

Cvičení 12. 4. 2013

Číslo a je kvadratický zbytek modulo n , pokud existuje m , že $m^2 \equiv a \pmod{n}$.
Ne každé číslo je kvadratický zbytek.

Značení: Pro p prvočíslo větší než dva zachycuje vlastnost „ a je kvadratický zbytek modulo p “ takzvaný Legendreův symbol $\left(\frac{a}{p}\right)$ s hodnotou 0 pokud $p|a$, 1 pokud a je kvadratický zbytek a -1 pokud a je kvadratický nezbytek (tj. není kvadratický zbytek).

S Legendreovými symboly jde rozumně počítat:

1. Pokud $a \equiv b \pmod{p}$, tak $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
2. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,
3. platí $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$,
4. $\left(\frac{2}{p}\right) = 1$ pro $p \equiv 1, 7 \pmod{8}$ a -1 pro $p \equiv 3, 5 \pmod{8}$.
5. Pokud p, q jsou prvočísla různá od 2, tak platí kvadratická reciprocita

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

(Tj. napravo vychází -1 , právě když $p, q \equiv 3 \pmod{4}$, jinak vyjde 1.)

Příklad 1. Spočtete:

1. $\left(\frac{24}{37}\right)$
2. $\left(\frac{31}{71}\right)$
3. $\left(\frac{512}{29}\right)$
4. $\left(\frac{12345}{331}\right)$

Příklad 2. Najděte všechny kvadratické zbytky modulo:

1. 17,
2. 15.

Příklad 3. Kolik řešení má rovnice $x^2 \equiv 23 \pmod{113}$? A co rovnice $x^2 \equiv 37 \pmod{91}$ (pozor, není prvočíslo)?

Příklad 4. Mějme rovnici $ax^2 + bx + c \equiv 0 \pmod{p}$, kde prvočíslo $p > 2$ nedělí a . Označme $D = b^2 - 4ac$. Dokažte, že tato rovnice má řešení, právě když $\left(\frac{D}{p}\right) \geq 0$. Jak je to s počtem řešení?

Příklad 5. Buď $p > 2$ prvočíslo, $n \in \mathbb{N}$. Dokažte, že a nesoudělné s p je kvadratický zbytek modulo p^n , právě když $\left(\frac{a}{p}\right) = 1$.

Kreativní příklady

Příklad 6. Spočtete $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)$ pro p prvočíslo.

Příklad 7. Pomocí zákona kvadratické reciprocity vyjádřete v závislosti na p hodnoty $\left(\frac{3}{p}\right)$ a $\left(\frac{5}{p}\right)$.

Příklad 8. Buď $p > 2$ prvočíslo. Označme X součin všech kvadratických zbytků modulo p (zbytky bereme z množiny $\{1, \dots, p-1\}$). Dokažte, že pokud $p = 4k + 1$, tak $X \equiv -1 \pmod{p}$ a pokud $p = 4k + 3$, tak $X \equiv 1 \pmod{p}$.

Opakování: Řády prvků v grupách

Příklad 9. Rozhodněte, zda následující grupy jsou cyklické:

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$,
2. \mathbb{Z}_{13}^* ,
3. \mathbb{Z}_{14}^* ,
4. \mathbb{Z}_{24}^* .

Příklad 10. Pro danou grupu G najděte všechny prvky $g \in G$, že $\langle g \rangle = G$:

1. $G = \mathbb{Z}$,
2. $G = \mathbb{Z}_{10}$,
3. $G = \mathbb{Z}_5 \times \mathbb{Z}_8$,
4. $G = \mathbb{Z}_n$ pro obecné $n \in \mathbb{N}$.

Příklad 11. Určete, kolik prvků kterého řádu obsahuje grupa:

1. \mathbb{Z}_{10} ,
2. \mathbb{Z}_{11}^* ,
3. $\mathbb{Z}_5 \times \mathbb{Z}_8$.

Příklad 12. Najděte $m \neq n$ taková, že $\mathbb{Z}_n^* \simeq \mathbb{Z}_m^*$.

Příklad 13. Existuje n takové, že \mathbb{Z}_n^* je isomorfní:

1. \mathbb{Z}_7 ,
2. \mathbb{Z}_8 ,
3. \mathbb{Z}_9 ?