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.

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.)