5. cvičení z MB154, podzim 2021

Příklad 1. Dořeště podstatné příklady z minula, v mém případě: Rozhodněte, zda je 58 kvadratický zbytek modulo 163 (pomocí pravidel pro počítání Jacobiho symbolu; poté lze ověřit na kalkulačce pomocí $58^{81} \pmod{163}$). Vyřešte kongruence (druhou v rychlosti)

$$x^2 \equiv 58 \pmod{163}, \quad x^2 \equiv 58 \pmod{157}$$

Příklad 2. Ukažte, že $p = 1105 = 5 \cdot 13 \cdot 17$ projde Fermatovým testem $a^{p-1} \equiv 1 \pmod{p}$ pro libovolné a nesoudělné s p.

Počítejte zvlášť modulo 5, 13, 17 a zjistíte, že řád každého takového čísla a je dělitelem $48 \mid 1104$.

Příklad 3. Ukažte, že $p = 1105$ neprojde Eulerovým testem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ pro vhodné a nesoudělné s p, například pro $a = 7$.

Příklad 4. Ukažte, že $p = 341$ projde Eulerovým testem pro $a = 2$, ale nikoliv Eulerovým–Jacobiho testem $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ pro $a = 2$ (vpravo se jedná o Jacobiho symbol, který má vyjádření vlevo jen pro p prvočíslo; stejně tak pro vztah ke kvadratickým zbytkům – tady ale něco znamená, interpretujte).

Příklad 5. Zpráva M byla zašifrována pomocí RSA s veřejným klíčem $(13, 51)$ (tj. $e = 13, n = 51$) do tvaru $7, 48, 11$. Pokuste se šifru prolomit a najít M.

Příklad 6. Pomocí RSA s veřejným klíčem $(95, 551)$ (tj. $e = 95, n = 551 = 19 \cdot 29$) zašifrujte a poté dešifrujte zprávu $M = 25$.

Zatímco RSA bych určitě chtěl pokrýt, DH a ElGamal už nemusíte, bude na ně ještě jedno cvičení společně s Rabinem a případným opakováním.

Příklad 7. Najděte primitivní kořen modulo 23 a demonstrujte DH protokol pro $a = 7$ a $b = 13$.

Příklad 8. Tomáš a Petr chtějí komunikovat šifrou ElGamal. Tomáš si zvolil prvočíslo $p = 31$, primitivní kořen $g = 12$ a číslo $x = 6$. Zveřejnil pak trojici $(31, 12, h)$, kde $h \equiv 12^6 \pmod{31}$. Petr mu poslal dvojici $(21, 27)$. Jakou zprávu poslal Petr Tomášovi?