Divisibility (Apostol Ch. 1).

Until further notice: $a, b, c, d, e, m, n, x, y \in \mathbb{Z}$;
$p \in \{\text{primes} > 0\}$.

A. Definition: Say d divides n, written $d|n$, if
$\exists\, c:\ dc = n$. Otherwise, write $d \nmid n$.

Properties (Thm. 1.1). (proofs omitted.)

(a) $n|n$
(b) $d|n$ and $n|m \Rightarrow d|m$ (transitivity)
(c) $d|n$ and $d|m \Rightarrow d|(an+bm)$ (linearity)
(d) $d|n \Rightarrow ad|an$
(e) $ad|an$ and $a \neq 0 \Rightarrow d|n$
(f) $1|n$
(g) $n|0$
(h) $0|n \Rightarrow n = 0$
(i) $d|n$ and $n \neq 0 \Rightarrow |d| \leq |n|$
(j) $d|n$ and $n|d \Rightarrow |d| = |n|$
(k) $d|n$ and $d \neq 0 \Rightarrow (n/d)|n$

B. Common divisors.

Definition: If $d|a$ and $d|b$, then d is a common divisor of a and b.

Theorem 1.2. Given a and b, $\exists$ a unique $d \geq 0$ such that $d|a$, $d|b$, and

$$d = ax + by$$

for some $x, y \in \mathbb{Z}$.

This d is the greatest common divisor, or gcd, of a and b, denoted (a,b).

Moreover, if $e|a$ and $e|b$, then $e|(a,b)$.

Proof. Since

$$(a,b) = (|a|,|b|) \quad \text{(DIY: check this)},$$

it's enough to consider $a,b \geq 0$.

Induction on $a+b$: base case is $a=b=0=a+b$. In this case, the thm. holds for any $x,y \in \mathbb{Z}$, and for $(a,b)=0$.

Now assume the thm. for $0 \leq a+b \leq k-1$: wish to deduce it for $a+b=k>0$. Two cases:

(i) $b=0$. Then the thm. is true with $x=1$, $y=0$, $(a,b)=a$.

(ii) $b \geq 1$. Assume $a \geq b$ ($a \leq b$ is similar).

Write $b'=b$ and $a'=a-b$. Then $a',b' \geq 0$, and

$$0 \leq a'+b' = a-b+b = a = k-b \leq k-1.$$

By the induction hypothesis, thm. holds for a',b'.

Let $d=(a',b')$: then $\exists\, x',y' \in \mathbb{Z}$:

$$d = a'x'+b'y' = (a-b)x'+by' = ax'+b(y'-x') = ax+by, \quad (*)$$

with $x = x'$, $y = y' - x'$.

Since $d = (a', b') = (a-b, b)$, we have $d | (a-b)$ and $d | b$, so by linearity $d | [(a-b)+b]$, so $d | a$. So $d | a$ and $d | b$.

Moreover, if $e | a$ and $e | b$, then $e | (ax+by)$ by linearity, so by $(*)$, $e | d$.

Finally, d is unique since, given $d' \in \mathbb{Z}$ with these properties, we have $d | d'$ and $d' | d$, so $|d'| = |d|$ or, since $d, d' \geq 0$, $d' = d$. □

Theorem 1.4: properties of (a,b). (proofs omitted.)

(i) $(a,b) = (b,a)$
(ii) $(a,(b,c)) = ((a,b),c)$ (denote the common value by (a,b,c));
(iii) $(ac, bc) = |a|(b,c)$
(iv) $(a,1) = 1$; (v) $(a,0) = |a|$.

Definition: if $(a,b) = 1$, say a and b are <u>relatively prime</u>, or <u>coprime</u>.

Theorem 1.5 (Euclid's Lemma)
If a, b are coprime and $a | bc$, then $a | c$.

Proof: If $(a,b) = 1$, then $\exists\, x, y \in \mathbb{Z} : ax + by = 1$. So

$$c = cax + cby.$$

Certainly $a | cax$; by assumption, $a | bc$. So $a | c$ by linearity. □