Binomické kongruence

Primitivní kořeny

Příklad 1. Určete všechny primitivní kořeny modulo 11.

Lemma. *Je-li řád a roven r, pak řád a^n je roven $\frac{r}{(r,n)}$.*

Důsledek. *Primitivní kořen g je řádu $\varphi(m)$, proto g^n je primitivní kořen, právě když $(n,\varphi(m))=1$.*

Řešení. Z rozkladu $\varphi(11)=2\cdot 5$ dostáváme, že g je primitivní kořen modulo 11 právě tehdy, když $g^2 \not\equiv 1 \not\equiv g^5 \pmod{11}$. Každý další primitivní kořen je pak tvaru g^n, kde $(n,\varphi(11))=1$.

k	2	3	4	5	6	7	8	9	10
$2^k \pmod{11}$	4	8	5	10	9	7	3	6	1

Nesoudělné s 10 jsou $1,3,7,9$. Primitivní kořeny jsou tedy $2,8,7,6$.

Příklad 2. Určete všechny primitivní kořeny modulo 23 a nalezněte nějaký primitivní kořen modulo $529=23^2$ a $1058=2\cdot 23^2$.

Věta. *Je-li g primitivní kořen modulo $p\neq 2$ s vlastností $g^{p-1}\not\equiv 1 \pmod{p^2}$, pak je g primitivní kořen modulo p^l pro každé $l\in\mathbb{N}$.*

Řešení. Protože $\varphi(23)=2\cdot 11$, stačí ověřit, že $g^2\not\equiv 1\not\equiv g^{11} \pmod{23}$.

k	2	3	4	5	6	11
$2^k \pmod{23}$	4	8	16	9	-5	1
$3^k \pmod{23}$	9	4	12	13	-7	1
$5^k \pmod{23}$	2	10	4	-3	8	-1

Primitivní kořeny jsou tedy 5^k pro $k\in\{1,3,5,7,9,13,15,17,19,21\}$.
Hledáme-li primitivní kořeny modulo 23^2, pak stačí uvážit primitivní kořen modulo 23 a pak ověřit, zda

$$g^{22}\not\equiv 1 \pmod{23^2}.$$

Pokud je tato podmínka splněna, pak dle předchozí věty bude g primitivní kořen modulo 23^2. V opačném případě jím bude $g+23$.

$$5^{22}=\left(5^2\right)^{11}=(23+2)^{11}\equiv 2^{11}+2^{10}\cdot 11\cdot 23=4\cdot 2^9+2^9(23-1)\cdot 23\equiv$$
$$\equiv 4\cdot(-17)+(-17)(-23)\equiv 23\cdot 17-4\cdot 17\equiv 323\not\equiv 1 \pmod{23^2}$$

Primitivním kořenem modulo 529 je 5. Promitivním kořenem modulo 1058 je též 5.

Binomické kongruence - teorie

Lemma. *Nechť g je primitivní kořen modulo m. Pak*

- $g^0, g^1, \ldots, g^{\varphi(m)-1}$ *je redukovaná soustava zbytků modulo m,*
- $g^r \equiv g^s \pmod{m} \Leftrightarrow r \equiv s \pmod{\varphi(m)}$.

Věta (O řešitelnosti binomických kongruencí)**.** *Buď $m \in \mathbb{N}$ pro něž existují primitivní kořeny, $a \in \mathbb{Z}$, $(a,m) = 1$, $n \in \mathbb{N}$. Označme $d = (n, \varphi(m))$.*

- *Kongruence $x^n \equiv a \pmod{m}$ je řešitelná $\Leftrightarrow a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$.*
- *Pokud je tato kongruence řešitelná, pak má právě d řešení.*

Myšlenka důkazu. Označme g primitivní kořen modulo m. Neznámou x nahradíme neznámou y pro něž platí vztah

$$x \equiv g^y \pmod{m}.$$

Podobně existuje, a to jediné, $b \in \{0, 1, \ldots \varphi(m) - 1\}$ takové, že

$$a \equiv g^b \pmod{m}.$$

Dostáváme

$$(g^y)^n \equiv g^b \pmod{m},$$

což dává lineární kongruenci

$$ny \equiv b \pmod{\varphi(m)}.$$

Důsledek. *Za předpokladů věty pokud navíc $(n, \varphi(m)) = 1$, pak má kongruence $x^n \equiv a \pmod{m}$ vždy jediné řešení.*

Věta. *Buď p prvočíslo $a \in \mathbb{Z}$, α, $n \in \mathbb{N}$ takové, že $p \nmid an$. Je-li kongruence $x^n \equiv a \pmod{p}$ řešitelná, je řešitelná i kongruence $x^n \equiv a \pmod{p^\alpha}$ a má stejný počet řešení.*

Binomické kongruence - příklady

Příklad 3. Řeště

$$x^3 \equiv 1 \pmod{23}.$$

Řešení. Přímou aplikací důsledku věty o řešitelnosti binomických kongruencí dostáváme, že kongruence má právě jedno řešení. Tím je $x \equiv 1 \pmod{23}$.

Příklad 4. Řeště

$$x^3 \equiv 5 \pmod{23}.$$

Řešení. Opět aplikací důsledku věty o řešitelnosti binomických kongruencí dostáváme, že kongruene má právě jedno řešení. Z důkazu věty plyne i metoda, jak tento kořen získat. Vyjádříme pravou i levou stranu jako mocninu primitivního kořene. Díky tomu, že 5 je primitivní kořen, dostáváme substitucí $x = 5^y$

$$5^{3y} \equiv 5^1 \pmod{23}.$$

Odtud

$$3y \equiv 1 \pmod{22},$$

Vynásobením -7 dostáváme

$$y \equiv -7 \equiv 15 \pmod{22}.$$

To dává řešení

$$x = 5^{15} \equiv 5 \cdot 25^7 \equiv 5 \cdot 2^7 \equiv 5 \cdot 4 \cdot 9 \equiv -27 \equiv -4 \pmod{23}.$$

Skutečně

$$(-4)^3 = -64 \equiv 5 \pmod{23}.$$

Příklad 5. Řeště

$$x^8 \equiv 8 \pmod{23}$$

Řešení. Protože $(8,22) \neq 1$, nelze aplikovat jen důsledek. Musíme tedy použít větu o řešitelnosti binomických kongruencí. Máme

$$a = 8, \quad m = 23, \quad n = 8, \quad d = 2.$$

Protože $(a,m) = 1$, lze větu aplikovat. Ověřme, zda má kongruence řešení:

$$8^{11} = 2^{33} \equiv 2^{11} \equiv 2 \cdot 9^2 = 162 = 1 + 23 \cdot 7 \equiv 1 \pmod{23}.$$

Kongruence má tedy 2 řešení. Opět $x = 5^y$. Nyní musíme nalézt takové k, aby $5^k \equiv 8 \pmod{23}$. Z druhého příkladu máme

$$5^6 \equiv 8 \pmod{23}.$$

To dává

$$5^{8y} \equiv 5^6 \pmod{23}.$$

Odtud

$$\begin{aligned} 8y &\equiv 6 \pmod{22}, \\ 4y &\equiv 3 \pmod{11}, \\ y &\equiv 9 \pmod{11}. \end{aligned}$$

Dostáváme, že $y \equiv 9, 20 \pmod{22}$. To dává dvě řešení

$$x = 5^9, 5^{20} \equiv \pm 12 \pmod{23}.$$

Skutečně

$$(\pm 12)^8 \equiv 6^4 \equiv 13^2 \equiv 8 \pmod{23}.$$

Doplňující příklad. Řešte

$$x^8 \equiv 5 \pmod{23}.$$

Řešení. Protože $(5,23) = 1$, můžeme použít větu o řešitelnosti binomických kongruencí. Máme $d = (8,22) = 2$ a 5 je primitivní kořen modulo 23, je

$$5^{11} \equiv -1 \pmod{23}$$

a kongruence tedy nemá řešení. Vždyť kdybychom položili $x = 5^y$, dostáváme

$$\begin{aligned} 5^{8y} &\equiv 5^1 \pmod{23}, \\ 8y &\equiv 1 \pmod{22}. \end{aligned}$$

Tj. chceme, aby $22 \mid (8y-1)$, což vzhledem k paritě $8y-1$ není možné.

Příklad 6. Řešte

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \pmod{29}$$

Řešení. Vynásobením $x-1$ dostáváme binomickou rovnici

$$x^7 \equiv 1 \pmod{29}.$$

Protože $d = (7\varphi(29)) = 7$, existuje dle věty o řešitelnosti kongruencí právě 7 řešení. Nalezněme nejprve primitivní kořen. Protože $\varphi(29) = 2^2 \cdot 7$, musíme ověřit $g^{14} \not\equiv 1 \not\equiv g^4$. Přes Legendrův symbol máme ihned

$$2^{14} \equiv \left(\frac{2}{29}\right) = (-1)^{\frac{29^2-1}{8}} = -1 \pmod{29},$$

bez něj musíme uvážit

k	4	7	14
$2^k \pmod{29}$	16	12	-1

.

Máme primitivní kořen $g = 2$. Zjevně $2^{28} = 1$. Dostáváme

$$\begin{aligned} 2^{7y} &\equiv 2^{28} \pmod{29} \\ 7y &\equiv 28 \equiv 0 \pmod{28} \\ y &\equiv 0 \pmod{4} \end{aligned}$$

Dostáváme řešení $x = 1, 2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}$. Protože původní kongruence byla stupně 6, může mít nejvýše 6 řešení - vždyť jsme při tvorbě binomické kongruence přidali řešení $x = 1$. Celkem tedy

$$x = 16^k, \quad k \in \{1,2,3,4,5,6\}.$$

Věta (Hanselovo lemma)**.** *Buď p prvočíslo, $f \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$ takové, že $p \mid f(a)$ a $p \nmid f'(a)$ (tj. a je kořenem polynomu f modulo p, ale už není kořenem f'), pak pro každé $n \in \mathbb{N}$ má soustava*

$$\begin{aligned} f(x) &\equiv 0 \pmod{p^n}, \\ x &\equiv a \pmod{p} \end{aligned}$$

právě jedno řešení modulo p^n.

Příklad 7. Určete počet řešení kongruence

$$5x^{30} \equiv 37 \pmod{41^2}.$$

Řešení. Využijeme Hanselova lemmatu: vyřešíme tedy kongruenci modulo 41 a pak se podíváme, zda jsou splněny předpoklady.

$$\begin{aligned} 5x^{30} &\equiv 37 \pmod{41} \\ x^{30} &\equiv -8 \cdot (-4) \equiv 32 \pmod{41} \end{aligned}$$

Jistě $(32, 41) = 1$. Nejprve určíme, že $d = (30, \varphi(41)) = 10$. Nyní musíme o věřit, že

$$32^4 \equiv (-9)^4 = 81^2 \equiv (-1)^2 = 1 \pmod{41}.$$

Kongruence má tedy $d = 10$ řešení, každé nenulové. Hanselovo lemma bychom aplikovali na trochu jiný polynom (neboť inverzi k 5 bychom museli počítat modulo 41^2 a ne jen 41) ten má však stejné kořeny modulo p a liší se jen v absolutním členu (ten bude jistě i nadále nedělitelný 41). Protože $f' = 30x^{29}$ a jeho kořeny jsou jen 0, máme pro každý kořen modulo p právě jeden kořen modulo p^2. Dostáváme tedy 10 řešení.

Příklad 8. Určete počet řešení kongruence

$$x^7 \equiv 12 \pmod{29^2}.$$

Řešení. Řešme nejprve modulo 29. Protože $d = (7, \varphi(29)) = 7$, ověřujeme

$$12^{\frac{\varphi(29)}{7}} = 12^4 \equiv (-1)^2 = 1 \pmod{29}.$$

Z věty o řešení binomických kongruencí dostáváme, že existuje právě 7 řešení modulo 29, každé zřejmě nenulové. Protože derivace polynomu $x^7 - 12$ má jen nulové kořeny, existuje pro každé řešení modulo 29 dle Hanselova lemmatu právě jedno řešení modulo 29^2. Dostáváme tedy, že existuje právě 7 řešení.