(1) Řešte kongruenci $3x^2-5x+8\equiv 0\ (13)$

normujeme: $3\cdot u\equiv 1\ (13)$

$u\equiv -4\ (13)$

i) $3x^2-5x+8\equiv 0\ (13)\ |\cdot(-4)$

$x^2+\overset{7}{20}x-32\equiv 0\ (13)$

doplníme na □: $(x+10)^2-100-32\equiv 0\ (13)$

$\underbrace{(x+10)}_{y}{}^2\equiv 2\ (13)$

$y^2\equiv 2\ (13)$

Legendreův symbol: $\left(\frac{2}{13}\right)=-1$ ⇒ kongruence nemá řešení

$13\equiv -3\ (8)$

ii) $3x^2-5x+8\equiv 0\ (13)$

$3x^2-18x+21\equiv 0\ (13)\ |:3$

$x^2-6x+7\equiv 0\ (13)$

← analogicky

Pozn: $x^2\equiv a\ (p)$, pro $\left(\frac{a}{p}\right)=1$ má 2 řešení, nalézt lze efektivně (pouze pro $p\equiv 3\ (4)$)

V případě $p\equiv 1\ (4)$ lze efektivně určit pouze pro spec. případy

(např. $a\equiv 1 \Rightarrow x\equiv \pm 1$, $a\equiv -1 \Rightarrow$ pro g p.k. mod p je $x\equiv \pm g^{\frac{p-1}{4}}\ (p)$)

(2) Určete počet řešení kongruence

$x^2\equiv 1234 \pmod{2017}$, kde 2017 je prvočíslo

Vypočteme Leg. symbol: $\left(\frac{1234}{2017}\right) = \left(\frac{2}{2017}\right)\cdot\left(\frac{617}{2017}\right) =$

$2017\equiv 1\ (8)$ $\quad 2017\equiv 1\ (4)$ $\quad 1234 = 2\cdot 617$ $\quad$ není třeba ověřovat, že 617 je prvočíslo (viz Jacobiho symbol)

$= (+1)\cdot(+1)\left(\frac{2017}{617}\right) = \dots$

$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$, snadnější než $\frac{2017^2-1}{8}$ vypočteme $2017\equiv ? \pmod 8$

$\dots = \left(\frac{2017}{617}\right) = \left(\frac{166}{617}\right) = \left(\frac{2}{617}\right)\cdot\left(\frac{83}{617}\right) = (+1)\cdot(+1)\left(\frac{617}{83}\right) =$

$166 = 2\cdot 83$ $\quad 617\equiv 1\ (8)$ $\quad 617\equiv 1\ (4)$

$= \left(\frac{36}{83}\right) = \Big(\underbrace{\tfrac{6}{83}}_{\pm 1}\Big)^2 = 1$ ⇒ kongruence má 2 řešení.

(3) Řešte kongruenci $x^2\equiv 7 \pmod{83}$

Leg. symbol: $\left(\frac{7}{83}\right) = (-1)\cdot\left(\frac{83}{7}\right) = (-1)\left(\frac{-1}{7}\right) = (-1)\cdot(-1) = 1$

$83\equiv 7\equiv 3\ (4)$ $\quad 7\equiv 3\ (4)$

$x^2 \equiv a\ (p)$

$p \equiv 3(4), \left(\frac{a}{p}\right)=1$

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

Kongruence tedy má 2 řešení a protože $83 \equiv 3(4)$, jsou tvaru: $x \equiv \pm 7^{\frac{83+1}{4}}$

$7^{21} \pmod{83}$, využijeme algoritmus modulárního umocňování

$(10101)_2 = 21$, $= 7^{2^0} \cdot 7^{2^2} \cdot 7^{2^4}$

exp	base	result	last digit of exp
21	7	1	1
10	$49 \equiv -34$	7	0
5	-6	7	1
2	36	-42	0
1	51	41	1
0	...	16	

$49^2 = (50-1)^2 = 2401 \equiv -6\ (83)$

$2401 : 83 = 29$
-166
741
-747
-6

$51 \cdot 41 = 41 + 50 \cdot 41 \equiv$
$\equiv 41 + 25 \cdot (2 \cdot 41) \equiv$
$\equiv 41 + 25(-1) \equiv 16$

$36^2 = 3 \cdot 3 \cdot 12 \cdot 12 \equiv 108 \cdot 12$
$\equiv 25 \cdot 12 \equiv 300 \equiv 51\ (83)$

Závěr: řešením kongruence je $x \equiv \pm 16 \pmod{83}$

4

a) Určete všechna prvočísla p, pro něž je kongruence $x^2 \equiv 3 \pmod p$ řešitelná

spec. případy: $p=2$, $p \mid 3$ (tj. $p=3$):
$x^2 \equiv 3(2)$ ✓ $\quad x^2 \equiv 3(3)$ ✓

$p \neq 2,3$: kongruence je řešitelná $\iff \left(\frac{3}{p}\right)=1$

Podle ZKR: $1 = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right)$

$\iff$
- $(-1)^{\frac{p-1}{2}} = 1 \wedge \left(\frac{p}{3}\right)=1 \iff p \equiv 1(4) \wedge p \equiv 1(3) \iff p \equiv 1\ (12)$
- $(-1)^{\frac{p-1}{2}} = -1 \wedge \left(\frac{p}{3}\right)=-1 \iff p \equiv 3(4) \wedge p \equiv 2\ (3) \iff p \equiv -1\ (12)$

Kongruence $x^2 \equiv 3(p)$ je řešitelná $\iff p=2, p=3, p \equiv \pm 1\ (12)$

b)

Rozhodněte, pro která prvočísla p je $\left(\frac{-5}{p}\right)=1$

$p=2, p=5$ ✗

$1 = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} \cdot \left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right)$

$5 \equiv 1(4)$

$\iff$
- $(-1)^{\frac{p-1}{2}} = 1 \wedge \left(\frac{p}{5}\right)=1 \iff p \equiv 1(4) \wedge p \equiv \pm 1(5) \iff p \equiv 1, 9\ (20)$
- $(-1)^{\frac{p-1}{2}} = -1 \wedge \left(\frac{p}{5}\right)=-1 \iff p \equiv -1(4) \wedge p \equiv \pm 2(5) \iff p \equiv 3, 7\ (20)$

(5) Diffie-Hellman systém na výměnu klíčů („sdílení tajného čísla")
pro symetrickou kryptografii

Alice, Bob: dohodnou se na prvočísle p a p.t. g mod p
$p = 23$, $g = 5$

A: $a = 6$, $g^a = 5^6 \equiv 8 \pmod{23}$

B: $b = 15$, $g^b = 5^{15} \equiv 19 \pmod{23}$

A: $K \equiv 19^6 \equiv 2 \pmod{23}$ DLP ... discrete log problem

B: $K \equiv 8^{15} \equiv 2 \pmod{23}$

Vyzkoušejte po skupinkách v Breakout Rooms.