

BASIC NUMBER THEORY, PROBLEM SET 5

Wilson's Theorem; Sums of Squares

- (1) Find the least positive integer x such that $13|(x^2 + 1)$.
- (2) Prove that 19 is not a divisor of $4n^2 + 4$ for any integer n .
- (3) Show that an integer $m > 1$ is a prime if and only if m divides $(m - 1)! + 1$. (You may use Wilson's theorem to solve this problem; we aren't asking you to re-prove it.)
- (4) If p is an odd prime, show that

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p - 2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

and

$$2^2 \cdot 4^2 \cdot 6^2 \cdots (p - 1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

- (5) Exhibit $6057576 = 2^3 \cdot 3^2 \cdot 7^2 \cdot 17 \cdot 101$ as the sum of two squares, using the technique demonstrated in class.

Polynomials mod p

- (6) Let $f(x) = x^3 + 2x - 3$. Find all the roots of $f(x)$ mod 5; mod 9; and mod 45.
- (7) Let $g(x) = x^2 + x + 7$. Find all the roots of $f(x)$ mod 3; mod 5; and mod 15.
- (8) Reduce the congruence $x^{11} + x^8 + 5 \equiv 0 \pmod{7}$ to an equivalent congruence involving a polynomial of degree ≤ 6 .
- (9) Show that $f(x) = x^p - x$ factors (mod p) as $f(x) = x(x - 1) \cdots (x - (p - 1))$.

A couple of miscellaneous questions

- (10) Exhibit a complete residue system module 7 composed entirely of 0 and of powers of 3.
- (11) Show that $7|(3^{2n+1} + 2^{n+2})$ for all n .