14 березня

§7. Лишки за модулем степенів простих чисел. Лема Гензеля.

Скільки розв'язків x має

$$x^5 + x + 1 \equiv 0 \pmod{675}?$$

$675 = 5^2 \cdot 3^3$

Кожна пара розв'язків

$$x^5 + x + 1 \equiv 0 \pmod{5^2}$$

та

$$x^5 + x + 1 \equiv 0 \pmod{3^3}$$

однозначно підноситься до розв'язку mod 675 за китайською теоремою про лишки.

Тому достатньо навчитися розв'язувати для $f(x) \in \mathbb{Z}[x]$ конгруенції виду

$$f(x) \equiv 0 \mod p^n$$

для $n = 1, 2, 3, \ldots$

mod 3

x	0	1	2
x^5+x+1	1	0	2

mod 5

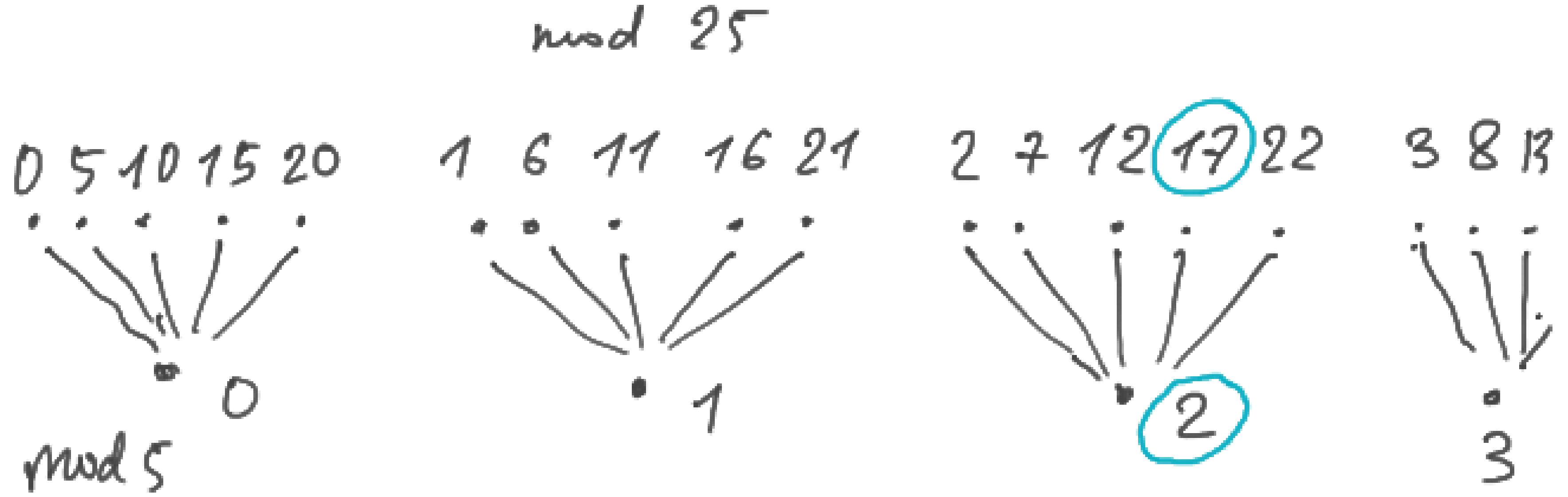
x	0	1	2	3	4
x^5+x+1	1	3	0	2	4

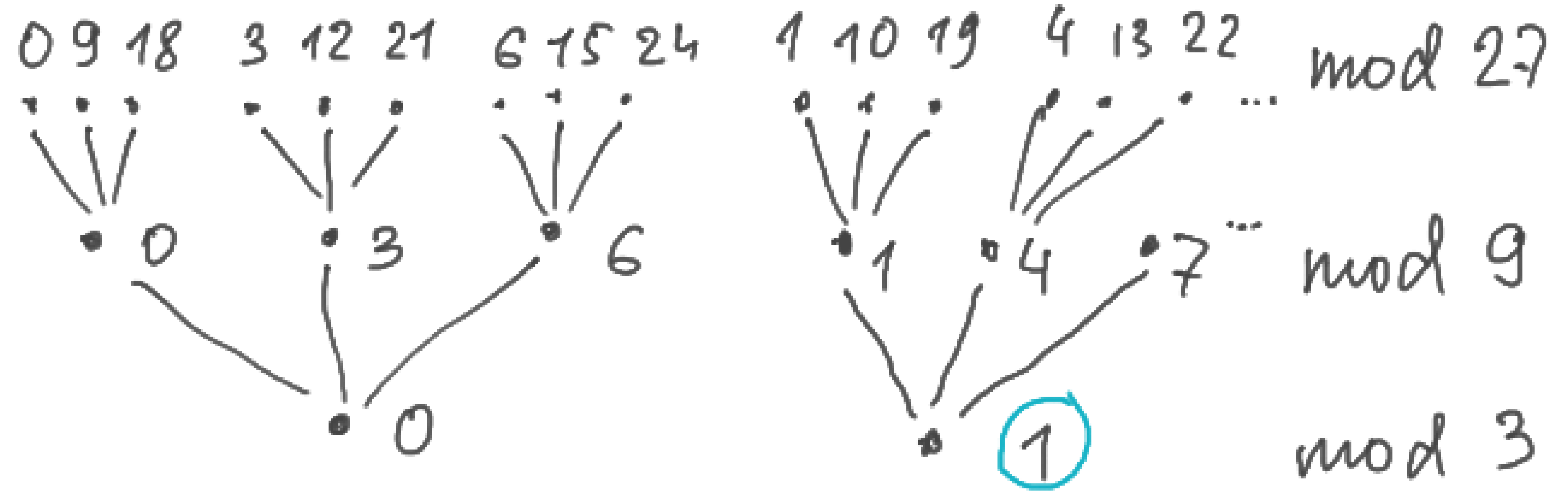
<u>Спостереження</u>: якщо $a \mod p^n$ є розв'язком $f(a) \equiv 0 \mod p^n$ тоді також $f(a) \equiv 0 \mod p^{n-1}$.

Озн-ня Лишок $a \bmod p^n$ є піднесенням лишку $b \bmod p^{n-1}$ якщо $a \equiv b \pmod{p^{n-1}}$. b є обмеженням a.

Кожен розв'язок $f(x) \equiv 0 \ (p^n)$ є піднесенням деякого (єдиного) розв'язку $f(x) \equiv 0 \ (p^{n-1})$.

Стратегія: щоби знайти розв'язки $f(x) \equiv 0 \pmod{p^n}$ починаємо з $f(x) \equiv 0 \pmod{p}$, намагаємося піднести розв'язки mod p^2, p^3 і так далі.





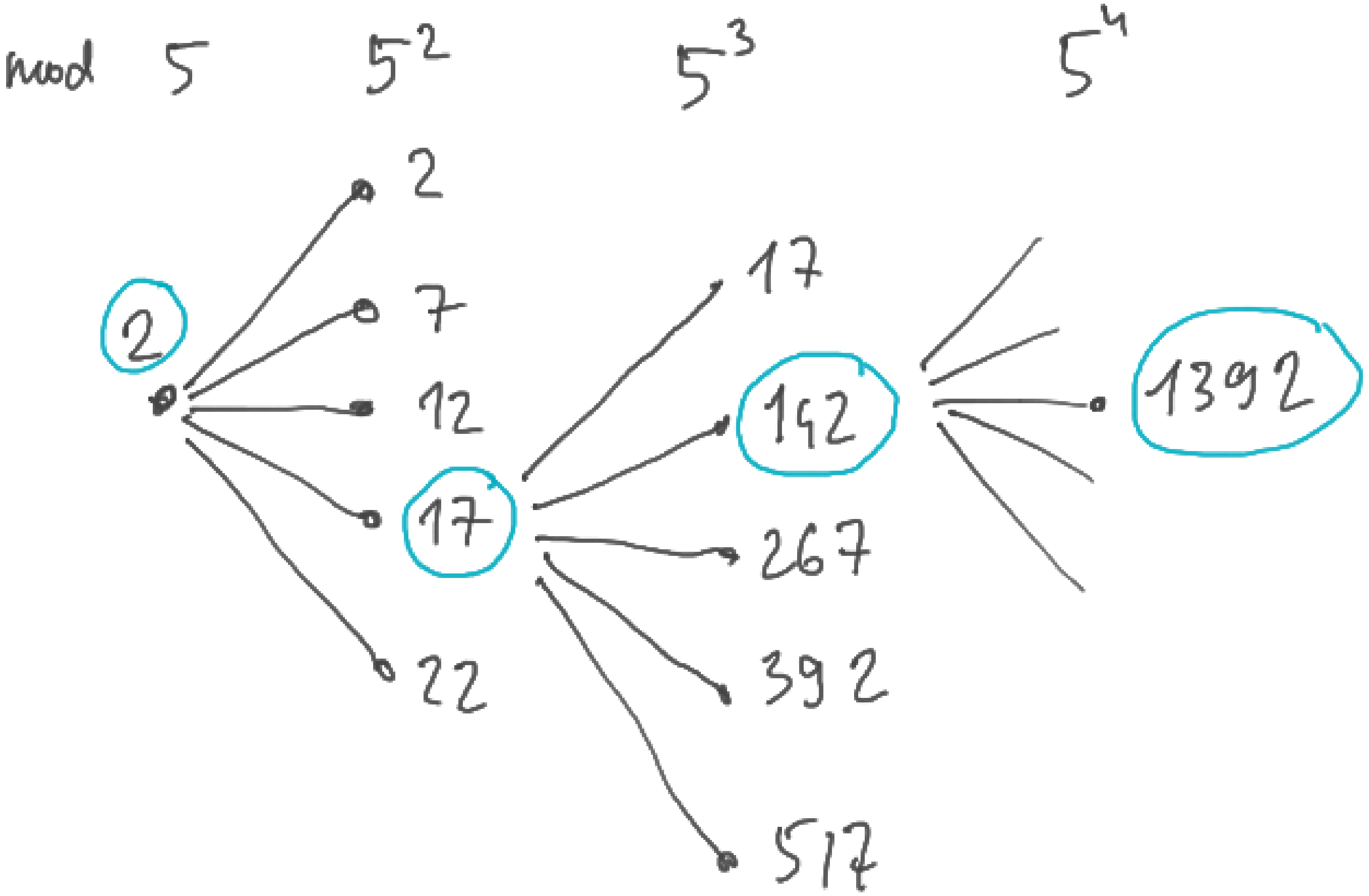
x	1	4	7
x^5+x+1	3	3	3

mod 9

немає розв'язків mod 9

Наприклад:

$$x^5 + x + 1 \equiv 0 \pmod{5^n}$$



Припустимо $f(a) \equiv 0 \pmod{p^n}$.

Піднесення a за модулем p^{n+1} це

$$a + tp^n \qquad t = 0, \dots, p-1$$

Розклад Тейлора $f(x)$ в $x = a$:

$$f(a+tp^n) = f(a) + tp^n f'(a) + t^2 p^{2n} \frac{f''(a)}{2!} + \dots + t^d p^{nd} \frac{f^{(d)}(a)}{d!} \qquad (*)$$

де $d = \deg(f)$

Лема 1 Для $f \in \mathbb{Z}[x]$ маємо

$$\frac{f^{(k)}(a)}{k!} \in \mathbb{Z} \quad \text{для } \forall a \in \mathbb{Z},\ k \geq 0.$$

Дов-ня достатньо для $f(x) = x^s$

$$\frac{f^{(k)}(a)}{k!} = \frac{s(s-1)\dots(s-k+1)}{k!} a^{s-k} = \binom{s}{k} a^{s-k} \in \mathbb{Z} \ \boxtimes$$

$(*) \Rightarrow$

$$\binom{*}{*}\ f(a+tp^n) \equiv f(a) + tp^n f'(a) \mod p^{n+1}$$

$f(a) \equiv 0\ (p^n)$ тому $\binom{*}{*} \Rightarrow$

$a+tp^n$ є коренем $\mod p^{n+1}$

т.т.т.к.

$$\binom{**}{*}\ \frac{f(a)}{p^n} + t f'(a) \equiv 0 \pmod p$$

Два варіанти:

(i) $f'(a) \not\equiv 0 \mod p$

Тоді існує u т.щ.

$$f'(a)u \equiv 1 \mod p$$

Позначимо $\underset{\mod p}{u}$ як $f'(a)^{-1}$

$\binom{**}{*} \Rightarrow t = -f'(a)^{-1}\dfrac{f(a)}{p^n}$

Тобто

$$a + tp^n = a - f'(a)^{-1} f(a)$$

це <u>єдине</u> піднесення a до кореня $\mod p^{n+1}$

(ii) $f'(a) \equiv 0 \pmod p$

$f(a+tp^n) \equiv f(a) \mod p^{n+1}$

Тобто або маємо p піднесень кореня (коли $f(a) \equiv 0 \mod p^{n+1}$)

або жодного піднесення

(якщо $f(a) \not\equiv 0 \mod p^{n+1}$)

Випадок (i) відповідає наступному тв-ню, яке ми довели вище:

Тв-ня 2 Нехай p просте і $f \in \mathbb{Z}[x]$.

Якщо $f(a) \equiv 0 \mod p^n$ і $f'(a) \not\equiv 0 \mod p$ то існує єдине $t \mod p$ таке що

$$f(a + tp^n) \equiv 0 \mod p^{n+1}.$$

Наслідок 3 (Лема Гензеля)
Кожен простий корінь $f(x)$ за модулем p, тобто $\alpha \mod p$ т. щ. $f(\alpha) \equiv 0 \mod p$, $f'(\alpha) \not\equiv 0 \mod p$, має єдине піднесення до кореня $\mod p^n$ для кожного $n = 2, 3, 4, \dots$:
$\exists!\ a_n \mod p^n$ т. щ.

$$f(a_n) \equiv 0 \mod p^n$$

і $a_n \equiv \alpha \mod p$.

Ці a_n можна отримати як:

$$a_1 = \alpha$$

$$a_{n+1} = a_n - f'(a)^{-1} f(a_n) \mod p^{n+1}$$

§8. Первісні корені за модулем m

Чи є група $(\mathbb{Z}/m\mathbb{Z})^{\times}$ циклічною?

<u>Озн-ня</u> Лишок $a \bmod m$ наз-ся <u>первісним коренем</u> якщо

$$a^{\varphi(m)} \equiv 1 \pmod m$$

і

$$a^{k} \not\equiv 1 \pmod m$$

для $1 \le k < \varphi(m)$.

<u>Вправа</u>: чи первісний корінь єдиний? скільки їх є?

Нагадаємо:

$$\varphi(n) = \#\{1 \le a \le n : (a,n) = 1\}$$

<u>Лема 1</u> $$\sum_{d \mid n} \varphi(d) = n$$

<u>Дов-ня</u> Розглянемо циклічну групу порядка n

$$C_n = \{1, a, a^2, \dots, a^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$$

(адитивна)

Нехай

$$C_n^{(d)} = \{x \in C_n : \operatorname{ord}(x) = d\}$$

Тоді

$$C_n = \bigsqcup_{d \mid n} C_n^{(d)}$$

$$n = \# C_n = \sum_{d \mid n} \# C_n^{(d)}$$

доведемо, що $\# C_n^{(d)} = \varphi(d)$

$\text{ord}(a^m) = d \iff$

$$\begin{cases} n \mid md \iff m = b\frac{n}{d}, \; 1 \le b \le d \\ n \nmid mk \\ \text{для } 1 \le k \le d-1 \Rightarrow n \nmid bk\frac{n}{d} \end{cases}$$

$\iff d \nmid bk \quad 1 \le k \le d-1$

$\iff (b, d) = 1$

$\text{ord}(a^m) = d \iff$

$$m \in \left\{ b \cdot \frac{n}{d} : \begin{array}{l} 1 \le b \le d \\ (b,d) = 1 \end{array} \right\}$$

$\# C_n^{(d)} = \varphi(d)$ $\boxtimes$

Вправа: покажіть що для $\forall d \mid n$

$$\#\{x \in C_n : x^d = 1\} = d.$$

Лема 2 Нехай H це скінченна група порядка n. Припустимо що для $\forall d \mid n$ виконується

$$\#\{x \in H : x^d = 1\} \le d.$$

Тоді H є циклічною.

Дов-ня Нехай $d \mid n$. Припустимо існує $x \in H$ т. щ. $\text{ord}(x) = d$. Розглянемо

$$\langle x \rangle = \{1, x, x^2, \dots, x^{d-1}\} \subset H.$$

Всі елементи $(x^k)^d = 1$, і $\#\langle x \rangle = d$. З припущення леми випливає що коли $y \in H$, $\text{ord}(y) = d$, то $y \in \langle x \rangle$.

$$H = \bigsqcup_{d \mid n} H^{(d)} \quad \text{де } H^{(d)} = \{x \in H : \text{ord}(x) = d\}$$

З того що вище випливає, що $\# H^{(d)} = 0$ або $\varphi(d)$.

$$n = \#H = \sum_{d|n} \#H^{(d)} \leq \sum_{d|n} \varphi(d) = n$$

Лема 1 $\Rightarrow \#H^{(d)} \neq 0 \quad \forall\, d | n$.

Зокрема $\#H^{(n)} \neq 0$, тобто

є елемент порядка n, який породжує H як циклічну групу. $\boxtimes$

<u>Теорема 3</u> p просте число

$(\mathbb{Z}/p\mathbb{Z})^\times$ є циклічною групою порядка $p-1$

<u>Дов-ня</u> Нехай $H = (\mathbb{Z}/p\mathbb{Z})^\times$.

Ел-ти $x \in H$ т.щ. $x^d = 1$ є коренями $x^d - 1$ в полі $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. За Тв-ням 5 з §6 многочлен степеня d має $\leq d$ різних розв'язків у заданому полі. Тому H задовольняє умові леми 2 $\Rightarrow H$ є циклічною. $\boxtimes$.

<u>Теорема 4</u> p <u>непарне</u> просте

Тоді $(\mathbb{Z}/p^n\mathbb{Z})^\times$ є циклічною

для кожного $n \geq 1$.

<u>Лема 5</u> $(\mathbb{Z}/p^2\mathbb{Z})^\times$ є

циклічною; кожний

первісний корінь mod p

має $p-1$ піднесення до

первісного кореня mod p^2.

<u>Дов-ня</u> Розглянемо

$$b = a + tp \mod p^2$$

первісний корінь mod p

Нехай $m = \operatorname{ord}(b)$ в $(\mathbb{Z}/p^2\mathbb{Z})^\times$.

$\varphi(p^2) = p(p-1)$

$\Rightarrow m \mid p(p-1)$

$b^m \equiv 1 \ (p^2) \Rightarrow a^m \equiv b^m \equiv 1 \ (p)$

a – первісний $\Rightarrow (p-1) \mid m$

Тобто $m = (p-1)$ або $m = p(p-1)$

; в цьому випадку b є первісним mod p^2

Знайдемо такі t що $b^{p-1} \not\equiv 1 \ (p^2)$:

$$\begin{aligned} b^{p-1} &= (a + tp)^{p-1} \\ &\equiv a^{p-1} + \binom{p-1}{1} tp \mod p^2 \\ &\equiv a^{p-1} - tp \mod p^2 \end{aligned}$$

$b^{p-1} \equiv a^{p-1} - tp \mod p^2$

Нехай $a^{p-1} = 1 + up \ (p^2)$

Тоді

$b^{p-1} = 1 + (u-t)p \quad (p^2)$

$\not\equiv 1$ в точності для всіх $t \not\equiv u \pmod p$.

$\boxtimes$

<u>Зауваження</u> Лема 5 також вірно для $p = 2$.

$(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \overline{-1}\} \cong \mathbb{Z}/_2\mathbb{Z}$

циклічна (адитивна)

Але $(\mathbb{Z}/8\mathbb{Z})^\times$ не циклічна:

x	1	3	5	7
x^2	1	1	1	1

mod 8

<u>Лема 6</u> p <u>непарне</u> просте

Тоді кожне піднесення первісного кореня mod p^2 також є первісним коренем mod p^n для $n = 3, 4, 5, \ldots$

<u>Довед</u> Нехай $b \in \mathbb{Z}$ є первісним коренем mod p^2. Позначимо $m = \operatorname{ord}(b)$ в $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Тоді $\varphi(p^2) \mid m \mid \varphi(p^n)$

оскільки b первісний mod p^2

$(p-1)p \mid m \mid (p-1)p^{n-1}$

$\Rightarrow$ достатньо показати, що $b^{(p-1)p^{n-2}} \not\equiv 1 \pmod{p^n}$.

Будемо доводити індукцією за n що

$$b^{(p-1)p^{n-2}} \not\equiv 1 \mod p^n.$$

$n=2$: $b^{p-1} \equiv 1 + tp \pmod{p^2}$

$t \not\equiv 0 \mod p$

b первісний mod p^2

Помітимо, що $a \equiv c \mod p^s$

$\Rightarrow a^p \equiv c^p \mod p^{s+1}$

(вправа). Тоді

$$b^{p(p-1)} \equiv (1+tp)^p \mod p^3$$
$$\equiv 1 + tp^2 \mod p^3$$

Крок індукції:

$$b^{p^{n-2}(p-1)} \equiv 1 + tp^{n-1} \pmod{p^n}$$

$\Downarrow$

$$b^{p^{n-1}(p-1)} \equiv (1+tp^{n-1})^p \pmod{p^{n+1}}$$
$$\equiv 1 + tp^n \pmod{p^{n+1}}$$

$\boxtimes$

<u>Вправа</u>: чому це доведення не працює для $p=2$?

Лема 5, лема 6 $\Rightarrow$ Теорема 4.

<u>Теорема 7</u> Первісні корені mod m існують т.т.т.к.

$m = 1, 2, 4$, p^n або $2p^n$ для деякого непарного простого p та $n \geq 1$. <u>Дов-ня</u>: вправа.