Теорія чисел - весняний семестр 2023 року
§7. Лишки за модулем степернів простих чисел. Лема Гензеля.
§8. Первісні корені за модулем m.

1. За малою теоремою Ферма кожен ненульовий лишок $a \mod p$ є розв'язком конгруенції $x^{p-1} \equiv 1 \mod p$. Для $n \geq 2$ покажіть, що існує єдиний розв'язок $x = a_n \mod p^n$ конгруенції $x^{p-1} \equiv 1 \mod p^n$ такий, що $a_n \equiv a \mod p$. Спробуйте сконструювати a_n явно, тобто знайти якусь формулу для цього лишка.

2. Нехай $f(\mathbf{x})$ є многочленом від n змінних $x_1, \ldots, x_n$ з цілими коефіцієнтами. Припустимо, що для деякого $\mathbf{a} \in \mathbb{Z}^n$ маємо $f(\mathbf{a}) \equiv 0 \mod p$ та $\frac{\partial f}{\partial x_i}(\mathbf{a}) \not\equiv 0 \mod p$ для деякого $0 \leq i \leq n$. Доведіть, що конгруенція $f(\mathbf{x}) \equiv 0 \mod p^s$ має розв'язки для будь-яких $s \geq 2$.

3. Лишок $0 \neq a \mod p$ називається *лишком nго степеня* якщо конгруенція $x^n \equiv a \mod p$ має розв'язки. Доведіть, що a є лишком nго степеня тоді і тільки тоді коли

$$a^{(p-1)/(p-1,n)} \equiv 1 \mod p.$$

   Нехай a є лишком nго степеня. Скільки розв'язків у $\mathbb{Z}/p\mathbb{Z}$ має конгруенція $x^n \equiv a \mod p$?

4. Гаусс довів, що добуток всіх первісних коренів за модулем p дорівнює 1 для всіх простих чисел p з кількома винятками. Для яких p це твердження не виконується?

5. Доведіть Теорему 7 з лекції, яка характеризує числа $m \geq 2$ для яких група оборотних лишків за модулем m є циклічною.