Testing...

Number Theory Section Summary: 2.2
The Greatest Common Divisor

"Of special interest is the case in which the remainder in the Division Algorithm turns out to be zero." (p. 20)

1. Definitions

Divisible: An integer b is said to be **divisible** by an integer $a \neq 0$, written $a|b$, if there exists some integer c such that $b = ac$.

common divisor: An integer d is said to be **a common divisor** of a and b if both $d|a$ and $d|b$.

greatest common divisor: Let a and b be given integers, with at least one of them non-zero. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the positive integer d satisfying the following:

(a) $d|a$ and $d|b$

(b) If $c|a$ and $c|b$, then $c \leq d$.

relatively prime: Two integers a and b, not both zero, are said to be **relatively prime** whenever $\gcd(a, b) = 1$.

2. Theorems

Theorem 2.2: For integers a, b, c, the following hold:

(a) $a|0$, $1|a$, $a|a$

(b) $a|1$ if and only if $a = \pm 1$

(c) If $a|b$ and $c|d$, then $ac|bd$.

(d) If $a|b$ and $b|c$, then $a|c$.

(e) $a|b$ and $b|a$ if and only if $a = \pm b$

(f) If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

(g) If $a|b$ and $a|c$, then $a|(bx + cy)$ for arbitrary integers x and y.

Theorem 2.3: Given integers a and b, not both zero, there exists integers x and y such that

$$\gcd(a, b) = ax + by$$

Can be written as a linear combination

Corollary: If a and b are given integers, not both zero, then the set

$$T = \{ax + by | x, y \text{ are integers}\}$$

is precisely the set of all multiples of $d = \gcd(a, b)$.

Theorem 2.4: Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

$d = ax + by$

Corollary 1: If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$. $1 = (\frac{a}{d})x + (\frac{b}{d})y$

Corollary 2: If $a|c$ and $b|c$, with $\gcd(a, b) = 1$, then $ab|c$.

Theorem 2.5 (Euclid's lemma): If $a|bc$, with $\gcd(a, b) = 1$, then $a|c$.

Theorem 2.6: Let a and b be integers, not both zero. For a positive integer d, $d = \gcd(a, b)$ if and only if

(a) $d|a$ and $d|b$, and

(b) Whenever $c|a$ and $c|b$, then $c|d$.

3. Properties/Tricks/Hints/Etc.

Whenever we write $a|b$, we assume that $a \neq 0$.

Theorem 2.3

WLOG $a \neq 0$

Let $S = \{au + bv \mid au + bv > 0 \text{ and } (u,v) \in \mathbb{Z} \times \mathbb{Z}\}$

Claim: S is nonempty:

$|a| = a \cdot (\pm 1) \in S$

$= a \cdot \text{signum}(a)$

$u = \text{signum}(a)$

$(v = 0)$

By well-ordering $\exists$ a least element:

$d = ax + by$

Show that d is a common divisor:

By D.A $\exists (q, r) \in \mathbb{Z} \times \mathbb{Z}$ /

$a = qd + r \quad 0 \leq r < d$

Rewrite:

$r = a - qd$

$= a - q(ax + by)$

$= \underbrace{a(1 - qx) + b(-qy)}$

looks like an element of S

If $r > 0$ then $r \in S$, which contradicts choice of d as least element. So $r = 0$.

$a = qd$, so

$d \mid a$;

Similarly for b.

Hence d is a common divisor.

To show: it's the greatest.

Given $c \neq 0$ $c \mid a$ and $c \mid b$.

Then $c \mid ax+by$ (2.2, g);

so $c \mid d \Rightarrow |c| \leq |d|$ (2.2, f)

So d is the gcd.

QED

4. Summary

Divisibility is where it's at, and we get our share of it in this section. It's a lot of "theorem-proof", but that's good practice! Try to enjoy looking over the proofs, and get into the swing of them.

In the next section, we'll see how to find the gcd quickly (using the *Euclidean Algorithm*).

#2c (on the board)

#4c $5 \mid 3^{3n+1} + 2^{n+1}$, $n \geq 1$

Anchor: $n = 1$

$3^{3+1} + 2^{1+1} = 81 + 4 = 85$

$= 5 \cdot 17$ ✓

Inductive step:

Assume true for all integers up to k.

Consider $3^{3(k+1)+1} + 2^{(k+1)+1}$

$= 27 \cdot 3^{3k+1} + 2\,2^{k+1}$

$= 27\,3^{3k+1} + 2 \cdot 2^{k+1} + 27\left(2^{k+1} - 2^{k+1}\right)$

$= 27\left[3^{3k+1} + 2^{k+1}\right] + 2^{k+1}\left[2 - 27\right]$

k^{th} term, so call it a ; -25 (b)

$$= 27 \cdot a + 2^{k+1} \cdot b$$

$5 \mid a$ and $5 \mid b$, so by Theorem 2.7 (g)

$$5 \mid 3^{3(k+1)+1} + 2^{(k+1)+1}$$

Q.E.D. ✓

6.c. If a is odd, then

$$32 \mid (a^2+3)(a^2+7)$$

a odd $\Rightarrow$ $a = 2k+1$ $\exists k \in \mathbb{Z}$

$$(a^2+3)(a^2+7) = ((2k+1)^2+3)((2k+1)^2+7)$$

$$= (4k^2+4k+4)(4k^2+4k+8)$$

$$= 4^2(k^2+k+1)(k^2+k+2)$$

$$= 4^2 \cdot 2 \frac{(k^2+k+1)(k^2+k+2)}{2}$$

$$= 32 \cdot t_{k^2+k+1}$$

t_{k^2+k+1} triangular, $\in \mathbb{Z}$

p19 : odd square can be written as $8q+1$, so $(a^2 = 8q+1)$

$$(a^2+3)(a^2+7) = (8q+4)(8q+8)$$
$$= 32(2q+1)(q+1)$$ ✓

8b. $n(n+1)(n+2)(n+3) = p^2 - 1$

$$(n^2+n)(n^2+5n+6) + 1 = p^2$$

$$n^4 + 6n^3 + 11n^2 + 6n + 1 = p^2$$

$$(n^2 + 3n + 1)^2 = p^2$$

19c. If a & b are odd, then

$$8 \mid a^2 - b^2$$

Since a & b are odd $\exists (u,v) \in \mathbb{Z}\times\mathbb{Z}$ such that

$$a^2 = 8u+1$$
$$b^2 = 8v+1$$

Hence

$$a^2 - b^2 = (8u+1) - (8v+1)$$
$$= 8(u-v)$$

and $8 \mid a^2 - b^2$

13b $\exists (x,y) \;/\; ax + by = \gcd(a,b)$.

Claim: $\gcd(x,y) = 1$

Let $d = \gcd(a,b)$.

By contradiction:

Suppose $\gcd(x,y) \equiv c > 1$.

Then $c \mid x$ and $c \mid y$, so

$\exists (u,v) \in \mathbb{Z} \times \mathbb{Z} \;/\; cu = x$ and $cv = y$.

So $d = ax + by = acu + bcv$

$= c(au + bv)$

So $c \mid d$.

Hence $au + bv = \frac{d}{c} \leq d$

But d is the smallest such linear combination; so $c = 1$.

Contradiction, hence

$\gcd(x,y) = 1$

Alternatively:

$ax + by = d$

$d \mid a$ and $d \mid b$, so

$\exists (u,v) \in \mathbb{Z} \times \mathbb{Z}$ / $du = a$, $dv = b$

$dux + dvy = d \Rightarrow$

$ux + vy = 1$

$x + y$ are hence relatively prime by Theorem 2.4.

$gcd(x,y) = 1$

R.E. Sarah's question (problem 19b, p26).

The fact that 24 divides $a(a^2-1)$ can be attacked directly (i.e., factor 24 out), or indirectly, via Corollary 2, p. 24. The hint helps with 8 ....