5. procvičení z MB154, podzim 2023

Příklad 1. Ukažte, že $p = 1729 = 7 \cdot 13 \cdot 19$ projde Fermatovým testem $a^{p-1} \equiv 1 \pmod{p}$ pro libovolné a nesoudělné s p. Bonus: Ukažte, že p projde i Eulerovým testem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ pro libovolné a nesoudělné s p. (Počítejte zvlášť modulo 7, 13, 19 a zjistíte, že řád každého takového čísla a je dělitelem $36 \mid 1728$.)

Příklad 2. Ukažte, že $p = 2821 = 7 \cdot 13 \cdot 31$ neprojde Eulerovým testem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ pro vhodné a nesoudělné s p, například pro $a = 2$. (Výsledek: $2^{1410} \equiv 1520 \pmod{2821}$.)

Příklad 3. Ukažte, že $p = 217$ projde Eulerovým testem pro $a = 5$, ale nikoliv Eulerovým–Jacobiho testem $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ pro $a = 5$. (Výsledek: levá strana 1, pravá strana -1.)

Příklad 4. Zpráva M byla zašifrována pomocí RSA s veřejným klíčem $(23, 55)$ (tj. $e = 23, n = 55$) do tvaru $8, 9, 17$. Pokuste se šifru prolomit a najít M. (Výsledek: dešifrovací exponent $d = 7$, dešifrované zprávy 2, 4, 8.)

Příklad 5. Pomocí RSA s veřejným klíčem $(151, 323)$ (tj. $e = 151, n = 323 = 17 \cdot 19$) zašifrujte a poté dešifrujte zprávu $M = 21$. (Výsledek: dešifrovací exponent $d = 103$, zašifrovaná zpráva 166.)