5. Довести, що первісні

Корені mod m існують т.т.т.к. $m = 1, 2, 4, p^n$ або $2p^n$ для деякого непарного простого p та $n \geq 1$.

Ми знаємо, що при $m = p^n$ $(\mathbb{Z}/m\mathbb{Z})^\times$ є циклічною.

При $m = 2, 4$ це легко перевірити вручну.

Покажемо, що $(\mathbb{Z}/2p^n\mathbb{Z})^\times$ є циклічною.

$$(\mathbb{Z}/2p^n\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$$

Нехай $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle g \rangle$

Покажемо, що $(1, g)$ породжує $(\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Нехай $a \in (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$

Тоді $a = (\tau, b)$ де b - деякий елемент $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Тоді існує $k \in \mathbb{Z}$: $b = g^k$ тому $a = (\tau, b) = (\tau^k, g^k) = (\tau, g)^k$.

Отже $(\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$ - циклічна, а тому $(\mathbb{Z}/rp^n\mathbb{Z})^\times$ циклічна.

Тепер покажемо, що для всіх інших m, $(\mathbb{Z}/m\mathbb{Z})^\times$ не є циклічною. Маємо два випадки:

1) m має лише один простий дільник. Тоді цей дільник це 2 і $m = 2^n$ з $n \geq 3$. Тоді $(\mathbb{Z}/m\mathbb{Z})^\times$ не є циклічною адже містить два елементи порядку 2 наприклад

$2^{n-1}+1$ і $2^n - 1$

$(2^{n-1}+1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \pmod{2^n}$,

бо при $n \geq 3$ маємо $2n-2 \geq n$

$(2^n-1)^2 = 2^{2n}$ $2^{n+1}+1 \equiv 1 \pmod{2^n}$

і при цьому $1 < 2^{n-1}+1 < 2^n-1 < 2^n$.

~~Ще~~ Середня нерівність виконується завдяки $n \geq 3$.

2) m має більш ніж один простий дільник. Тоді m має два непарних простих дільників p і q. ~~Позначимо~~ Тоді $m = p^{n-1}q^{n-1}m'$ де $p \nmid m$ і $q \nmid m$. Тоді

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p^{n-1}\mathbb{Z})^\times \times (\mathbb{Z}/q^{n-1}\mathbb{Z})^\times (\mathbb{Z}/m'\mathbb{Z})^\times$$

Доведемо дві леми:

Лема 1: Якщо прямий добуток груп $G \times H$ - циклічний і $G \times H = \langle (a, b) \rangle$. Тоді $G = \langle a \rangle$ і $H = \langle b \rangle$

Доведення: ~~$G \times H = \langle (a, b) \rangle \Rightarrow$~~

~~$\Rightarrow \exists k \in \mathbb{Z} : (a, e)$~~

З міркувань симетрії достатньо довести $G = \langle a \rangle$.

Нехай c - довільний елемент G. $(c, e) \in G \times H \Rightarrow \exists k \in \mathbb{Z}$:

$(c, e) = (a, b)^k = (a^k, b^k) \Rightarrow$

$\Rightarrow \exists k \in \mathbb{Z} : c = a^k$

З довільності c маємо $G = \langle a \rangle$ ☒

Лема 2: ~~Якщо~~ Якщо p і q - натуральні прості, то

$(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/q^m\mathbb{Z})^\times$ – не є циклічною

Дов. Припустимо, що це не так і $\langle (a,b) \rangle = (\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/q^m\mathbb{Z})^\times$

Тоді з леми 1: $\langle a \rangle = (\mathbb{Z}/p^n\mathbb{Z})^\times$ і $\langle b \rangle = (\mathbb{Z}/q^m\mathbb{Z})^\times$. Тоді

$|a| = \varphi(p^n) = p^{n-1}(p-1)$

$|b| = \varphi(q^m) = q^{m-1}(q-1)$

Зрозуміло, що

$(a,b)^{\text{lcm}(|a|,|b|)} = (a^{\text{lcm}(|a|,|b|)}, b^{\text{lcm}(|a|,|b|)}) =$

$= (e\ e)$. Тому $|(a,b)| \le \text{lcm}(|a|,|b|) =$

$= \frac{|a||b|}{\gcd(|a|,|b|)} \le \left[\begin{array}{l} |a| \text{ і } |b| - \\ \text{-парні} \end{array}\right] \le \frac{|a||b|}{2} < |a||b|$

Але $\langle (a,b) \rangle = (\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/q^m\mathbb{Z})^\times$

тому $|(a,b)| = |(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/q^m\mathbb{Z})^\times| =$

$= |a||b| > |(a,b)|$. Суперечність. ∎

Тоді $\overset{\text{з леми 2}}{\downarrow}$ $(\mathbb{Z}/p^{n_1}\mathbb{Z})^\times \times (\mathbb{Z}/q^{n_2}\mathbb{Z})^\times$ – не є циклічною. Тоді з леми 1

$(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/q^m\mathbb{Z})^\times \times (\mathbb{Z}/r^l\mathbb{Z})^\times$

тем не ∈ циклическое.

□