

HOMEWORK 4: MATH 124 (NUMBER THEORY)

1. EXERCISES

Exercise 1.1. Fix a prime p . We showed in class that if $f(x) \in \mathbb{Z}[x]$ has leading term $a_n x^n$, where $n \geq 0$ and $p \nmid a_n$, then one of the following is true:

(1) Every $u \in \mathbb{Z}/p\mathbb{Z}$ is a solution to

$$f(x) \equiv 0 \pmod{p}.$$

(2) There exists a monic polynomial $g(x) \in \mathbb{Z}[x]$ of degree $m < p$ such that the solutions to

$$g(x) \equiv 0 \pmod{p}$$

in $\mathbb{Z}/p\mathbb{Z}$ are exactly the solutions to

$$f(x) \equiv 0 \pmod{p}.$$

We specialize to the case that $p = 7$. For the following $f(x)$ construct a corresponding $g(x)$ satisfying the assumptions of the theorem (Hint: What was done in the proof of this theorem?).

- | | |
|---------------------------------|----------|
| (1) $x^{11} + x^8 + 5$ | (3 pts). |
| (2) $x^{20} + x^{13} + x^7 + 2$ | (3 pts). |
| (3) $x^{15} - x^{10} + 4x - 3$ | (3 pts). |

Exercise 1.2. The goal of this exercise will be to show the following theorem.

Theorem (Wilson's Theorem). Let p be a prime. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

We will do this as follows.

(1) Combine the results in class on polynomials modulo a prime p and Fermat's theorem to show that we have the following equality of polynomials $\pmod{p}$.

$$x^{p-1} - 1 \cong (x-1)(x-2) \cdots (x-(p-1)) \pmod{p}$$

and

$$x^p - x \cong x(x-1)(x-2) \cdots (x-(p-1)) \pmod{p}$$

(4 pts).

(2) Compare the coefficients of x in Part (1) and deduce Wilson's theorem. (2 pts).

Exercise 1.3. Compute the number of primitive roots modulo n for each of the following n , and, when primitive roots exist, provide an example.

- | | |
|--------------|----------|
| (1) $n = 3$ | (2 pts). |
| (2) $n = 5$ | (2 pts). |
| (3) $n = 7$ | (3 pts). |
| (4) $n = 8$ | (3 pts). |
| (5) $n = 23$ | (4 pts). |

Exercise 1.4. Fix $n > 1$, and let $a, b \in \mathbb{Z}$ such that $(a, n) = (b, n) = 1$. Let the order of $a \pmod{n}$ (resp. $b \pmod{n}$) be given by h (resp. k). Show that the order of ab modulo n divides hk . Prove that if $(h, k) = 1$, then the order of ab is exactly hk (5 pts).

Exercise 1.5. *Prove that if a has order 3 modulo a prime p , then*

$$1 + a + a^2 \equiv 0 \pmod{p},$$

and $1 + a$ has order 6 modulo p .

(4 pts)