Př. 5.1 i) $x^2 \equiv 1 \mod 30$

$30 = 2 \cdot 3 \cdot 5$

ČZV

$x^2 \equiv 1 \mod 2 \rightsquigarrow x \equiv 1$

$x^2 \equiv 1 \mod 3 \rightsquigarrow x \equiv \pm 1$

$x^2 \equiv 1 \mod 5 \rightsquigarrow x \equiv \pm 1$

$\Rightarrow$ celkem 4 řešení

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv \pm 1 \mod 3 \\ x &\equiv \pm 1 \mod 5 \end{aligned}$$

$\rightsquigarrow x = 2y + 1$

$2y + 1 \equiv \pm 1 \mod 3 \quad /\cdot 2$

$2y + 1 \equiv \pm 1 \mod 5 \quad /-3$

$y \equiv -2 \pm 2 \mod 3$

$y \equiv -3 \pm 3 \mod 5$

$y \equiv 1 \mp 1 \mod 5$

$y \equiv 2 \mp 2 \mod 5$

$\Rightarrow y = 3k - 1 \mp 1$ ... atd.

$y \in \{0, 5, 9, 14\} \mod 15$

$x = 2y + 1 \in \{1, 11, 19, 29\} \mod 30$

(ii) $x^3 + x + 3 \equiv 0 \mod 25$ = 5^2

„Hanselova lemma"

- $x^3 + x + 3 \equiv 0 \mod 5$

přímý výpočet: ~~0~~, ~~1~~, ~~2~~, ~~3~~, ~~4~~

↳ jediné řešení

$x = 5y + 1$

- $(5y+1)^3 + (5y+1) + 3 \equiv 0 \mod 25$

$(5y)^3 + 3(5y)^2 + 3 \cdot 5y + 1 + 5y + 1 + 5$

$\equiv 20y + 5 \equiv 0 \mod 25$

$:5$

$4y + 1 \equiv 5$

$-y \equiv -1 \mod 5$

$y \equiv 1 \mod 5$

$y = 5r + 1$

$x = 5(5r + 1) + 1$

$\Rightarrow 5r + 5 + 1$

$\equiv 6 \mod 25$

Zinės: $\boxed{x \equiv 6 \mod 25}$

5.1 (iii) $5x^2 + x + 8 \equiv 0 \mod 11 / \cdot 2$

$5^{\varphi(11)} = 5^{10} \equiv 1 \mod 11$

$5 \cdot 5^9 \equiv 1 \mod 11$

$\rightarrow -x^2 + 2x + 16 \equiv 0 \mod 11$

$x^2 - 2x - 16 \equiv 0 \mod 11$

$(x-1)^2 - 1 - 16 \equiv 0 \mod 11$

$y = x - 1 \rightsquigarrow \boxed{y^2 \equiv 6 \mod 11}$

Kvitérium prvočíselnosti:

$d = (2, \varphi(11)) = (2, 10) = 2$

má řešení

$\Leftrightarrow$

$6^{\frac{\varphi(11)}{d}} \equiv 1 \mod 11$

$6^{\frac{10}{2}} = 6^5 = 6 \cdot 36^2 \equiv$

$\equiv 6 \cdot 3^2 = 3 \cdot 18$

$\equiv 3 \cdot 7 \equiv -1 \mod 11$

$\Rightarrow$ nemá řešení

19

Jinak: $5x^2 + x + 8 \equiv 0 \mod 11$

$45x^2 + 9x + 72 \equiv 0 \mod 11$

$x^2 + (9+11)x - 5 \equiv 0 \mod 11$

$x^2 + 20x - 5 \equiv 0$

$(x+10)^2 - 100 - 5 \equiv 0 \mod 11$

$y = x + 10$ - - - .

Legendreův symbol:

$$\left(\frac{a}{p}\right) \begin{cases} 1 & p \nmid a,\ x^2 \equiv a \bmod p \text{ má řešení} \\ 0 & p \mid a \\ -1 & p \nmid a,\ x^2 \equiv a \bmod p \text{ nemá řešení} \end{cases}$$

$a \in \mathbb{Z}$

p prvočíslo (liché)

$\Rightarrow p-1 = \varphi(p)$
$z = (z, \varphi(p))$

- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $\left(\frac{p}{q}\right) = \pm\left(\frac{q}{p}\right)$

p, q liché prvočísla

platí $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Nejjednodušší čitatel

$$\left(\frac{1}{p}\right) = 1$$

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

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

$1987 \equiv \quad \mod 101$

$19 \cdot 101 = 1919$

Pr 5.2: $\left(\frac{101}{1987}\right) = \left(\frac{1987}{101}\right) = \left(\frac{68}{101}\right)$

$68 = 4 \cdot 17$

$101 \equiv -1 \mod 17$

$6 \cdot 17 = 102$

$= \underbrace{\left(\frac{2}{101}\right) \cdot \left(\frac{2}{101}\right)}_{=1} \cdot \left(\frac{17}{101}\right)$

$= \left(\frac{101}{17}\right) = \left(\frac{-1}{17}\right) = (-1)^{\frac{16}{2}} = 1$

$x^2 \equiv 101 \mod 1987$

nu i risolve

$\left(\frac{-35}{97}\right) = \left(\frac{5}{97}\right)\left(\frac{7}{97}\right)\left(\frac{-1}{97}\right)$

$= (-1)^{\frac{97-1}{2}} \left(\frac{97}{5}\right)\left(\frac{97}{7}\right) =$

$= \left(\frac{2}{5}\right)\left(\frac{-1}{7}\right) = (-1)^{\frac{5^2-1}{8}} \cdot (-1)^{\frac{7-1}{2}} = (-1)\,|\,(-1) = 1$

$\left(\frac{-23}{85}\right)$ — Jacobiho symbol

(zobecňuje Legendreův symbol)

Př. 5.3 (i) $x^2 \equiv 5 \mod 227$

↓

původně

- kvitérium

$$5^{\frac{\varphi(227)}{2}} = 5^{\frac{226}{2}} \equiv 5^{113} \equiv$$

$$\equiv 1 \Leftrightarrow \text{možná}$$

$d = (2, \varphi(227)) = 2$

- - - - -

- Legendreův symbol

$$\left(\frac{5}{227}\right) = \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = (-1)^3 = -1$$

$\Rightarrow$ není čtverec

(ii) $x^2 \equiv 5 \mod 229$

↳ premier

$$\left(\frac{5}{229}\right) = \left(\frac{229}{5}\right) = \left(\frac{-1}{5}\right) =$$

$$= (-1)^{\frac{5-1}{2}} = 1$$ mod premier

(iii) $x^2 \equiv 38 \mod 65$

$=$

$5 \cdot 13$

$x^2 \equiv 38 \equiv 3 \mod 5$

$x^2 \equiv 38 \equiv -1 \mod 13$

$x^2 \equiv 3 \mod 5$

$x^2 \equiv -1 \mod 13$

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right)$$

$$= (-1)^{\frac{3-1}{2}} = -1$$

$\Rightarrow$ même résidu

(ii) $x^2 - 23 \equiv 0 \mod 77$

$x^2 \equiv 23 \mod 77$

$77 = 7 \cdot 11$

$x^2 \equiv 23 \equiv 2 \mod 7$

$x^2 \equiv 23 \equiv 1 \mod 11$ $\rightsquigarrow$ má ± 1 v řešení

$\left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = (-1)^6 = +1$

má v řešení

- Má v řešení
- tato v řešení je $x \equiv \pm 3 \mod 7$

$\rightsquigarrow$ $x \equiv \pm 1 \mod 11$

$x \equiv \pm 3 \mod 7$

$x \in \{10, 32, 45, 67\} \mod 77$

Spec. prip.: $p \equiv 3 \mod 4 \wedge \left(\frac{a}{p}\right) = 1$

$x^2 \equiv a \mod p$ má v řešení

$\boxed{x = \pm a^{\frac{p+1}{4}}}$ $x^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a$, $a^{\frac{p-1}{2}} = 1$

Rabinův kryptosystém

- Alice zvolí dvě velká prvočísla p, q t. ž.

$$p, q \equiv 3 \bmod 4$$

$n := pq$ veřejný klíč

dvojice (p, q) soukromý klíč

šifrování zprávy M (posílá Bob)

$$C := M^2 \bmod n$$

dešifrování (provádí Alice)

řešíme

$$x^2 \equiv C \bmod p$$
$$x^2 = C \bmod q$$

$$x \equiv \pm C^{\frac{p+1}{4}} \mod p$$

$$y \equiv \pm C^{\frac{q+1}{4}} \mod q$$

---

mg 4 řešení (a mich se vybere to "správné")