1 Diskrétní matematika – příklady

1. přednáška

Příklad 15/47

$$n^2 - 1 = (n+1)(n-1) \Rightarrow (n+1 \mid n^2 - 1)$$

$$(n+1 \mid n^2+1) \wedge (n+1 \mid n^2-1) \Rightarrow \big(n+1 \mid (n^2+1) - (n^2-1)\big)$$

$$\Rightarrow (n+1 \mid 2) \Rightarrow n+1 \leqslant 2 \Rightarrow n \leqslant 1 \Rightarrow n \in \mathbb{N} = 1$$

Příklad 25/47

$$\exists s,t \in \mathbb{Z} : \left(\begin{array}{cccc} \wedge & a & = & s \cdot m + 1 \\ & b & = & t \cdot m + 1 \end{array} \right) \Rightarrow \exists u \in \mathbb{Z} : ab = u \cdot m + 1$$

$$ab = (s \cdot m + 1)(t \cdot m + 1) = stm^2 + tm + sm + 1 = (stm + t + s)m + 1$$

$$\exists u = stm + t + s : ab = u \cdot m + 1$$

2. přednáška

Příklad 9.1/24

$$5^{20} \ \% \ 26 = ?$$

$$(5^2 = 25) \equiv -1 \pmod{26}$$

$$(5^{20} = (5^2)^{10}) \equiv (-1)^{10} \pmod{26}$$

$$5^{20} \equiv 1 \pmod{26}$$

$$5^{20} \ \% \ 26 = 1 \ \% \ 26 = 1$$

Příklad 9.2/24

$\forall n \in \mathbb{N} : 7 \mid 37^{n+2} + 16^{n+1} + 23^n$?

$37 \equiv 16 \equiv 23 \equiv 2 \pmod 7$

$37^{n+2} \equiv 2^{n+2} \pmod 7$

$16^{n+1} \equiv 2^{n+1} \pmod 7$

$23^n \equiv 2^n \pmod 7$

$$\begin{aligned} 37^{n+2} + 16^{n+1} + 23^n &\equiv 2^{n+2} + 2^{n+1} + 2^n \pmod 7 \\ &\equiv 2^n(4 + 2 + 1) = 2^n \cdot 7 = 0 \pmod 7 \end{aligned}$$

$7 \mid 37^{n+2} + 16^{n+1} + 23^n$

Příklad 10/24

$n = (835^5 + 6)^{18} - 1$

$112 \mid n \iff 16 \mid n \wedge 7 \mid n$ $\qquad [16, 7] = 16 \cdot 7 = 112$

$7 \mid n$:

$$\begin{aligned} (835^5 + 6)^{18} - 1 &\equiv (2^5 + 6)^{18} - 1 \\ &\equiv 38^{18} - 1 \\ &\equiv 3^{18} - 1 = 27^6 - 1 \\ &\equiv (-1)^6 - 1 = 0 \pmod 7 \end{aligned}$$

$16 \mid n$:

$$\begin{aligned} (835^5 + 6)^{18} - 1 &\equiv (3^5 + 6)^{18} - 1 = (3 \cdot 81 + 6)^{18} - 1 \\ &\equiv (3 \cdot 1 + 6)^{18} - 1 \\ &\equiv 9^{18} - 1 = 81^9 - 1 \\ &\equiv 1^9 - 1 = 0 \pmod{16} \end{aligned}$$

3. přednáška

Příklad 48.1/73

$\varphi(72) = ?$

$$\begin{aligned} \varphi(72) &= \varphi(2^3 \cdot 3^2) \\ &= 72 \cdot \left(1 - \tfrac{1}{2}\right) \cdot \left(1 - \tfrac{1}{3}\right) \\ &= 72 \cdot \tfrac{1}{2} \cdot \tfrac{1}{3} \end{aligned}$$

Alternativně:

$$\begin{aligned} \varphi(72) &= \varphi(8) \cdot \varphi(9) \\ &= 4 \cdot 6 \\ &= 24 \end{aligned}$$

Příklad 48.2/73

Dokažte, že pro $\forall n \in \mathbb{N}$ platí $\varphi(4n + 2) = \varphi(2n + 1)$

$$\begin{aligned} \varphi(4n+2) &= \varphi(2) \cdot \varphi(2n+1) \\ &= \varphi(2n+1) \end{aligned}$$

Příklad 61/73

Určete řád čísla 2 modulo 7.

$$\begin{aligned} 2^1 = 2 &\not\equiv 1 \pmod 7 \\ 2^2 = 4 &\not\equiv 1 \pmod 7 \\ 2^3 = 8 &\equiv 1 \pmod 7 \end{aligned}$$

Řádem čísla 2 modulo 7 je 3.

4. přednáška

Příklad 23/62

Řešte $39x \equiv 41 \pmod{47}$

1) Řešení pomocí Eulerovy věty

$$\begin{aligned} 39 \cdot x &\equiv 41 \pmod{47} \\ 39^{\varphi(m)-1} \cdot 39 \cdot x &\equiv 39^{\varphi(m)-1} \cdot 41 \pmod{47} \\ x &\equiv 39^{45} \cdot 41 \pmod{47} \end{aligned}$$

Toto řešení je neoptimální, jelikož vyžaduje výpočet vysoké mocniny.

2) Řešení pomocí Bezoutovy věty

$$\begin{aligned} \exists k, l \in \mathbb{Z} : 39k + 47l &= 1 \\ 39k &\equiv 1 \pmod{47} \end{aligned}$$

Zjevně je, v modulo 47, k inverzním prvkem k 39, což nám umožňuje provést následující:

$$\begin{aligned} 39x &\equiv 41 \pmod{47} \\ (39k \equiv 1) \cdot x &\equiv 41k \pmod{47} \end{aligned}$$

Zbývá nám nalézt hodnotu k pomocí Euklidova algoritmu:

$$\begin{aligned} 47 &= 1 \cdot 39 + 8 \\ 39 &= 4 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 8 - 7 \\ &= 8 - (39 - 4 \cdot 8) \\ &= 5 \cdot 8 - 39 \\ &= 5 \cdot (47 - 39) - 39 \\ &= 5 \cdot 47 - 6 \cdot 39 \end{aligned}$$

Platí tedy $k = -6$ a proto

$$\begin{aligned} x &\equiv 41 \cdot (-6) \pmod{47} \\ &\equiv -246 \pmod{47} \\ &\equiv -11 \pmod{47} \\ &\equiv 36 \pmod{47} \end{aligned}$$

3) Řešení ad-hoc

$$\begin{aligned} 39x &\equiv 41 \pmod{47} \\ -8x &\equiv -6 \pmod{47} \\ 4x &\equiv 3 \pmod{47} \\ 4x &\equiv -44 \pmod{47} \\ x &\equiv -11 \pmod{47} \\ &\equiv 36 \pmod{47} \end{aligned}$$

Příklad 42/62 Řešte soustavu

$$\begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 5 \pmod{18} \\ x &\equiv -4 \pmod{25} \end{aligned}$$

Řešení Existuje řešení v modulu $\mathsf{lcm}(10, 18, 25) = 450$:

$$\begin{aligned} x &= 10r + 1 \\ 10r + 1 &\equiv 5 \pmod{18} \\ 10r &\equiv 4 \pmod{18} \\ 5r &\equiv 2 \pmod{9} \\ &\equiv 20 \pmod{9} \\ r &\equiv 4 \pmod{9} \\ r &= 9s + 4 \end{aligned}$$

$$\begin{aligned} x &= 10r + 1 \\ &= 10(9s + 4) + 1 \\ &= 90s + 41 \end{aligned}$$

$$\begin{aligned} x &\equiv -4 \pmod{25} \\ 90s + 41 &\equiv -4 \pmod{25} \\ 90s &\equiv -45 \pmod{25} \\ 18s &\equiv -9 \pmod{5} \\ 2s &\equiv -1 \pmod{5} \\ &\equiv 4 \pmod{5} \\ s &\equiv 2 \pmod{5} \\ &= 5t + 2 \end{aligned}$$

$$\begin{aligned} x &= 90(5t + 2) + 41 \\ &= 450t + 221 \\ &\equiv 221 \pmod{450} \end{aligned}$$

Příklad Řešte lineární kongruenci $1723x \equiv 4321 \pmod{104}$.

Řešení Možným řešením je řešení rovnice

$$x \equiv 4321 \cdot 1723^{\varphi(104)-1} \pmod{104}$$

nicméně úprava pravé části kongruence by vyžadovala značné úsilí. CRT nám dává elegantnější nástroj pro řešení takovýchto případů. Provedeme prvočíselný rozklad $104 = 8 \cdot 13$ a vyjádříme zadanou lineární kongruenci v těchto modulech:

$$\begin{aligned} 3x &\equiv 1 \pmod{8} \\ 7x &\equiv 5 \pmod{13} \end{aligned}$$

CRT nám nyní zajišťuje, že existuje právě jedno řešení této soustavy modulo $8 \cdot 13 = 4321$, což je právě námi hledané řešení. Počítáme tedy:

$$\begin{aligned} 3x &\equiv 1 && \pmod{8} \\ &\equiv 9 && \pmod{8} \\ x &\equiv 3 && \pmod{8} \\ x &= 8k + 3 \end{aligned}$$

$$\begin{aligned} 7x &\equiv 5 && \pmod{13} \\ 7(8k + 3) &\equiv 5 && \pmod{13} \\ 56k &\equiv -16 && \pmod{13} \\ 4k &\equiv \\ k &\equiv -4 && \pmod{13} \\ &= 13t - 4 \end{aligned}$$

$$\begin{aligned} x &= 8k + 3 \\ &= 8(13t - 4) + 3 \\ &= 104t - 29 \\ &\equiv 75 && \pmod{104} \end{aligned}$$

Příklad Řešte $x \equiv 15^{14^{13}} \pmod{11}$.

Řešení

$$
\begin{aligned}
x &\equiv 4^{14^{13}} && \pmod{11} \\
x \equiv 4^t, 4^t &\equiv 4^{14^{13}} && \pmod{11} \\
\iff t &\equiv 4^{13} && \pmod{5}, \text{ kde 5 je řád 4 modulo 11} \\
t \equiv 4^s, 4^s &\equiv 4^{13} && \pmod{5} \\
\iff s &\equiv 1 && \pmod{2}, \text{ kde 2 je řád 4 modulo 5} \\
\Rightarrow t &\equiv 4^1 \equiv 4 \pmod{5} \\
\Rightarrow x &\equiv 4^4 \equiv 3 \pmod{11}
\end{aligned}
$$

1. vnitrosemestrálka

Příklad Nalezněte všechna $k, n \in \mathbb{N}^+$, pro které je číslo $k^{n+2}+2k^n$ prvočíslo.

Řešení Zjevně $k^{n+2} + 2k^n = k(k^{n+1} + 2k^{n-1})$, tzn. $k = \{1\}$. Zároveň platí, že pro $\forall n \in \mathbb{N} : 1^{n+2} + 2 \cdot 1^n = 3$, což je prvočíslo. Tímto jsme dostali naše řešení.

Příklad Řešte soustavu

$$\begin{aligned} 33x &\equiv 45 \pmod{63} \\ 12x &\equiv 5 \pmod{17} \end{aligned}$$

Řešení

$$\begin{aligned} 12x &\equiv 5 \pmod{17} \\ -5x &\equiv 5 \pmod{17} \\ x &\equiv -1 \pmod{17} \\ x &= 17k - 1 \end{aligned}$$

$$\begin{aligned} 33x &\equiv 45 \pmod{63} \\ 11x &\equiv 15 \pmod{21} \\ 11(17k-1) &\equiv 15 \pmod{21} \\ 187k &\equiv 26 \pmod{21} \\ 19k &\equiv 26 \pmod{21} \\ -2k &\equiv 26 \pmod{21} \\ k &\equiv -13 \pmod{21} \\ k &\equiv 8 \pmod{21} \\ k &= 21s + 8 \end{aligned}$$

$$\begin{aligned} x &= 17k - 1 \\ x &= 17(21s + 8) - 1 \\ x &= 357s + 135 \\ x &\equiv 135 \pmod{357} \end{aligned}$$

Příklad Určete poslední dvě cifry čísla $4^{7^{8^9}}$.

Řešení Řešíme lineární kongruenci $x \equiv 4^{7^{8^9}} \pmod{100}$. Využijeme opět obrácenou CRT a provedeme prvočíselný rozklad $100 = 2^2 \cdot 5^2$. Řešením kongruence je tedy řešení soustavy

$$\begin{aligned} x &\equiv 4^{7^{8^9}} \pmod{2^2} \\ x &\equiv 4^{7^{8^9}} \pmod{5^2} \end{aligned}$$

Řešíme

$$\begin{aligned} x &\equiv 4^{7^{8^9}} = (2^2)^{7^{8^9}} && \pmod{2^2} \\ &\equiv 0 && \pmod{2^2} \\ &= 4s \end{aligned}$$

$$\begin{aligned} x &\equiv 4^{7^{8^9}} && \pmod{5^2} \\ 4s &\equiv 4^{7^{8^9}} && \pmod{5^2} \\ s &\equiv 4^{7^{8^9}-1} && \pmod{5^2} \\ s \equiv 4^t, 4^t &\equiv 4^{7^{8^9}-1} && \pmod{5^2} \end{aligned}$$

$$\begin{aligned} \iff t &\equiv 7^{8^9} - 1 && \pmod{10}, \text{ kde } 10 \text{ je řád } 4 \text{ modulo } 5^2 \\ t+1 &\equiv 7^{8^9} && \pmod{10} \\ t+1 \equiv 7^u, 7^u &\equiv 7^{8^9} && \pmod{10} \end{aligned}$$

$$\begin{aligned} \iff u &\equiv 8^9 && \pmod{4}, \text{ kde } 4 \text{ je řád } 7 \text{ modulo } 10 \\ u &\equiv 0 && \pmod{4} \end{aligned}$$

$$\begin{aligned} t+1 &\equiv 3^u = 3^0 = 1 && \pmod{10} \\ t &\equiv 0 && \pmod{10} \end{aligned}$$

$$\begin{aligned} s &\equiv 4^t = 4^0 = 1 && \pmod{25} \\ &= 25v + 1 \end{aligned}$$

$$\begin{aligned} x &= 4s = 4(25v+1) \\ &= 100v + 4 \\ &\equiv 4 \pmod{100} \end{aligned}$$

Příklad Určete poslední dvě cifry čísla $2^{7^{8^9}}$.

Řešení Řešíme lineární kongruenci $x \equiv 2^{7^{8^9}} \pmod{100}$. Využijeme opět obrácenou CRT a provedeme prvočíselný rozklad $100 = 2^2 \cdot 5^2$. Řešením kongruence je tedy řešení soustavy

$$\begin{aligned} x &\equiv 2^{7^{8^9}} \pmod{2^2} \\ x &\equiv 2^{7^{8^9}} \pmod{5^2} \end{aligned}$$

Řešíme

$$\begin{aligned} x &\equiv 2^{7^{8^9}} && \pmod{2^2} \\ &\equiv 2^2 \cdot 2^{7^{8^9}-1} && \pmod{2^2} \\ &\equiv 0 \cdot 2^{7^{8^9}-1} && \pmod{2^2} \\ &\equiv 0 && \pmod{2^2} \\ &= 4s \end{aligned}$$

$$\begin{aligned} x &\equiv 2^{7^{8^9}} && \pmod{5^2} \\ 4s &\equiv 2^{7^{8^9}} && \pmod{5^2} \\ s &\equiv 2^{7^{8^9}-2} && \pmod{5^2} \\ s \equiv 2^t, 2^t &\equiv 2^{7^{8^9}-2} && \pmod{5^2} \end{aligned}$$

$$\begin{aligned} \iff t &\equiv 7^{8^9} - 2 && \pmod{\varphi(25) = 20} \\ t+2 &\equiv 7^{8^9} && \pmod{20} \\ t+2 \equiv 7^u, 7^u &\equiv 7^{8^9} && \pmod{20} \end{aligned}$$

$$\begin{aligned} \iff u &\equiv 8^9 && \pmod{4}, \text{ kde } 4 \text{ je řád } 7 \text{ modulo } 20 \\ &\equiv 4^9 \cdot 2^9 && \pmod{4} \\ &\equiv 4^9 \cdot 0 && \pmod{4} \\ &\equiv 0 && \pmod{4} \end{aligned}$$

$$\begin{aligned} t+2 &\equiv 7^u = 7^0 = 1 && \pmod{20} \\ t &\equiv -1 \equiv 19 && \pmod{20} \end{aligned}$$

$$\begin{aligned} s &\equiv 2^t = 2^{19} && \pmod{25} \\ 2s &\equiv 2^{20} \equiv 1 \equiv 26 && \pmod{25}, \text{ protože } 20 \text{ je kořen } 2 \text{ modulo } 25 \\ s &\equiv 13 && \pmod{25} \\ &= 25v + 13 \end{aligned}$$

$$\begin{aligned} x &= 4s = 4(25v + 13) \\ &= 100v + 52 \\ &\equiv 52 && \pmod{100} \end{aligned}$$

Příklad Vyřešte soustavu kongruencí:

$$\begin{aligned} 20x &\equiv 150 \pmod{250} \\ 11x &\equiv 17 \pmod{21} \end{aligned}$$

Řešení Platí, že $\gcd(20, 250) = 10 \wedge 10 \mid 150$ a $\gcd(11, 21) = 1 \wedge 1 \mid 21$. Obě lineární kongruence tedy mají řešení. Řešíme:

$$\begin{aligned} 20x &\equiv 150 \pmod{250} \,/ : 10 \\ 2x &\equiv 15 \pmod{25} \\ 2x &\equiv 40 \pmod{25} \,/ : 2 \\ x &\equiv 20 \pmod{25} \\ x &= 25s + 20 \end{aligned}$$

$$\begin{aligned} 11x &\equiv 17 \pmod{21} \\ 11(25s + 20) &\equiv 17 \pmod{21} \\ 275s &\equiv -203 \pmod{21} \\ 2s &\equiv -14 \pmod{21} \,/ : 2 \\ s &\equiv -7 \equiv 14 \pmod{21} \\ s &= 21t + 14 \end{aligned}$$

$$\begin{aligned} x &= 25(21t + 14) + 20 \\ x &= 525t + 370 \\ x &\equiv 370 \pmod{525} \end{aligned}$$

5. přednáška

Příklad Drsně a svižně, st 634 - 637, příklady

Příklad **Drsně a svižně, st 636, př 10.91**

Mocněním na -1 (dělením) dostáváme v modulární aritmetice inverzní prvek daného čísla v aktuálním modulu. Tedy $(-9)^{-1} \pmod{41}$ je takové číslo, že

$$(-9)^{-1} \cdot (-9) \equiv 1 \pmod{41}$$

Pokud se tedy vrátíme k našemu příkladu, platí, že

$$-9 \cdot 9 \equiv -81 \equiv 1 \pmod{41}$$

a zjevně tedy $(-9)^{-1} \equiv 9 \pmod{41}$. Pro samotné zjištění inverzního prvku aplikujeme postup z příkladu ze strany 4. Následující ukázka využívá postup s pomocí Bezoutovy věty. Řešíme tedy lineární kongruenci

$$-9x \equiv 1 \pmod{41}$$

Jelikož $(9, 41) = 1$, platí podle Bezoutovy věty

$$\begin{aligned} \exists k, l \in \mathbb{Z} : -9k + 41l &= 1 \\ -9k &\equiv 1 \pmod{41} \end{aligned}$$

Zjevně tedy k je hledaný inverzní prvek k -9 v modulu 41. Zbývá nám nalézt hodnotu k pomocí Euklidova algoritmu:

$$\begin{aligned} 41 &= 4 \cdot 9 + 5 \\ 9 &= 1 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (9 - 1 \cdot 5) \\ &= 2 \cdot 5 - 9 \\ &= 2 \cdot (41 - 4 \cdot 9) - 9 \\ &= 2 \cdot 41 - 9 \cdot 9 \end{aligned}$$

Tedy vidíme, že k je skutečně 9.

2. vnitrosemestrálka

Příklad Určete generující a kontrolní matice lineárního $(8, 3)$-kódu s polynomem $p(x) = x^5 + x^4 + x + 1$. V tomto kódování jste obdrželi kódové slovo 10111011. Určete odeslanou zprávu ze předpokladu, že během přenosu došlo k minimálnímu počtu chyb.[1][2][3]

Řešení Hledáme generující matici $G = \begin{pmatrix} P \\ \mathbb{I}_k \end{pmatrix} = \begin{pmatrix} r_1 & r_2 & r_3 \\ e_1 & e_2 & e_3 \end{pmatrix}$:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 1, \text{ kde } e_i \text{ představuje } k\text{-ární přenášenou zprávu}$$

$$r_1 \equiv e_1 \cdot x^{n-k} \equiv x^5 \equiv x^4 + x + 1 \pmod{p(x)} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = x, \qquad r_2 \equiv x^6 \equiv x^4 + x^2 + 1 \pmod{p(x)} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

$$e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = x^2, \qquad r_3 \equiv x^7 \equiv x^4 + x^3 + 1 \pmod{p(x)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

$$G = \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right), H = \left(\mathbb{I}_{n-k} \; P\right) = \left(\begin{array}{ccccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

[1] Teorie: Drsně a svižně, st 700 - 704

[2] Příklady: Drsně a svižně, st 700, př 11.141

[3] Pro pochopení fungování viz *Poznámky, 1.11.4 – Lineární kódy* a Lineární algebra (klíčová slova: *Jádro zobrazení, faktorové prostory, podprostory (přednášky MB201: 6 a 7)*)

Nyní spočítáme syndrom $\vec{s}$ přijatého slova $\vec{u} = 10111011$ jako $H \cdot \vec{u}$:

$$\vec{s} = H \cdot \vec{u} = \left(\begin{array}{ccccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Syndrom $\vec{s}$ je nenulový, zpráva tedy byla přenesena s chybami. Nejprve nalezneme kódová slova s nejmenší hammingovou vzdáleností od syndromu $\vec{s}$:

Zpráva $\vec{m}$	Kód. slovo $\vec{v} = G \cdot \vec{m}$	Reprezentant $\vec{v} - \vec{s}$	Hamm. vzdálenost
000	00000|000	10001|000	*2*
001	10011|001	00010|001	*2*
010	10101|010	00100|010	*2*
011	00110|011	10111|011	6
100	11001|100	01000|100	*2*
101	01010|101	11011|101	6
110	01100|110	11101|110	6
111	11111|111	01110|111	6

V posledním kroku odečteme od přijatého kódového slova $\vec{u}$ vedoucí reprezentanty $\vec{w}$ s nejmenší hammingovskou vzdáleností od syndromu $\vec{s}$:

Kódové slovo $\vec{u}$	Reprezentant w	$\vec{u} - \vec{w}$	Opravená zpráva $\vec{m}'$
10111|011	10001|000	00110|011	011
10111|011	00010|001	10101|010	010
10111|011	00100|010	10011|001	001
10111|011	01000|100	11111|111	111

Možnými přijatými zprávami tedy jsou $\{000, 010, 001, 111\}$.

1. závěrečná písemka

Příklad Najděte nějaký primitivní kořen modulo 79.

Řešení Pro primitivní kořen g modulo 79 musí platit následující:

1. $g^{\frac{79-1}{2}} \equiv -1 \pmod{79}$
2. $\varphi(79)$ je řádem g modulo 79

Nejprve hledáme kandidátní primitivní kořen podle prvního z požadavků:

1. Testujeme 2 jako kandidátní primitivní kořen modulo 79:
   (a) $2^{39} = 2^{32} \cdot 2^4 \cdot 2^3 = ((((2^2)^2)^2)^2)^2 \cdot (2^2)^2 \cdot 2^3$
   (b) $2^2 \equiv 4 \pmod{79}$
   (c) $2^4 \equiv 4^2 \equiv 16 \pmod{79}$
   (d) $2^8 \equiv 16^2 \equiv 19 \pmod{79}$
   (e) $2^{16} \equiv 19^2 \equiv 45 \pmod{79}$
   (f) $2^{32} \equiv 45^2 \equiv 50 \pmod{79}$
   (g) $2^{39} \equiv 2^{32} \cdot 2^4 \cdot 2^3 \equiv 50 \cdot 16 \cdot 8 \equiv 10 \cdot 8 \equiv 1 \not\equiv -1 \pmod{79}$
2. Testujeme 3 jako kandidátní primitivní kořen modulo 79:
   (a) $3^{39} = 3^{32} \cdot 3^4 \cdot 3^3 = ((((3^2)^2)^2)^2)^2 \cdot (3^2)^2 \cdot 3^3$
   (b) $3^2 \equiv 9 \pmod{79}$
   (c) $3^4 \equiv 9^2 \equiv 2 \pmod{79}$
   (d) $3^8 \equiv 2^2 \equiv 4 \pmod{79}$
   (e) $3^{16} \equiv 4^2 \equiv 16 \pmod{79}$
   (f) $3^{32} \equiv 16^2 \equiv 19 \pmod{79}$
   (g) $3^{39} \equiv 3^{32} \cdot 3^4 \cdot 3^3 \equiv 19 \cdot 2 \cdot 27 \equiv 38 \cdot 27 \equiv -1 \pmod{79}$

3 je kandidátní primitivní kořen modulo 79. Nyní musíme zkontrolovat, že $\varphi(79)$ je řádem r čísla 3 modulo 79. Jelikož platí, že $r \mid \varphi(79)$ a $a^n \equiv 1 \pmod{m} \iff r \mid n$, tak nám stačí pouze zkontrolovat, že pro všechny prvočíselné dělitele d čísla $\varphi(79) = 78 = 2 \cdot 3 \cdot 13$ platí $3^{\varphi(79)/d} \not\equiv 1 \pmod{79}$:

1. $3^{78/2} = 3^{39} \equiv -1 \not\equiv 1 \pmod{79}$
2. $3^{78/3} = 3^{26} \equiv 23 \not\equiv 1 \pmod{79}$
3. $3^{78/13} = 3^6 = 3^4 \cdot 3^2 \equiv 2 \cdot 9 \equiv 18 \not\equiv 1 \pmod{79}$

3 je tedy skutečně primitivním kořenem modulo 79.

Příklad Najděte nějaký primitivní kořen modulo 97.

Řešení Hledáme kandidátní primitivní kořen g splňující $g^{48} \equiv -1 \pmod{97}$.

1. Testujeme 2 jako kandidátní primitivní kořen modulo 79:
   (a) $2^{48} = 2^{32} \cdot 2^{16} = ((((2^2)^2)^2)^2)^2 \cdot (((2^2)^2)^2)^2$
   (b) $2^2 \equiv 4 \pmod{97}$
   (c) $2^4 \equiv 4^2 \equiv 16 \pmod{97}$
   (d) $2^8 \equiv 16^2 \equiv 62 \pmod{97}$
   (e) $2^{16} \equiv 62^2 \equiv 61 \pmod{97}$
   (f) $2^{32} \equiv 61^2 \equiv 35 \pmod{97}$
   (g) $2^{39} \equiv 2^{32} \cdot 2^{16} \equiv 35 \cdot 61 \equiv 1 \not\equiv -1 \pmod{97}$
2. Testujeme 3 jako kandidátní primitivní kořen modulo 79:
   (a) $3^{48} = 3^{32} \cdot 3^{16} = ((((3^2)^2)^2)^2)^2 \cdot (((3^2)^2)^2)^2$
   (b) $3^2 \equiv 9 \pmod{97}$
   (c) $3^4 \equiv 9^2 \equiv 81 \pmod{97}$
   (d) $3^8 \equiv 81^2 \equiv 62 \pmod{97}$
   (e) $3^{16} \equiv 62^2 \equiv 61 \pmod{97}$
   (f) $3^{32} \equiv 61^2 \equiv 35 \pmod{97}$
   (g) $3^{39} \equiv 3^{32} \cdot 3^{16} \equiv 35 \cdot 61 \equiv 1 \not\equiv -1 \pmod{97}$
3. Testujeme 4 jako kandidátní primitivní kořen modulo 79:
   (a) $4^{48} = (2^{48})^2 \equiv 1^2 = 1 \not\equiv -1 \pmod{97}$
4. Testujeme 5 jako kandidátní primitivní kořen modulo 79:
   (a) $5^{48} = 5^{32} \cdot 5^{16} = ((((5^2)^2)^2)^2)^2 \cdot (((5^2)^2)^2)^2$
   (b) $5^2 \equiv 25 \pmod{97}$
   (c) $5^4 \equiv 25^2 \equiv 43 \pmod{97}$
   (d) $5^8 \equiv 43^2 \equiv 6 \pmod{97}$
   (e) $5^{16} \equiv 6^2 \equiv 36 \pmod{97}$
   (f) $5^{32} \equiv 36^2 \equiv 35 \pmod{97}$

(g) $5^{39} \equiv 5^{32} \cdot 5^{16} \equiv 36 \cdot 35 \equiv -1 \pmod{97}$

5 je kandidátní primitivní kořen modulo 97. Nyní musíme zkontrolovat, že pro všechny prvočíselné dělitele d čísla $\varphi(97) = 96 = 2^5 \cdot 3$ platí $3^{\varphi(97)/d} \not\equiv 1 \pmod{97}$:

1. $5^{96/2} = 5^{48} \equiv -1 \not\equiv 1 \pmod{79}$
2. $5^{96/3} = 5^{32} \equiv 35 \not\equiv 1 \pmod{79}$

5 je tedy skutečně primitivním kořenem modulo 79.

Příklad Najděte všechna čísla, která mohou být $\mathsf{gcd}\big((5n+4),(8n+1)\big)$ pro nějaké $n \in \mathbb{Z}$.

Řešení Platí, že gcd čísel musí dělit libovolnou jejich lineární kombinaci, tedy i

$$8(5n+4) - 5(8n+1) = 32 - 5 = 27$$

Řešením tedy mohou být všechny kladné dělitele 27 (tzn $\{1, 3, 9, 27\}$), přičemž vidíme, že skutečně jsou:

$$\begin{array}{rrcl} n = 0: & \mathsf{gcd}(4,\,1) & = & 1 \\ n = 1: & \mathsf{gcd}(9,\,9) & = & 9 \\ n = 4: & \mathsf{gcd}(24,\,33) & = & 3 \\ n = 10: & \mathsf{gcd}(54,\,81) & = & 27 \end{array}$$

Příklad Najděte všechna čísla, která mohou být $\mathsf{gcd}\big((5n+6),(8n+7)\big)$ pro nějaké $n \in \mathbb{Z}$.

Řešení Platí, že gcd čísel musí dělit libovolnou jejich lineární kombinaci, tedy i

$$8(5n+6) - 5(8n+7) = 48 - 35 = 13$$

Řešením tedy mohou být všechny kladné dělitele 13 (tzn $\{1, 13\}$), přičemž vidíme, že skutečně jsou:

$$\begin{array}{rrcl} n = 0: & \mathsf{gcd}(6,\,7) & = & 1 \\ n = 4: & \mathsf{gcd}(26,\,39) & = & 13 \end{array}$$

Příklad Kolika způsoby lze vybrat 60 kuliček tří barev (červených, modrých a zelených), přičemž počet červených a modrých je sudý?

Řešení Víme, že:

1. $60 \mid (\text{č+m+z}) \Rightarrow 2 \mid (\text{č+m+z}),\ 2 \mid \text{č},\ 2 \mid \text{m}$
2. $2 \mid (\text{č+m+z}) \wedge 2 \mid \text{č} \Rightarrow 2 \mid (\text{m+z})$
3. $2 \mid (\text{m+z}) \wedge 2 \mid \text{m} \Rightarrow 2 \mid \text{z}$

Z tohoto vyplývá, že počet kuliček každé barvy je sudý a úloha se tedy redukuje na náhodný výběr 30 kuliček tří barev, tzn.:

$$\left(\!\!\binom{3}{30}\!\!\right) = \binom{32}{2}$$

Příklad Určete zbytek čísla $14^{15^{14^{13}}}$ po dělení číslem 80.

Řešení Rovnici můžeme řešit přímo následujícím způsobem[4]:

$$\begin{aligned}
x &\equiv 14^{15^{14^{13}}} \equiv 2^{15^{14^{13}}} \cdot 7^{15^{14^{13}}} && \pmod{80}\ /:16\\
\tfrac{x}{16} &\equiv 2^{15^{14^{13}}-4} \cdot 7^{15^{14^{13}}} && \pmod 5\\
&\equiv 2^{15^{14^{13}}-4} \cdot 2^{15^{14^{13}}} && \pmod 5\\
&\equiv 2^{15^{14^{13}}-4} \cdot 2^{15^{14^{13}}-\varphi(5)} && \pmod 5\\
&\equiv 2^{15^{14^{13}}-4} \cdot 2^{15^{14^{13}}-4} && \pmod 5\\
\tfrac{x}{16} \equiv 4^s, 4^s &\equiv 4^{15^{14^{13}}-4} && \pmod 5\\
\iff s &\equiv 15^{14^{13}} - 4 && \pmod 2, \text{ kde 2 je řád 4 modulo 5}\\
&\equiv 1^{14^{13}} - 4 && \pmod 2\\
&\equiv 1 - 4 \equiv -3 \equiv 1 && \pmod 2\\
\tfrac{x}{16} &\equiv 4^1 \equiv 4 && \pmod 5\ /\cdot 16\\
x &\equiv 64 && \pmod{80}
\end{aligned}$$

[4] http://forum.matematika.cz/viewtopic.php?pid=434615#p434615

Řešení Řešíme lineární kongruenci $x \equiv 14^{15^{14^{13}}} \pmod{80}$. Využijeme obrácenou CRT a provedeme prvočíselný rozklad $80 = 2^4 \cdot 5$. Řešením kongruence je tedy řešení soustavy

$$\begin{aligned} x &\equiv 14^{15^{14^{13}}} \pmod{5} \\ x &\equiv 14^{15^{14^{13}}} \pmod{2^4} \end{aligned}$$

Řešíme

$$\begin{aligned} x &\equiv 14^{15^{14^{13}}} && \pmod{5} \\ &\equiv (-1)^{15^{14^{13}}} && \pmod{5}, \text{ přičemž exponent } 15^n \text{ je lichý} \\ &\equiv -1 && \pmod{5} \\ x &= 5s - 1 \end{aligned}$$

$$\begin{aligned} x &\equiv 14^{15^{14^{13}}} && \pmod{2^4 = 16} \\ &\equiv (-2)^{15^{14^{13}}} && \pmod{16} \\ &\equiv (-2)^4 \cdot (-2)^{15^{14^{13}}-4} && \pmod{16} \\ &\equiv 16 \cdot (-2)^{15^{14^{13}}-4} && \pmod{16} \\ &\equiv 0 && \pmod{16} \\ 5s - 1 &\equiv 0 && \pmod{16} \\ 5s &\equiv 1 \equiv -15 && \pmod{16} \ / : 5 \\ s &\equiv -3 && \pmod{16} \\ s &= 16t - 3 \end{aligned}$$

$$\begin{aligned} x &= 5s - 1 \\ &= 5(16t - 3) - 1 \\ &= 80t - 16 \\ x &\equiv -16 \equiv 64 \pmod{80} \end{aligned}$$

2. závěrečná písemka

Příklad V šifře ElGamal zveřejnil Honza klíč $(53, 3, 12)$. Následně přijal od Martina šifru $(2, 17)$. Jakou zprávu Martin odeslal?

Řešení Honza zasílá:

1. $p = 53$
2. $g = 3$
3. $h = g^a = 3^a \equiv 12 \pmod{53}$

Martin zasílá:

1. $C_1 = g^b \equiv 2 \pmod{53}$
2. $C_2 = M \cdot h^b \equiv M \cdot g^{a \cdot b} \equiv 17 \pmod{53}$

Nejprve nalezneme a, tzn vypočítáme diskrétní logaritmus 19 pro primitivní kořen 2 v modulu 83:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{53} \\ 3^2 &\equiv 9 \pmod{53} \\ 3^3 &\equiv 27 \pmod{53} \\ &\dots \\ 3^{19} &\equiv -19 \pmod{53} \\ 3^{20} &\equiv -4 \pmod{53} \\ 3^{21} &\equiv -12 \pmod{53} \end{aligned}$$

Diskrétní logaritmus 12 pro primitivní kořen 3 v modulu 53 je tedy $21 + \frac{53-1}{2} = 47$. Následně hledáme hodnotu $g^{a \cdot b}$. Počítáme tedy rovnici $C_1^a = (g^b)^a \equiv 2^{47} \pmod{53}$:

1. $2^{47} = 2^{32} \cdot 2^8 \cdot 2^4 \cdot 2^3 = ((((2^2)^2)^2)^2)^2 \cdot ((2^2)^2)^2 \cdot (2^2)^2 \cdot 2^3$
2. $2^2 \equiv 4 \pmod{53}$
3. $2^4 \equiv 4^2 \equiv 16 \pmod{53}$

4. $2^8 \equiv 16^2 \equiv 256 \equiv -9 \pmod{53}$

5. $2^{16} \equiv (-9)^2 \equiv 28 \pmod{53}$

6. $2^{32} \equiv 28^2 \equiv -11 \pmod{53}$

7. $$\begin{aligned} 2^{47} &= 2^{32} \cdot 2^8 \cdot 2^4 \cdot 2^3 = (-11) \cdot (-9) \cdot 16 \cdot 8 \\ &\equiv -7 \cdot 16 \cdot 8 \equiv -6 \cdot 8 \equiv 5 \pmod{53} \end{aligned}$$

Nyní hledáme hodnotu $(g^{a \cdot b})^{-1} \equiv (C_1^a)^{-1} \equiv 5^{-1} \pmod{53}$. Hledáme tedy prvek k takový, že

$$5k \equiv 1 \pmod{53}$$
$$5k + 53l = 1$$

Uvedené hodnoty $k, l \in \mathbb{Z}$ existují podle Bezoutovy věty a spočítáme je pomocí rozšířeného Euklidova algoritmu:

$$\begin{aligned} 53 &= 10 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 1 &= 1 \cdot 3 - 1 \cdot 2 \\ &= 1 \cdot 3 - 1 \cdot (1 \cdot 5 - 1 \cdot 3) \\ &= 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (1 \cdot 53 - 10 \cdot 5) - 1 \cdot 5 \\ &= 2 \cdot 53 - 21 \cdot 5 \end{aligned}$$

Hledaná hodnota je tedy $5^{-1} \equiv -21 \pmod{53}$. Následně spočítáme $M = C_2 \cdot (C_1^a)^{-1} \equiv 17 \cdot (-21) \equiv 14 \pmod{53}$. Hledaná zpráva M je tedy 14. Zkouška: $M \cdot g^{a \cdot b} \equiv 14 \cdot 5 \equiv 17 \pmod{53}$

Příklad Kolika způsoby lze vybrat 80 kuliček čtyř barev (červených, modrých, zelených a žlutých), přičemž součet počtu červených a modrých i zelených a žlutých je sudý?

Řešení

$$\begin{aligned} \sum_{0 \leqslant n \leqslant 80, 2 \mid n} \left(\!\!\binom{2}{n}\!\!\right) \cdot \left(\!\!\binom{2}{80-n}\!\!\right) &= \sum_{0 \leqslant n \leqslant 80, 2 \mid n} \binom{n+1}{1} \cdot \binom{81-n}{1} \\ &= \sum_{n=0}^{40} (2n+1) \cdot (81-2n) \\ &= \sum_{n=0}^{40} -4n^2 + 160n + 81 = 45961 \end{aligned}$$

Kryptografie

Příklad 10.87 Šifrou RSA s veřejným klíčem $(7, 33)$ byla poslána čísla $29, 7, 21$. Prolomte šifru.

Řešení Veřejný RSA klíč:

$$\begin{aligned} e &= 7 \\ n = p \cdot q &= 33 \end{aligned}$$

V prvním kroku provedeme prvočíselný rozklad n na $n = p \cdot q = 11 \cdot 3$. Toto nám umožňuje vypočítat $\varphi(n)$:

$$\begin{aligned} \varphi(n) &= \varphi(p) \cdot \varphi(q) \\ &= 10 \cdot 2 = 20 \end{aligned}$$

S touto znalostí jsme již schopni spočítat soukromý klíč $d, e \cdot d \equiv 1 \pmod{\varphi(n)}$:

$$\begin{aligned} e \cdot d &\equiv 1 && (\text{mod } \varphi(n) = 20) \\ 7d &\equiv 1 && (\text{mod } 20) \\ &\equiv 21 && (\text{mod } 20) \ / : 7 \\ d &\equiv 3 && (\text{mod } 20) \end{aligned}$$

Se znalostí soukromého klíče můžeme nyní dešifrovat zadané zprávy:

$$\begin{aligned} 29^d &\equiv 29^3 \equiv (-4)^3 \equiv 2 && (\text{mod } n = 33) \\ 7^d &\equiv 7^3 \equiv 13 && (\text{mod } 33) \\ 21^d &\equiv 21^3 \equiv 21 && (\text{mod } 33) \end{aligned}$$

Příklad 10.92 V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23, q = 31$. Veřejným klíčem je pak $n = pq = 713$. Zašifrujte pro Alici zprávu $M = 327$ a ukažte, jak bude Alice tuto zprávu dešifrovat.

Řešení Nejprve demonstrujeme šifrování:

$$C \equiv M^2 \equiv 327^2 \equiv 692 \pmod{n = 713}$$

V následujícím kroku tuto zprávu opět dešifrujeme.

Nejprve vyřešíme soustavu

$$\begin{aligned} r &\equiv C^{\frac{p+1}{4}} \pmod{p = 23} \\ s &\equiv C^{\frac{q+1}{4}} \pmod{q = 31} \end{aligned}$$

Řešíme:

$$\begin{aligned} r &\equiv 692^{\frac{24}{4}} \equiv 2^6 \equiv 18 \pmod{23} \\ s &\equiv 692^{\frac{32}{4}} \equiv 10^8 \equiv 14 \pmod{31} \end{aligned}$$

Následně hledáme pomocí Euklidova algoritmu $a, b \in \mathbb{Z}$ takové, že

$$a \cdot p + b \cdot q = 1$$

Existenci a, b nám zajišťuje Bezoutova věta. Řešíme:

$$\begin{aligned} 31 &= 1 \cdot 23 + 8 \\ 23 &= 2 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 1 &= 1 \cdot 8 - 1 \cdot 7 \\ &= 1 \cdot 8 - 1 \cdot (1 \cdot 23 - 2 \cdot 8) \\ &= 3 \cdot 8 - 1 \cdot 23 \\ &= 3 \cdot (1 \cdot 31 - 1 \cdot 23) - 1 \cdot 23 \\ &= 3 \cdot 31 - 4 \cdot 23 \end{aligned}$$

Hledaná a, b jsou tedy $-4, 3$. Množina možných řešení je pak

$$\begin{aligned} \pm aps \pm bqr &\equiv \pm(-4 \cdot 23 \cdot 14) \pm (3 \cdot 31 \cdot 18) \pmod{n = 713} \\ &\equiv \pm 138 \pm 248 \pmod{713} \end{aligned}$$

Řešíme:

1. $+138 + 248 \equiv 386 \pmod{713}$
2. $-138 + 248 \equiv 110 \pmod{713}$
3. $+138 - 248 \equiv 603 \pmod{713}$
4. $-138 - 248 \equiv 327 \pmod{713}$

Příklad V šifře ElGamal zveřejnil Honza klíč $(83, 2, 19)$. Následně přijal od Martina šifru $(3, 16)$. Jakou zprávu Martin odeslal?

Řešení Honza zasílá:

1. $p = 83$
2. $g = 2$
3. $h = g^a = 2^a \equiv 19 \pmod{83}$

Martin zasílá:

1. $C_1 = g^b \equiv 3 \pmod{83}$
2. $C_2 = M \cdot h^b \equiv M \cdot g^{a \cdot b} \equiv 16 \pmod{83}$

Nejprve nalezneme a, tzn vypočítáme diskrétní logaritmus 19 pro primitivní kořen 2 v modulu 83:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{83} \\ 2^2 &\equiv 4 \pmod{83} \\ 2^3 &\equiv 8 \pmod{83} \\ 2^4 &\equiv 16 \pmod{83} \\ 2^5 &\equiv 32 \pmod{83} \\ 2^6 &\equiv 64 \pmod{83} \\ &\equiv -19 \pmod{83} \end{aligned}$$

Diskrétní logaritmus 19 pro primitivní kořen 2 v modulu 83 je tedy $6 + \frac{83-1}{2} = 47$. Následně hledáme hodnotu $g^{a \cdot b}$. Počítáme tedy rovnici $C_1^a = (g^b)^a \equiv 3^{47} \pmod{83}$:

1. $3^{47} = 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3^3$
2. $3^2 \equiv 9 \pmod{83}$
3. $3^4 \equiv 9^2 \equiv 81 \equiv -2 \pmod{83}$
4. $3^8 \equiv (-2)^2 \equiv 4 \pmod{83}$

5. $3^{16} \equiv 4^2 \equiv 16 \pmod{83}$

6. $3^{32} \equiv 16^2 \equiv 256 \equiv 7 \pmod{83}$

7. $3^{47} = 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3^3 = 7 \cdot 4 \cdot (-2) \cdot 27 \equiv -56 \cdot 27 \equiv 27^2 \equiv 65 \pmod{83}$

Nyní hledáme hodnotu $(g^{a \cdot b})^{-1} \equiv (C_1^a)^{-1} \equiv 65^{-1} \pmod{83}$. Hledáme tedy prvek k takový, že

$$65k \equiv 1 \pmod{83}$$
$$65k + 83l = 1$$

Uvedené hodnoty $k, l \in \mathbb{Z}$ existují podle Bezoutovy věty a spočítáme je pomocí rozšířeného Euklidova algoritmu:

$$\begin{aligned} 83 &= 1 \cdot 65 + 8 \\ 65 &= 3 \cdot 18 + 7 \\ 18 &= 1 \cdot 11 + 7 \\ 11 &= 1 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 1 \cdot 4 - 1 \cdot 3 \\ &= 1 \cdot 4 - 1 \cdot (1 \cdot 7 - 1 \cdot 4) \\ &= 2 \cdot 4 - 1 \cdot 7 \\ &= 2 \cdot (1 \cdot 11 - 1 \cdot 7) - 1 \cdot 7 \\ &= 2 \cdot 11 - 3 \cdot 7 \\ &= 2 \cdot 11 - 3 \cdot (1 \cdot 18 - 1 \cdot 11) \\ &= 5 \cdot 11 - 3 \cdot 18 \\ &= 5 \cdot (1 \cdot 65 - 3 \cdot 18) - 3 \cdot 18 \\ &= 5 \cdot 65 - 18 \cdot 18 \\ &= 5 \cdot 65 - 18 \cdot (1 \cdot 83 - 1 \cdot 65) \\ &= 23 \cdot 65 - 18 \cdot 83 \end{aligned}$$

Hledaná hodnota je tedy $65^{-1} \equiv 23 \pmod{83}$. Následně spočítáme $M = C_2 \cdot (C_1^a)^{-1} \equiv 16 \cdot 23 \equiv 36 \pmod{83}$. Hledaná zpráva M je tedy 36. Zkouška: $M \cdot g^{a \cdot b} \equiv 36 \cdot 65 \equiv 16 \pmod{83}$