(1)

MATH 407

2/23/18

* Divisibility on prime factorization:

If $a = p_1^{r_1} \cdots p_k^{r_k} \cdots$

$b = p_1^{s_1} \cdots p_k^{s_k} \cdots$

then $a \mid b$ iff $r_i \leq s_i$ all i

$\gcd(a,b) = p_1^{m_1} \cdots p_k^{m_k} \cdots$, $m_i = \min(r_i, s_i)$

* Least Common Multiple:

Def. $c = \operatorname{lcm}(a,b)$ iff i) $a \mid c$, $b \mid c$
and ii) if $a \mid d$, $b \mid d$, then $c \mid d$

Thm. $c = p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k} \cdots$, $M_i = \max(r_i, s_i)$

Lemma. Let x, y be positive real
$m = \min(x,y)$, $M = \max(x,y)$
i) $x + y = m + M$
ii) $x \cdot y = m \cdot M$

Thm. $a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$

Pf. $a \cdot b = \left(p_1^{r_1} \cdots p_k^{r_k} \cdots\right)\left(p_1^{s_1} \cdots p_k^{s_k} \cdots\right)$

$$= p_1^{r_1+s_1} p_2^{r_2+s_2} \cdots p_k^{r_k+s_k}$$

$$= p_1^{(m_1+M_1)} p_2^{(m_2+M_2)} \cdots p_k^{(m_k+M_k)} \cdots$$

$$= \left(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \cdots\right)\left(p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k} \cdots\right)$$

$$= \gcd(a,b) \cdot \operatorname{lcm}(a,b)$$

* $\operatorname{lcm}(a,b) = \dfrac{a \cdot b}{\gcd(a,b)}$

Example: $a = 126$, $b = 35$, $\gcd(a,b) = 7$

$$\operatorname{lcm}(a,b) = \frac{126 \cdot 35}{7} = 630$$

* Congruence Modulo $n \in \mathbb{N}' = \{2, 3, \dots\}$

Def. $a \equiv b \pmod{n}$ iff $n \mid a-b$
iff $(a-b) \equiv 0 \pmod{n}$

If $a = nq_1 + r_1$ and $b = nq_2 + r_2$

$r_1, r_2 \in \{0, \dots, n-1\}$
$r(a) = r_1$ $\quad (r : \mathbb{N}' \to \{r_1, r_2\} = \{0, \dots, n-1\})$
$r(b) = r_2$

$a \equiv r(a) \pmod{n}$
$b \equiv r(b) \pmod{n}$

$a \equiv b \pmod{n}$
$a - b \equiv 0 \pmod{n}$
$n(q_1 - q_2) - (r_1 - r_2) \equiv 0 \pmod{n}$
$\therefore \; r_1 = r_2$

Therefore, $a \equiv b \pmod{n}$ iff $r(a) = r(b)$

Thm. '$\equiv$' is the equivalence relation $\sim_r$ on $\mathbb{Z}$

③

$a \equiv b \pmod{n} \Rightarrow n \mid (a-b)$
$b \equiv c \pmod{n} \Rightarrow n \mid (b-c)$
so, $n \mid (a-b)+(b-c)$
$= n \mid (a-c)$

$* \ [a]_n = \{b : a \equiv b \pmod{n}\}$ (notation for $[a]_{\sim r}$)

$= \{b : r(b) = r(a)\}$

$= [r(a)] = [r_1]$

$\mathbb{Z}/\bmod n = \{[0]_n, [1]_n, \ldots, [n-1]_n\} = n\mathbb{Z}$

$= \mathbb{Z}_n$

Prop 1.3.3 a, b, c, d are integers $n \in \mathbb{N}$!

a) Let $a \equiv c \pmod{n}$
$b \equiv d \pmod{n}$
Then $a+b \equiv (c+d) \pmod{n}$
$a-b \equiv (c-d) \pmod{n}$
$a \cdot b \equiv (c \cdot d) \pmod{n}$

b) If $(a+c) \equiv (a+d) \pmod{n}$
then $c \equiv d \pmod{n}$ (cancellation property of addition)

If $ac = ad$ and $(a, n) = 1$
then $c \equiv d \pmod{n}$ (cancellation property of multiplication)

Pf. (Prop 1.3.3 Part a)) Look at $a \cdot b \equiv c \cdot d$

Want $a \cdot b - c \cdot d \equiv 0$

that is, $n \mid (ab - cd)$

$$= (ab - cd) + (cb - cd)$$
$$= (a - c)b + c(b - d)$$

Since $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$,

$n \mid (a-c)$ and $n \mid (b-d)$

So, $n \mid (a-c)b + c(b-d)$

$= n \mid (ab - cd)$

Pf. (Prop 1.33 Part b))

$(a-c) \equiv (a+d)$

$-a \equiv -a \pmod{n}$

Thus, $(a+c) + (-a) \equiv ((a+d) + (-a)) \pmod{n}$

$\therefore c \equiv d$

To show $n \mid (c-d)$

have

$n \mid (ac - ad) = n \mid a(c-d)$

$(a, n) = 1$

$n \mid (c-d)$