Math 580/780I Notes 13

Lagrange's Theorem:

• **Theorem 18.** *Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. In other words, $f(x)$ has integer coefficients and leading coefficient 1. Let p be a prime, and let $n = \deg f$. Then the congruence*

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

has at most n incongruent roots modulo p.

• **Proof.** If $n = 0$, then, since $f(x)$ is monic, we have $f(x) = 1$. In this case, $f(x)$ has 0 roots, and we are done. Let m be a positive integer, and suppose the theorem holds for $n = m - 1$. Consider $f(x) \in \mathbb{Z}[x]$ with $\deg f = m$. If $(*)$ has no solutions, then the desired conclusion follows for $f(x)$. Suppose then that $(*)$ has a solution, say a. Hence, there is an integer k such that $f(a) = kp$. This implies that $x - a$ is a factor of $f(x) - kp$ (by the Remainder Theorem). In other words, there is a $g(x) \in \mathbb{Z}[x]$ such that $f(x) = (x - a)g(x) + kp$. Observe that $\deg g = m - 1$. Also, $f(x) \equiv g(x)(x - a) \pmod{p}$. We deduce that $f(b) \equiv 0 \pmod{p}$ if and only if either $g(b) \equiv 0 \pmod{p}$ or $b \equiv a \pmod{p}$. Since $\deg g = m - 1$, we deduce that there are at most $m - 1$ incongruent integers b modulo p that can satisfy $g(b) \equiv 0 \pmod{p}$. The theorem follows.

• **Comment:** Theorem 18 is not true if the prime p is replaced by a composite number n. For example, $x^2 - 1 \equiv 0 \pmod{8}$ has 4 incongruent solutions modulo 8. Also, $3x \equiv 0 \pmod{9}$ has 3 incongruent solutions modulo 9.

• **Corollary.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n, and let p be a prime. Suppose $f(x) \equiv 0 \pmod{p}$ has n incongruent solutions modulo p, say $a_1, \dots, a_n$. Then*

$$f(x) \equiv (x - a_1) \cdots (x - a_n) \pmod{p}.$$

• **Proof.** Let $g(x) = f(x) - (x - a_1) \cdots (x - a_n)$. Since $f(x)$ is monic, $g(x)$ has at most degree $n - 1$. We will use that $g(x)$ has each of $a_1, a_2, \dots, a_n$ as roots modulo p. The idea is that this will contradict Theorem 18 since $g(x)$ has degree at most $n - 1$. However, some further justification is needed as $g(x)$ may not be monic so that Theorem 18 may not apply.

If we show that $g(x)$ is identically 0 modulo p, then we are done. So assume there is a coefficient of $g(x)$ that is not divisible by p. Let b be the coefficient of the highest degree term of $g(x)$ that is not divisible by p. In other words,

$$g(x) \equiv bx^m + \text{(smaller degree terms)} \pmod{p},$$

where again we note that $m \le n - 1$. Let b' be an inverse for b mod p. Finally, let $h(x)$ be a monic polynomial in $\mathbb{Z}[x]$ satisfying $h(x) \equiv b'g(x) \pmod{p}$. Observe that $h(x)$ exists since $b'b \equiv 1 \pmod{p}$. Also, $h(a_j) \equiv b'g(a_j) \equiv 0 \pmod{p}$ for each $j \in \{1, 2, \dots, n\}$. On the other hand, $\deg h = \deg g \le n - 1$. Since $h(x)$ is a monic polynomial of degree $\le n - 1$ with n roots modulo p, we get a contradiction to Theorem 18. Hence, $g(x)$ is identically 0 modulo p, completing the proof.

• Wilson's theorem can be established with the aid of Theorem 18. Let p be a prime. We want to prove $(p - 1)! \equiv -1 \pmod{p}$. Let $f(x) = x^{p-1} - 1$. By Fermat's Little Theorem and the above Corollary, we deduce

$$f(x) \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

Letting $x = 0$, we obtain the desired result.

Homework:

(1) (a) Let $f(x) = x^2 - 3$. Determine the primes $p \leq 13$ for which $f(x)$ has a root modulo p and how many incongruent roots $f(x)$ has modulo p. This should be a direct computation.

(b) For all primes $p > 3$, explain why $f(x)$ either has 2 incongruent roots modulo p or $f(x)$ has 0 incongruent roots modulo p. Clarify why your explanation does not work when $p = 2$ and when $p = 3$.

(2) For a prime p, let

$$S_p = 1^2 + 2^2 + 3^2 + \cdots + (p-2)^2 + (p-1)^2.$$

So

$$S_2 = 1^2, \quad S_3 = 1^2 + 2^2, \quad S_5 = 1^2 + 2^2 + 3^2 + 4^2, \ldots.$$

Observe that $S_2 \equiv 1 \pmod{2}$ and $S_3 \equiv 2 \pmod{3}$. Explain why S_p is divisible by p for each $p > 3$. (Hint: Look at the proof of Wilson's Theorem above and think elementary symmetric functions.)