1. vnitrosemestrální písemka, skupina A

Příklad 1. [body: 2+1]

a) Petr zkoumal řády zbytkových tříd modulo 341 a zjistil, že řád zbytku 185 je 10. Spočtěte Jacobiho symbol $\left(\frac{185}{341}\right)$ a pomocí Eulerova-Jacobiho testu odhalte, že 341 není prvočíslo.

b) Toto zjištění přimělo Petra zkoušením rozložit $341 = 11 \cdot 31$. Dále pak Petr zkoumal řády všech zbytkových tříd nesoudělných s modulem 341. Jaký maximální řád našel? Najděte nějaký zbytek tohoto maximálního řádu. (Mohlo by se vám hodit, že 21 je primitivním kořenem modulo 31.)

Příklad 2. [body: 2+2]

a) Pomozte Alici ověřit, že 5 je primitivní kořen modulo 23.

b) Alice si pak jako svůj soukromý klíč zvolila exponent $a = 7$ a zveřejnila svůj veřejný klíč $(p = 23, g \equiv 5, g^a \equiv 17)$. Bob při šifrování zprávy pro Alici zvolil soukromý klíč $b = ?$ a poslal Alici zašifrovanou zprávu $(g^b \equiv 20, c \equiv 4)$. Pomozte Alici zprávu dešifrovat.

Příklad 3. [body: 2+1]

a) U Eulerovy věty je předpoklad nesoudělnosti základu a modulu podstatný. Určete zbytek $2^{\varphi(3328)}$ po dělení 3328, přičemž určitě využijte rozkladu $3328 = 256 \cdot 13$ a počítejte prvně zvlášť modulo 256 a 13 a pak dejte tyto výsledky dohromady.

b) Pokud budeme namísto základu 2 uvažovat všechny možné zbytkové třídy a modulo 3328, kolik různých výsledků $a^{\varphi(3328)} \pmod{3328}$ takto dostaneme? Tyto další výsledky už nemusíte počítat.