Zavedeme značení

$$a \equiv b \pmod{m}$$

(čteme *a je kongruentní s b modulo m*), pokud platí následující ekvivalentní podmínky:

- a a b dávají stejný zbytek po dělení m;
- $a = mq_1 + r$ a $b = mq_2 + r$, pro nějaká q_1, q_2, r;
- $m \mid a - b$.

Tato relace je ekvivalencí a platí následující užitečné vlastnosti:

- je-li $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, pak

  $$a \pm c \equiv b \pm d \pmod{m}, \qquad a \cdot c \equiv b \cdot d \pmod{m}$$

  a $a^k \equiv b^k \pmod{m}$ pro každé $k \in \mathbb{N}$;
- $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{cm}$;
- jsou-li c, m nesoudělná, pak $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{m}$;
- jsou-li m, n nesoudělná, pak

  $$a \equiv b \pmod{mn} \Leftrightarrow a \equiv b \pmod{m} \text{ a } a \equiv b \pmod{n}.$$

1. Urči, kolik je 5^{20} mod 26.

2. Dokaž, že $7 \mid 37^{n+2} + 16^{n+1} + 23^n$ pro každé přirozené n.

3. Dokaž, že $112 \mid (835^5 + 6)^{18} - 1$.

4. Dokaž, že $11 \mid 5^{5k+1} + 4^{5m+2} + 3^{5n}$ pro všechna přirozená k, m, n.

5. Odvoď kritérium dělitelnosti 9, 11 a 7.

6. Pro libovolná celá čísla a, b a prvočíslo p platí $a^p + b^p \equiv (a+b)^p \pmod{p}$.

Zavedeme *Eulerovu funkci* předpisem

$$\varphi(n) = \text{ počet prvků v intervalu } 1, \ldots, n-1 \text{ nesoudělných s } n.$$

Je-li $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ prvočíselný rozklad čísla n, platí

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \cdot \ldots \cdot p_m^{k_m-1}(p_1 - 1)(p_2 - 1) \cdot \ldots \cdot (p_m - 1).$$

Eulerova věta. Jsou-li a, n nesoudělná, pak

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Malá Fermatova věta. Je-li p prvočíslo a $p \nmid a$, pak

$$a^{p-1} \equiv 1 \pmod{p}.$$

7. Spočtěte 8^{7^6} a) mod 21, b) mod 12.

8. Dokažte, že $11 \mid 3^{2000} + 4^{2002} + 5^{2001}$.

9. Spočtěte $2^{3^{4^{5^{6^7}}}} \mod 9$.

10. Spočtěte poslední dvě cifry čísla $2^{3^{2^{3^{2^3}}}}$.

11. Dokažte, že $5 \mid n^9 + 2n^7 + 3n^3 + 4n$ pro každé $n \in \mathbb{N}$.

12. Řešte v $\mathbb{Z}$ rovnici $x^6 + x + xy \equiv 1 \pmod 7$.

13. Dokažte Malou Fermatovu větu. Návod: indukcí podle a dokažte, že $a^p \equiv a \pmod p$.

14. Mějme různá prvočísla p a q. Dokaž, že $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

15. * $19 \cdot 8^n + 17$ je složené číslo.