1 Základné pojmy

5. Najprv dokážeme, že
$$(a,b)=1,(a,c)=1 \;\Rightarrow\; (a,bc)=1 \tag{1}$$
Existujú x,y,z,w tak, že $ax+by=1$, $az+cw=1$. Potom $abz+bcw=b$ a $ax+by=ax+(abz+bcw)y=ax+abyz+bcwy=a(x+byz)+bc.wy=1$. Potom $(a,bc)=1$ podľa cvičenia 2.

Ďalej dokážeme
$$(a,b_j)=1 \text{ pre } j=1,\dots,m \;\Rightarrow\; (a,b_1\dots b_m)=1 \tag{2}$$
indukciou vzhľadom na m. Pre $m=1$ to je vlastne (1). Nech (2) platí pre m, ukážeme, že platí pre $m+1$. Ak $(a,b_j)=1$ pre $j=1,\dots,m+1$, tak $(a,b_1\dots b_m)=1$ (indukčný predpoklad) a súčasne $(a,b_{m+1})=1$. Podľa (1) potom $(a,b_1\dots b_mb_{m+1})=1$.

Zostáva dokázať
$$(a_i,b_j)=1 \text{ pre } i=1,\dots,n, j=1,\dots,m \;\Rightarrow\; (a_1\dots a_n,b_1\dots b_m)=1. \tag{3}$$
Môžeme opäť použiť indukciu vzhľadom na n alebo jednoducho vymeniť úlohy a_i a b_j v (2). (Pomocou (2) dostaneme najprv, že $(b_1\dots b_m,a_i)=1$ pre všetky prípustné i a z toho vyplýva, že $(b_1\dots b_m,a_1\dots a_n)=1$.)

7. Ak $a\neq 0$, $b\neq 0$, tak (a,b) existuje. Označme $d:=(a,b)$.
$\boxed{\Rightarrow}$ $d\mid a$, $d\mid b \Rightarrow d\mid ax+by=c$
$\boxed{\Leftarrow}$ Nech $d\mid c$. Potom $c=c'd$. Keďže $d=(a,b)$, existujú $u,v\in\mathbb{Z}$ tak, že $d=au+bv$. Potom $c=c'd=ac'u+bc'v$, čiže $x=c'u$, $y=c'v$ je riešenie rovnice $ax+by=d$.

Ešte popíšeme ako vyzerá množina riešení rovnice
$$ax+by=c \tag{4}$$
Nech x_0, y_0 je nejaké riešenie tejto rovnice a x, y je ľubovoľné iné jej riešenie . Potom $a(x-x_0)+b(y-y_0)=ax+by-(ax_0+by_0)=0$ a $a(x-x_0)=-b(y-y_0)$. Vydelením tejto rovnice číslom d dostaneme
$$\frac{a}{d}(x-x_0)=-\frac{b}{d}(y-y_0).$$
$\left(\frac{a}{d},\frac{b}{d}\right)=1$ (inak by mali väčšieho spoločného deliteľa). Potom $\frac{a}{d}\mid y-y_0$ a $\frac{b}{d}\mid x-x_0$ (veta z prednášky), t.j. $x-x_0=t.\frac{b}{d}$, $y-y_0=s.\frac{a}{d}$. Dostaneme teda, že každé riešenie možno vyjadriť ako
$$x=x_0+\frac{b}{d}t \qquad y=y_0-\frac{a}{d}t,$$
kde parametre $t,u\in\mathbb{Z}$. (Ľahko sa overí, že je to skutočne riešenie.)

8. Ak mám v niektorej nádobe x litrov a $x\leq 13$, tak viem odmerať aj $x+4$ litrov. (x dám do 13litrovej nádoby, naplním 17l nádobu. Koľko sa zmestí prelejem do 13l nádoby a v 17l mi zostane $x+4$ litrov.)

Ak mám x litrov a $x\geq 13$, tak viem dostať $x-13$. (Prelejem, čo sa dá, do 13l nádoby, a dám pritom pozor aby som neporozlieval.)

Ľahko vyrátame, že $15=7.4-13$. Použitím spomínaných dvoch postupov teda budem vedieť dostať aj 15l.

Treba dať pozor, aby som sa nedostal do záporných čísel alebo nepresiahol obsah nádob. Prípustný postup je napríklad odmerať postupne 4, 8, 12, 16 litrov (1.spôsob), potom 16-13=3 litre (2) a ďalej 7, 11, 15 litrov. (Netvrdím, že sa to nedá jednoduchšie, však skúste;-)

10. Označme: A = všetky prirodzené čísla menšie ako 10^6. $|A| = 999\,999$,
A_2 = tie z nich, ktoré sú deliteľné 2, $|A_2| = \lfloor \frac{999\,999}{2} \rfloor = 499\,999$
A_3 = tie z nich, ktoré sú deliteľné 3, $|A_3| = 333\,333$
$A_2 \cap A_3$ obsahuje práve tie čísla, ktoré sú deliteľné 6, teda $|A_2 \cap A_3| = 166\,666$. Potom $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 499\,999 + 333\,333 - 166\,666 = 566\,666$
Toto je počet čísel súdeliteľných s číslom 6, nesúdeliteľných je teda $999\,999 - 566\,666 = 333\,333$.

Prípad b) je podobný, len treba skúmať deliteľnosť 2, 3, a 5 a použiť $|A_2 \cup A_3 \cup A_5| = |A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|$.

15. Rozoberme 3 možné prípady:
Ak $a = 3k$, tak $3 \mid a$.
Ak $a = 3k + 1$, tak $a + 2 = 3k + 3 = 3(k + 1)$, čiže $3 \mid a + 2$.
Ak $a = 3k + 2$, tak $a + 1 = 3k + 3 = 3(k + 1)$ a $3 \mid a + 1$.
(Ak $a = 3k + 2$, tak $a + 4 = 3k + 6 = 3(k + 2)$ a $3 \mid a + 4$.)

19. a)

$$\begin{aligned} (2n+1) = 1.(2n-1) + 2 \quad &\Rightarrow \quad 2 = (2n+1) - (2n-1) \\ (2n+1) = n.2 + 2 \quad &\Rightarrow \quad 1 = 2n + 1 - 2n = 2n + 1 - [(2n+1) - (2n-1)]n = \\ &\qquad = (2n+1)(1-n) + (2n-1)n \end{aligned}$$

Podľa cvičenia 2 potom $1 = (2n + 1, 2n - 1)$.
b) $n^2 - 1 = (n - 1)(n + 1)$ a $n^2 + n = n(n + 1)$. Teda $n + 1$ je spoločným deliteľom týchto čísel.

Súčasne platí $n^2 + n - n^2 - 1 = n(n + 1) - (n - 1)(n + 1) = n + 1$, preto každý ich spoločný deliteľ delí aj $n + 1$ a $n + 1 = (n^2 + n, n^2 - 1)$.

c) $n^3 - 1 = (n - 1)(n^2 + n + 1)$, $n^2 - 1 = (n - 1)(n + 1)$ a $n^2 + n + 1 - n(n + 1) = 1$, z čoho dostaneme $(n^2 + n + 1, n + 1) = 1$, a $(n^3 - 1, n^2 - 1) = n - 1$.

d) Pomocou delenia so zvyškom dostaneme: $(n^3 + 2) = (n^2 - n + 1)(n + 1) + 1$ a $(n^3 + 2, n + 1) = (n + 1, 1) = 1$.

2 Prvočísla

4. Sporom. Nech by k nebolo prvočíslo. Potom $k = n.l$ pre nejaké $1 < n, l < k$. Z toho, že $l \mid k$ a $k \mid m$ dostaneme, že $l \mid m$, čo je spor s tým, že k bolo najmenšie takéto číslo.

5. Nepriamo. Prepokladajme, že n je zložené číslo, ukážeme, že aj $2^n - 1$ je zložené číslo. Ak $n = k.l$, kde $1 < k, l < n$, tak $2^n - 1 = 2^{k.l} - 1 = (2^k)^l - 1 = (2^k - 1)(1 + 2^k + ... + 2^{k.(l-1)})$. (Použili sme vzorec $(a^m - b^m) = (a - b)(a^{m-1} + a^{m-2}b + \ldots + ab^{m-2} + b^{m-1}$.) Pretože $l > 1$, platí $2^k - 1 < 2^{k.l} - 1 = 2^n - 1$. Teda číslo $2^n - 1$ je zložené.

6. Nepriamo. Nech $n \neq 2^m$, t.j. $n = 2^m.(2k + 1)$ pre nejaké $k > 1$. Potom $2^n + 1 = \left(2^{2^m}\right)^{(2k+1)} + 1$. Použitím vzorca $a^{2k+1} + 1 = (a + 1)(a^{2k} - a^{2k-1} + \ldots - a + 1)$ pre

$a = 2^{2^m}$ dostaneme, že $2^n + 1 = (2^{2^m} + 1).\left(\left(2^{2^m}\right)^{2k} - \left(2^{2^m}\right)^{2k-1} + \ldots - 2^{2^m} + 1\right)$. Pretože $2^{2^m} + 1 > 1$, číslo $2^n - 1$ je zložené.

8. Označme $m = n! - 1$. Ak m je prvočíslo, tak niet čo dokazovať. Ak m je zložené číslo, tak je deliteľné nejakým menším číslom. m nemôže byť deliteľné žiadnym z čísel $1, \ldots, n$, pretože pre $k \leq n$ platí $(m, k) = (n! - 1, k) = 1$. [$1 = n! - (n! - 1) = 1 \ldots (k-1)(k+1) \ldots n.k - m$. Teda $1 = uk + vm$, pre celé čísla $u = 1 \ldots (k-1)(k+1) \ldots n$, $v = -1$, z čoho už vyplýva $(m, k) = 1$.] Preto je m deliteľné nejakým číslom medzi n a $n! - 1$ a najmenšie takéto číslo je prvočíslo. (cvičenie 4)

10. Označme $d = p_1^{u_1} \ldots p_k^{u_k}$. Pretože $u_i \leq t_i$, $u_i \leq s_i$ pre všetky prípustné i, $d \mid a$ aj $d \mid b$. Teda d je spoločný deliteľ a aj b.

    Ak $d' \mid a$, $d' \mid b$ a $d' > 0$, tak v kanonickom rozklade čísla d' sa nemôžu vyskytovať iné prvočísla, než $p_1, \ldots, p_k$. Teda $d' = p_1^{r_1} \ldots p_k^{r_k}$. $d' \mid a$, preto $r_i \leq t_i$. Podobne z $d' \mid a$ vyplýva $r_i \leq s_i$. Celkove teda dostávame $r_i \leq \min\{s_i, t_i\} = u_i$ a $d' \mid d$, $d' < d$. Teda d je najväčší spoločný deliteľ čísel a a b.

    Dokázali sme, že $(a, b) = p_1^{u_1} \ldots p_k^{u_k}$. Potom $[a, b] = \frac{a.b}{(a,b)} = p_1^{s_1+t_1-u_1} \ldots p_k^{s_k+t_k-u_k} = p_1^{v_1} \ldots p_k^{v_k}$.

12. $72 = 2^3.3^2$ má deliteľe $2^0.3^0 = 1$, $2^0.3^1 = 3$, $2^0.3^2 = 9$, $2^1.3^0 = 2$, $2^1.3^1 = 6$, $2^1.3^2 = 18$, $2^2.3^0 = 4$, $2^2.3^1 = 12$, $2^2.3^2 = 36$, $2^3.3^0 = 8$, $2^3.3^1 = 24$, $2^3.3^2 = 72$.

    Delitele $11^5.7^2 = \{7^k.11^l; 0 \leq k \leq 2, 0 \leq l \leq 5\}$.

14. Ak n nie je deliteľné 5, tak zvyšok n^4 po delení 5 je 1 (stačí overiť 4 prípady, tiež to vyplýva z Eulerovej vety, ktorú sa naučíme neskôr) a $5 \mid n^4 + 4$.

15. Ak sa číslo rovná druhej mocnine prirodzeného čísla, tak všetky prvočísla v jeho kanonickom rozklade musia mať párny exponent. Teda a) ani b) nie sú druhé mocniny prirodzených čísel. Pre c) urobíme kanonický rozklad a zistíme, že $1234321 = 1111^2$.

    157996443 nie je druhá mocnina prirodzeného čísla, lebo druhá mocnina prirodzeného čísla môže mať po delení 4 iba zvyšok 0 alebo 1.

18*. Máme $a_1 = 0$, $a_2 = 2$, $a_3 = 5$. Ak $n = 2k$ pre $k \geq 2$, tak $a_n = k(2k + 1) - 1 = 2k^2 + k - 1 = (2k - 1)(k + 1)$ je zložené číslo ($2k - 1 \geq 3$, $k + 1 \geq 3$). Ak $n = 2k + 1$ pre $k \geq 2$, tak $a_n = (2k + 1)(k + 1) - 1 = 2k^2 + 3k = (2k + 3).k$ je tiež zložené.

19. Sporom. Predpokladajme, že existuje len konečný počet prvočísel takého tvaru. Nech $p_1, \ldots, p_k$ sú všetky takéto prvočísla. Položme $n = 6p_1 \ldots p_k - 1$. Potom $p_1 \nmid n, \ldots, p_k \nmid n$. Čiže v prvočíselnom rozklade $n = q_1 \ldots q_l$ vystupujú len prvočísla so zvyškom 1 po delení 6, a teda aj $n = 6m + 1$ pre nejaké m - spor.

20. p je nepárne prvočíslo, preto $p + 1$ je párne a $2 \mid p + 1$. Ešte treba ukázať, že $3 \mid p + 1$. Rozoberme tri možné prípady:
    $p = 3k \Rightarrow p$ nie je prvočíslo,
    $p = 3k + 1 \Rightarrow p + 2 = 3k + 3 = 3(k + 1) \Rightarrow p + 2$ nie je prvočíslo,
    zostáva teda prípad $p = 3k + 2$, vtedy $p + 1 = 3k + 3 = 3(k + 1)$ a $3 \mid p$.

3 Číselné sústavy

1. $217 : 3 = 72 : 3 = 24 : 3 = 8 : 3 = 2$
   $1 \quad 0 \quad 0 \quad 2$
   $1513 : 3 = 504 : 3 = 168 : 3 = 56 : 3 = 18 : 3 = 6 : 3 = 2$
   $1 \quad 0 \quad 0 \quad 2 \quad 0 \quad 0$
   $2120 : 3 = 706 : 3 = 235 : 3 = 78 : 3 = 26 : 3 = 8 : 3 = 2$
   $2 \quad 1 \quad 1 \quad 0 \quad 2 \quad 2$
   $217 = (22001)_3$, $1513 = (2002001)_3$, $2120 = (2220112)_3$

2. $12892 = (403032)_5 = (135404)_6$
   $(10321)_4 = 1 + 2.4 + 3.16 + 256 = 313$

3. Jedna cifra v štvorkovej sústave zodpovedá dvom cifrám v dvojkovej. Jedna cifra v osmičkovej = 3 cifry v dvojkovej.
   $(301)_4 = (110001)_2$
   $(257)_8 = (10101111)_2$
   $(111100101)_2 = (13211)_4 = (745)_8$
   $(1100101)_2 = (1211)_4 = (145)_8$

5. $9a_1 + a_0 = 10a_0 + a_1 \Rightarrow 8a_1 = 9a_0$
   Hľadáme iba celočíselné riešenia medzi číslami $1, \ldots, 8$. (Nulu sme vylúčili, lebo zápis čísla v ľubovoľnej číselnej sústave nesmie začínať nulou.) Vidíme, že platí $9 \mid a_1$, teda riešenie neexistuje.

4 Kongruencie

1. $213^{174} + 25^{17} \equiv 3^{174} + 5^{17} \equiv (3^4)^{43} + 5 \equiv 9 + 5 \equiv 4 (mod\ 10)$
   (Použili sme to, že $3^4 \equiv 1\,(mod\ 10)$ a $5^n \equiv 5\,(mod\ 10)$ pre každé $n \in \mathbb{N}$.)
   b) $9^{99} + (7^{17})^{17} \equiv (9^2)^{49}.9 + ((7^4)^4.7)^{17} \equiv 1^{49}.9 + 7^{17} \equiv 9 + 7 \equiv 6 (mod\ 10)$
   c) $127^{37} + 45^{131} + 109^{18} \equiv 7^{37} + 5^{131} + 9^{18} \equiv 7^{9.4+1} + 5 + 9^{2.9} \equiv 7 + 5 + 1 \equiv 3 (mod\ 10)$

2. Indukciou sa dá ľahko dokázať, že $2^{3k} \equiv 1\,(mod\ 7)$, $2^{(3k+1)} \equiv 2\,(mod\ 7)$, $2^{(3k+2)} \equiv 4\,(mod\ 7)$. (Zvyšky 2^n po delení siedmimi sú $1, 2, 4, 1, 2, 4, \ldots$) Teda
   a) $7 \mid 2^n - 1 \Leftrightarrow 2^n \equiv 1\,(mod\ 7) \Leftrightarrow n = 3k$, $k \in \mathbb{N}$.
   b) $7 \mid 2^n - 1 \Leftrightarrow 2^n \equiv 6\,(mod\ 7)$, toto neplatí pre žiadne n.

3. Budeme dokazovať dve implikácie.
   $19 \mid 10a + b \Rightarrow 19 \mid 20a + 2b \Rightarrow 19 \mid (20a + 2b) - 19a$, t.j. $19 \mid a + 2b$
   $19 \mid a + 2b \Rightarrow 10 \mid 10a + 20b \Rightarrow 10 \mid (10a + 20b) - 19b$, t.j. $19 \mid 10a + b$.
   To isté môžeme zapísať pomocou kongruencií:
   $10a + b \equiv 0\,(mod\ 19) \Rightarrow 20a + 2b \equiv 0\,(mod\ 19) \Rightarrow a + 2b \equiv 0\,(mod\ 19)$
   $a + 2b \equiv 0\,(mod\ 19) \Rightarrow 10a + 20b \equiv 0\,(mod\ 19) \Rightarrow 10a + b \equiv 0\,(mod\ 19)$

4. $19 \mid 539\,828 \Leftrightarrow 19 \mid 53\,998 \Leftrightarrow 19 \mid 5\,415 \Leftrightarrow 19 \mid 551 \Leftrightarrow 19 \mid 57 \Leftrightarrow 19 \mid 19$.
   Teda $19 \mid 539\,828$.

5. x je párne $\Rightarrow x \equiv 4\,(mod\ 2) \Rightarrow f(x) \equiv f(4)\,(mod\ 2)$. Teda $f(x)$ je nepárne celé číslo, čiže $f(x) \neq 0$.
   Podobne ak x je nepárne, tak $x \equiv 5\,(mod\ 2) \Rightarrow f(x) \equiv f(5)\,(mod\ 2)$. Opäť $f(x)$ je nepárne, $f(x) \neq 0$.

8. Ak $a \equiv b\,(mod\ n)$, tak $n \mid a-b$. Z toho, že $m \mid n$ a $n \mid a-b$ dostaneme, že $m \mid a-b$, $a \equiv b\,(mod\ m)$.

5 Použitie kongruencií pri kritériách deliteľnosti prirodzených čísel

1. Všimnime si najprv, že $27.37 = 999$. Zrejme platí $1 \equiv 1000\,(mod\ 999)$, a teda aj $n \equiv 1000n\,(mod\ 999)$ pre ľubovoľné n. Z toho dostaneme:

$$\begin{array}{c} c_0 + c_1.10 + c_2.10^2 \equiv c_0 + c_1.10 + c_2.10^2\,(mod\ 999) \\ c_3 + c_4.10 + c_5.10^2 \equiv c_3.10^3 + c_4.10^4 + c_5.10^5\,(mod\ 999) \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ \hline (c_0 + c_1.10 + c_2.10^2) + (c_3 + c_4.10 + c_5.10^2) + \ldots \equiv n\,(mod\ 999) \end{array}$$

   Z toho už vyplýva $(c_0 + c_1.10 + c_2.10^2) + (c_3 + c_4.10 + c_5.10^2) + \ldots \equiv n\,(mod\ 27)$ a $(c_0 + c_1.10 + c_2.10^2) + (c_3 + c_4.10 + c_5.10^2) + \ldots \equiv n\,(mod\ 37)$.
   Možno sa na to pozrieť tiež tak, že keď číslo $1000a + b$ nahradíme číslom $a + b$, tak ho zmenšíme o $999a$, čiže o násobok 999, teda deliteľnosť 999 tým neovplyvníme.

4. Nepriamo: Nech m je zložené, t.j. $m = k.l$, $1 < k, l < m$. Dokážeme, že aj p je zložené. Platí, že $p = (10^{k-1}+10^{k-2}+\ldots+10+1)(10^k+10^{2k}+\ldots+10^{(l-1)k})$, teda p je zložené. Inak:

$$\begin{array}{r} 11\ldots1 \\ 11\ldots100\ldots0 \\ \vdots \qquad\qquad \vdots \\ 11\ldots100\ldots0\ldots00\ldots0 \\ \hline 11\ldots111\ldots1\ldots11\ldots1 \end{array}$$

   Všetky sčitované čísla sú násobkami čísla $\overbrace{11\ldots1}^{k}$, teda p je zložené.

   Obrátená veta neplatí, lebo číslo 111 nie je prvočíslo (je deliteľné 3).

6. a) $4 \mid 100 \Rightarrow 4 \mid c_2 10^2 + c_3 10^3 + \ldots + c_k 10^k = n - (10c_1 + c_0)$, teda $n \equiv 10c_1 + c_0\,(mod\ 4)$.
   b) $8 \mid 1000 \Rightarrow 8 \mid c_3 10^3 + c_2 10^2 + c_3 10^3 + \ldots + c_k 10^k = n - (100c_2 + 10c_1 + c_0)$, teda $n \equiv 100c_2 + 10c_1 + c_0\,(mod\ 4)$.

7. $7 + 8 + 1 + 2 = 18 \Rightarrow 8 \nmid (7812)_9$
   $7 - 8 + 1 - 2 = -2 \Rightarrow 10 \nmid (7812)_9$.

6 Eulerova veta

1. a) Z Eulerovej vety alebo z jej dôsledku dostaneme, že:
   $7 \mid n$ alebo $7 \mid n^6 - 1$
   $3 \mid n$ alebo $3 \mid n^2 - 1$
   $2 \mid n$ alebo $2 \mid n - 1$
   Pritom $n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = n(n-1)(n^2 + n + 1)(n^3 + 1)$, teda $2, 3, 7 \mid n^7 - n$. Sú to navzájom rôzne prvočísla, preto $2.3.7 = 42 \mid n^7 - n$.
   b) Ak $(n, 7) = 1$, tak podľa Eulerovej vety $n^6 \equiv 1\,(mod\ 7)$. Umocnením tejto kongruencie na k-tu dostaneme $n^{6k} \equiv 1\,(mod\ 7)$.

c) $2 \mid n \vee 2 \mid n-1$, $3 \mid n \vee 3 \mid n^2-1$, $5 \mid n \vee 5 \mid n^4-1$, $7 \mid n \vee 7 \mid n^6-1$, $13 \mid n \vee 13 \mid n^{12}-1$. $n^{13} - n = n(n^{12} - 1) = n(n^6 + 1)(n^6 - 1) = n(n^3 - 1)(n^9 + n^6 + n^3 + 1) = n(n^4 - 1)(n^8 + n^4 + 1) = n(n^2 - 1)(n^{10} + n^8 + n^6 + n^4 + n^2 + 1)$
Z toho už vyplýva dokazované tvrdenie.

2. Podľa malej Fermatovej vety $p \mid a^p - a$ a $p \mid (a^q)^p - a^q = a^{pq} - a^q$. Odčítaním dostaneme $p \mid a^{pq} - a^p - a^q + a$. Podobne dostaneme, že $q \mid a^{pq} - a^p - a^q + a$, teda celkove $pq \mid a^{pq} - a^p - a^q + a$.

3. Má platiť $2^m - 1 = 3^n$. Ak $m \geq 3$, tak $8 \mid 2^m$ a $2^m - 1 \equiv 7 \,(mod\ 8)$. Ľahko zistíme, že zvyšky 3^n po delení 8 sú striedavo 1 (pre párne n) a 3 (pre nepárne). Teda 3^n je kongruentné s 1 alebo 3, čo znamená, že riešenie s $m \geq 3$ neexistuje. Jediné riešenie je teda $m = 2$, $n = 1$.

4. Ak $(n, 10) = 1$, tak podľa Eulerovej vety $n \mid 10^{\varphi(n)} - 1$, čo je číslo, ktorého zápis v desiatkovej sústave pozostáva z $\varphi(n)$ deviatok.

5. a) $\varphi(11) = 10$ (pre každé prvočíslo platí $\varphi(p) = p - 1$). Ak $11 \nmid n$, tak $(11, n) = 1$, teda podľa Eulerovej vety $n^{10} \equiv 1 \,(mod\ 11)$.
b) $\varphi(13) = 12$. Ak $13 \nmid n$, tak $(13, n) = 1$, teda podľa Eulerovej vety $n^{12} \equiv 1 \,(mod\ 13)$.
c) $\varphi(25) = 20$, preto ak $(n, 25) = 1$, tak $n^{20} \equiv 1 \,(mod\ 25)$. Ak je n súdeliteľné s 25, tak $5 \mid n$, a preto $5^2 = 25 \mid n^2 \mid n^{20}$.

7. a) Chceme nájsť najmenšie n také, že $253^n \equiv 1 \,(mod\ 257)$. 257 je prvočíslo, $\varphi(257) = 256$. Podľa cvičenia 6 potom $n \mid 256 = 2^8$. $253 \equiv -4 \,(mod\ 257)$, umocnením na druhú dostaneme $253^2 \equiv (-4)^2 \equiv 16 \,(mod\ 257)$, $253^4 \equiv 256 \equiv -1 \,(mod\ 257)$, $253^8 \equiv 1 \,(mod\ 257)$. Teda $n = 8$.
b) $2^1 \equiv 2 \,(mod\ 257)$, $2^2 \equiv 4 \,(mod\ 257), \ldots, 2^8 \equiv 256 \equiv -1 \,(mod\ 257), \ldots 2^{16} \equiv 1 \,(mod\ 257)$. $n = 16$.

8. Podľa Malej Fermatovej vety $p^{q-1} \equiv 1 \,(mod\ q)$ a $q^{p-1} \equiv 1 \,(mod\ p)$, t.j. $q \mid p^{q-1} - 1$ a $p \mid q^{p-1}$. Keďže p a q sú navzájom rôzne prvočísla, dostaneme z toho, že $pq \mid (p^{q-1} - 1)(q^{p-1} - 1) = p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1$, a teda $pq \mid p^{q-1} + q^{p-1} - 1$.

   Z kongruencie $p^{q-1} + q^{p-1} \equiv 1 \,(mod\ pq)$ vyplýva $p^q \equiv p^q + pq^{p-1} \equiv p \,(mod\ pq)$ a $q^p \equiv p^{q-1}q + q^p \equiv q \,(mod\ pq)$. Sčítaním dostaneme $p^q + q^p \equiv p + q \,(mod\ pq)$.

9. Napríklad $a = 2$, $n = 4$, $\varphi(n) = 2$.

11*. Označme d najväčší spoločný deliteľ čísel z množiny $\{n^{13} - n, n \in \mathbb{Z}\}$. Z cvičenia 1c) vieme, že $2, 3, 5, 7, 13 \mid n^{13} - n$, čiže $2.3.5.7.13 \mid d$.

   Priamym výpočtom overíme, že $2^{13} - 2 = 8190 = 2.3^2.5.7.13$, preto $d \mid 2.3^2.5.7.13$.

   Pre $n = 3$ dostaneme $3^{13} - 3 \equiv 6 \,(mod\ 9)$, lebo $9 \mid 3^{13}$. To znamená, že $9 \nmid d$ a $d = 2.3.5.7.13 = 2730$.

7 Lineárne kongruencie

2. Podľa vety z prednášky má kongruencia $ax \equiv b \,(mod\ n)$ riešenie práve vtedy, keď $(a, n) = d \mid b$. Ak má riešenie, tak počet riešení je d.
a) $(6, 9) = 3 \nmid 1$ nemá riešenie,
b) $(9, 6) = 3 \mid 6$ má 3 riešenia,
c) $(14, 70) = 14 \nmid 21$ nemá riešenie.

3. a) $20x \equiv 4\,(mod\ 30)$, $(20, 30) = 10 \nmid 4 \Rightarrow$ nemá riešenie.
   b) Táto kongruencia je ekvivalentná s kongruenciou $0 \equiv 2\,(mod\ 4)$, čiže nemá riešenie.
   c) $(353, 254) = 1$, Euklidovým algoritmom zistíme, že

$$\begin{aligned} 400 = 353 + 47 &\quad\Rightarrow\quad 47 = 400 - 353 \\ 353 = 47.7 + 24 &\quad\Rightarrow\quad 24 = 353 - 7.47 = 8.353 - 7.400 \\ 47 = 1.24 + 23 &\quad\Rightarrow\quad 23 = 47 - 24 = 17.353 - 15.400 \\ 24 = 23 + 1 &\quad\Rightarrow\quad 1 = 24 - 23 = 17.353 - 15.400 \end{aligned}$$

   $353.17 - 1 = 15.400 \Rightarrow 353.17 \equiv 1\,(mod\ 400)$
   Poslednú rovnosť vynásobíme 254.
   $17.254 \equiv 318\,(mod\ 400) \Rightarrow 353.318 \equiv 254\,(mod\ 400)$
   Jediné riešenie je $\underline{\underline{x = 318}}$.

8 Aritmetické funkcie

$144 = 2^4.3^2$
$\varphi(144) = 144\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 144 \cdot \frac{1}{2} \cdot \frac{2}{3} = 48$
$\sigma(144) = \frac{2^5-1}{1} \cdot \frac{3^3-1}{3-1} = \frac{31.26}{2} = 31.13 = 403$

$1000 = 2^3.5^3$
$\varphi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$
$\sigma(1000) = \frac{2^4-1}{1} \cdot \frac{5^4-1}{5-1} = \frac{15.624}{4} = 15.156 = 2340$

9 g-adické rozvoje

1. a) Sporom. Nech by $a = \sqrt{3}+\sqrt{5}$ bolo racionálne. Potom $a-2\sqrt{3} = \sqrt{5}-\sqrt{3} \notin \mathbb{Q}$ (súčet racionálneho a iracionálneho čísla je iracionálne) a $a(a-2\sqrt{3}) = (\sqrt{5}+\sqrt{3})(\sqrt{5}-\sqrt{3}) = 5 - 3 = 2$. Súčin racionálneho a iracionálneho čísla je však iracionálne, čiže sme dostali spor.

   b) $\sqrt{3}(\sqrt{6} - 3) = 3(\sqrt{2} - \sqrt{3})$. V d) ukážeme, že $\sqrt{3} - \sqrt{2} \notin Q$, čiže aj toto číslo je iracionálne.

   c) Súčet racionálneho a iracionálneho čísla je iracionálne.

   d) Sporom. $a = \sqrt{3} - \sqrt{2} \in \mathbb{Q}$, $\sqrt{3} + \sqrt{2} = a + 2\sqrt{2} \notin \mathbb{Q}$, $a.b = 1 \in \mathbb{Q}$, spor.

   e) Nech by $a = \sqrt[3]{3} + \sqrt{3} \in \mathbb{Q}$.

$$\begin{aligned} a - \sqrt{2} &= \sqrt[3]{3} \quad /^3 \\ a^3 - 3a^2\sqrt{2} + 6a - 2\sqrt{2} &= 3 \\ a^3 + 6a - 3 &= (3a^2 + 2)\sqrt{2} \\ \sqrt{2} &= \frac{a^3 + 6a - 3}{3a^2 + 2} \in \mathbb{Q}, \end{aligned}$$

   čo je spor. (Deliť v poslednej úprave sme mohli vďaka tomu, že $3a^2 + 2 > 0$.)

   f) $\log 2 + \log 3 = \log 6 \notin \mathbb{Q}$ podľa vety z prednášky.

3.

$$\begin{aligned}
\frac{35}{11} &= 3 + \frac{2}{11} & \qquad \frac{13}{9} &= 1 + \frac{4}{9} \\
5 \cdot \frac{2}{11} = \frac{10}{11} &= 0 + \frac{10}{11} & 5 \cdot \frac{4}{9} = \frac{20}{9} &= 2 + \frac{2}{9} \\
5 \cdot \frac{10}{11} = \frac{50}{11} &= 4 + \frac{6}{11} & 5 \cdot \frac{2}{9} = \frac{10}{9} &= 1 + \frac{1}{9} \\
5 \cdot \frac{6}{11} = \frac{30}{11} &= 2 + \frac{8}{11} & 5 \cdot \frac{1}{9} = \frac{5}{9} &= 0 + \frac{5}{9} \\
5 \cdot \frac{8}{11} = \frac{40}{11} &= 3 + \frac{7}{11} & 5 \cdot \frac{5}{9} = \frac{25}{9} &= 2 + \frac{7}{9} \\
5 \cdot \frac{7}{11} = \frac{35}{11} &= 3 + \frac{2}{11} & 5 \cdot \frac{7}{9} = \frac{35}{9} &= 3 + \frac{8}{9} \\
\frac{35}{11} &= \underline{\underline{(3, \overline{04233})_5}} & 5 \cdot \frac{8}{9} = \frac{40}{9} &= 4 + \frac{4}{9} \\
& & \frac{13}{9} &= \underline{\underline{(1, \overline{210234})_5}}
\end{aligned}$$

Zišlo by sa urobiť aj nejakú skúšku správnosti. Jedna z možností je použiť postup z príkladu 5, ale pri dlhých periódach je tento postup veľmi pracný. Mne by sa zdalo jednoduchšie vynásobiť tie výsledok menovateľom ($11 = (21)_5$) v 5-kovej sústave. (Ak prídete na lepší nápad, ako urobiť skúšku dajte mi vedieť.)

a)
$$\begin{array}{r}
(3,\overline{04233})_5 \\
\hline
(21)_5 \\
(3,\overline{04233})_5 \\
\hline
(111,\overline{40211})_5 \\
\hline
(114,\overline{44444}) = (115)_5
\end{array}$$

$x = \frac{(115)_5}{(21)_5} = \frac{35}{9}$

b) $a = (1, \overline{210234})_5$
$10a = (20)_5 a = (2\overline{4}, \overline{20468})$. Tento zápis ale ešte nie je korektný zápis čísla v 5-kovej sústave, preto ho musíme ešte upraviť:
$10a = (2\overline{4}, \overline{21023})_5$
$9a = 10a - a = (24, \overline{210234})_5 - (1, \overline{210234})_5 = (23)_5 = 13$
$a = \frac{13}{9}$

c) $\frac{1}{24} = \frac{1}{5^2 - 1} = \frac{1}{5^2}(\frac{1}{1 - 5^{-2}}) = \frac{1}{5^2}(1 + \frac{1}{5^2} + \frac{1}{5^4} + \ldots) = (0, \overline{01})_5$

5. $x = (2, \overline{13})_5$, $25x = (213, \overline{13})_5 \Rightarrow 24x = (211)_5 = 56$, $x = \underline{\underline{\frac{7}{3}}}$
$x = (3, 2\overline{3})_7$, $2x = (6, 4\overline{6})_7 = (6, 5)_7$, $7.2x = (65)_7 = 47 \Rightarrow x = \underline{\underline{\frac{47}{14}}}$