Elementary number theory: divisibility properties of the integers (cf. Apostol, Chapter 1).

Until further notice, $a, b, c, d, e, m, n, x, y$ denote integers; p denotes a positive prime.

A. <u>Definition</u>: We say "d divides n," written $d|n$, if $\exists\, c$: $dc = n$.
Otherwise, write $d \nmid n$.

<u>Properties (Thm. 1.1).</u> (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.

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

<u>Theorem 1.2.</u> Given a and b, $\exists$ a unique non-negative common divisor d of a and b such that

$$d = ax + by \qquad (*)$$

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

We call this d 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. First: suppose the thm. is true for all $a,b \geq 0$. Then, for any $a,b \in \mathbb{Z}$, we find that the thm. is true for

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

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

We proceed by induction on $a+b$. Since $a,b \geq 0$, the base case is $a+b = 0+0 = 0$. We see that the thm. is true in this case with $x,y \in \mathbb{Z}$ chosen arbitrarily, and $(a,b) = 0$.

We now assume the theorem to be true for $0 \leq a+b \leq k-1$: we wish to deduce that it's true for $a+b=k$. There are two cases to consider:

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

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

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

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

By the induction hypothesis, the thm. holds for the pair 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 $d \mid (a-b)$ and $d \mid b$, so by linearity $d \mid [(a-b)+b]$, so $d \mid a$. So $d \mid a$ and $d \mid b$.

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

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

<u>Theorem 1.4</u>: properties of (a,b). (proofs omitted.)

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

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

We have:

<u>Theorem 1.5</u> (Euclid's Lemma)

If a and b are relatively prime and $a|bc$, then $a|c$.

<u>Proof.</u>

If $(a,b)=1$, then $\exists\, x,y \in \mathbb{Z}$:

$$ax+by=1.$$

But then

$$cax+cby=c.$$

Certainly $a|cax$, and by assumption $a|bc$, so $a|cby$. By linearity, then, $a|c$.

$\square$