THEOREM
LET $a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}$ AND $b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n}$ AS BEFORE. THEN

$$LCM(a,b) = p_1^{\max(x_1,y_1)} \cdot p_2^{\max(x_2,y_2)} \cdots p_n^{\max(x_n,y_n)}.$$

PROOF: EXCERCISE.

EX. $LCM(60,90) = 2^2 \cdot 3^2 \cdot 5 = 180$

THEOREM
LET $a,b \in \mathbb{Z}$. THEN $a \cdot b = GCD(a,b) \cdot LCM(a,b)$

PROOF: EXCERCISE (USE $x+y = \min(x,y) + \max(x,y)$).

DEFN
LET $a,b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. WE SAY a IS CONGRUENT TO b MODULO m IFF $m \mid (a-b)$.

NOTATION: $a \equiv b \pmod{m}$

EX $8 \equiv 22 \pmod 7$ SINCE $7 \mid (8-22)$
$51 \equiv 18 \pmod{11}$ SINCE $11 \mid (51-18)$

THEOREM
$a \equiv b \pmod{m}$ IFF $a = b + km$ FOR SOME $k \in \mathbb{Z}$.

PROOF:
$a \equiv b \pmod{m}$ IFF $m \mid (a-b)$ IFF $a - b = km$ FOR SOME $k \in \mathbb{Z}$ IFF $a = b + km$ FOR SOME $k \in \mathbb{Z}$. ///

THEOREM
$a \equiv b \pmod{m}$ IFF a AND b HAVE THE SAME REMAINDER UPON DIVISION BY m.

PROOF:
($\Rightarrow$) LET $a \equiv b \pmod{m}$ SO THAT $a - b = km$ FOR SOME $k \in \mathbb{Z}$. BY THE DIVISION ALGORITHM

$$a = q_1 m + r_1 \qquad 0 \le r_1 < m$$
AND $$b = q_2 m + r_2 \qquad 0 \le r_2 < m$$

THUS
$$km = a - b = (q_1 - q_2)m + (r_1 - r_2)$$
$$\therefore \; r_1 - r_2 = (q_1 - q_2 - k)m$$

THEREFORE $m \mid (r_1 - r_2)$ AND LIKEWISE $m \mid (r_2 - r_1)$. AT LEAST ONE OF $r_1 - r_2$ OR $r_2 - r_1$ IS NON-NEGATIVE AND LESS THAN m, SAY

$$0 \leq r_1 - r_2 < m$$

BUT THEN $m \mid (r_1 - r_2)$ IMPLIES $r_1 - r_2 = 0$,
$\therefore r_1 = r_2$. $\therefore$ a AND b HAVE THE SAME REMAINDER WHEN DIVIDED BY m.

($\Leftarrow$) SUPPOSE a AND b HAVE THE SAME REMAINDERS UPON DIVISION BY m, i.e.

$$a = q_1 m + r$$
$$b = q_2 m + r$$
$$\therefore \quad a - b = (q_1 m - q_2 m) + (r - r)$$
$$\therefore \quad a - b = (q_1 - q_2) m$$
$$\therefore \quad m \mid (a - b)$$

HENCE $a \equiv b \pmod{m}$. ///

DEFN.
WE DEFINE OPERATIONS *mod* AND *div* AS FOLLOWS

a *mod* m = REMAINDER OF a UPON DIVISION BY m

a *div* m = QUOTIENT OF a UPON DIVISION BY m

THUS

$$a = m \cdot (a \text{ div } m) + (a \text{ mod } m)$$

THE PRECEDING THEOREM CAN NOW BE STATED AS

$$a \equiv b \pmod{m} \text{ IFF } a \bmod m = b \bmod m.$$

WARNING: DO NOT CONFUSE THE TWO MEANINGS OF 'mod'. BOLDFACE mod IS AN OPERATION ON INTEGERS WHILE $\cdot \equiv \cdot \pmod{m}$ IS A RELATION.

THEOREM
IF $a \equiv b \pmod{m}$ AND $c \equiv d \pmod{m}$ THEN $a + c \equiv b + d \pmod{m}$.

PROOF: EXERCISE OR SEE BOOK.

THEOREM
WITH SAME HYPOTHESES AS ABOVE WE HAVE $ac \equiv bd \pmod{m}$.

PROOF:

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + (c-d)b \\ &= k_1 m \cdot c + k_2 m \cdot b \quad \text{(BY HYPOTHESES)} \\ &= (k_1 c + k_2 b) m. \end{aligned}$$

$\therefore m \mid (ac - bd) \quad \therefore ac \equiv bd \pmod{m}.$

///

STUDENTS ARE OFTEN TEMPTED TO BELIEVE THAT SINCE

$$\left.\begin{array}{l} a \equiv c \pmod{m} \\ b \equiv d \pmod{m} \end{array}\right\} \text{ IMPLIES } a+b \equiv c+d \pmod{m}$$

IT MUST ALSO BE TRUE THAT

$$* \quad (a \bmod m) + (b \bmod m) \stackrel{?}{=} (a+b) \bmod m .$$

IN FACT * IS IN GENERAL FALSE.

EXERCISE: FIND A COUNTEREXAMPLE TO *.

(2.4) Euclidean Algorithm (p. 177)

Ex. Find GCD(198, 84)

$$198 = 2 \cdot 84 + 30$$
$$84 = 2 \cdot 30 + 24$$
$$30 = 1 \cdot 24 + (6) \longrightarrow GCD(198, 84) = 6$$
$$24 = 4 \cdot 6 + 0$$

long way: $198 = 2 \cdot 3^2 \cdot 11$, $84 = 2^2 \cdot 3 \cdot 7$

$\therefore GCD(198, 84) = 2^1 \cdot 3^1 \cdot 7^0 \cdot 11^0 = 6$.

Lemma

If $a, b, q, r \in \mathbb{Z}$ and $a = qb + r$ then $GCD(a, b) = GCD(b, r)$.

Proof:

If $d \mid a$ and $d \mid b$ then $d \mid (a - qb) = r$.

If $d \mid b$ and $d \mid r$ then $d \mid qb + r = a$.

Thus the set of common divisors of a and b is identical to the set of common divisors of b and r. Therefore the maximum element in that set is both $GCD(a, b)$ and $GCD(b, r)$.

$\therefore GCD(a, b) = GCD(b, r)$.

///

THEOREM

EUCLID'S ALGORITHM CORRECTLY DETERMINES THE GCD OF TWO NUMBERS.

PROOF

LET $a, b \in \mathbb{Z}^+$ WITH $a \geq b$. SET $r_0 = a$, $r_1 = b$ AND APPLY DIVISION ALGORITHM TO OBTAIN:

$$r_0 = q_1 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$
$$r_1 = q_2 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$
$$r_2 = q_3 r_3 + r_4 \qquad 0 \leq r_4 < r_3$$
$$\vdots$$
$$r_{n-2} = q_{n-1} r_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = q_n r_n + 0$$

SINCE THE SEQUENCE $r_1 > r_2 > r_3 > \ldots \geq 0$ IS STRICTLY DECREASING, SOME REMAINDER MUST BE ZERO, SAY $r_{n+1} = 0$. BY THE PRECEDING LEMMA:

$$GCD(a,b) = GCD(r_0, r_1) = GCD(r_1, r_2) = \cdots = GCD(r_n, 0) = r_n.$$

$\therefore GCD(a,b) = r_n$, THE LAST NON-ZERO REMAINDER. //

EX. $GCD(1001, 513) = 1$.

(3.1) Proof Strategy

Read this section carefully, especially Examples 1 – 5 (p. 214-217).

I will not lecture directly on this section, but there will be a few HW problems assigned.