2. domácí úloha z MIN401, jaro 2024

Příklad 1.

a) Číslo 67 je primitivním kořenem modulo 47, ale nikoliv modulo $47^2 = 2209$. **Jaký** musí být řád 67 modulo 2209? (Asi se vám bude hodit, že řád každého prvku dělí $\varphi(2209)$. Žádné mocniny není potřeba počítat explicitně.)

b) Umocněním $48^{47} = (1+47)^{47}$ podle binomické věty **určete** zbytek $48^{47} \pmod{2209}$. **Jaký** musí být řád 48 modulo 2209?

c) **Ukažte**, že číslo $67 \cdot 48$ je primitivní kořen modulo 2209 tím, že nebudete potřebné mocniny počítat přímo, ale zjednodušíte je s využitím předchozích dvou bodů.

Řešení.

a) Protože $\varphi(47^2) = 2 \cdot 23 \cdot 47$ a $67 \pmod{47}$ je primitivní kořen, dostáváme $67^{2\cdot 47} \equiv 67^2 \not\equiv 1 \pmod{47}$ a stejně tak $67^{23\cdot 47} \equiv 67^{23} \not\equiv 1 \pmod{47}$, takže nemůže vyjít 1 ani modulo 47^2, a protože není 67 primitivní kořen modulo 47^2, zbývá jediná možnost $67^{2\cdot 23} \equiv 1 \pmod{47^2}$ a řád $67 \pmod{47^2}$ je nějaký dělitel $2 \cdot 23 = 46$. Ze stejného důvodu $67^2 \not\equiv 1 \pmod{47}$ a také $67^{23} \not\equiv 1 \pmod{47}$, takže ani modulo 47^2 a tedy řád musí vyjít 46.

b) Dostáváme

$$48^{47} \equiv (1+47)^{47} \equiv 1 + \binom{47}{1} \cdot 47^1 + \binom{47}{2} \cdot 47^2 + \cdots \equiv 1 \pmod{47^2},$$

a protože exponent 47 je prvočíslo, musí být řád 48 modulo 47^2 roven 47.

c) Z předchozích bodů dostáváme

$$\begin{aligned}(67 \cdot 48)^{2\cdot 47} &\equiv 67^{2\cdot 47} \cdot 1 \not\equiv 1 \pmod{47^2}\\ (67 \cdot 48)^{23\cdot 47} &\equiv 67^{23\cdot 47} \cdot 1 \not\equiv 1 \pmod{47^2}\\ (67 \cdot 48)^{2\cdot 23} &\equiv 1 \cdot 48^{2\cdot 23} \not\equiv 1 \pmod{47^2}\end{aligned}$$

□

Příklad 2.

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.)

Řešení.

a) Standardním způsobem spočítáme

$$\left(\tfrac{185}{341}\right) = +\left(\tfrac{341}{185}\right) = \left(\tfrac{156}{185}\right) = \underbrace{\left(\tfrac{2}{185}\right)^2}_{(+1)^2} \cdot \left(\tfrac{39}{185}\right) = +\left(\tfrac{185}{39}\right) = \left(\tfrac{29}{39}\right)$$

$$= +\left(\tfrac{39}{29}\right) = \left(\tfrac{10}{29}\right) = \underbrace{\left(\tfrac{2}{29}\right)}_{-1} \cdot \left(\tfrac{5}{29}\right) = -\left(\tfrac{29}{5}\right) = -\left(\tfrac{4}{5}\right) = -\underbrace{\left(\tfrac{2}{5}\right)^2}_{(-1)^2} = -1.$$

Protože je řád 185 modulo 341 roven 10, dostáváme

$$185^{\frac{341-1}{2}} \equiv 185^{170} \equiv 1 \not\equiv \left(\tfrac{185}{341}\right) \pmod{341}.$$

b) Je-li $x \pmod{341}$ nesoudělné s modulem, pak

$$x^{10} \equiv 1 \pmod{11} \qquad\qquad x^{30} \equiv 1 \pmod{31}$$

takže dohromady $x^{30} \equiv 1 \pmod{341}$. Zároveň, protože 21 je primitivní kořen modulo 31, má řád 30 modulo 31, tím spíš modulo 341 a tedy 21 mám maximální možný řád 30.

□