Cvičení MB204 Teorie čísel

Úvod

Podmínky zápočtu atd.

1. Dělitelnost

1.1. Nalezněte všechna celá čísla $a \neq 3$, pro která platí $a-3|a^3-3$.

Řešení. $a-3|a^3-27$ a proto $a-3|a^3-3 \Leftrightarrow a-3|a^3-3-a^3+27=24$. □

1.2. Pro která celá čísla n je $7n+1$ dělitelné $3n+4$?

Řešení. $3n+4|7n+1 \Rightarrow 3n+4|7(3n+4)-3(7n+1)=25$. Odtud $n \in \{-3,-1,7\}$ □

1.3. Dokažte, že pro všechna celá čísla a, b platí $17|2a+3b \Leftrightarrow 17|9a+5b$.

Řešení. $2a+3b=4(9a+5b)-17(2a+b)$. Koeficienty lze odvodit z Bezoutových koeficientů (Euclid). □

1.4. Dokažte, že pro všechna přirozená čísla n platí $9|4^n+15n-1$

Řešení. Indukcí nebo Binomickou větou. □

2. Dělení se zbytkem, GCD, LCM, Euklidův algoritmus, Bezoutova věta

2.1. Dokažte, že mezi m po sobě jdoucími čísly existuje právě jedno dělitelné m.

Řešení. Označme čísla $a+1,\dots,a+m$. Podle věty o dělení se zbytkem $\exists! q, r < m : a = q.m + r$. Pak $a+(m-r)=m(q+1)$ je hledané číslo. Ostatní nenulový zbytek. □

2.2. Určete největší společný dělitel $(21, 98)$ a najděte koeficienty v Bezoutově rovnosti.

Řešení. $(21, 98) = 7 = 5.21 - 98$. □

2.3. Určete největší společný dělitel $(10175, 2277)$ a najděte koeficienty v Bezoutově rovnosti.

Řešení. $(10175, 2277) = 11 = (-32).10175 + 143.2277$. □

2.4. Určete největší společný dělitel $(2n+1, 9n+4)$ a $(2n-1, 9n+4)$.

Řešení. $(2n+1, 9n+4) = (2n+1, n) = (n, 1) = 1$ a $(2n-1, 9n+4) = (2n+1, n+8) = (-17, n+8)$. Odtud $17|n+8 \Rightarrow GCD = 17$ a $17 \nmid n+8 \Rightarrow GCD = 1$. □

2.5. Určete největší společný dělitel čísel $2^{63}-1$ a $2^{91}-1$.

Řešení. $2^{91}-1 = 2^{28}(2^{63}-1) + 2^{28} - 1$ a $2^{63}-1 = (2^{35}+2^7)(2^{28}-1) + 2^7 - 1$. Protože $2^7-1|2^{28}-1$, je GCD$=2^7-1$. □

2.6. Spočítejte největší společný dělitel tří čísel $(252, 364, 455)$.

Řešení. $455 = 364 + 91, 364 = 4.91$ a $252 = 2.91 + 70, 91 = 70 + 21, 70 = 3.21 + 7, 21 = 3.7$. Odtud $(252, 364, 455) = 7$. □

2.7. Dokažte $(a, b).(c, d) = (ac, ad, bc, bd)$.

Řešení. Označme dělitele d_1, d_2, d_3. Bezout: $\exists k, l : ak+bl = d_1$ a $\exists m, n : cm+dn = d_2$. Odtud $d_1d_2 = km.ac+kn.ad+lm.bc+ln.bd$ a podle Bezouta pro P pak $d_3|d_1d_2$. Naopak zřejmě $d_1|a, d_2|c$, tj. $d_1d_2|ac$ atd. Dohromady $d_1d_2|d_3$.

Nebo: $(ac, ad, bc, bd) = (a(c, d), b(c, d)) = (a, b).(c, d)$. □

2.8. Dokažte $abc = [a,b,c].(ab,ac,bc)$

Řešení. $d := (ab,ac,bc)$. Pak $\frac{abc}{d} \in \mathbb{N}$ a $a,b,c|\frac{abc}{d}$. Odtud $\frac{abc}{d} = q.[a,b,c]$. Dále $q|\frac{ab}{d}, \frac{ac}{d}, \frac{bc}{d}$ a proto $q|(\frac{ab}{d}, \frac{ac}{d}, \frac{bc}{d}) = 1$. □

3. Prvočísla

3.1. Mezi kterými deseti po sobě jdoucími čísly je nejvíce prvočísel?

Řešení. $1,2,.. \rightsquigarrow 4$, $2,3,.. \rightsquigarrow 5$, $3,4,.. \rightsquigarrow 4$, $4,5,.. \rightsquigarrow 4$. Pět sudých, jedno ze tří po sobě jdoucích lichých je vždy dělitelné třemi. □

3.2. Nalezněte všechna prvočísla, která jsou zároveň součtem i rozdílem nějakých dvou prvočísel.

Řešení. Parita dá, že jedno musí být rovno 2. Je tedy $p-2, p, p+2$ prvočísla. Jedno z nich dělitelné třemi. Odtud $p = 5$ □

3.3. Dokažte, že pro žádné n není možné $6n+5$ vyjádřit jako součet dvou prvočísel.

Řešení. Parita dá, že jedno musí být rovno 2. Je tedy $6n+5 = p+2$, tj. $p = 3(2n+1)$. □

3.4. Nalezněte všechna prvočísla p, taková, že i $2p^2+1$ je prvočíslo.

Řešení. Zkusit začátek, pak $p > 3 \Rightarrow p = 3k \pm 1$. Odtud $2p^2+1 = 3(6k^2 \pm 4k + 1)$. □

3.5. Dokažte: $(a,b) = 1 \Rightarrow (a+b, ab) = 1$.

Řešení. Sporem. $(a,b) = 1 \wedge (a+b,ab) \neq 1$. Z druhého $\exists p : p|(a+b) \wedge p|ab$. Z druhého (Euclid) $p|a \vee p|b$. Dohromady $p|a \wedge p|b$, tj. $p|(a,b) = 1$. □

3.6. Dokažte: $(a+b, [a,b]) = (a,b)$.

Řešení. Lze převést na předchozí příklad. $a := \frac{a}{(a,b)}$, $b := \frac{b}{(a,b)}$. □

3.7. Dokažte: a složené $\Rightarrow a|(a-1)!$.

Řešení. Nejprv zkusit pro malá a. Pak: $a = b.c$. Pokud $b \neq c$, pak $1 < b < c < a$, a proto $(a-1)! = 1..b..c..(a-1)$, tj. $a = bc|(a-1)!$. Pokud $b = c$, tj. $a = b^2$, pak z $a = b^2 > 4$ plyne $b > 2$ a tedy i $a = b^2 > 2b$, a proto $(a-1)! = 1..b..2b..(a-1)$. Odtud $a = b^2|(a-1)!$. □

Def. funkce v_p. Pro $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$v_p(a) = \begin{cases} \alpha_i \text{ pokud } p = p_i \\ 0 \text{ jinak} \end{cases}$$

Vlastnosti:

$$\begin{aligned} &\text{součin: } v_p(a.b) = v_p(a) + v_p(b) \\ &\text{součet: } v_p(a+b) = v_p(a), \text{ pokud } v_p(a) < v_p(b) \\ &\qquad\quad\; v_p(a+b) \geq v_p(a), \text{ pokud } v_p(a) = v_p(b) \\ &\text{gcd: } v_p((a,b)) = v_p(a) \\ &\text{lcm: } v_p([a,b]) = v_p(b) \text{ v obou případech } v_p(a) \leq v_p(b) \end{aligned}$$

3.8. Dokažte: $(a,b) = 1 \Rightarrow (ab,c) = (a,c) \cdot (b,c)$.

Řešení. $(a,b) = 1 \Rightarrow min\{v_p(a), v_p(b)\} = 0$. Odtud w.l.o.g. $v_p(0) = 1$. Pak i $v_p((a,c)) = 0$ a tedy

$$v_p(L) = min\{v_p(b), v_p(c)\} = v_p(P).$$

□

3.9. Dokažte, že pokud $\sqrt[m]{n} \in \mathbb{Q}$, pak $\sqrt[m]{n} \in \mathbb{N}$.

Řešení. Předpoklad implikace říká, že existují $r, s \in \mathbb{N}$ tak, že $\sqrt[m]{n} = \frac{r}{s}$, tj. $n \cdot s^m = r^m$. Odtud $v_p(n) + m \cdot v_p(s) = m \cdot v_p(r)$, tj. $m | v_p(n)$. □

Minipísemka

3.10. Spočítejte $GCD(728, 3^{36} - 1, 3^{45} - 1)$ a napište Bezoutovu rovnost.

Řešení. $728 = 3^6 - 1$ a proto $GCD = 3^{(6,36,45)} - 1 = 3^3 - 1 = 26$. □

3.11. Spočítejte $GCD(4095, 2^{42} - 1, 2^{63} - 1)$ a napište Bezoutovu rovnost.

Řešení. $4095 = 2^{12} - 1$ a proto $GCD = 2^{(12,42,63)} - 1 = 2^3 - 1 = 7$. □

4. Kongruence I.

4.1. Spočítejte zbytek po dělení čísla a^b číslem m pro náhodně zvolené a, b, m.

4.2. Dokažte, že pro všechna $k, m, n \in \mathbb{N}$ platí

$$11 | 5^{5k+1} + 4^{5m+2} + 3^{5n}.$$

Řešení. Spočítáme modulární mocniny čísel 3,4,5 a zjistíme $3^5 \equiv 4^5 \equiv 5^5 \equiv 1 \mod 11$. Proto $5^{5k+1} + 4^{5m+2} + 3^{5n} \equiv 5^1 + 4^2 + 3^0 = 22 \equiv 0 \mod 11$. □

4.3. Dokažte, že pro všechna $a, b \in \mathbb{Z}$ platí

$$a^2 + b^2 \equiv 0 \mod 3 \Rightarrow a \equiv b \equiv 0 \mod 3.$$

Řešení. Pokud $a \equiv 0$, pak $a^2 \equiv 0$ a tedy i $b^2 \equiv 0$, tj. $b \equiv 0$. Pokud $a \equiv \pm 1$, pak $a^2 \equiv 1$, a proto $b^2 \equiv -1$, což není možné. (plyne i z malé Fermatovy věty) □

4.4. Dokažte, že pro všechna $a, b \in \mathbb{Z}$ platí

$$a^2 + b^2 \equiv 0 \mod 7 \Rightarrow a \equiv b \equiv 0 \mod 7.$$

Řešení. Pokud $a \equiv 0$, pak $a^2 \equiv 0$ a tedy i $b^2 \equiv 0$, tj. $b \equiv 0$. Pokud $a \equiv \pm 1, \pm 2, \pm 3$, pak $a^2 \equiv 1, 4, 2$, a proto $b^2 \equiv 6, 3, 5$, což není možné. □

4.5. Nalezněte všechna $n \in \mathbb{N}$ tak, že platí $3 | n2^n + 1$.

Řešení. $n2^n + 1 \equiv n(-1)^n + 1 \mod 3$. Odtud buď $n \equiv 0 \mod 2$ a $n \equiv -1 \mod 3$, nebo $n \equiv 1 \mod 2$ a $n \equiv 1 \mod 3$, tj. buď $n \equiv 2 \mod 6$ nebo $n \equiv 1 \mod 6$. □

4.6. Dokažte, že lze po obvodu kružnice rozmístit čísla $1, 2, \cdots, 12$ tak, aby libovolné tři sousední čísla a, b, c splňovaly $13 | b^2 - ac$.

Řešení. Rozmístíme popořadě čísla $2^1, 2^2, \cdots, 2^{12}$ a uvážíme jejich zbytky po dělení 13. Pro tři sousední čísla $2^{k-1}, 2^k, 2^{k+1}$ platí $(2^k)^2 - 2^{k-1} \cdot 2^{k+1} = 0$ a proto i jejich zbytky splňují $b^2 - ac \equiv 0 \mod 13$. Zároveň mocniny 2 vygenerují celou zbytkovou třídu až na nulu, tj. právě čísla $1, 2, \cdots, 12$ (řád 2 modulo 13 je maximální, je to primitivní kořen). Dostáváme

$$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$$

. □

4.7. Úlohy o pokrytí ... např. $f(x, y) = 2x + 3y \mod 7$ přiřadí každé celočíselné souřadnici nějaký zbytek modulo 7 a tím rovinu rozparceluje. Ukazuje to, že rovinu lze beze zbytku pokrýt všemi útvary, které vzniknou spojením sedmi čtverečků odpovídajícím různým zbytkům.

4.8. Odvoďte kritéria dělitelnosti čísly $2, 3, \cdots, 11$.

Řešení. Univerzální kritérium = analýza zbytků mocnin 10^k. Např. pokud

$$a = a_k \cdots a_0 = a_0 + a_1 \cdot 10 + \cdots a_k \cdot 10^k,$$

pak $10 \equiv -1 \mod 11$ dá $a \equiv a_0 - a_1 + \cdots + (-1)^k a_k \mod 11$. Modulo 7 dostaneme $10^0 \equiv 1$, $10^1 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv -1$, $10^4 \equiv -3$, $10^5 \equiv -2$, $10^6 \equiv 1$. Odtud $a \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 +$ atd. $\mod 7$. □

5. Eulerova funkce

5.1. Spočítejte Eulerovu funkci $\varphi(n)$ pro $n = 180, 636, 1000, 1001$.

Řešení. $\varphi(180) = \varphi(2^2.3^2.5) = 2(2-1).3(3-1).(5-1) = 48$. Podobně $\varphi(635) = 504$, $\varphi(1000) = 400$, $\varphi(1001) = 720$. □

5.2. Vyřešte rovnici $\varphi(3^x 5^y) = 600$.

Řešení. $\varphi(3^x 5^y) = 2.3^{x-1}.4.5^{y-1}$ pro $x, y \geq 1$. Odtud $x = 2, y = 3$. □

5.3. Vyřešte rovnici $\varphi(m) = 6$.

Řešení. Pokud $p|m$, pak $p-1|\varphi(m)$. Odtud $m = 2^x 3^y 7^z$, tedy $\varphi(m) = 2^{x-1}.2.3^{y-1}.6.7^{z-1}$ pro pro $x, y, z \geq 1$. Diskuze dělitelnosti dá $x, y \leq 2$ a $z \leq 3$. Dalším rozborem dostaneme $z = 1, y = 0, x = 0$, $z = 1, y = 0, x = 1$, $z = 0, y = 2, x = 0$ a $z = 1, y = 2, x = 1$, tj. $m = 7, 14, 9, 18$. □

5.4. Vyřešte rovnici $\varphi(m) = 14$.

Řešení. 8 a 15 jsou složená, proto $7^2|m$ a tedy $6.7 = 42|\varphi(m)$. Žádné řešení neexistuje. □

5.5. Vyřešte rovnici $\varphi(m) = \frac{m}{2}$.

Řešení. Především $\frac{m}{2} \in \mathbb{Z}$. Položme $m = 2^a t$, kde $2 \nmid t$ a $a \geq 1$. Pak $\varphi(m) = 2^{a-1}\varphi(t)$. Tedy $\varphi(t) = t$, tj. $t = 1$. Řešení je $m = 2^a$ pro $a \geq 1$. □

5.6. Vyřešte rovnici $\varphi(m) = \frac{m}{3}$.

Řešení. Položme $m = 3^a t$, kde $(3, t) = 1$ a $a \geq 1$. Pak $\varphi(m) = 3^{a-1}.2.\varphi(t)$. Tedy $\varphi(t) = \frac{t}{2}$. Z minulého příkladu víme $t = 2^b$. Řešení je $m = 3^a 2^b$ pro $a, b \geq 1$. □

5.7. Vyřešte rovnici $\varphi(pm) = \varphi(m)$.

Řešení. Pokud $p|m$, pak $\varphi(pm) = p\varphi(m)$ a pokud $p \nmid m$, pak $\varphi(pm) = (p-1)\varphi(m)$. Řešením je $p = 2$, m liché. □

6. Eulerova věta

6.1. Jaký zbytek dává a^{100} po dělení číslem 125?

Řešení. Platí $\varphi(125) = 5^2(5-1) = 100$, a proto pro libovolné a nesoudělné s 5 je $a^{100} \equiv 1 \mod 125$. Pokud $5|a$, pak $125|a^{100}$, tj. $a \equiv 0 \mod 125$. □

6.2. Dokažte $2^{341} \equiv 2 \mod 341$.

Řešení. $341 = 11.31$. Podle Eulerovy věty platí $2^{10} \equiv 1 \mod 11$ a $2^{30} \equiv 1 \mod 31$. Proto $2^{341} \equiv 2 \mod 11$ a $2^{341} \equiv 2^{11} \equiv 2 \mod 31$. □

6.3. Určete poslední cifru čísla $37^{37^{37}}$.

Řešení. Platí $\varphi(10) = 4$ a $37^{37} \equiv 1 \mod 4$. Proto $37^{37^{37}} \equiv 37 \equiv 7 \mod 10$. □

6.4. Určete poslední dvě cifry čísla 7^{2014}.

Řešení. Platí $\varphi(100) = 40$ a $(7, 100) = 1$. Proto podle Eulerovy věty platí $7^{40} \equiv 1 \mod 100$. A protože $2014 \equiv 14 \mod 40$, je $7^{2014} \equiv 7^{14}$. Dále máme $7^3 = 343 \equiv 43 \mod 100$ a $7^4 \equiv 43.7 = 301 \equiv 1 \mod 100$, a proto $7^{2014} \equiv 7^{14} \equiv 7^2 = 49$. □

6.5. Dokažte, že číslo $2^{2^{4n+1}} + 7$ je složené.

Řešení. Vyzkoušíme, jaké zbytky dává mocnina čísla 2 modulo malá prvočísla. Zjistíme, že modulo 11 máme $2^{10} \equiv 1$. Zároveň jsou zbytky mocnin 2 modulo 10 periodicky $2, 4, 8, 6$, tj. $2^{4n+1} \equiv 2 \mod 10$. Odtud $2^{2^{4n+1}} + 7 \equiv 2^2 + 7 = 11 \equiv 0 \mod 11$. □

Minipísemka

6.6. Vyřešte nerovnici $\varphi(n) < 6$.

Řešení. Prvočísla $p|n$ musí splňovat $p-1|\varphi(n) \in \{1, 2, 4\}$ ($\varphi(n)$ nemůže být liché). Odtud $n = 2^x 3^y 5^z$. Pro $\varphi(n) = 1$ je pouze $n = 1$ nebo $n = 2$, pro $\varphi(n) = 2$ je $z = 0$ a $x, y \leq 1$, tj. $n = 3$ nebo $n = 6$. Pro $\varphi(n) = 4$ je $z = 1$, $y = 0$ a $x \leq 1$ nebo $z = 0$, $y = 1$ a $x = 2$ nebo $z = 0$, $y = 0$ a $x = 3$, tj. $n = 5, 10, 12, 8$. Celkem $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. □

6.7. Určete poslední dvě cifry čísla $2014^{2013^{2012}}$ (těžké).

Řešení. Protože $\varphi(100) = 40$ a $(2014, 40) = 2$, nelze aplikovat Eulerovu větu přímo, ale dostaneme soustavu $2014^{2013^{2012}} \equiv x \mod 25$ a $x \equiv 0 \mod 4$. Na první už můžeme použít Eulerovu větu. $\varphi(25) = 20$ a tedy $2014^{20} \equiv 14^{20} \equiv 1 \mod 25$. Protože $\varphi(20) = 8$, pro exponent je $2013^{2012} = 1013^{8.26+4} \equiv (-7)^4 \equiv 9^2 \equiv 1 \mod 20$. Odut $2014^{2013^{2012}} \equiv 14 \mod 25$. Máme tedy soustavu $x \equiv 14 \mod 25$ a $x \equiv 0 \mod 4$. Z první je $x \in \{14, 39, 64, 89\} \mod 100$. Aby byla splněna i druhá, musí být $x \equiv 64 \mod 100$. □

7. Lineární kongruence

7.1. Obecné kongruence s jednou neznámou. Postupné dosazování reprezentantů zbytkových tříd.

7.2. Vyřešte $29x \equiv 1 \mod 17$.

Řešení. (a) Euler: $(17, 29) = 1$ a $\varphi(17) = 16 \Rightarrow x \equiv 29^{15} \equiv 12^{15} \mod 17$.
(b) Bezout: Z Euklida $1 = 12.17 - 7.29$, tj. $-7.29 \equiv 1 \mod 17$, a proto $x \equiv -7 \equiv 10$.
(c) Ad hoc: $12x \equiv 1 \equiv 18 \mod 17$, tj. $2x \equiv 3 \equiv 20$, tj. $x \equiv 10 \mod 17$. □

7.3. Vyřešte $14x \equiv 23 \mod 31$.

Řešení. Z Bezouta $1 = 5.31 - 11.14$, tj. $x \equiv 23.(-11) \equiv -5$. Ad hoc: $14x \equiv -8$, tj. $7x \equiv -4 \equiv -35$, tj. $x \equiv -5 \mod 31$. □

7.4. Vyřešte $6x \equiv 27 \mod 12$.

Řešení. $(6, 12) = 6 \nmid 27$. Nemá řešení. □

7.5. Vyřešte $8x \equiv 20 \mod 12$.

Řešení. Vydělením dostaneme ekvivalentní kongruenci $2x \equiv 5 \mod 3$, tj. $x \equiv 1 \mod 3$. Modulo 12 pak jsou 4 řešení $x \equiv 1, 4, 7, 10$. □

8. Soustavy lineárních kongruencí

8.1. Vyřešte

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 8 \mod 11 \end{aligned}$$

Řešení. (a) Pomocí čínské zbytkové věty $x \equiv 2.11.[11]_5^{-1} + 8.5.[5]_{11}^{-1} \mod 55$. Pomocí Bezouta a Euklida zjistíme inverze $[11]_5^{-1} = 1$, $[5]_{11}^{-1} = 9$, tj. $x \equiv 22+360 = 382 \equiv -3 \mod 55$.
(b) Ad hoc: Z první kongruence $x = 5t + 2$ dosadíme do druhé $5t + 2 \equiv 8 \mod 11$, tj. $5t \equiv 6 \equiv -5 \mod 11$, tj. $x \equiv -1 \mod 11$. Dosadíme zpět: $x = 5(11s - 1) + 2 = 55s - 3$. □

8.2. Vyřešte

$$\begin{aligned} 4x &\equiv 3 \mod 7 \\ 5x &\equiv 4 \mod 6 \end{aligned}$$

Řešení. $x \equiv 20 \mod 42$. □

8.3. Vyřešte

$$\begin{aligned} 2x &\equiv a \mod 4 \\ 3x &\equiv 4 \mod 10 \end{aligned}$$

Řešení. $4 \nmid a$ nemá řešení, pokud $4|a$, pak $x \equiv -2 \mod 10$. □

8.4. Vyřešte

$$\begin{aligned} 3x &\equiv 5 \mod 7 \\ 2x &\equiv 3 \mod 5 \\ 3x &\equiv 3 \mod 9 \end{aligned}$$

Řešení. Třetí kongruence je ekvivalentní $x \equiv 1 \mod 3$, tj. $x = 3t + 1$. Dosazením do druhé: $2(3t+1) \equiv 3 \mod 5$, tj. $t \equiv 1 \mod 5$, tj. $t = 5s+1$, tj. $x = 3(5s+1)+1 = 15s + 4$. Dosazením do první: $3(15s + 4) \equiv 5 \mod 7$, tj. $3s \equiv 0$, tj. $s = 7r$. Celkem $x = 15.7r + 4$, neboli $x \equiv 4 \mod 105$. □

8.5. Piráti se hádají o mince $\rightsquigarrow$

$$\begin{aligned} x &\equiv 10 \mod 13 \\ x &\equiv 3 \mod 12 \\ x &\equiv 0 \mod 11 \end{aligned}$$

Řešení. $x \equiv 231 \mod 11.12.13$. □

8.6. Počítání vojaků pomocí čtverců. Např. $x = 55863$ vojáků lze modulárně reprezentovat pomocí čtverců 5×5, 7×7 a 9×9 jako

$$\begin{aligned} x &\equiv 13 \mod 25 \\ x &\equiv 3 \mod 49 \\ x &\equiv 54 \mod 81 \end{aligned}$$

Řešení. $x \equiv 55863 \mod 25.49.81$. □

8.7. CRT reversed: Vyřešte lineární kongruenci $3446x \equiv 8642 \mod 208$.

Řešení. Vydělením dvěma: $1723x \equiv 4321 \mod 104$. Rozděláme na soustavu podle faktorů modulu, tj. $104 = 8.13$ a dostaneme

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

Tu vyřešíme a dostaneme $x \equiv 75 \mod 104$. □

9. Binomické kongruence, primitivní kořeny

9.1. Vyřešte kongruenci $x^5 \equiv 10 \mod 11$.

Řešení. Výčtem:

x	0	1	2	3	4	5	6	7	8	9	10
$x^5 - 10 \mod 11$	1	2	0	2	2	2	0	0	0	2	0

Mocniny $g = 2$ generují celou zbytkovou třídu (bez 0):

k	0	1	2	3	4	5	6	7	8	9	10
$2^k \mod 11$	1	2	4	28	5	10	9	7	3	6	1

a proto $x^5 - 10 \mod 11$ je ekvivalentní $2^{5x_a} \equiv 2^5 \mod 11$ a to je ekvivalentní $5x_a \equiv 5 \mod 10$. Tato lineární kongruence je ekvivalentní kongruenci $x_a \equiv 1 \mod 2$, tj. řešením dané kongruence jsou $x \equiv 2^1, 2^3, 2^5, 2^7, 2^9$, tj. $x \equiv 2, 8, 10, 7, 6$. □

9.2. Najděte primitivní kořeny modulo 23.

Řešení. Protože $\varphi(23) = 22 = 2.11$, tak stačí testovat g^2 a g^{11}.

g	2	3	4	5	6	7	8	9	10	11	12	13
$g^2 \mod 23$	4	9	16	2	13	3	18	12	8	6	6	8
$g^{11} \mod 23$	1	1	1	-1	1	-1	1	1	-1	-1	1	1

g	14	15	16	17	18	19	20	21	22
$g^2 \mod 23$	12	18	3	13	2	16	9	4	1
$g^{11} \mod 23$	-1	-1	1	-1	1	-1	-1	-1	-1

Primitivní kořeny jsou $g = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22$. □

9.3. Dokažte neexistenci primitivních kořenů modulo 8.

Řešení. Protože $\varphi(8) = 4$ tak stačí testovat g^2. Uděláme ale celou tabulku

x	3	5	7
$x^2 \mod 8$	1	1	1
$x^3 \mod 8$	3	5	7
$x^4 \mod 8$	1	1	1

Všechna nesoudělná čísla dávají v druhé mocnině jedničku. □

9.4. Najděte nejmenší primitivní kořen modulo 41 a vyřešte kongruenci $7x^{17} \equiv 11 \mod 41$.

Řešení. Protože $\varphi(41) = 40$ tak stačí testovat g^8 a g^{20}:

g	2	3	4	5	6
$g^8 \mod 8$	10	1	18	18	10
$g^{20} \mod 8$	1	-1	1	1	-1

Máme tedy $g = 6$. Kongruenci upravíme na $x^{17} \equiv 25 \mod 41$ a zjistíme $25 \equiv 6^4$, tj. ekvivalentní kongruence je $17x_a \equiv 4 \mod 40$. Tu rozdělíme podle faktorů modulu na soustavu $x_a \equiv 4 \mod 8$ a $2x_a \equiv 4 \mod 5$. Ta má řešení $x_a \equiv 12 \mod 40$, a proto $x \equiv 6^{12} \equiv 4 \mod 41$. □

9.5. Najděte nejmenší primitivní kořen modulo 17 a vyřešte kongruenci $x^4 \equiv 8 \mod 17$.

Řešení. Zjistíme $g = 3$. $8 = 3^{10}$, a proto máme $4x_a \equiv 10 \mod 16$. Tato kongruence ale nemá řešení, protože $(4, 16) = 4 \nmid 10$. Lze vidět i přímo z kritéria pro řešitelnost binomické kongruence: $8^{16/4} = 8^4 \equiv -1 \mod 17$. □

10. Kvadratické kongruence

10.1. Mějme kongruenci $x^2 \equiv 271 \pmod{323}$. Zjistěte, jestli má řešení a kolik a pak řešení najděte. Přezkoumejte řešitelnost pomocí Legenreova symbolu.

Řešení. Zjistíme $323 = 17 \cdot 19$. Odtud dostaneme ekvivalentní soustavu:

$$x^2 \equiv 271 \equiv -1 \pmod{17}$$

$$x^2 \equiv 271 \equiv 5 \pmod{19}.$$

Pro první je $(-1)^{\frac{17-1}{2}} = 1$, pro druhou $5^{\frac{19-1}{2}} = 5^9 \equiv 1 \pmod{19}$. Každá kongruence má tedy právě dvě řešení, tj. zadaná kongruence má čtyři řešení. Primitivní kořen pro 17 je $g = 3$ (testujeme g^8), pro 19 je $g = 2$ (testujeme g^6 a g^9). Přitom $-1 \equiv 3^8 \pmod{17}$ a $5 \equiv 2^{16} \pmod{19}$. Soustava je tedy ekvivalentní soustavě

$$3^{2x_a} \equiv 3^8 \pmod{17}$$

$$2^{2x_b} \equiv 2^{16} \pmod{19},$$

kde $x \equiv 3^{x_a} \pmod{17}$ a $x \equiv 2^{x_b} \pmod{19}$, tj. $2x_a \equiv 8 \pmod{16}$ a $2x_b \equiv 16 \pmod{18}$. Odtud $x \equiv 3^4 \equiv 13$ nebo $x \equiv 3^{12} \equiv 4 \pmod{17}$ a $x \equiv 2^8 \equiv 9$ nebo $x \equiv 2^{17} \equiv 10 \pmod{19}$. Z Euklidova algoritmu dostaneme Bezoutovu rovnost $1 = 9.17 - 8.19$, a proto je řešenízadané kongruence $x \equiv 9.17.(9 \text{ nebo } 10) - 8.19.(13 \text{ nebo } 4)$, tj. $x \equiv 47, 123, 200$ nebo $276 \pmod{323}$. □

Legendreův symbol. Ověření řešitelnosti kvadratické kongruence bez počítání modulární mocniny. Definice $\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} = \pm 1$. Vlastnosti: $\left(\frac{a.b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$, $a \equiv b \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv -1 \pmod{4} \end{cases},$$

těžší je dokázat

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

a kvadratickou reciprocitu

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \pmod{4} \text{ nebo } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{jinak} \end{cases}$$

V minulém příkladě ihned dostáváme $\left(\frac{-1}{17}\right) = 1$ a $\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{-1}{5}\right) = 1$. Protože $5^{\frac{19+1}{2}} \equiv 5$ a $4 | 19 + 1$, můžeme hned napsat řešení druhé kongruence $\pm 5^{\frac{19+1}{4}} = \pm 5^5 = \pm 9$.

10.2. Nalezněte všechna x taková, že $x^2 \equiv 7 \pmod{43}$.

Řešení. $\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) = -\left(\frac{1}{7}\right) = -1$. Kongruence nemá řešení. □

10.3. Má kongruence $x^2 \equiv 79 \pmod{101}$ řešení?

Řešení. $\left(\frac{79}{101}\right) = \left(\frac{101}{79}\right) = \left(\frac{22}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{11}{79}\right) = \left(\frac{11}{79}\right) = -\left(\frac{79}{11}\right) = \left(\frac{2}{11}\right) = 1$. Kongruence má řešení. □

Jacobiho symbol. Zobecnění Legendreova. Ty samé vlastnosti, nemusí být prvočísla. Je-li symbol 1, pak řešení může i nemusí existovat.

10.4. Má kongruence $x^2 \equiv 38 \pmod{165}$ řešení?

Řešení. Spočítáme nejdřív Jacobiho symbol: $\left(\frac{38}{165}\right) = \left(\frac{2}{165}\right)\left(\frac{19}{165}\right) = -\left(\frac{19}{165}\right) = -\left(\frac{165}{19}\right) = -\left(\frac{13}{19}\right) = -\left(\frac{19}{13}\right) = -\left(\frac{6}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$. řešení může i nemusí existovat. Spočteme jednotlivé Legendrovy symboly. Kongruence je ekvivalentní soustavě

$$x^2 \equiv 38 \equiv 2 \pmod 3$$
$$x^2 \equiv 38 \equiv 3 \pmod 5$$
$$x^2 \equiv 38 \equiv 5 \pmod{11}.$$

Symboly jsou $\left(\frac{2}{3}\right) = -1$, $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ a $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$. Vidíme, že dvě z těchto tří kongruencí nemají řešení, a proto i zadaná kongruence není řešitelná. □

10.5. Spočtěte $\left(\frac{1001}{9907}\right)$ pomocí Legendrových symbolů a pomocí Jacobiho symbolu.

Řešení. L: Potřebujeme faktorizovat! $1001 = 7.11.13$, 9907 je prvočíslo. $\left(\frac{1001}{9907}\right) = \left(\frac{7}{9907}\right)\left(\frac{11}{9907}\right)\left(\frac{13}{9907}\right)$. $\left(\frac{7}{9907}\right) = -\left(\frac{9907}{7}\right) = -\left(\frac{2}{7}\right) = -1$, $\left(\frac{11}{9907}\right) = -\left(\frac{9907}{11}\right) = -\left(\frac{7}{11}\right) = \left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1$ a $\left(\frac{13}{9907}\right) = \left(\frac{9907}{13}\right) = \left(\frac{1}{13}\right) = 1$. Dohromady $\left(\frac{1001}{9907}\right) = -1$.
J: Nepotřebujeme faktorizovat! $\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right) = \left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right) = \left(\frac{449}{103}\right) = \left(\frac{37}{103}\right) = \left(\frac{103}{37}\right) = \left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3 = -1$. □

Použití. Rabinův kryptosystém, Euler-Jacobiho test prvočíselnosti.
Fermatův test N: $a^{N-1} \equiv 1 \pmod N$, Euler-Jacobiho test N: $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right)$. Absolutní Fermatova pseudoprvočísla = Carmichaelova čísla - projdou Fermatovým testem pro každou bázi a. Korseltovo kritérium: $p^2 \nmid N$ Carmichaelovo právě tehdy, když $p|N \Rightarrow p-1|N-1$.

10.6. Ukažte, že 2465 je Carmichaelovo číslo.

Řešení. $2465 = 5.17.29$ a $4, 16, 28|2464$. Podle Fermatovy věty pak $a^{2464} = (a^{616})^4 \equiv 1 \pmod 5$, $a^{2464} = (a^{164})^{16} \equiv 1 \pmod{17}$ a $a^{2464} = (a^{88})^{28} \equiv 1 \pmod{29}$, tj. $a^{2464} \equiv 1 \pmod{5.17.29 = 2465}$. □

10.7. Ukažte, že 341 je Fermatovo pseudoprvočíslo o základu 2 a není Euler-Jacobiho pseudoprvočíslo o základu 2. Ukažte, že 561 je E-J pseudoprvočíslo o základu 2. (pozn.: tyto pseudoprvočísla jsou nejmenší o daném základu)

Řešení. $2^{10} \equiv 1 \pmod{341}$ Proto $2^{340} \equiv 1 \pmod{341}$ i $2^{170} \equiv 1 \pmod{341}$. Zároveň ale $\left(\frac{2}{341}\right) = -1$. Pro 561 máme $2^{280} \equiv 1 \pmod{561} = 1$ a $\left(\frac{2}{561}\right) = 1$. □

10.8. Prolomte šifru ElGammal. Honza zveřejnil klíč $(53, 2, 19)$ a přijal od Martina šifru $(2, 16)$. Jakou zprávu mu Martin poslal?

Řešení. Potřebujeme zjistit Honzův soukromý klíč h. Ten je dán diskrétním logaritmem, $2^h \equiv 19 \pmod{53}$. Počítejme tedy modulární mocniny dvojky modulo 53. Zjistíme $2^{11} \equiv -19 \pmod{53}$. Protože $\left(\frac{2}{53}\right) = -1$, je $2^{26} \equiv -1 \pmod{53}$ a tedy $2^{37} \equiv 19 \pmod{53}$, tj. $h = 37$. Tím je šifra prolomena a protože $19^{-1} \equiv 14 \pmod{53}$, je zpráva $14 \cdot 16 \equiv 47 \pmod{53}$. □

Minipísemka

10.9. Je řešitelná kongruence $x^2 \equiv 72 \pmod{1219}$?

Řešení. $\left(\frac{72}{1219}\right) = \left(\frac{2}{1219}\right)\left(\frac{9}{1219}\right) = (-1)\left(\frac{3}{1219}\right)^2 = -1$. Kongruemce nemá řešení. □

10.10. Je řešitelná kongruence $x^2 \equiv 14 \pmod{1363}$?

Řešení. $\left(\frac{14}{1363}\right) = \left(\frac{2}{1363}\right)\left(\frac{7}{1363}\right) = (-1)\cdot(-1)\left(\frac{1363}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$
Kongruemce nemá řešení. $\square$

11. Kódování