$$\begin{aligned} x \cdot y &\equiv (a^{\text{ind}_{a,p}(x)} \pmod{p}) \cdot (a^{\text{ind}_{a,p}(y)} \pmod{p}) = \\ &= (a^{\text{ind}_{a,p}(x)} \cdot a^{\text{ind}_{a,p}(y)}) \pmod{p} = (a^{\text{ind}_{a,p}(x)+\text{ind}_{a,p}(y)}) \pmod{p} \end{aligned}$$

Na druhej strane  $x \cdot y \equiv a^{\text{ind}_{a,p}(x \cdot y)} \pmod{p}$ , a teda uvedená rovnosť (6.14) platí.

Podľa Eulerovej vety pre dve ľubovoľné nesúdeliteľné čísla  $a, n$  platí

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Ak  $z$  je celé kladné číslo, potom ho možno podľa vety o delení so zvyškom vyjadriť v tvare

$$z = \phi(n) \cdot k + q \quad 0 \leq q < \phi(n)$$

kde  $q$  je zvyšok po delení čísla  $z$  číslom  $\phi(n)$ .

Číslo  $z$  možno vyjadriť aj v tvare

$$z \equiv q \pmod{\phi(n)}$$

Potom platí

$$a^z = a^{\phi(n) \cdot k + q} = \underbrace{\left[ a^{\phi(n)} \right]^k}_{\equiv 1 \pmod{n}} \cdot a^q \equiv 1^k \cdot a^q \pmod{n} = a^q \pmod{n}$$

Teda ak  $z \equiv q \pmod{\phi(n)}$ , potom  $a^z \equiv a^q \pmod{n}$ .

Ak uvedený postup platí pre ľubovoľné číslo  $n$  nesúdeliteľné s číslom  $a$ , tak platí aj pre prvočíslo  $p$ .

Teda ak  $z \equiv q \pmod{\phi(p)}$ , potom  $a^z \equiv a^q \pmod{p}$ .

Z uvedeného postupu vyplýva, že platí

$$(a^{ind_{a,p}(x)+ind_{a,p}(y)}) \bmod p = a^{ind_{a,p}(x+y)} \bmod p$$

platí ak

$$ind_{a,p}(x \cdot y) = [ind_{a,p}(x) + ind_{a,p}(y)] \bmod \phi(p)$$

Analogickým postupom možno ukázať, že platí

$$ind_{a,p}(y^r) = [r \cdot ind_{a,p}(y)] \bmod \phi(p)$$

Uvedené vzťahy potvrdzujú analógiu s logaritmickou funkciou, preto sa funkcia  $ind_{a,p}(b)$  nazýva **diskrétny logaritmus čísla b pre základ a mod p**. Zároveň je potrebné poznamenať, že diskrétny logaritmus čísla b existuje iba ak číslo a je primitívny koreň prvočísla p.

### 6.9.2 Výpočet diskrétnych logaritmov

Na ilustráciu výpočtu diskrétnych logaritmov uvedieme výpočet diskrétnych algoritmov i pre čísla  $b=1,2,3,\dots,18$  ak  $p=19$ . Prvočíslo 19 podľa Tab. 6.2 má primitívne korene  $a=2,3,10,13,14,15$ .

Pre primitívny koreň  $a=2$  platí

$$b \equiv 2^{ind_{a,p}(b)} \bmod 19,$$

resp.  $b \equiv 2^i \bmod 19$  pre  $1 \leq i \leq 18$ .

Ked'že pre zvolené b je riešenie takejto kongruencie ťažké, určíme hodnotu  $2^i \bmod 19$  pre  $i=1,2,\dots,18$  a takto získané čísla predstavujú hodnoty b z množiny  $\{1,2,\dots,18\}$ , pre ktoré diskrétny logaritmus je rovný  $ind_{2,19}(b)=i$ .

$$\begin{aligned} 2^1 &= 2 \bmod 19 = 2 \\ 2^2 &= 4 \bmod 19 = 4 \\ 2^3 &= 8 \bmod 19 = 8 \\ 2^4 &= 16 \bmod 19 = 16 \\ 2^5 &= 32 \bmod 19 = 13 \\ 2^6 &= 64 \bmod 19 = 7 \\ 2^7 &= 128 \bmod 19 = 14 \\ 2^8 &= 256 \bmod 19 = 9 \\ 2^9 &= 512 \bmod 19 = 18 \\ 2^{10} &= 1024 \bmod 19 = 17 \\ 2^{11} &= 2048 \bmod 19 = 15 \\ 2^{12} &= 4096 \bmod 19 = 11 \\ 2^{13} &= 8192 \bmod 19 = 3 \\ 2^{14} &= 16384 \bmod 19 = 6 \\ 2^{15} &= 33778 \bmod 19 = 12 \end{aligned}$$

teda

$$\begin{aligned} i=1, b &= 2 \\ i=2, b &= 4 \\ i=3, b &= 8 \\ i=4, b &= 16 \\ i=5, b &= 13 \\ i=6, b &= 7 \\ i=7, b &= 14 \\ i=8, b &= 9 \\ i=9, b &= 18 \\ i=10, b &= 17 \\ i=11, b &= 15 \\ i=12, b &= 11 \\ i=13, b &= 3 \\ i=14, b &= 6 \\ i=15, b &= 12 \end{aligned}$$

$$2^{16} = 65376 \bmod 19 = 5$$

$$i = 16, b = 5$$

$$2^{17} = 131112 \bmod 19 = 10$$

$$i = 17, b = 10$$

$$2^{18} = 262224 \bmod 19 = 1$$

$$i = 18, b = 1$$

Ak čísla b usporiadame podľa veľkosti, potom výsledok je uvedený v Tab. 6.3a.

V Tab. 6.3b,c,d,e,f sú uvedené hodnoty diskrétneho logaritmu pre primitívne korene 3,10,13,14 a 15.

Tab. 6.3 Hodnoty diskrétnych logaritmov modulo 19

$a = 2, p = 19$																		
b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
i	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

a.

$a = 3, p = 19$																		
b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
i	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

b.

$a = 10, p = 19$																		
b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
i	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

c.

$a = 13, p = 19$																		
b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
i	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

d.

$a = 14, p = 19$																		
b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
i	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	14	9

e.

$a = 15, p = 19$																		
b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
i	18	5	11	10	8	16	1											