MAT 311 LECTURE 2:

- CONGRUENCES
- FERMAT'S LITTLE THM
- CHINESE REMAINDER THM

DEFINITION: WE SAY $a \equiv b$ MODULO m, $m \neq 0$ IF $m \mid (b-a)$.

EXAMPLE: $1 \equiv 6 \bmod 5$ SINCE $5 \mid (6-1)$.

THEOREM: CONGRUENCES SATISFY THE FOLLOWING PROPERTIES

(1) IF $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ THEN $a \equiv c \pmod{m}$.

(2) IF $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ THEN $a+c \equiv b+d \pmod{m}$

(3) IF $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ THEN $ac \equiv bd \pmod{m}$

(4) IF $a \equiv b \pmod{m}$ AND $d \mid m$ THEN $a \equiv b \pmod{d}$

(5) IF $a \equiv b \pmod{m}$, $c > 0$, THEN $ac \equiv bc \pmod{mc}$

PROOF: (1) $a \equiv b \pmod m$ MEANS $m \mid (b-a)$. THUS $mc \mid c\cdot(b-a) = (bc-ac)$. □

IN PARTICULAR, $\equiv \pmod m$ IS AN EQUIVALENCE RELATION.

NOTE: $\mathbb{Z}$ IS A RING, $m\mathbb{Z}$ IS AN IDEAL. $\mathbb{Z}/m\mathbb{Z}$ IS THE QUOTIENT IDEAL.

THEOREM: LET $f \in \mathbb{Z}[x]$ BE A POLYNOMIAL WITH INTEGER COEFFICIENTS. THEN IF $a \equiv b \bmod m$ WE HAVE $f(a) \equiv f(b) \bmod m$.

PROOF: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

$$f(b) - f(a) = a_n(b^n - a^n) + a_{n-1}(b^{n-1} - a^{n-1}) + \dots + a_1(b-a).$$

NOTICE $b-a \mid b^m - a^m$ ALL $m \geq 1$

$$= (b-a)(b^{m-1} + b^{m-2}a + \dots + a^{m-1})$$

SO $m \mid (b-a) \Rightarrow m \mid b^k - a^k$ ALL k.

THUS $m \mid f(b) - f(a)$. $\square$

THEOREM: (1) WE HAVE

$aX \equiv ay \bmod m$ IFF

$X \equiv y \bmod \frac{m}{(a,m)}$

(2) GIVEN $m_1, \ldots, m_r$, $X \equiv y \bmod m_i$ FOR EACH i IFF $X \equiv y \bmod [m_1, \ldots, m_r]$

PROOF: (1) $m \mid a(x-y)$ IFF $\frac{m}{(m,a)} \mid (x-y)$.

(2) IF $m_i \mid x-y$ FOR $i = 1, 2, \ldots, r$ THEN $[m_1, \ldots, m_r] \mid x-y$ AND CONVERSELY.

NOTE: $X \equiv y \bmod m$ IS EQUIV TO $X - y \in m\mathbb{Z}$. (IDEAL)

$\bigcap_{i=1}^{r} m_i \mathbb{Z} = [m_1, \ldots, m_r]\mathbb{Z}$.

DEFINITION: A **REDUCED RESIDUE SYSTEM** MODULO m IS A COLLECTION $r_1, \ldots, r_k$ OF INTEGERS SUCH THAT $(r_i, m) = 1$, IF $i \neq j$, $r_i \not\equiv r_j \bmod m$, IF $(x, m) = 1$ THEN $x \equiv r_i$ FOR SOME i.

EXAMPLE: MODULO 6, $\{1, 5\}$ ARE A REDUCED RESIDUE SYSTEM.

NOTE: REDUCED RESIDUES ARE **UNITS** IN $\mathbb{Z}/m\mathbb{Z}$.

THE EULER φ FUNCTION OF m, $\varphi(m)$ = SIZE OF A REDUCED RES. SYSTEM.

$\varphi(6) = 2$.

THEOREM: IF $(a,m)=1$, AND $r_1,\dots,r_k$ ARE A RED. RES. SYSTEM MOD m. THEN $ar_1,\dots,ar_k$ ARE A REDUCED RES. SYSTEM.

PROOF: IF $m \nmid (r_i - r_j)$

THEN $m \nmid (ar_i - ar_j)$

SINCE $(m,a) = 1$

ALSO, SINCE $(m, r_i) = 1$

$\Rightarrow (m, ar_i) = 1$.

FINALLY, ALL RED. RES. SYSTEMS HAVE SAME SIZE, SINCE (mod n) EACH $ar_i \equiv r_j$ FOR SOME j.

□

FERMAT'S LITTLE THEOREM:

IF $(a,m)=1$, THEN

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

PROOF: EACH ELEM r_i MOD m OF A REDUCED RES SYSTEM IS CONGRUENT TO ar_j FOR A UNIQUE j.

THUS $\prod_{i=1}^{\varphi(m)} r_i \equiv \prod_{i=1}^{\varphi(m)} (ar_i)$

$$\Rightarrow a^{\varphi(m)} \equiv 1 \bmod m.$$

NOTE: $(\mathbb{Z}/m\mathbb{Z})^\times$ (THE UNITS) ARE A GP. IN ANY GP G, $x^{|G|} = e$ (IDENTITY).

THEOREM: IF $(a, m) = 1$, THEN THERE EXISTS x MOD m

$ax \equiv 1 \mod m$.

(FREQUENTLY WE WRITE

$x = a^{-1}$ OR $x = \overline{a}$).

PROOF: 1 MOD m IS A REDUCED RES, AND $ar_1, \ldots, ar_{\varphi(m)}$ IS A RED. RES. SYSTEM IF $r_1, \ldots, r_{\varphi(m)}$ IS, SO $ar_j \equiv 1 \pmod m$ FOR SOME j. □

NOTE IF $(a,m)>1$ THEN $\nexists$ x SUCH THAT $ax\equiv 1 (m)$ SINCE $(ax,m)\geq(a,m)$.

THUS THE REDULED RESIDUES ARE EXACTLY THE GROUP OF UNITS OF $\mathbb{Z}/m\mathbb{Z}$.

THEOREM (WILSON'S THEOREM): LET p BE PRIME. THEN $(p-1)! \equiv -1 \mod p$.

PROOF: $\{1, 2, \ldots, p-1\}$ IS A REDUCED RES SYSTEM MOD p. FOR EACH $1 \leq x < p$ THERE EXISTS y SUCH THAT $1 \equiv xy \equiv yx \mod p$. THIS y IS UNIQUE. IF $x \equiv x^{-1}$ THEN $x^2 \equiv 1 \mod p$.

$X^2 \equiv 1 \mod p \iff$

$X^2 - 1 = (x+1)(x-1) \equiv 0 \mod p$

So $X \equiv 1$ OR $p-1 \mod p$.

Split $\{2, 3, 4, \ldots, p-2\}$ into $\frac{p-3}{2}$ pairs $\{x, x^{-1}\}$. Thus

$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \mod p$.

Thus $(p-1)! \equiv -1 \mod p$. $\square$

THEOREM: $X^2 \equiv -1 \bmod p$ HAS A SOLUTION IFF EITHER $p=2$ OR $p \equiv 1 \bmod 4$.

(ASSUME p ODD)

PROOF: $X^{p-1} \equiv 1 \bmod p$ SO $(X^2)^{\frac{p-1}{2}} \equiv 1 \bmod p$. THUS IF $X^2 \equiv -1 \bmod p$ THEN $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$. THUS $\frac{p-1}{2}$ IS EVEN SO $p \equiv 1 \bmod 4$.

CONSIDER:

$$-1 \equiv \prod_{j=1}^{(p-1)/2} j \cdot (-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} (-j)^2 \bmod p.$$

IF $p \equiv 1 \bmod 4$ THEN $\frac{p-1}{2}$ EVEN

$$\Rightarrow \prod_{j=1}^{(p-1)/2} j^2 \equiv \left(\prod_{j=1}^{\frac{p-1}{2}} j\right)^2 \equiv -1 \bmod p.$$

□

LEMMA: IF $p \equiv 1 \bmod 4$ IS PRIME, THEN THERE EXIST a, b WITH $a^2+b^2=p$.

PROOF: CHOOSE A REDUCED RESIDUE X SO THAT $X^2 \equiv -1 \bmod p$.

CONSIDER THE FUNCTION $f(u,v) = u+Xv$.

LET $K = \lfloor \sqrt{p} \rfloor$ AND CONSIDER THE $(K+1)^2$ PAIRS

$$\{(u,v): 0 \le u,v \le K\}.$$

$(K+1)^2 > p$. SO TWO PAIRS $(u_1,v_1), (u_2,v_2)$ HAVE

$$f(u_1,v_1) \equiv f(u_2,v_2) \text{ MOD } p.$$

THUS $u_1 + xv_1 \equiv u_2 + xv_2$ MOD p

OR $u_1 - u_2 \equiv x(v_2 - v_1)$ MOD p.

LET $a = u_1 - u_2$, $b = v_1 - v_2$.

NOTICE $|a| < \sqrt{p}$, $|b| < \sqrt{p}$.

$a^2 \equiv x^2 b^2 \equiv -b^2$ MOD p, SO

$$a^2 + b^2 \equiv 0 \text{ MOD } p.$$

BUT $0 < a^2 + b^2 < 2p$ SO

$p = a^2 + b^2$. □

LEMMA: If $q \equiv 3 \bmod 4$ is prime, and $q \mid (a^2+b^2)$ then $q \mid a$ and $q \mid b$.

PROOF: Suppose otherwise. Then, say, a is a red. rep. mod q, $a^2 \equiv -b^2 \bmod q$

$\Rightarrow -1 \equiv (a^{-1})^2 b^2 \bmod q$,

contradiction.

Hence $q \mid a$, $q \mid b$. $\square$

THEOREM: A NUMBER $n \geq 1$ IS THE SUM OF TWO SQUARES IF AND ONLY IF, IN ITS PRIME FACTORIZATION

$$n = 2^{\alpha} \prod_{\substack{p \equiv 1 \bmod 4 \\ \text{prime}}} p^{\beta_p} \prod_{\substack{q \equiv 3 \bmod 4 \\ \text{prime}}} q^{\gamma_q}$$

EACH γ_i IS EVEN.

EXAMPLE: 3, 15 CANNOT BE WRITTEN AS A SUM OF TWO SQUARES

$5 = 1^2 + 2^2$, $45 = 3^2 + 6^2$.

PROOF: IF $n = 2^{\gamma} \prod_{p \equiv 1 \bmod 4} p^{\beta_p} \prod_{q \equiv 3 \bmod 4} q^{\gamma_q}$

IS THE SUM OF TWO SQUARES,

$$n = a^2 + b^2$$

AND IF $q \equiv 3 \bmod 4$, $q \mid n$

THEN $q \mid a$, $q \mid b$ SO $q^2 \mid n$

AND $\frac{n}{q^2} = \left(\frac{a}{q}\right)^2 + \left(\frac{b}{q}\right)^2$.

THUS THE STATED

CONDITION IS NECESSARY.

TO PROVE SUFFICIENT, CONSIDER GAUSSIAN INTEGERS $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$

$N(a+bi) = a^2+b^2$.
$= (a+bi)(a-bi)$.

$i = \sqrt{-1}$.

$N((a+bi)(c+di)) = \frac{(a+bi)(c+di)}{(a+bi)(c+di)}$

$= N(a+bi) \cdot N(c+di)$.

SO SUMS OF 2 $\square$ = NORMS OF GAUSSIAN INTEGERS.

IF m,n ARE A SUM OF 2 $\square$ THEN SO IS $m \cdot n$.

$2 = 1^2+1^2$

$4 = 2^2+0^2$.

IF $p \equiv 1 \bmod 4$, $p = a^2+b^2$ SOME a,b.

IF $n = a^2+b^2$ THEN $q^2 n = (qa)^2+(qb)^2$.

THIS PROVES THAT IF

$$n = 2^\alpha \prod_{p \equiv 1 \bmod 4} p^{\beta_p} \prod_{q \equiv 3 \bmod 4} q^{2\gamma_q}$$

THEN n IS A SUM OF 2 $\square$s. $\square$

THE CHINESE REMAINDER THEOREM:

IF $m_1, m_2, \ldots, m_r$ ARE PAIRWISE COPRIME, FOR EACH

$x_1 \bmod m_1, \ldots, x_r \bmod m_r$

THERE IS A UNIQUE

$x \bmod m_1 \ldots m_r$

SUCH THAT $x \equiv x_i \bmod m_i$ FOR EACH i.

NOTE: AS RINGS

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \cong \mathbb{Z}/m_1 \cdots m_r\mathbb{Z}.$$

PROOF: LET

$$n_j = \frac{m_1 m_2 \cdots m_r}{m_j}.$$

THUS $(n_j, m_j) = 1$.

LET $\overline{n_j}$ BE AN INTEGER SUCH THAT $n_j \overline{n_j} \equiv 1 \bmod m_j$.

DEFINE:

$$X = x_1 n_1 \overline{n_1} + x_2 n_2 \overline{n_2} + \cdots + x_r n_r \overline{n_r}.$$

MODULO m_i, $m_i \mid n_j$ IF $i \neq j$.

$$X \equiv x_i n_i \overline{n_i} \bmod m_i.$$
$$\equiv x_i \bmod m_i.$$

THIS GIVES A MAP

$$(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}) \to \mathbb{Z}/m_1 \cdots m_r\mathbb{Z}.$$

WHICH IS ONTO, HENCE 1-1, SINCE THEY HAVE THE SAME SIZE. □

COROLLARY: If $(m,n)=1$,

$$\varphi(mn)=\varphi(m)\varphi(n)$$

SINCE $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times (\mathbb{Z}/n\mathbb{Z})^\times$

COROLLARY: IF $f(x) \in \mathbb{Z}[x]$ IS A POLYNOMIAL, m, n ARE CO-PRIME, THEN

$$\#\{r \bmod mn : f(r) \equiv 0 \bmod mn\}$$

$$= \#\{r \bmod m : f(r) \equiv 0 \bmod m\} \cdot \#\{r \bmod n : f(r) \equiv 0 \bmod n\}.$$