1. cvičení (28. února 2007)

Co jsme dělali?

Zabývali jsme se grupou $\mathbb{Z}_n^*$. Je to vskutku grupa, tedy například pro každé $a \in \mathbb{Z}_n^*$ existuje právě jedno $b \in \mathbb{Z}_n^*$ takové, že $ab = 1$. Toto b často značíme a^{-1} nebo $\frac{1}{a}$.

Definovali jsme Eulerovu funkci $\varphi(n) = |\mathbb{Z}_n^*|$, řekli si, že pro $a \in \mathbb{Z}_n^*$ jsou aditivní) grupy $a\mathbb{Z}_n$ a $\mathbb{Z}_n$ izomorfní (z čehož jde dokázat malá Fermatova věta).

Připomněli jsme si, co je to řád prvku a grupy a jak z Lagrangeovy věty vyplývá malá Fermatova věta. Pak jsme definovali primitivní prvek (prvek řádu $\varphi(n)$). Grupa invertibilních prvků $\mathbb{Z}_p^*$, kde p je prvočíslo, je cyklická ($\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$), neboli v ní existuje primitivní prvek.

Příklady

-1. (2 různými způsoby - využitím $a\mathbb{Z}_n^* \simeq \mathbb{Z}_n^*$ nebo pomocí Lagrangeovy věty) Dokaž malou Fermatovu větu, tedy že pro prvočíslo p a a, p nedělí a, platí $a^{p-1} \equiv 1 \pmod{p}$.

0. Dokaž, že 2 je primitivní prvek modulo 29.

1. Najdi všechny primitivní prvky modulo 19.

2. (opět 2 různými způsoby) Dokaž Eulerovu větu, tedy že pokud $(a, n) = 1$, platí $a^{\varphi(n)} \equiv 1 \pmod{n}$.

3. Dokaž, že 198 dělí $13^{62} + 29$.

4. Dokaž, že je-li a primitivní prvek modulo p, platí $a^{(p-1)/2} \equiv -1 \pmod{p}$.

5. Dokaž, že prvočíslo p dělí čitatele zlomku $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$.

6. Kolik je primitivních prvků modulo p?

7. Každé prvočíslo $p \neq 2, 5$ dělí nekonečně mnoho čísel tvaru $111 \ldots 1$.

8. Dokaž, že součin všech primitivních prvků modulo prvočíslo p je kongruentní s $(-1)^{\varphi(p-1)} \pmod{p}$.

Těžší příklady

1. p^2 dělí čitatele zlomku $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ ($p \geq 5$ je prvočíslo).

2. Dokaž, že je-li $2^n + 1 = p$ prvočíslo, je 3 primitivní prvek modulo p.