Tuesday, October 1

Definition: Let $f(X), g(X) \in \mathbb{Z}[X]$. We say $f(X) \equiv g(X) \pmod m$ (the polynomials are congruent) if their coefficients of x^j are congruent to each other (mod m), for every $j \in \mathbb{N}_0$.

Example: $f(x) = 15X^2 + 3X + 8$.

- $f(x) \equiv 3x^2 - X \pmod 4$
- $f(x) \equiv 3X + 3 \pmod 5$
- $f(x) \equiv 2 \pmod 3$.

We'll say that $f(x)$ has:

- degree 2 modulo 4
- degree 1 modulo 5
- degree 0 modulo 3.

Lemma: Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$, and let $f(X) \in \mathbb{Z}[X]$ with degree $d \geq 1$ (mod m). Suppose $f(a) \equiv 0 \pmod m$. Then there exists $g(X) \in \mathbb{Z}[X]$, of degree $d-1$ (mod m), such that

$$f(X) \equiv (X-a)g(X) \pmod m.$$

Proof: We use the following formula:

$$f(a+h) = f(a) + hf'(a) + h^2\frac{f''(a)}{2} + \dots + h^d\frac{f^{(d)}(a)}{d!},$$

with $h = X - a$:

$$f(X) = f(a) + (X-a)f'(a) + \dots + (X-a)^d\frac{f^{(d)}(a)}{d!}.$$

If we set $g(X) = \sum_{j=1}^{d}(X-a)^{j-1}\frac{f^{(j)}(a)}{j!}$,

then
$$f(X) = f(a) + (X-a)g(X)$$
$$\equiv 0 + (X-a)g(X) \pmod m. \quad //$$

Example: $f(x) = x^2 - 1$, $m = 24$.

Then $x = 5$ is a root of $f(x) \pmod{24}$, since $f(5) = 5^2 - 1 = 24 \equiv 0 \pmod{24}$.

By the lemma, $f(x) \equiv (x-5)g(x) \pmod{24}$ for some $g(x)$ of degree 1.

Indeed, $(x-5)(x+5) = x^2 - 25$
$$\equiv x^2 - 1 \pmod{24}.$$

$f(x)$ doesn't have unique factorization $\pmod{24}$:

$$f(x) \equiv (x-5)(x+5) \equiv (x-1)(x+1)$$
$$\equiv (x-7)(x+7) \equiv (x-11)(x+11) \pmod{24}.$$

But: For prime modulus, things do work nicely.

Theorem: Let $f(x) \in \mathbb{Z}[x]$ have degree $d \pmod{p}$. If $r_1, r_2, \ldots, r_k$ are distinct roots of $f(x) \pmod{p}$, then there exists $g(x) \in \mathbb{Z}[x]$ of degree $d-k$ with
$$f(x) \equiv (x-r_1)\cdots(x-r_k)\,g(x) \pmod{p}.$$
In particular, $k \leq d$.

Proof: Induction on k. Base case $k=1$: previous lemma. Key step: r_2 is a root of $f(x) \equiv (x-r_1)g_1(x)$, so $p \mid (r_2 - r_1)g_1(r_2)$. By Euclid's lemma either $p \mid (r_2 - r_1)$ (but no, by hypothesis) or else $p \mid g_1(r_2)$. So r_2 is a root of $g_1(x)$, so inducting ....

//