Pracovní list: Dělitelnost 1

Úloha 1

Anča má čtvercovou čokoládu ($n \times n$ dílků). Snědla z ní prvočíselný počet dílků a zbylých 400 si schovala na příště. Kolik dílků Anča snědla? Nalezněte všechny možnosti.

Úloha 2

Nalezněte $\mathrm{NSD}(126, 132)$.

Úloha 3

Určete počet přirozených čísel k, pro která je $\mathrm{nsn}(6^6, 8^8, k) = 12^{12}$.

Úloha 4

Najděte všechna přirozená čísla a, b, která splňují

$$\mathrm{NSD}(a, b) = 21 \quad \wedge \quad \mathrm{nsn}(a, b) = 1\,764.$$

Úloha 5

Nalezněte přirozená čísla k, l, pro která platí $k = l - 4$, $\mathrm{NSD}(k, l) \cdot \mathrm{nsn}(k, l) = 480$.

Úloha 6

Mějme přirozené číslo $a = 10^k \cdot x_k + 10^{k-1} \cdot x_{k-1} + \ldots + 10^0 \cdot x_0$, $k \in \mathbb{N}_0$, $i \in \{0, 1, \ldots k\}$, $x_i \in \{0, 1, \ldots 9\}$. Dokažte, že číslo a je dělitelné číslem 3, jestliže součet $x_k + x_{k-1} + \ldots + x_0$ je dělitelný číslem 3.

Pracovní list: Dělitelnost 2

Úloha 1

Určete celou dolní část čísel.

(a) $\lfloor 17 \rfloor =$ **(b)** $\lfloor 12{,}2 \rfloor =$ **(c)** $\lfloor -5{,}8 \rfloor =$ **(d)** $\lfloor \pi \rfloor =$

Úloha 2

Vypočtěte.

(a) $284 \pmod{25}$

(b) $-729 \pmod{42}$

(c) $638 \pmod{-27}$

(d) $-584 \pmod{-62}$

Úloha 3

Nápověda

Dokažte, že pro všechna přirozená čísla n je číslo $(7n + 4)$ nesoudělné s číslem $(5n + 3)$.

Úloha 4

Matematickou indukcí dokažte, že pro všechna přirozená čísla n je výraz $n^3 + 2n$ dělitelný číslem 3.

Úloha 5

Pomocí rozšířeného Euklidova algoritmu nalezněte čísla a, b, pro která platí

$$105 \cdot a + 38 \cdot b = \text{NSD}(105, 38).$$

Pracovní list: Kongruence 1

Úloha 1

Dokažte, že druhá mocnina čísla, které není dělitelné číslem 3, leží ve zbytkové třídě $[1]_3$.

Úloha 2

Pomocí rozšířeného Euklidova algoritmu nalezněte multiplikativní inverzi čísla 81 modulo 1 510.

Úloha 3

Nápověda

Dokažte, že číslo 2 279 dělí beze zbytku výraz $(1\,286)^n - (1\,157)^n - (1\,339)^n + (1\,210)^n$.

Úloha 4

Pomocí malé Fermatovy věty vypočítejte $13^{200} \pmod{19}$.

Pracovní list: Kongruence 2

Úloha 1

Dokažte, že pro libovolné přirozené číslo k platí kongruence $2^{2k} \equiv 3^{2k} \pmod 5$.

Úloha 2

Určete hodnoty Eulerovy funkce.

(a) $\varphi(7) =$ **(b)** $\varphi(95) =$ **(c)** $\varphi(675) =$

Úloha 3

Pomocí Eulerovy věty vypočítejte $1\,991^{2\,023} \pmod{2\,022}$.

Úloha 4 **Nápověda**

Nechť $\mathrm{NSD}(m, n) = 1$. Pak $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{m \cdot n}$. Dokažte.

Úloha 5 **Nápověda**

Ukažte, že číslo $4^{3k+1} + 2^{3k+1} + 1$ je dělitelné číslem 7.

Pracovní list: Kongruence 3

Úloha 1

Pomocí rozšířeného Euklidova algoritmu nalezněte multiplikativní inverzi čísla 651 modulo 754.

Úloha 2

Ukažte, že $2^{2k+1} + 1$ je dělitelné číslem 3.

Úloha 3

Terka má v knihovně mezi dvěma sty a dvěma sty padesáti knihami. Pokud bude knihy při stěhování ukládat do krabic po třech, zbydou jí dvě knihy, po čtyřech jí zbydou tři knihy a po pěti jí zbydou též dvě knihy. Kolik knih má Terka v knihovně?

Pracovní list: Šifrování RSA

Úloha 1

Zvolte prvočísla p, q a spočítejte modul šifrovací a dešifrovací transformace $m = p \cdot q$.

Úloha 2

Určete hodnotu $\varphi(m)$ pro m z úlohy 1.

Úloha 3

Vygenerujte veřejný klíč (e, m) a soukromý klíč (d, m) pro m z úlohy 1.

(a) Zvolte **šifrovací exponent** e takový, že

$$1 < e < \varphi(m) \wedge \mathrm{NSD}(e, \varphi(m)) = 1.$$

(b) Dopočítejte **dešifrovací exponent** d tak, aby

$$d \cdot e \equiv 1 \,(\mathrm{mod}\ \varphi(m)).$$

Úloha 4

Funkčnost vygenerovaných klíčů (e, m), (d, m) ověřte pomocí Šifrátoru a Dešifrátoru. Zašifrujte a dešifrujte zprávu „`Hello World!`“.

Úloha 5

(a) Se spolužákem si vyměňte své vygenerované veřejné klíče (e, m). Obdrženým veřejným klíčem zašifrujte zprávu pomocí Šifrátoru. Vygenerovaný poznámkový blok odešlete adresátovi.

(b) Obdrženou zprávu dešifrujte pomocí Dešifrátoru svým soukromým klíčem.

Úloha 6

Zachytili jste cizí zprávu v poznámkovém bloku. Na prvním řádku zprávy naleznete veřejný klíč. Přepočítejte jej na soukromý klíč a zprávu dešifrujte pomocí Dešifrátoru.