Math 580/780I Notes 12

Polynomials Modulo Integers, A First Look at Quadratics:

- **Theorem 16.** *Let p be an odd prime. The congruence $x^2+1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

- **Proof:** First suppose $p \equiv 1 \pmod{4}$. Then $p = 4k+1$ for some positive integer k. Thus, $(p-1)/2$ is even. By Wilson's Theorem, we obtain

$$\begin{aligned}
-1 \equiv (p-1)! &\equiv 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+1}{2}\right) \times \cdots \times (p-2) \times (p-1) \\
&\equiv 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(-\frac{p-1}{2}\right) \times \cdots \times (-2) \times (-1) \\
&\equiv (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)! \left(\frac{p-1}{2}\right)! \pmod{p}.
\end{aligned}$$

Thus, in this case, $x^2+1 \equiv 0 \pmod{p}$ has the solution $x = ((p-1)/2)!$.

Now, suppose $p \equiv 3 \pmod{4}$. Then $(p-1)/2$ is odd. Assume there is an integer x such that $x^2+1 \equiv 0 \pmod{p}$. Then $x^2 \equiv -1 \pmod{p}$ implies (since $(p-1)/2$ is odd) that

$$x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv -1 \pmod{p}.$$

This contradicts Fermat's Little Theorem. Hence, the theorem follows.

- **Corollary.** *There exist infinitely many primes $\equiv 1 \pmod{4}$.*
- Before proving the corollary, we establish

Theorem 17. *There exist infinitely many primes.*

Proof 1 (Euclid's). Assume there are only finitely many primes, say $p_1, \dots, p_r$. Then the number $p_1 \cdots p_r + 1$ is not divisible by any of the primes $p_1, \dots, p_r$, contradicting the Fundamental Theorem of Arithmetic.

Proof 2. The Fermat numbers $F_n = 2^{2^n} + 1$ are odd numbers > 1 satisfying

$$F_{n+1} - 2 = \prod_{j=0}^{n} F_j.$$

Hence, they are relatively prime, so there must exist infinitely many primes.

- **Proof of Corollary.** Consider the numbers n^2+1 where n is an integer. By Theorem 16, the only primes dividing any such number are 2 and primes $\equiv 1 \pmod{4}$. Thus, it suffices to show there exist infinitely many primes dividing numbers of the form n^2+1. Assume otherwise. Let $p_1, \dots, p_r$ be the primes which divide numbers of the form n^2+1. Since $(p_1 \cdots p_r)^2 + 1$ is not divisible by any of the primes $p_1, \dots, p_r$, we obtain a contradiction.

Homework:

(1) (a) Let $p_1, \dots, p_r$ be r primes. Show that

$$2^{(p_1-1)(p_2-1)\cdots(p_r-1)} + 1$$

is not divisible by any of the primes $p_1, \dots, p_r$.

(b) Explain why part (a) implies that there are infinitely many primes.

(2) Use an argument similar to Euclid's to prove there exist infinitely many primes $\equiv 3 \pmod 4$. (Hint: If $p_1, \dots, p_r$ are primes > 3 that are $\equiv 3 \pmod 4$, then what can you say about the odd number $4p_1 \cdots p_r + 3$?)

(3) Prove that there are infinitely many primes that are $\equiv 2 \pmod 3$.

(4) (a) Let n be an integer. Explain why Theorem 16 implies that each prime divisor of $16n^4 + 1$ is either of the form $8k + 1$ for some integer k or of the form $8k + 5$ for some integer k.

(b) Assume p is a prime of the form $8k+5$, where $k \in \mathbb{Z}$, that divides $16n^4+1$ for some integer n. Explain why

$$(2n)^{p-1} \equiv -1 \pmod p.$$

(c) Let n be an integer. Why do parts (a) and (b) imply that every prime divisor of $16n^4 + 1$ is of the form $8k + 1$ for some integer k?

(d) Prove that there are infinitely many primes $\equiv 1 \pmod 8$.

(5) Explain why are there infinitely many primes $\not\equiv 1 \pmod 8$.