NUMBER THEORY
FALL 2023

PRIMITIVE ROOTS PRACTICE EXERCISES

Exercise 1. If $f(X), g(X) \in \mathbb{Z}[X]$ are nonzero polynomials satisfying

$$f(X) = (X - a)g(X) + b$$

for some $a, b \in \mathbb{Z}$, show that $f(X)$ and $g(X)$ have the same leading coeficient.

Exercise 2. If $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are integers satisfying $0 \leq a_k \leq b_k$ for all k, show that

$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} b_k \;\Rightarrow\; a_k = b_k \text{ for all } k.$$

Exercise 3. Let p be an odd prime. Use the Binomial Theorem to verify the following assertions made during Monday's lecture.

- **a.** For any $r \in \mathbb{Z}$ one has $(r+p)^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}$.
- **b.** For any $k \geq 2$ and $a \in \mathbb{Z}$ one has $(1 + ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}$.

Exercise 4. Textbook exercise 8.3.1

Exercise 5. Textbook exercise 8.3.3

Exercise 6. Textbook exercise 8.3.4

Exercise 7. Textbook exercise 8.3.6a

Exercise 8. Textbook exercise 8.3.8

Exercise 9. Textbook exercise 8.3.11