(2.4) Integers and Division

Defn

Let $a, b \in \mathbb{Z}$, $a \neq 0$. We say a divides b if $b = ak$ for some $k \in \mathbb{Z}$.

Notation: $a \mid b$

We also say:

- a is a **factor** of b
- a is a **divisor** of b
- b is a **multiple** of a
- b is **divisible** by a

Ex. $3 \mid 24$, $5 \nmid 21$

Theorem

Let $a, b, c \in \mathbb{Z}$.

(1) $a \mid b \wedge a \mid c \rightarrow a \mid (b+c)$

(2) $a \mid b \rightarrow \forall d : a \mid bd$

(3) $a \mid b \wedge b \mid c \rightarrow a \mid c$

Book proves (1). (3) is Problem 4 in 2.4. Do (1) & (2).

Note: For any $a \in \mathbb{Z}$, $1 \mid a$. If $a \neq 0$, then $a \mid a$. Also $a \mid 0$.

Corollary
Let $a, b, c, m, n \in \mathbb{Z}$. Then

$$a|b \wedge a|c \rightarrow a|(mb+nc)$$

Proof:

$$\left.\begin{array}{l} a|b \rightarrow a|mb \\ a|c \rightarrow a|nc \end{array}\right\} \rightarrow a|(mb+nc)$$

↑ By (2) ↑ By (1). ///.

Defn
Let $p \in \mathbb{Z}$, $p > 1$. We say p is Prime if it's only positive factors are 1 and p. A positive integer which is not prime is called Composite.

Prime: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...
Composite: 1, 4, 6, 8, 9, 10, 12, 14, 15, 16, ...

Note: 1 is not Prime.

THEOREM (FUNDAMENTAL THEOREM OF ARITHMETIC)
EVERY POSITIVE INTEGER CAN BE EXPRESSED UNIQUELY (UP TO ORDER) AS THE PRODUCT OF (ZERO OR MORE) PRIMES.

NOTE:
- 'UP TO ORDER' MEANS ORDER DOES NOT COUNT, i.e. $2 \cdot 3$ AND $3 \cdot 2$ ARE THE SAME FACTORIZATION OF 6.
- THE PRODUCT MAY CONTAIN ZERO, ONE, OR MORE PRIME FACTORS. THE 'EMPTY PRODUCT' IS DEFINED TO BE 1.

EX. $100 = 2^2 \cdot 5^2$, $999 = 3^3 \cdot 37$

THEOREM
LET $n \neq 1$ BE COMPOSITE. THEN n HAS A PRIME FACTOR p SATISFYING $p \leq \sqrt{n}$.

COROLLARY (CONTRAPOSITIVE)
IF $n > 0$ IS NOT DIVISIBLE BY ANY PRIME $p \leq \sqrt{n}$, THEN n MUST BE PRIME.

EX 113 IS NOT DIVISIBLE BY 2, 3, 5, 7
HENCE IS PRIME. IT IS UNNECESSARY TO TEST FOR DIVISIBILITY BY 11 SINCE $11^2 = 121 > 113$.

PROOF

SINCE n IS COMPOSITE IT HAS A FACTOR a SATISFYING $1 < a < n$. THUS $n = ab$ WHERE ALSO $1 < b < n$. IF BOTH $a > \sqrt{n}$ AND $b > \sqrt{n}$ THEN $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, A CONTRADICTION. THUS EITHER $a \leq \sqrt{n}$ OR $b \leq \sqrt{n}$, SAY FOR DEFINITENESS $a \leq \sqrt{n}$. IF a IS PRIME WE ARE DONE. OTHERWISE a HAS A PRIME DIVISOR $p \leq a \leq \sqrt{n}$. SINCE $p|a$ AND $a|n$ WE HAVE $p|n$. THUS IN ANY CASE, n HAS A PRIME DIVISOR NOT EXCEEDING $\sqrt{n}$. ///.

THEOREM (EUCLID)

THERE EXIST INFINITELY MANY PRIMES.

PROOF

ASSUME, TO GET A CONTRADICTION, THAT THERE ARE ONLY FINITELY MANY PRIMES. SAY $\{p_1, p_2, \ldots, p_n\}$ ARE ALL THE PRIMES.

LET $N = (p_1 \cdot p_2 \cdots p_n) + 1$. NOW $N > 1$ AND N IS NOT ONE OF THE PRIMES $\{p_1, \ldots, p_n\}$ SO BY THE FUNDAMENTAL THEOREM, N HAS A PRIME FACTOR, SAY p_i. THUS $N = p_i \cdot K$ FOR SOME $K \in \mathbb{Z}$.

LET $M = \frac{p_1 \cdot p_2 \cdots p_n}{p_i}$, SO $N = p_i M + 1$.
THUS

$$p_i \cdot K = N = p_i M + 1$$

$$\therefore \quad 1 = p_i (K - M)$$

$$\therefore \quad p_i \mid 1$$

BUT 1 HAS NO PRIME FACTORS. THIS CONTRADICTION SHOWS OUR ASSUMPTION WAS FALSE, AND HENCE THE SET OF PRIMES IS INFINITE.

///

NOTE: WE NEVER ACTUALLY DETERMINED A PRIME LARGER THAN p_n, SO THIS WAS A NON-CONSTRUCTIVE EXISTENCE PROOF.

THEOREM (DIVISION 'ALGORITHM')
LET $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$. THEN THERE EXIST UNIQUE $q, r \in \mathbb{Z}$ SUCH THAT

* $$a = dq + r \quad \text{AND} \quad 0 \leq r < d$$

WE CALL a THE DIVIDEND, d THE DIVISOR, q THE QUOTIENT, AND r THE REMAINDER

PROOF:

LET $q = \left\lfloor \frac{a}{d} \right\rfloor$ AND $r = a - dq$. THEN $a = dq + r$, AND

$$q \le \frac{a}{d} < q+1$$
$$\therefore \quad dq \le a < dq + d$$
$$\therefore \quad 0 \le a - dq < d$$
$$\therefore \quad 0 \le r < d$$

THUS q AND r EXIST SATISFYING $*$.

EXCERCISE: SHOW THAT q AND r ABOVE ARE UNIQUE, i.e. SUPPOSE $a = dq' + r'$ AND $0 \le r' < d$, THEN PROVE $r' = r$ AND $q' = q$. ///

EX.
$$123 = 12 \cdot 10 + 3 \qquad 0 \le 3 < 12$$
$$91 = 11 \cdot 8 + 3 \qquad 0 \le 3 < 11$$
$$-35 = 8 \cdot (-5) + 5 \qquad 0 \le 5 < 8$$

DEFN

LET $a, b \in \mathbb{Z} - \{0\}$. THE GREATEST COMMON DIVISOR (GCD) OF a AND b IS THE LARGEST d SUCH THAT BOTH $d \mid a$ AND $d \mid b$.

NOTATION: $d = GCD(a, b)$

Ex. $GCD(12,18) = 6$

$\{1,2,3,4,6,12\} \cap \{1,2,3,6,9,18\} = \{1,2,3,6\}$

Ex. $GCD(13,44) = 1$.

NOTE: $GCD(a,b)$ EXISTS SINCE THE SET OF COMMON DIVISORS OF a AND b IS FINITE AND NON-EMPTY (CONTAINING 1), HENCE CONTAINS A MAXIMUM ELEMENT. IN PARTICULAR $GCD(a,b) \geq 1$.

DEFN

$a, b \in \mathbb{Z} - \{0\}$ ARE SAID TO BE RELATIVELY PRIME IFF $GCD(a,b) = 1$. EQUIVALENTLY a, b ARE RELATIVELY PRIME IFF THEY HAVE NO PRIME FACTORS IN COMMON.

Ex. $GCD(13,44) = 1$, $GCD(12,25) = 1$.

THEOREM

LET ALL PRIMES WHICH DIVIDE a OR b BE LISTED: $p_1, p_2, \ldots, p_n$ SO THAT $a = p_1^{x_1} \cdot p_2^{x_2} \cdots p_n^{x_n}$ AND $b = p_1^{y_1} \cdot p_2^{y_2} \cdots p_n^{y_n}$ WHERE $x_i \geq 0$, $y_i \geq 0$ FOR $1 \leq i \leq n$. THEN

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

Ex. $60 = 2^2 \cdot 3 \cdot 5$, $90 = 2 \cdot 3^2 \cdot 5$

$\therefore GCD(60,90) = 2 \cdot 3 \cdot 5 = 30$

Proof

The RHS obviously divides a since it has the same prime factors as a to powers not exceeding those in a. Likewise the RHS also divides b. No larger integer can divide both a and b since we cannot increase the exponents or add prime factors to the RHS without losing divisibility. Therefor the right hand side of the above formula must be the GCD of a and b. ///

Defn

Let $a, b \in \mathbb{Z}$. The <u>least common multiple</u> (LCM) of a and b is the smallest m such that both $a|m$ and $b|m$.

Notation: $m = LCM(a,b)$.

Not surprisingly the GCD and LCM are closely related.