Lecture 8

22/8/2022, Monday

Let $f(x)$ be a polynomial with integer coefficients.

<u>Definition 1:</u> Let $r_1, \ldots, r_m$ denote a complete residue system modulo m. The number of solutions of $f(x) \equiv 0 \pmod{m}$ is the number of the r_i such that $f(r_i) \equiv 0 \pmod{m}$.

<u>Ex:</u>
- $x^2+1 \equiv 0 \pmod 7$ has no solution
- $x^2+1 \equiv 0 \pmod 5$ has two solutions: $x=2$ and $x=3$.
- $x^2-1 \equiv 0 \pmod 8$ has four solutions: $x = 1, 3, 5, 7$.

<u>Definition 2:</u> Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$.

If $a_n \not\equiv 0 \pmod{m}$, then the degree of the congruence $f(x) \equiv 0 \pmod{m}$ is defined to be n. If $a_n \equiv 0 \pmod{m}$, let j be the largest integer

such that $a_j \not\equiv 0 \pmod{m}$; then the degree of the congruence is j.
If $a_k \equiv 0 \pmod{m}$ $\forall k$, then degree of $f(x) \equiv 0 \pmod{m}$ is <u>not</u> defined.

<u>Theorem 1:</u> Let a, b and $m \geq 1$ be given integers, and put $g = \gcd(a, m)$.
The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $g \mid b$.
If this condition is met, then $ax \equiv b \pmod{m}$ has exactly g many solutions.

<u>Proof</u>: $ax \equiv b \pmod{m}$ has a solution $x_0 \iff m \mid (ax_0 - b)$
$\iff ax_0 - b = my_0$ for some $y_0 \in \mathbb{Z} \iff ax_0 - my_0 = b \iff \gcd(a,m) \mid b$
Thus, $ax \equiv b \pmod{m}$ has a solution $\iff g \mid b$, where $g = \gcd(a, m)$.

For the 2nd part, let $g \mid b$. We write $a = g \cdot \alpha$, $b = g \cdot \beta$, $m = g \cdot m_1$

Then, $ax_0 \equiv b \pmod{m} \iff \alpha x_0 \equiv \beta \pmod{m_1}$

Since $\gcd(\alpha, m_1) = 1$, so $\exists$ unique $\gamma \pmod{m_1}$ such that

$$\alpha\gamma \equiv 1 \pmod{m_1}.$$

$\therefore \quad \alpha x_0 \equiv \beta \pmod{m_1} \iff x_0 \equiv \gamma\beta \pmod{m_1}.$

$$m_1 = \frac{m}{\gcd(a,m)} = \frac{m}{g}$$

Thus, the set of solutions x satisfying $ax \equiv b \pmod{m}$ is precisely the arithmetic progression of numbers of the form $\gamma\beta + k m_1$.

We allow k to take on the values $0, 1, 2, \ldots, g-1$; and obtain g values of x that are distinct $\pmod{m}$. #

__Theorem 2:__ Let $f(x)$ be a polynomial with integer coefficients. For any positive integer m, let $N(m)$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$. If $m = m_1 m_2$, where $\gcd(m_1, m_2) = 1$, then

$$N(m) = N(m_1) \cdot N(m_2).$$

__Proof:__ Let $\mathcal{C}(m) = \{1, 2, \dots, m\}$, $\mathcal{C}(m_1) = \{1, 2, \dots, m_1\}$, $\mathcal{C}(m_2) = \{1, 2, \dots, m_2\}$

Let $x_0 \in \mathcal{C}(m)$ be such that $f(x_0) \equiv 0 \pmod{m}$.

Then, $f(x_0) \equiv 0 \pmod{m_1}$ and $f(x_0) \equiv 0 \pmod{m_2}$.

Hence, there exist unique $a_0 \in \mathcal{C}(m_1)$ and unique $b_0 \in \mathcal{C}(m_2)$ such that $x_0 \equiv a_0 \pmod{m_1}$ and $x_0 \equiv b_0 \pmod{m_2}$.

$\Rightarrow f(a_0) \equiv 0 \pmod{m_1}$ and $f(b_0) \equiv 0 \pmod{m_2}$.

Let $S_m = \{k \in \mathcal{C}(m) \mid f(k) \equiv 0 \pmod{m}\}$

$S_{m_1} = \{k \in \mathcal{C}(m_1) \mid f(k) \equiv 0 \pmod{m_1}\}$

$S_{m_2} = \{k \in \mathcal{C}(m_2) \mid f(k) \equiv 0 \pmod{m_2}\}$

Define, $\psi : S_m \longrightarrow S_{m_1} \times S_{m_2}$, where $a_0 \in S_m$ & $a_0 \equiv x_0 \pmod{m_1}$

$x_0 \longmapsto (a_0, b_0)$ $\qquad b_0 \in S_{m_2}$ & $b_0 \equiv x_0 \pmod{m_2}$.

Easy to check that ψ is well-defined and one-to-one.

We now prove that ψ is onto. Suppose that $(a_1, a_2) \in S_{m_1} \times S_{m_2}$.

By CRT, $\exists$ unique $x_1 \in \mathcal{C}(m)$ such that $x_1 \equiv a_1 \pmod{m_1}$

$x_1 \equiv a_2 \pmod{m_2}$.

Then, $f(x_1) \equiv 0 \pmod{m_1}$ & $f(x_1) \equiv 0 \pmod{m_2} \Rightarrow f(x_1) \equiv 0 \pmod{m}$

$\Rightarrow x_1 \in S_m$ and clearly, $\psi(x_1) = (a_1, a_2)$. Hence, ψ is onto.

Hence, ψ is a bijection. This proves that

$$N(m) = \# S_m = \# S_{m_1} \cdot \# S_{m_2} = N(m_1) \cdot N(m_2).$$

#

Corollary: If $m = \prod_{p \mid m} p^{\alpha}$ is the factorization of m into primes,

then $N(m) = \prod_{p \mid m} N(p^{\alpha})$.

Ex: $f(x) = x^2 + x + 7$. Find all the roots of $f(x) \equiv 0 \pmod{15}$.

Solution: $f(x) \equiv 0 \pmod{15} \iff f(x) \equiv 0 \pmod 3$ & $f(x) \equiv 0 \pmod 5$.

$\iff x^2 + x + 1 \equiv 0 \pmod 3$ & $x^2 + x + 2 \equiv 0 \pmod 5$

But $x^2 + x + 2 \equiv 0 \pmod 5$ has no solution, and hence $f(x) \equiv 0 \pmod{15}$ has no solution.

§ Prime power moduli:

Theorem 3: (Hensel's lifting lemma): Let $f(x)$ be a polynomial with integer coefficients. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Proof: The idea is to find a solution $x = a + tp^j$, where t is to be determined.

Using Taylor's expansion, we have

$$f(a+tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} f'(a)/2! + \cdots + t^n p^{nj} f^{(n)}(a)/n!.$$

Claim: For $2 \le k \le n$, $\dfrac{f^{(k)}(a)}{k!}$ is an integer.

Proof of the claim: Let $c \cdot x^r$ be a representative term from $f(x)$.

If $r < k$, then the corresponding term in $f^{(k)}(a)$ is zero.
If $r \geq k$, then the corresponding term in $f^{(k)}(a)$ is

$$c\, r \cdot (r-1) \cdot \ldots \cdot (r-k+1)\, a^{r-k}.$$

<u>Exercise:</u> Product of k consecutive integers is divisible by $k!$

$\therefore$ $r \cdot (r-1) \cdot \ldots \cdot (r-k+1)$ is divisible by $k!$

$\Rightarrow$ $\dfrac{f^{(k)}(a)}{k!}$ is an integer.

$\therefore$ $f(a+tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$.

Thus, we want t to be a solution of $f(a) + t\,p^j f'(a) \equiv 0 \pmod{p^{j+1}}$.
Since $f(a) \equiv 0 \pmod{p^j}$, so $t\, f'(a) \equiv -f(a)/p^j \pmod{p}$.

$t \cdot f'(a) \equiv -\frac{f(a)}{p^j} \pmod{p}$ is a linear congruence in t.

If $f'(a) \not\equiv 0 \pmod{p}$, then $x \cdot f'(a) \equiv 1 \pmod{p}$ has a unique solution, say $\overline{f'(a)}$.

Thus, we obtain unique $t \pmod{p}$ which is given by

$$t \equiv -\overline{f'(a)} \cdot \frac{f(a)}{p^j} \pmod{p}.$$

This completes the proof.

---x---

Important: If $f(a) \equiv 0 \pmod{p^j}$, $f(b) \equiv 0 \pmod{p^k}$, $j < k$ and $a \equiv b \pmod{p^j}$, we say that 'a' lifts to 'b' or 'b' lies above 'a'.

If $f(a) \equiv 0 \pmod{p^j}$, then the root 'a' is called non-singular if $f'(a) \not\equiv 0 \pmod{p}$; otherwise it is called singular.

By Hensel's lemma, a nonsingular root $a \pmod{p}$ lifts to a unique root $a_2 \pmod{p^2}$. Since $a_2 \equiv a \pmod{p}$, so $f'(a_2) \equiv f'(a) \not\equiv 0 \pmod{p}$. Applying Hensel's lemma again, we may lift a_2 to form a root a_3 of $f(x)$ modulo p^3, and so on.

In general, by applying Hensel's lemma repeatedly, we find that a nonsingular root $a \bmod p$ lifts to a unique root $a_j \bmod p^j$ for $j = 2, 3, \ldots$. This sequence is generated by means of the recursion:

$$a_{j+1} = a_j - \frac{f(a_j)}{p^j} p^j \overline{f'(a)} = a_j - f(a_j)\overline{f'(a)},$$

where $\overline{f'(a)}$ is an integer chosen so that $f'(a) \cdot \overline{f'(a)} \equiv 1 \pmod{p}$.

Ex: Solve $x^2 + x + 47 \equiv 0 \pmod{7^3}$. Here, $f(x) = x^2 + x + 47$.

Solution: $x^2 + x + 47 \equiv x^2 + x + 5 \equiv 0 \pmod 7$ has two solutions $x = 1, 5$.

Now, $f'(x) = 2x + 1$ $\therefore$ $f'(1) = 3 \not\equiv 0 \pmod 7$ and $f'(5) = 11 \not\equiv 0 \pmod 7$

$\therefore$ $a = 1, 5$ are nonsingular roots of $f(x) \equiv 0 \pmod 7$.

$\overline{f'(1)} = 5 \pmod 7$ and $\overline{f'(5)} \equiv 2 \pmod 7$

Now, $a = 1$ lifts to $a_2 = 1 - 49 \times 5$

we take $a_2 \pmod{7^2}$, so $a_2 \equiv 1 \pmod{7^2}$.

Now, $a_3 = a_2 - 49 \times 5 \equiv 99 \pmod{7^3}$.

$\therefore$ 99 is a root of $x^2 + x + 47 \equiv 0 \pmod{7^3}$.

The other root is 243.

#