Note Title 8/15/2022

Lecture 7

Tuesday, 16/8/2022

Theorem 1: Let p be a prime. Then, $p = a^2 + b^2$ for some integers a and b if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Proof: If $p = 2$, then $p = 1^2 + 1^2$.

If $p \geq 3$, and $p = a^2 + b^2$, then a is even and b is odd. (or a is odd and b is even).

$\Rightarrow p \equiv 1 \pmod 4$.

Now, we prove that, if $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Let $x_0 \in \mathbb{Z}$ be such that $x_0^2 \equiv -1 \pmod p$.

Let $k = [\sqrt{p}]$. Then, $k < \sqrt{p} < k+1$

$\therefore \{(u, v) \mid 0 \leq u \leq k,\ 0 \leq v \leq k\}$ has $(k+1)^2$-elements.

Since $(k+1)^2 > p$, so by Pigeonhole principle, $\exists\, (u_1, v_1) \neq (u_2, v_2)$ such that $u_1 + x_0 \cdot v_1 \equiv u_2 + x_0 \cdot v_2 \pmod{p}$

$\Rightarrow u_1 - u_2 \equiv -x_0 (v_1 - v_2) \pmod{p}$. Let $a = u_1 - u_2$, $b = v_1 - v_2$.

$\Rightarrow a \equiv -x_0 \cdot b \pmod{p} \Rightarrow a^2 \equiv x_0^2 \cdot b^2 \pmod{p} \Rightarrow a^2 + b^2 \equiv 0 \pmod{p}$

Since $(u_1, v_1) \neq (u_2, v_2)$, so either $a \neq 0$ or $b \neq 0$. Hence, $a^2 + b^2 > 0$.

Also, $a^2 < p$ and $b^2 < p$. Thus, $0 < a^2 + b^2 < 2p \Rightarrow a^2 + b^2 = p$.

#

—x—

<u>Theorem 2</u>: Let p be a prime such that $p \equiv 3 \pmod{4}$. If $p \mid (a^2 + b^2)$, then $p \mid a$ and $p \mid b$. Hence, if $p \mid (a^2 + b^2)$, then $p^2 \mid (a^2 + b^2)$.

<u>Proof</u>: If possible, suppose that $p \nmid a$. Then, $\gcd(a, p) = 1$.

$\Rightarrow a x_0 \equiv 1 \pmod{p}$ for some $x_0 \in \mathbb{Z}$

Now, $p \mid a^2+b^2$. $\Rightarrow a^2+b^2 \equiv 0 \pmod{p}$

$\Rightarrow a^2 \cdot x_0^2 + b^2 \cdot x_0^2 \equiv 0 \pmod{p}$

$\Rightarrow (b x_0)^2 \equiv -1 \pmod{p} \Rightarrow p \equiv 1 \pmod{4}$.

which is a contradiction.

$\therefore p \mid a$. Similarly, $p \mid b$.

Thus, if $p \equiv 3 \pmod{4}$ and $p \mid a^2+b^2$, then $p \mid a$ and $p \mid b$.

——— x ———

<u>Theorem 3 (Euler)</u>: Let $n \geq 2$. We write $n = 2^{\alpha} \prod_{p \equiv 1 \pmod{4}} p^{\beta} \prod_{q \equiv 3 \pmod{4}} q^{\gamma}$

Then, n can be expressed as a sum of two squares

$\Leftrightarrow$ all γ are even.

Proof: For any integers a, b, c, d, we have

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

$2 = 1^2+1^2$ and if $p \equiv 1 \pmod 4$, then $p = x^2+y^2$.

$\Rightarrow 2^\alpha \prod_{p \equiv 1 \pmod 4} p^\alpha$ can be expressed as a sum of two squares.

Hence, n can be expressed as a sum of two squares

$\Leftrightarrow \prod_{q \equiv 3 \pmod 4} q^\gamma$ can be expressed as a sum of two squares.

If each γ is even, then $\prod_{q \equiv 3 \pmod 4} q^\gamma$ is a sum of two squares as $q^\gamma = q^\gamma + 0^2$ is a sum of two squares.

Conversely, suppose that $m = \prod_{q \equiv 3 \pmod 4} q^{\gamma} = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Then, $q \mid x^2 + y^2$. By Theorem 2, $q^2 \mid (x^2 + y^2)$. That is, q^2 is a factor of $x^2 + y^2$. We next proceed with $\frac{m}{q^2}$ and following similar steps, we find that γ must be even.

This completes the proof of the theorem. #

---

§ **Chinese Remainder Theorem:** Let $m_1, m_2, \ldots, m_r$ denote r positive integers that are pairwise coprime, and let $a_1, \ldots, a_r$ denote any r integers. Then, the system of congruences $x_1 \equiv a_1 \pmod{m_1}, \ldots, x_r \equiv a_r \pmod{m_r}$ has a common solution. Also, the solution is unique modulo $m_1 \cdot m_2 \cdots m_r$.

__Proof:__ Let $m = m_1 m_2 \cdots m_r$. Then, $\gcd\left(\frac{m}{m_j}, m_j\right) = 1 \quad \forall j$.

$\therefore$ for each j, $\exists\, b_j$ such that $\frac{m}{m_j} \cdot b_j \equiv 1 \pmod{m_j}$

Clearly, $\frac{m}{m_j} b_j \equiv 0 \pmod{m_i}$ if $i \neq j$.

Put $x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$

Then, $x_0 \equiv \frac{m}{m_i} b_i a_i \pmod{m_i} \equiv a_i \pmod{m_i}$

$\therefore x_0$ is a common solution.

Suppose that x_0 and x_1 are two common solutions.

Then, $x_0 \equiv x_1 \pmod{m_i}\ \forall i \Leftrightarrow x_0 \equiv x_1 (\mathrm{mod}\ \mathrm{lcm}(m_1, m_2, \cdots, m_r))$

$\Longleftrightarrow x_0 \equiv x_1 \pmod{m}$

Hence, the solution is unique modulo $m = m_1 m_2 \cdots m_r$. #

Theorem 4 (An application of CRT): Euler φ-function is multiplicative. That is, if m_1 and m_2 denote two positive relatively prime integers, then

$$\varphi(m_1 m_2) = \varphi(m_1)\,\varphi(m_2).$$

Moreover, if m has the canonical factorization $m = \prod_{p \mid m} p^{\alpha}$, then

$$\varphi(m) = \prod_{p \mid m} \left(p^{\alpha} - p^{\alpha-1}\right) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right).$$

Proof: Let $m = m_1 m_2$. Let $R(m) = \{k \mid 1 \le k \le m,\ \gcd(k, m) = 1\}$.
Similarly, we define $R(m_1)$ and $R(m_2)$.

Define

$$\begin{aligned} \psi : R(m) &\longrightarrow R(m_1) \times R(m_2) \\ x &\longmapsto (x_0, x_1), \end{aligned}$$

where $x_0 \in R(m_1)$, $x_0 \equiv x \pmod{m_1}$, $x_1 \in R(m_2)$, $x_1 \equiv x \pmod{m_2}$.

Easy to check that ψ is well-defined.

<u>ψ is injective:</u> Suppose that $\psi(x) = \psi(y)$.

$\Rightarrow (x_0, x_1) = (y_0, y_1)$, where $x \equiv x_0 \pmod{m_1}$, $x \equiv x_1 \pmod{m_2}$, $y \equiv y_0 \pmod{m_1}$, $y \equiv y_1 \pmod{m_2}$ $\quad x_0, y_0 \in R(m_1)$, $x_1, y_1 \in R(m_2)$

$\therefore x_0 = y_0$ and $x_1 = y_1$

$\Rightarrow x \equiv y \pmod{m_1}$ and $x \equiv y \pmod{m_2}$

$\Rightarrow x \equiv y \pmod{m}$. Since $x, y \in R(m)$, so $x = y$.

<u>ψ is surjective:</u> Let $(a, b) \in R(m_1) \times R(m_2)$.

Consider the linear congruences $x \equiv a \pmod{m_1}$ and $x \equiv b \pmod{m_2}$

Since $\gcd(m_1, m_2) = 1$, so by CRT, $\exists\, x_0 \in \mathbb{Z}$ s.t $x_0 \equiv a \pmod{m_1}$, $x_0 \equiv b \pmod{m_2}$

Now, $\gcd(x_0, m_1) = \gcd(a, m_1) = 1$ and $\gcd(x_0, m_2) \equiv \gcd(b, m_2) = 1$

$\therefore \gcd(x_0, m_1 m_2) = 1$.

$\Rightarrow \exists\, c \in R(m)$ s.t. $x_0 \equiv c \pmod{m}$ $\quad [\, m = m_1 m_2$

$\therefore c \in R(m)$ satisfies $c \equiv x_0 \equiv a \pmod{m_1}$ and $c \equiv x_0 \equiv b \pmod{m_2}$

$\Rightarrow \psi(c) = (a, b)$ $\quad \therefore \psi$ is surjective.

Hence, ψ is bijective.

Thus, $\# R(m) = \# R(m_1) \cdot \# R(m_2) \Rightarrow \varphi(m) = \varphi(m_1)\,\varphi(m_2)$.

Now, if $m = \prod_{p \mid m} p^{\alpha}$, then $\varphi(m) = \prod_{p \mid m} \varphi(p^{\alpha})$.

To complete the proof, we need to prove that $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

We have $R(p^\alpha) = \{k \mid 1 \le k \le p^\alpha,\ p \nmid k\}$.

Consider the numbers:

$$1, 2, 3, 4, \ldots, p-1, p, p+1, \ldots\ldots, p^\alpha - 1, p^\alpha.$$

If $1 \le k \le p^\alpha$ and k in a multiple of p, then k must be one of the following:

$1 \cdot p,\ 2 \cdot p,\ \ldots,\ (p^{\alpha-1} - 1)p,\ p^{\alpha-1} \cdot p$. Hence, there are $p^{\alpha-1}$ possible values of k.

$$\Rightarrow \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

$$\therefore \varphi(m) = \prod_{p \mid m} \varphi(p^\alpha) = \prod_{p \mid m} (p^\alpha - p^{\alpha-1}) = m \prod_{p \mid m} (1 - 1/p). \quad \#$$