§1. Divisors, Greatest Common Divisor, Prime Numbers

NOTATION

$\mathbb{N}$ is the set of positive integers, i.e. $\mathbb{N} = \{1, 2, 3, \ldots\}$.

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ is the set of integers.

$\mathbb{P}$ is the set of prime numbers, defined toward the bottom of the page.

DEF For $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, if $n = dq$ for some $q \in \mathbb{Z}$, we write $d \mid n$, and say

d divides n;

d is a divisor of n;

n is divisible by d;

n is a multiple of d.

(Underlining indicates that the underlined word is being defined.)

Using some of the symbols

$\forall$	for each	$\Rightarrow$	implies
$\exists$	for some	$\not\Rightarrow$	does not imply
$:$	so that		
$\Leftrightarrow$	if and only if		

the above definition can be written as follows:

$$\forall n \in \mathbb{Z}, \forall d \in \mathbb{N}, \text{"} d \mid n \text{"} \Leftrightarrow \exists q \in \mathbb{Z} : n = dq.$$

EXAMPLES. The divisors of 12 are 1, 2, 3, 4, 6, 12.
For each $d \in \mathbb{N}$, the multiples of d are $0, \pm d, \pm 2d, \ldots$.

DEF A prime number is an integer $p > 1$ with 1 and p as its only divisors.

EXAMPLES. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

THM A (Properties of Divisors)

(1) If $d|e$ and $e|f$, then $d|f$.

(2) If $d|m$ and $e|n$, then $de|mn$.

(3) If $d|n$ and $n \neq 0$, then $|n| \geq d$.

(4) If $c|m$ and $c|n$, then $c|xm+yn$ for all $x, y \in \mathbb{Z}$.

Proof of (1): $d|e \Rightarrow e = dq$ for some $q \in \mathbb{Z}$

$e|f \Rightarrow f = er$ for some $r \in \mathbb{Z}$

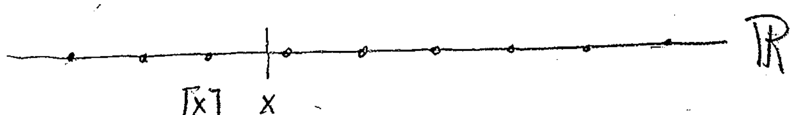
$\therefore$ $d|e$ & $e|f \Rightarrow f = ds$ with $s = qr \in \mathbb{Z}$, so $d|f$.

EXERCISE 1. Prove (2), (3), (4) similarly.

DEF For each real number x, i.e. $\forall x \in \mathbb{R}$,

$[x]$ denotes the largest integer $\leq x$

Thus $[x] \leq x < [x]+1$, i.e. $x-1 < [x] \leq x$.



EXAMPLES $[3] = 3$, $[\pi] = 3$, $[-\pi] = -4$.

THM B (division with remainder). For each $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, there are integers q and r so that both

$$\boxed{n = dq + r \text{ and } 0 \leq r < d}.$$

Proof. Put $q = [\frac{n}{d}]$. Then $q \leq \frac{n}{d} < q+1$

i.e. $dq \leq n < dq + d$

i.e. $0 \leq n - dq < d$,

giving $\Box$ with $r = n - dq$.

EXAMPLE. For $n = 30$ & $d = 7$, $q = 4$ & $r = 2$.

EXERCISE 2. Prove that the integers q and r in THM B are uniquely determined by n and d, i.e. for each $d \in \mathbb{N}$,

$$dq_1 + r_1 = dq_2 + r_2 \text{ with } q_1, q_2, r_1, r_2 \in \mathbb{Z} \ \& \ 0 \le r_1, r_2 < d \Rightarrow q_1 = q_2 \ \& \ r_1 = r_2.$$

DEF (greatest common divisor). Let $m, n \in \mathbb{Z}$, not both 0.
The <u>greatest</u> <u>common</u> <u>divisor</u> of m and n is the largest positive integer which divides both m and n. It is denoted by (m,n).

REMARKS (1) Each positive integer divides 0. For this reason, $m=0$, $n=0$ have no greatest common divisor. (2) 1 is a common divisor of every m and n in $\mathbb{Z}$. If $m \neq 0$, each divisor of m is $\le |m|$, and similarly for n. Therefore if m and n are not both 0, there is a (unique) greatest common divisor of m & n.

EXAMPLE $m=21$, $n=30$

divisors of 21: 1, 3, 7, 21;

divisors of 30: 1, 2, 3, 5, 6, 10, 15, 30;

common divisors of 21&30 : 1, 3; $\therefore (21,30) = 3$.

THM C (about the greatest common divisor) Let $m, n \in \mathbb{Z}$, not both 0. Then:

(1) (m,n) is the least positive integer of the form $xm+yn$ for $x, y \in \mathbb{Z}$;

(2) If $d|m$ & $d|n$, then $d|(m,n)$, i.e. (m,n) is divisible by each common divisor of m & n.

REMARK Statement (2) is stronger than "(m,n) is $\geqslant$ each common divisor of m & n."

Proof. (1) Let d be the least positive integer of the form $xm+yn$ with $x, y \in \mathbb{Z}$, say

✓ $$d = x_1 m + y_1 n. \quad (\text{with } x_1, y_1 \in \mathbb{Z})$$

We show first that $d|n$: In fact, by THM B,

✓✓ $$n = dq + r \text{ for some } q, r \in \mathbb{Z} \text{ with } 0 \le r < d$$

By ✓ & ✓✓,

$$r = n - dq = (-x_1 q)m + (1 - y_1 q)n = x_2 m + y_2 n$$

for some $x_2, y_2 \in \mathbb{Z}$. Since $0 \le r < d$, minimality of d implies $r = 0$, i.e. $d \mid n$.

Similarly, $d \mid m$.

Thus d is a common divisor of m and n, so

$$\boxed{d \le (m, n)}$$

By ✓ and THM A (4), d is divisible by every common divisor of m and n.

In particular, (m,n) divides d, so

$$\boxed{(m,n) \le d}$$

It follows from the two boxed statements that $(m,n) = d$, proving (1).

The two circled statements prove (2).

THM D. For $l, m \in \mathbb{Z}$, not both 0, and $n \in \mathbb{N}$,

$$\boxed{(ln, mn) = (l, m)n}$$

Proof By THM C, (ln, mn) is the least positive integer of the form

$$xln + ymn = (xl + ym)n, \quad \text{for } x, y \text{ in } \mathbb{Z},$$

so (ln, mn) is n times the least positive integer of the form $xl + ym$ for $x, y \in \mathbb{Z}$, i.e. $(ln, mn) = n(l, m)$.

THM E For $l, m, n \in \mathbb{N}$,

$$\boxed{l \mid mn \ \& \ (l, m) = 1 \Rightarrow l \mid n}$$

Proof. Since $l \mid ln$ and $l \mid mn$,

$$l \mid \underset{\substack{\uparrow \\ \text{THM C}}}{} (ln, mn) \underset{\substack{\uparrow \\ \text{THM D}}}{=} (l, m)n \underset{\substack{\uparrow \\ (l,m)=1}}{=} n.$$

THM F For each prime p, and $m, n \in \mathbb{N}$

$$\boxed{p \mid mn \Rightarrow p \mid m \text{ or}^{*)}\ p \mid n}$$

Proof If $p \mid m$ we are done, so we may suppose $p \nmid m$,
i.e. p is not a divisor of m. Therefore $(p, m) \neq p$.
Since (p, m) is a divisor of p, and the only divisors of p are 1 and p, and we have ruled out p, we get $(p, m) = 1$.

Now we have $p \mid mn$ and $(p, m) = 1$, so $p \mid n$, by THM E.

THM G If p and $q_1, \ldots, q_r$ are primes, and $p \mid q_1 \cdots q_r$, then $p = q_j$ for some j.

Proof. For $r = 1$, the statement is: $p \mid q$ with p, q prime $\Rightarrow p = q$.
This is true since the only divisors of q are 1 and q, and $p \neq 1$.
For $r > 1$, use THM F to get $p \mid q_1 \cdots q_{r-1}$ or $p \mid q_r$. If $p \mid q_r$ then $p = q_r$ as above. If $p \mid q_1 \cdots q_{r-1}$ repeat the argument (or use induction on r) to get $p = q_1$ or $\ldots$ or $p = q_{r-1}$. Either way, $p = q_1$ or $\ldots$ or $p = q_r$.

EXERCISE 3. Prove

(1) $\log x \to \infty$ for $x \to \infty$

(2) $\dfrac{\log x}{x^\delta} \to 0$ for $x \to \infty$, for each $\delta > 0$.

Hints: (1) $\log(e^n) = n$ for $n \in \mathbb{N}$

(2) $\log x = \int_1^x \frac{dt}{t} < x$ and $\log x = \frac{2}{\delta} \log x^{\frac{\delta}{2}}$ for $x > 0, \delta > 0$.

*) "or" includes "or both"