Kongruence

Výsledky úloh

VÝSLEDKY ÚLOH

1. a) $x = -6$; $r = 61$; $\xi = -5$; $\varrho = -4$.
   b) $x = 22$; $r = 6$; $\xi = 22$; $\varrho = 6$.
   c) $x = 0$; $r = 12$; $\xi = 0$; $\varrho = 12$.
   d) $x = -1$; $r = 23$; $\xi = 0$; $\varrho = -12$.

2. Podle definice 2 existuje celé číslo $x \neq 0$ tak, že $a = mx$. Poněvadž $|x| \geqq 1$, bude $|a| = |x|.m \geqq m$.

3. Plyne z definice největšího společného dělitele a úlohy 2.

4. Poněvadž $215 \equiv 5 \bmod 21$ a $79 \equiv -5 \bmod 21$, bude podle (18) $215^{20} \equiv 5^{20} \bmod 21$ a $79^{36} \equiv (-5)^{36} \bmod 21$, takže podle (17) a (16) dostaneme $5.215^{20} - 79^{36} \equiv 5^{20} - (-5)^{36} \bmod 21$. Avšak $5^{20} - (-5)^{36} = 5^{20}(1 - 5^{6}) = 5^{20}(1 - 125^{2})$. Protože $125 \equiv -1 \bmod 21$, bude opět podle (18) $125^{2} \equiv (-1)^{2} \bmod 21$, z čehož dostaneme $1 - 125^{2} \equiv 0 \bmod 21$. Podle (17) tedy bude $5^{20}(1 - 125^{2}) \equiv 0 \bmod 21$. Shrnutím nalezených výsledků dostaneme pak podle (11) $5.215^{20} - 79^{36} \equiv 0 \bmod 21$, tj. dané číslo je dělitelno číslem 21.

5. a) $r = 38$.
   b) $r = 25$.

6. Pro každé celé $k \geqq 1$ je $10^{k} \equiv 0 \bmod 2$, $10^{k} \equiv 0 \bmod 5$ a $10^{k} \equiv 0 \bmod 10$. Podobně pro každé celé $k \geqq 2$ bude $10^{k} \equiv 0 \bmod 4$ a $10^{k} \equiv 0 \bmod 25$ a konečně pro každé celé $k \geqq 3$ bude $10^{k} \equiv 0 \bmod 8$. Užitím dekadického zápisu (19) přirozeného čísla n plyne z posledních kongruencí

podle (17) a (15) $n \equiv a_0 \bmod 2$, $n \equiv a_0 \bmod 5$, $n \equiv a_0 \bmod 10$, $n \equiv (10a_1 + a_0) \bmod 4$, $n \equiv (10a_1 + a_0) \bmod 25$ a $n \equiv (10^2 a_2 + 10a_1 + a_0) \bmod 8$. Z toho vidíme, že o dělitelnosti přirozeného čísla n dvěma, pěti nebo desíti můžeme rozhodnout podle poslední cifry, o dělitelnosti 4 nebo 25 pomocí posledního dvojčíslí a o dělitelnosti 8 pomocí posledního trojčíslí dekadického rozvoje tohoto čísla.

7. a) Pro $n = 2k + 1$ je $n^2 = 4k^2 + 4k + 1$, tedy $n^2 \equiv 1 \bmod 4$, tj. $n^2 \in A_1^{(4)}$.

   b) Poněvadž $3 \nmid n$, bude buďto $n \equiv 1 \bmod 3$, nebo $n \equiv 2 \bmod 3$. Podle (18) bude tedy v prvním případě $n^2 \equiv 1 \bmod 3$ a ve druhém pak $n^2 \equiv 4 \equiv 1 \bmod 3$. V obou případech máme $n^2 \equiv 1 \bmod 3$, tj. $n^2 \in A_1^{(3)}$.

8. a) $a = 1, 5, 7, 11, 13, 17.$
   $k = 1, 6, 3, 6, 3, 2.$

   b) $a = 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.$
   $k = 1, 6, 6, 2, 6, 6, 6, 3, 2, 6, 3, 2.$

9. Nechť lze složené číslo m psát ve tvaru součinu $m = m_1 m_2$, kde $m_1 > 1$, $m_2 > 1$ a $(m_1, m_2) = 1$. Poněvadž $m_1 > 1$, bude $m_2 = \frac{m}{m_1} < m$. Obdobně bude i $m_1 < m$. Mezi čísly 1, 2, 3, ..., $m - 1$ bude tedy jistě ležet číslo m_1 i číslo m_2. Poněvadž $(m - 1)! = 1.2.3. \ldots .(m - 1)$, vidíme, že bude platit $(m - 1)! \equiv 0 \bmod m_1$ i $(m - 1)! \equiv 0 \bmod m_2$. Ježto $(m_1, m_2) = 1$, bude podle věty 20 též $(m - 1)! \equiv 0 \bmod m$.

   Nechť složené číslo m nemůžeme psát ve tvaru součinu dvou nesoudělných čísel větších než jedna. V tomto případě bude číslo m alespoň druhou mocninou jistého prvočísla p, tj. $m = p^\alpha$, kde $\alpha \geqq 2$. Na ní bude třeba rozlišit dva případy.

a) Nechť předně $p = 2$. Poněvadž $m > 4$, bude v tomto případě $\alpha \geqq 3$, takže mezi čísly 1, 2, 3, ..., $2^\alpha - 1$ leží jistě čísla $2^{\alpha-2}$ a $2^{\alpha-1}$. Můžeme proto psát $(2^\alpha - 1)! = 2^{\alpha-2}.2^{\alpha-1}.a = 2^{2\alpha-3}.a = 2^\alpha.2^{\alpha-3}.a$, kde a je jisté celé číslo. Protože $\alpha \geqq 3$, je i $2^{\alpha-3}$ celé číslo, takže z poslední rovnosti plyne $(2^\alpha - 1)! \equiv 0 \bmod 2^\alpha$.

b) Nechť nakonec $p \geqq 3$. Poněvadž $\alpha \geqq 2$, budou mezi čísly 1, 2, 3, ..., $p^\alpha - 1$ jistě ležet čísla $p^{\alpha-1}$ a $2p^{\alpha-1}$, takže můžeme najít opět celé číslo a tak, že platí $(p^\alpha - 1)! = p^{\alpha-1}.2p^{\alpha-1}.a = p^\alpha.p^{\alpha-2}.2a$. Poněvadž $\alpha \geqq 2$, bude číslo $p^{\alpha-2}$ rovněž celé, takže z poslední rovnosti ihned plyne, že $(p^\alpha - 1)! \equiv 0 \bmod p^\alpha$.

10. Položme $a = \underbrace{11\ldots1}_{p \text{ cifer}}$, $b = 123\,456\,789$.

Užijeme-li dekadického zápisu, dostaneme

$$a = 10^{p-1} + 10^{p-2} + \ldots + 10^2 + 10 + 1,$$

$$b = 10^8 + 2.10^7 + 3.10^6 + 4.10^5 + 5.10^4 + 6.10^3 + 7.10^2 + 8.10 + 9.$$

Dále snadno zjistíme, že platí

$$n = a.(10^{8p} + 2.10^{7p} + 3.10^{6p} + 4.10^{5p} + 5.10^{4p} + 6.10^{3p} + 7.10^{2p} + 8.10^p + 9) - b.$$

Podle (39) však bude $10^p \equiv 10 \bmod p$, takže podle (18) dostaneme, že pro každé přirozené k platí $10^{kp} \equiv 10^k \bmod p$.

Bude tedy

$$n \equiv a.(10^8 + 2.10^7 + 3.10^6 + 4.10^5 + 5.10^4 + 6.10^3 + 7.10^2 + 8.10 + 9) - b \bmod p$$

neboli

$$n \equiv ab - b \bmod p.$$

Podle př. 7 je číslo b dělitelno devíti, neboť $s(b) = 45$.

Je tedy $b = 9c$, takže dostaneme konečně

$$n \equiv 9(a - 1)c \bmod p.$$

Pro číslo a dále obdržíme vztah

$10a + 1 = 10^p + 10^{p-1} + 10^{p-2} + \ldots + 10^2 + 10 + 1$, tj.

$$10a + 1 = 10^p + a.$$

Odtud pak plyne, že $9a = 10^p - 1$ neboli $9(a - 1) = 10^p - 10$. Bude tedy

$$n \equiv (10^p - 10).c \bmod p.$$

Podle (39) je však $10^p - 10 \equiv 0 \bmod p$, takže dostáváme konečně $n \equiv 0 \bmod p$, tj. $p \mid n$.

11. a) $x \equiv 209 \bmod 311$;

b) $x \equiv 26 \bmod 243$;

c) $x \equiv 406 \bmod 420$.

12. $k = 8$; $x \equiv 51 \bmod 85$.

13. $k = 6$; $x \equiv 14 \bmod 65$.

14. a) Nechť ξ je řešením kongruence (43), tj. nechť $a\xi + b \equiv 0 \bmod m$. Poněvadž $d \mid m_1$, bude podle věty 18 též $a\xi + b \equiv 0 \bmod d$. Ježto však též $d \mid a$, bude $a\xi \equiv 0 \bmod d$. Z těchto kongruencí pak plyne, že $b \equiv 0 \bmod d$, což je proti předpokladu o číslu b.

b) Bez újmy na obecnosti se můžeme omezit na úplnou soustavu zbytků $\{0, 1, 2, \ldots, m - 1\}$ podle modulu m. Z předpokladů o číslech m, a, b a d plyne, že $d \mid m$, $d \mid a$ a $d \mid b$. Položíme-li $m_1 = \frac{m}{d}$, $a_1 = \frac{a}{d}$ a $b_1 = \frac{b}{d}$, bude zřejmě $(a_1, m_1) = 1$, takže kongruence $a_1 x + b_1 \equiv 0 \bmod m_1$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots,$

$m_1 - 1\}$ právě jedno řešení ξ. Každé řešení této kongruence můžeme pak psát ve tvaru $x = \xi + km_1$, kde k je libovolné celé číslo. Z rovnosti $\frac{ax + b}{m} = \frac{a_1x + b_1}{m_1}$ však dále plyne, že každé řešení kongruence (43) je též řešením kongruence $a_1x + b_1 \equiv 0 \bmod m_1$ a obráceně. Proto každé řešení kongruence (43) má tvar $x = \xi + km_1$. Abychom dostali řešení kongruence (43) z úplné soustavy zbytků $\{0, 1, 2, \ldots, m - 1\}$ podle modulu m, musí být $0 \leqq \xi + km_1 < m$. Přitom je $0 \leqq \xi < m_1$, takže $-m_1 < -\xi \leqq 0$. Sečtením nerovností $0 \leqq \xi + km_1 < m$ a $-m_1 < -\xi \leqq 0$ dostaneme dále $-m_1 < km_1 < m = dm_1$, tj. $-1 < k < d$. Celé číslo k může nabývat pouze d hodnot 0, 1, 2, ..., $d - 1$, což jsme chtěli dokázat.

15. $x \equiv 406 \bmod 420$.

16. a) $x \equiv 1098 \bmod 1825$;
    b) $x \equiv 61\,571 \bmod 228\,150$.

17. a) V úplné soustavě zbytků $\{0, 1, 2, \ldots, 1088\}$ podle modulu 1089 má kongruence devět vzájemně inkongruentních řešení. Těmito řešeními jsou čísla 4, 125, 246, 367, 488, 609, 730, 851 a 972.
    b) V úplné soustavě zbytků $\{0, 1, 2, \ldots, 5858\}$ podle modulu 5859 má kongruence sedm řešení vzájemně inkongruentních podle tohoto modulu. Těmito řešeními jsou čísla 760, 1597, 2434, 3271, 4108, 4945 a 5782.

18. a) $x \equiv 21 \bmod 42$, $y \equiv 14 \bmod 42$, $z \equiv 10 \bmod 42$;
    b) $x \equiv 690 \bmod 910$, $y \equiv 507 \bmod 910$, $z \equiv 631 \bmod 910$.

19. a) $x = 53 + 625k$, $y = 62 + 731k$, k celé;
    b) $x = -111 + 337k$, $y = 35 - 106k$, k celé.

20. Označíme-li a obnos, který máme vyplatit, x počet třikorun a y počet desetikorun, dostaneme neurčitou rovnici

$$3x + 10y = a,$$

přičemž hledáme celá nezáporná čísla x a y, která této rovnici vyhovují. Poněvadž je $(3, 10) = 1$, můžeme najít řešení kongruence $10y \equiv a \bmod 3$. Jedno z řešení této kongruence je zřejmě $y_0 = a$. Položíme-li ještě $x_0 = \frac{a - 10y_0}{3} = -3a$, budou mít všechna řešení vyšetřované neurčité rovnice tvar $x = -3a + 10k$, $y = a - 3k$, kde k probíhá množinou všech celých čísel. Ke splnění podmínek $x \geqq 0$ a $y \geqq 0$ je třeba volit k tak, aby platilo současně

$$-3a + 10k \geqq 0, \quad a - 3k \geqq 0.$$

Pro celé číslo k tedy budeme mít nerovnosti

$$\frac{3a}{10} \leqq k \leqq \frac{a}{3}.$$

Snadno nahlédneme, že pro $a = 18$, 19 nebo 20 vyhovuje těmto nerovnostem jediné číslo $k = 6$, pro $a = 21$, 22 nebo 23 pouze $k = 7$, pro $a = 24$, 25 nebo 26 pouze $k = 8$ a konečně pro $a = 27$, 28 nebo 29 pouze $k = 9$. Pro $a = 30$ dostaneme $k = 9$ nebo $k = 10$, takže dané neurčitá rovnice s doplňujícími podmínkami $x \geqq 0$, $y \geqq 0$ bude mít v tomto případě dvě řešení.

Je-li $a > 30$, je $\frac{a}{3} - \frac{3a}{10} = \frac{a}{30} > 1$, takže mezi čísly $\frac{3a}{10}$ a $\frac{a}{3}$ včetně bude ležet vždy alespoň jedno celé číslo k. Pro tato čísla a má tedy vyšetřovaná neurčitá rovnice vždy alespoň jedno řešení požadovaných vlastností.

Jednoduchým výpočtem se můžeme přesvědčit, že pro $a = 1$, 2, 4, 5, 7, 8, 11, 14 nebo 17 nemá úloha žádné

řešení, neboť neexistuje celé číslo k vyhovující požadovaným nerovnostem. Např. pro $a = 17$ bychom pro celé číslo dostali podmínky $\frac{51}{10} \leqq k \leqq \frac{17}{3}$, tj. $5 < k < 6$, což nelze splnit.

21. a) $\left(\frac{322}{307}\right) = 1$; b) $\left(\frac{623}{179}\right) = -1$; c) $\left(\frac{62}{83}\right) = -1$; d) $\left(\frac{-10}{659}\right) = 1$.

22. $x_1 \equiv 32 \bmod 109$, $x_2 \equiv 77 \bmod 109$.

23. $x_1 \equiv 16 \bmod 83$, $x_2 \equiv 67 \bmod 83$.

24. Kvadratická kongruence nemá řešení.

25. $D \equiv 37 \bmod 71$; $x_1 \equiv 12 \bmod 71$; $x_2 \equiv 54 \bmod 71$.

26. $D \equiv 0 \bmod 353$; existuje jediné řešení $x_1 \equiv 47 \bmod 353$.

27. $D \equiv 412 \bmod 571$; kongruence nemá žádné řešení.

28. Sestrojíme absolutně nejmenší zbytky při dělení prvočíslem p postupně k číslům $2, 4, 6, \ldots, 2.\frac{p-1}{2}$. Nechť prvočíslo p má tvar $p = 4m + s$, kde $s = 1$ nebo $s = 3$. Potom pro $k = 1, 2, \ldots, m$ bude zřejmě $\xi_k = 0$, $\varrho_k = 2k$. Avšak pro $k = m + 1, m + 2, \ldots, \frac{p-1}{2}$ bude $\xi_k = 1$ a $\varrho_k = 2k - p$, tedy $2m + 2 - p \leqq \varrho_k \leqq -1$. Snadno zjistíme, že $2m + 2 - p = 2m + 2 - 4m - s = -2m + 2 - s = -\frac{p-s}{2} + 2 - s = -\frac{p}{2} + 2 - \frac{s}{2} > -\frac{p}{2}$, takže pro tato k bude skutečně $-\frac{p}{2} < \varrho_k < 0$. Bude proto

$$v = \frac{p-1}{2} - m = 2m + \frac{s-1}{2} - m = m + \frac{s-1}{2}.$$

Avšak

$$\frac{p^2-1}{8} - v = \frac{16m^2 + 8ms + s^2 - 1}{8} - m - \frac{s-1}{2} =$$

$$= 2m^2 + m(s-1) + \frac{s^2-1}{8} - \frac{s-1}{2}$$

a poněvadž pro $s = 1$ i pro $s = 3$ je $\frac{s^2-1}{8} - \frac{s-1}{2} = 0$ a $s - 1$ je v obou případech sudé číslo, bude

$$(-1)^{\frac{p^2-1}{8} - v} = 1.$$

Odtud a ze vztahu (86) plyne

$$\left(\frac{2}{p}\right) = (-1)^v = (-1)^{\frac{p^2-1}{8}}.$$

což bylo dokázat.

29. Důkaz provedeme nepřímý. Předpokládejme, že daná kongruence má řešení x_1. Bude tedy $x_1^{p-1} + 1 \equiv 0 \bmod m$. Poněvadž však $p|m$, bude podle věty 18 též

$$x_1^{p-1} + 1 \equiv 0 \bmod p. \tag{95}$$

Je-li $x_1 \equiv 0 \bmod p$, plyne z této kongruence $1 \equiv 0 \bmod p$, což není možné. Jestliže však $x_1 \not\equiv 0 \bmod p$, bude podle (38) $x_1^{p-1} + 1 \equiv 1 + 1 \bmod p$, takže z kongruence (95) plyne $2 \equiv 0 \bmod p$. To rovněž není možné, neboť $p > 2$.

V obou případech tedy docházíme ke sporu, čímž je tvrzení úlohy 29 dokázáno.