Kapitola 5

Jacobiho symbol, testování prvočíselnosti, šifrování

5.1 Opakování z přednášky

Definice. Buďte čísla n *liché* a a libovolné. Nechť dále $n = p_1 \cdot \dots \cdot p_k$, kde p_i, $i = 1, \dots, k$, jsou (ne nutně různá) prvočísla. Definujeme *Jacobiho symbol*, čteno „a vzhledem k n“, vztahem

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \cdot \dots \cdot \left(\frac{a}{p_k}\right),$$

kde na pravé straně jsou Legendreovy symboly.

Jacobiho symbol má podobné vlastnosti jako Legendreův symbol, což zjednodušuje jeho výpočet. Uveďme je nyní.

i) Pokud $a \equiv b \pmod{n}$, pak $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

ii) $\left(\frac{a\,b}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$;

iii) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$;

iv) pro liché m platí $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{\frac{m-1}{2}\,\frac{n-1}{2}}$.

Opět máme u vlastností iii) a iv) vzorečky

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & n \equiv 1 \text{ nebo } 7 \pmod 8, \\ -1 & n \equiv 3 \text{ nebo } 5 \pmod 8. \end{cases}$$

a

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & m \equiv n \equiv 3 \pmod 4, \\ \left(\frac{n}{m}\right) & \text{jinak.} \end{cases}$$

jelikož při důkazu jsme využívali jen to, že jsme počítali s lichými čísly a nikoli nutně s prvočísly. Jacobiho symbol nemá nutně stejný vztah ke kvadratickým zbytkům, respektive máme pouze jednostrannou implikaci, tj. je-li a kvadratický zbytek modulo n, pak $\left(\frac{a}{n}\right) = 1$, jelikož a musí být kvadratický zbytek modulo všechna prvočísla v rozkladu n. Druhá implikace však neplatí. Například 2 není kvadratickým zbytkem modulo $15 = 3 \cdot 5$, ale $\left(\frac{2}{15}\right) = 1$. To je dáno tím, že se jedná o součin dvou prvočísel, modulo ani jednoho z nichž 2 není kvadratickým zbytkem.

Máme různé testy pro testování prvočíslenosti.

Věta (Fermatův test prvočíselnosti)**.** *Je-li p prvočíslo a a s ním nesoudělné, pak*

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

Věta (Eulerův test prvočíselnosti)**.** *Je-li p prvočíslo a a s ním nesoudělné, pak*

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Věta (Eulerův-Jacobiho test prvočíselnosti)**.** *Je-li p prvočíslo a a s ním nesoudělné, pak*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Při asymetrickém šifrování potřebuje každý účastník *veřejný klíč* V, sloužící k šifrování, a *soukromý klíč* S, který slouží k dešifrování. Pro asymetrické šifrování máme k disposici různé algoritmy.

RSA Pro generování klíčů zvolí účastník dvě *velká* prvočísla p a q, spočítá $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$, dále zvolí e nesoudělné s $\varphi(n)$ a spočítá (například pomocí Eukleidova algoritmu) modulární inverzi d, tedy $d \cdot e \equiv 1 \pmod{\varphi(n)}$. Veřejným klíčem je pak $V = (n, e)$, soukromým klíčem je $S = d$. Pří šifrování zprávy M spočítáme $C := V(M) \equiv M^e \pmod{n}$. Při dešifrování šifrované zprávy C pak účastník spočítá $M \equiv C^d \pmod{n}$.

protokol na výměnu klíčů DH Obě strany komunikace se dohodnou na prvočísle p a primitivním kořenu g modulo p pak každý z účastníků vybere a, respektive b, a pošle druhé straně g^a, resp. g^b modulo p. Společným klíčem pro komunikaci je pak $g^{a\,b} = (g^a)^b = (g^b)^a$, což mohou oba účastníci spočítat bez toho, aby jej mohl zjistit kdokoli jiný.

ElGamal Systém je odvozen z protokolu DH. Účastník zvolí prvočíslo p, primitivní kořen g modulo p, náhodné a a spočítá $h \equiv g^a \pmod{p}$. Veřejným klíčem pak je $V = (p, g, h)$ a soukromým klíčem je pak $S = a$. Při šifrování zprávy M zvolíme náhodné b a spočítáme $C_1 \equiv g^b \pmod{p}$ a $C_2 \equiv M \cdot h^b \pmod{p}$; následně pošleme $C = (C_1, C_2)$. Pro dešifrování pak účastník spočítá $M \equiv C_2 / C_1^a \pmod{p}$.

5.2 Příklady řešené na cvičení

Příklad 5.1. Ukažte, že $p = 1\,105 = 5 \cdot 13 \cdot 17$ projde Fermatovým testem $a^{p-1} \equiv 1 \pmod{p}$ pro libovolné a nesoudělné s p.

Řešení. Nechť a je nesoudělné s 1 105 libovolné. Pak a je nesoudělné i s 5, 13 i 17, o nichž víme, že jsou to prvočísla. Z malé Fermatovy věty proto máme

$$\begin{aligned} a^4 &\equiv 1 \pmod{5} \\ a^{12} &\equiv 1 \pmod{13} \\ a^{16} &\equiv 1 \pmod{17} \end{aligned}$$

Jelikož $[4, 12, 16] = 48$, máme dále $a^{48} \equiv 1 \pmod{5}$, $\pmod{13}$ i $\pmod{17}$. Pak tedy je $a^{48} \equiv 1 \pmod{1\,105}$. Jenže $1\,104 = 48 \cdot 23$, díky čemuž $a^{1\,104} \equiv 1 \pmod{1\,105}$. △

Příklad 5.2. Ukažte, že $p = 1\,105$ neprojde Eulerovým testem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ pro vhodné a nesoudělné s p, například pro $a = 7$.

Řešení. Z příkladu 5.1 víme, že pro libovolné a nesoudělné s 1 105 je $a^{48} \equiv 1$. Protože

$$\frac{1\,105 - 1}{2} = 552 = 48 \cdot 11 + 24,$$

máme $a^{552} \equiv a^{24} \pmod{1\,105}$. Hledáme některé a takové, že $a^{24} \not\equiv \pm 1 \pmod{1\,105}$. Opět z příkladu 5.1 víme, že $a^{24} \equiv 1 \pmod{5}$ i $\pmod{13}$, navíc také, že $a^{24} \equiv a^8 \pmod{17}$. Hledáme tedy takové a nesoudělné s 5 a 13, že $a^8 \equiv -1 \pmod{17}$. Pak totiž $x := a^{552}$ splňuje soustavu kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{13} \\ x &\equiv -1 \pmod{17} \end{aligned}$$

Sami ověřte, že jediným řešením je $x \equiv 781 \pmod{1\,105}$.

Vzhledem k tomu, že exponent 8 je sudý, víme, že kongruence budou platit pro $\pm a$. Modulo 17 tedy stačí zkoušet $a = 2$, 3, 4, 5, 6 a 7. Máme

$$\begin{aligned} 2^8 &= (2^4)^2 = 16^2 \equiv (-1)^2 = 1 \pmod{17}, \\ 3^8 &= (3^3)^2 \cdot 3^2 \equiv 10^2 \cdot 3^2 = 30^2 \equiv (-4)^2 = 16 \equiv -1 \pmod{17}, \\ 4^8 &= 2^{16} \equiv 1 \pmod{17}, \\ 5^8 &= (5^2)^4 = 25^4 \equiv 8^4 = 2^{12} \equiv 2^4 = 16 \equiv -1 \pmod{17}, \\ 6^8 &= 2^8 \cdot 3^8 \equiv 1 \cdot (-1) = -1 \pmod{17}, \\ 7^8 &= (7^2)^4 = 49^4 \equiv (-2)^4 = 16 \equiv -1 \pmod{17}. \end{aligned}$$

Máme tedy na výběr $a \in \{\pm 3, \pm 5, \pm 6, \pm 7\}$. Celkem tedy lze říci, že pro každé a kongruentní ± 3, ± 5, ± 6 nebo ± 7 modulo 17 nesoudělné s 5 i s 13 platí, že $a^{552} \equiv 781 \not\equiv 1 \pmod{1\,105}$. Například tedy pro $a = 3$, 6 nebo 7 číslo 1 105 neprojde Eulerovým testem. △

Příklad 5.3. Ukažte, že $p = 341$ projde Eulerovým testem pro $a = 2$, ale nikoli Eulerovým-Jacobiho testem pro $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ pro $a = 2$.

Řešení. Počítejme mocniny 2 modulo 341. Nejmenší mocnina, která se zkrátí je $2^9 = 512 \equiv 171 \pmod{341}$, pak $2^{10} \equiv 171 \cdot 2 = 342 \equiv 1 \pmod{341}$. Vidíme tedy, že

$$2^{\frac{341-1}{2}} = 2^{170} = (2^{10})^{17} \equiv 1 \pmod{341}.$$

Spočítejme nyní Jacobiho symbol $\left(\frac{2}{341}\right)$. Podle vlastnosti iii) máme

$$\left(\frac{2}{341}\right) = (-1)^{\frac{341^2-1}{8}} = -1$$

jelikož $341 = 42 \cdot 8 + 5$. Vidíme tedy, že $2^{170} \not\equiv \left(\frac{2}{341}\right) \pmod{341}$, tudíž 341 není prvočíslo. Skutečně máme rozklad $341 = 11 \cdot 31$, jedná se tedy o součin dvou prvočísel. To, že $\left(\frac{2}{341}\right) = -1$ pak znamená, že 2 je kvadratickým zbytkem modulo *právě jednoho* z prvočísel z rozkladu. Konkrétně $8^2 = 64 \equiv 2 \pmod{31}$. Navíc bychom z rozkladu mohli vidět, že $2^{10} \equiv 1 \pmod{11}$ a $2^{10} = 32^2 \equiv 1^2 = 1 \pmod{31}$, tedy i $2^{10} \equiv 1 \pmod{341}$. △

Příklad 5.4. Zpráva M byla zašifrována pomocí RSA s veřejným klíčem $(51, 13)$ (tj. $e = 13$, $n = 51$) do tvaru 7, 48, 11. Pokuste se šifru prolomit a najít M.

Řešení. Víme, že $n = 17 \cdot 3$. Pak $\varphi(n) = 2 \cdot 16 = 32$. Zjišťujeme tedy modulární inverzi k 13 modulo 32 pomocí hledání koeficientů Bézoutovy rovnosti.

$$\begin{pmatrix} 1 & 0 & 13 \\ 0 & 1 & 32 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 13 \\ -2 & 1 & 6 \end{pmatrix} \sim \begin{pmatrix} 5 & -2 & 1 \\ -32 & 13 & 0 \end{pmatrix}$$

a vidíme, že $d = 5$ Poté stačí dešifrovat

$$\begin{aligned} 7^5 = (7^2)^2 \cdot 7 \equiv (-2)^2 \cdot 7 = 4 \cdot 7 = 28 &\pmod{51} \\ 48^5 \equiv (-3)^5 = -3 \cdot 81 \equiv -3 \cdot 30 \equiv -90 \equiv 12 &\pmod{51} \\ 11^5 = 11^2 \cdot 11^3 = 121 \cdot 1\,331 \equiv 19 \cdot 5 = 95 \equiv 44 &\pmod{51} \end{aligned}$$

neboť $121 = 2 \cdot 51 + 19$ a $1331 = 26 \cdot 56 + 5$. Původní zpráva byla tedy 28, 12, 34. △

Příklad 5.5. Pomocí šifry RSA s veřejným klíčem $(551, 95)$, tj. $n = 551 = 19 \cdot 29$, $e = 95$, zašifrujte a poté dešifrujte zprávu $M = 25$.

Řešení. Zprávu $M = 25$ zašifrujeme tak, že počítáme

$$C \equiv M^{95} = 25^{95} = 25^{81+9+3+2}.$$

Máme $25^1 = 25$ a $25^2 = 625 \equiv 74 \pmod{551}$. Dále

$$25^3 \equiv 74 \cdot 25 = 1\,850 \equiv 197 \pmod{551}$$

$$\begin{aligned} 25^9 \equiv 197^3 = 7\,645\,373 \equiv 248 \pmod{551} \\ 25^{27} \equiv 248^3 = 15\,252\,992 \equiv 210 \pmod{551} \\ 25^{81} \equiv 210^3 = 9\,261\,000 \equiv 343 \pmod{551} \end{aligned}$$

tedy

$$\begin{aligned} 25^{95} &\equiv 343 \cdot 248 \cdot 197 \cdot 74 = \\ &= 85\,064 \cdot 14\,578 \equiv 210 \cdot 252 = \\ &= 52\,920 \equiv 24 \pmod{551} \end{aligned}$$

a vidíme, že $C \equiv 24 \pmod{551}$.

Pro dešifrování musíme zjistit soukromý klíč. Máme $\varphi(551) = 28 \cdot 18 = 504$, hledáme d – modulární inverzi k 95 modulo 504 – pomocí nalezení Bézoutových koeficientů.

$$\begin{pmatrix} 1 & 0 & 504 \\ 0 & 1 & 95 \end{pmatrix} \sim \begin{pmatrix} 1 & -5 & 29 \\ 0 & 1 & 95 \end{pmatrix} \sim \begin{pmatrix} 1 & -5 & 29 \\ -3 & 16 & 8 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 13 & -69 & -3 \\ -3 & 16 & 8 \end{pmatrix} \sim \begin{pmatrix} 13 & -69 & -3 \\ 23 & -122 & 2 \end{pmatrix} \sim \begin{pmatrix} -36 & 191 & 1 \\ -95 & 504 & 0 \end{pmatrix}$$

Vidíme, že $d = 191$. Při dešifrování počítáme $C^d = 24^{191}$ modulo 551. (Již víme, že to vyjde 25.) Protože $24^2 = 576 \equiv 25 \pmod{551}$, máme hned

$$M \equiv 24^{191} = 24^{2 \cdot 95 + 1} = (24^2)^{95} \cdot 24 \equiv 25^{95} \cdot 24 \equiv 24 \cdot 24 \equiv 25 \pmod{551}$$

a nemuseli jsme počítat vyšší mocniny. △

Příklad 5.6. Najděte primitivní kořen modulo 23 a demonstrujte DH protokol pro $a = 7$ a $b = 13$.

Řešení. Máme $\varphi(23) = 22 = 2 \cdot 11$. Zkoušíme různé mocniny čísel.

$$\begin{aligned} 2^2 &= 4 \\ 2^{11} &= (2^5)^2 \cdot 2 \equiv 9^2 \cdot 2 = 9 \cdot 18 \equiv 9 \cdot -5 = -45 \equiv 1 \pmod{23} \\ 3^2 &= 9 \\ 3^{11} &= (3^3)^3 \cdot 9 \equiv 4^3 \cdot 9 = 2^5 \cdot 2 \cdot 9 \equiv 9^2 \cdot 2 \equiv 1 \pmod{23} \\ 5^2 &= 25 \equiv 2 \pmod{23} \\ 5^{11} &\equiv 25^5 \cdot 5 \equiv 2^5 \cdot 5 = 32 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv -1 \pmod{23} \end{aligned}$$

Tudíž 5 je primitivní kořen modulo 23. Jiné primitivní kořeny jsou ty mocniny 5, kde exponent je nesoudělný s 22. Artem si zvolil exponent $a = 7$. Pošle tedy Barboře

$$5^7 = (5^2)^3 \cdot 5 \equiv 2^3 \cdot 5 = 40 \equiv -6 \pmod{23}.$$

Barbora si zvolila číslo $b = 13$. Pošle Artemovi

$$5^{13} = 25^6 \cdot 5 \equiv 2^6 \cdot 5 \equiv 9 \cdot 10 = 90 \equiv -2 \pmod{23}.$$

Společným klíčem pro komunikaci bude $5^{7 \cdot 13} = (5^{13})^7 \equiv (-2)^7 = -2^7 \equiv -9 \cdot 4 = -36 \equiv 10 \pmod{23}$. △

Příklad 5.7. Tomáš a Petr chtějí komunikovat šifrou ElGamal. Tomáš si zvolil prvočíslo $p = 31$, primitivní kořen $g = 12$ a číslo $x = 6$. Zveřejnil pak trijici $(31, 12, h)$, kde $h \equiv 12^6 \pmod{31}$. Petr mu poslal dvojici $(21, 27)$. Jakou zprávu poslal Petr Tomášovi?

Řešení. Nejprve spočítáme h. S využitím $2^5 \equiv 1$ a $3^3 \equiv -4 \pmod{31}$ máme

$$h \equiv 12^6 = 2^{12} \cdot 3^6 = 2^2 \cdot (-4)^2 = 2^6 \equiv 2 \pmod{31}.$$[1]

Musíme dešifrovat zprávu $(21, 27) \equiv (-10, -4) \pmod{31}$. Tomášův soukromý klíč je 6. Počítáme $(-10)^6 = 2^6 \cdot 5^6 \equiv 2 \cdot 1 = 2 \pmod{31}$. Inverze k 2 modulo 31 je 16 (ověřte sami), takže Petrova původní zpráva byla $-4 \cdot 16 = -64 \equiv -2 \equiv 29 \pmod{31}$. △

[1] K dešifrování vlastně nepotřebujeme znát číslo h, nicméně je dobré procvičení si jej spočítat.