$a = qb + r$

$r = 0$

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)

$a = qb$

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 $a = \pm b$

Proof of (c):

Given $a|b$ and $c|d$;

$\exists e \in \mathbb{Z}$ / $ae = b$ and

$\exists f \in \mathbb{Z}$ / $cf = d$.

$bd = (ae)(cf) = (ac)(ef)$

hence $ac|bd$.

(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

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

Proof: WLOG - without loss of generality — $a \neq 0$. Consider

$$S = \{ ax + by \mid x, y \in \mathbb{Z} \text{ and } ax + by > 0 \}.$$

Claim: S is non-empty.

Let $y = 0$, & take $x = \text{signum}(a)$

$$\text{signum}(a) = \begin{cases} 1 & a > 0 \\ -1 & a < 0 \end{cases}$$

Then $ax = |a| > 0$. So S is non-empty, & we can invoke well-ordering: S has a minimal element, call it d. Claim: $d = \gcd(a, b)$.

(1) Show that d is a divisor:

By the division algorithm, we can write

$$a = qd + r \qquad 0 \leq r < d.$$

d is an element of S, so $\exists\, u, v \in \mathbb{Z}$ |

$$d = au + bv.$$

So

$$\begin{aligned} r &= a - qd \\ &= a - q(au + bv) \\ &= a(1 - qu) + b(-qv), \end{aligned}$$

the form of an element of S. If $r > 0$, then $r < d$ is the smallest element of S - contradiction! Hence $r = 0$, and

$$a = qd,$$

so $d \mid a$. Similarly for b. So d is a common divisor.

(2) Show that it's the greatest common divisor.

Given $c \mid a$ and $c \mid b$. Then

$$c \mid ax + by,$$ so in particular

$$c \mid au + bv = d,$$

so $c \mid d$. Hence $d = \gcd(a, b)$

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

Fix $d = au + bv$

Let $M = \{n \cdot d \mid n \in \mathbb{Z}\}$. Claim: $T = M$

① $nd = a(nu) + b(nv) \in T \Rightarrow M \subseteq T$.

② $d \mid ax + by \Rightarrow ax + by \in M \Rightarrow T \subseteq M$,

$\therefore T = M$.

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 $1 = ax + by$.

$1 = \gcd(a, b) = ax + by$

(This is just an immediate consequence of Theorem 2.3 – I might have called it also a corollary of Theorem 2.3. It is, however, awfully useful! Don't overlook this one. One reason for calling it its own theorem is that the author wants to hang two corollaries off of this one!)

Let's look at some examples:

- 2 and 3

$1 = 2x + 3y = 2(-1) + 3(1)$

$$\begin{array}{r} 2 \\ 3 = 2 \cdot 1 + 1 \end{array}$$

$$\begin{array}{r} 3 \\ 3 - 2 = 1 \end{array}$$

- 7 and 12

$12 = 7 + 5$ mod 7

$5+5+5 \equiv 1 \bmod 7$

$1 = 7x + 12y$

$= 7(-5) + 12 \cdot 3$

$3 \cdot 12 = 3 \cdot 7 + 3 \cdot 5$

$= 3 \cdot 7 + 2 \cdot 7 + 1$

$= 5 \cdot 7 + 1$

$7(-5) + 12 \cdot 3 = 1$

- 10 and 27 (two non-primes)

$27 = 2 \cdot 10 + 7$

$3 \cdot 27 = 3[2 \cdot 10 + 7]$

$= 6 \cdot 10 + 21$

$= 8 \cdot 10 + 1$

$3 \cdot 27 + (-8)10 = 1$

Rough "Proof": (using algebra) – just for fun!

Corollary 1: If $\gcd(a,b) = d$, then $\gcd(a/d, b/d) = 1$.

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 $a|c$.

Proof: $\exists\ x, y \ /\ \ 1 = ax + by$

Multiply through by c:

$$c = a(cx) + b(cy)$$
$$= a(cx) + (bc)y$$

But $a \mid bc$; $\exists\ f \ /\ \ af = bc$

$$c = a[cx + fy]$$

integer, so

$a \mid c$.

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 $a \neq 0$.

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*).

6c p25 If a is odd then

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

1st Right : $a = 2k+1$

2nd Right : $a = 4k+1$ or $4k+3$

3rd Right : $a^2 = 8k+1$

$$\begin{aligned}(a^2+3)(a^2+7) &= (8k+1+3)(8k+1+7) \\ &= (8k+4)(8k+8) \\ &= 32(2k+1)(k+1)\end{aligned}$$

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

19e. $a \in \mathbb{Z}$; $360 \mid a^2(a^2-1)(a^2-4)$

[$360 = 2^3 3^2 5$ — we're after!]

factor the RHS

$$\underbrace{[(a-2)(a-1)a(a+1)(a+2)]}\cdot a$$

$5 \mid$ RHS

At least two are even; one is divisible by 4, so we've got $2^3 \mid$ RHS

$\underbrace{(a-2)(a-1)a}$ divisible by 3 · $\underbrace{a(a+1)(a+2)}$ divisible by 3

4e. $24 \mid 2\cdot 7^n + 3\cdot 5^n - 5$ $\quad n \geq 1$

Anchor: $n=1 \Rightarrow 2\cdot 7^1 + 3\cdot 5^1 - 5 = 24$ ✓

Implication: $P(k) \Rightarrow P(k+1)$

$P(k)$: $24 \mid 2\cdot 7^k + 3\cdot 5^k - 5$

$$2\cdot 7^{k+1} + 3\cdot 5^{k+1} - 5 \qquad (*)$$

$$2\cdot 7^k + 3\cdot 5^k - 5 = \underline{24\lambda}$$

$$2\cdot 7^k = 24\lambda - 3\cdot 5^k + 5$$

$(*)$: $7\cdot[24\lambda - 3\cdot 5^k + 5] + 3\cdot 5^{k+1} - 5$

$(*)$: $7 \cdot [2 \cdot 7^k] + 5 \cdot [3 \cdot 5^k] - 5$

$7 \cdot 2$

$= 7[2 \cdot 7^k + 3 \cdot 5^k + 0] - 2 \cdot 3 \cdot 5^k - 5$

$-5+5$

$= 7[2 \cdot 7^k + 3 \cdot 5^k - 5] + 35 - 2 \cdot 3 \cdot 5^k - 5$

$= 7 \cdot 24 l + 30 - 6 \cdot 5^k$

$= 7 \cdot 24 \cdot l + 6[5 - 5^k]$

$k \geq 1$

$= 7 \cdot 24 \cdot l +$

$= 7 \cdot 24 \cdot l + 6[(4+1) - (4+1)^k]$

$= 7 \cdot 24 \cdot l + 6[4+1 - (4^k + \binom{k}{1} 4^{k-1} + \ldots + \binom{k}{k-1} 4 + 1)]$

$= 7 \cdot 24 \cdot l + \underbrace{6 \cdot 4}_{24}[1 - (4^{k-1} + \ldots + \binom{k}{k-1})]$

8b Product of 4 consecutive integers is one less than a perfect square.

$k-1, k, k+1, k+2$;

$(k-1)k(k+1)(k+2) = p^2 - 1$ where $p \in \mathbb{Z}$

$\Leftrightarrow (k^2-1)(k^2+2k) = p^2 - 1$

$\Leftrightarrow k^4 + 2k^3 - 1k^2 - 2k = p^2 - 1$