

## Notes 3/6/08 Greatest Common Divisor

(We follow Rotman's *A First Course in Abstract Algebra* here.)

Recall how the induction argument goes. We have a sequence of statements  $P(n), n = 1, 2, \dots$  and we check that

- (i)  $P(1)$  holds true
- (ii)  $P(k)$  implies  $P(k + 1)$  for every  $k$

Then we conclude that  $P(n)$  holds for every  $n$ .

Here is a second form of an induction argument, so-called **complete induction**. We have a sequence of statements  $P(n), n = 1, 2, \dots$  and we check that

- (i)  $P(1)$  holds true
- (ii)  $P(1), P(2), \dots, P(k)$  together imply  $P(k + 1)$  for every  $k$

Then we conclude that  $P(n)$  holds for every  $n$ .

**Theorem 0.1.** *Every integer  $n \geq 2$  is either prime or product of primes.*

*Proof.* We will use prove this using complete induction.

- (i) Clearly,  $n = 2$  is prime.
- (ii) Assume each of  $2, 3, \dots, k$  is either prime or a product of primes. If  $k + 1$  is prime, we are done. If not, it is a product of two integers between 2 and  $k$ , that is

$$k + 1 = a \cdot b, \quad 2 \leq a \leq k, \quad 2 \leq b \leq k$$

By the induction assumption,  $a$  and  $b$  are either prime or products of primes:

$$a = p_1 \cdots p_s \quad a = q_1 \cdots q_t$$

Hence

$$k + 1 = ab = p_1 \cdots p_s \cdot q_1 \cdots q_t,$$

a product of primes. □

Given two integers,  $a$  and  $b$  with  $a \neq 0$ , the long division algorithm provides integers  $q$  and  $r$  such that

$$b = qa + r \quad \text{and} \quad 0 \leq r < |a|.$$

**Proposition 0.2.** *For given  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ , these  $q$  and  $r$  are unique.*

*Proof.* We will assume  $a > 0$ , the case  $a < 0$  is handled in a similar way. Suppose that

$$b = qa + r = q'a + r',$$

where

$$0 \leq r < a, \quad 0 \leq r' < a.$$

We get

$$(0.1) \quad (q - q')a = r' - r$$

We may assume that  $r' \geq r$ . Then  $r' - r \geq 0$  and  $q - q' \geq 0$ . If  $q - q' > 0$  then this difference is at least 1 and  $(q - q')a$  is at least  $a$ . But both  $r$  and  $r'$  are between 0 and  $a$  (strictly less than  $a$ ) hence the distance  $r' - r$  between them is strictly less than  $a$  and equality 0.1 is impossible. Hence  $q - q' = 0$ , and  $q = q'$ ,  $r = r'$ .  $\square$

The integers  $q$  and  $r$  are called the **quotient** and the **remainder** after dividing  $b$  by  $a$ .

**Example 1.** Let's divide 60 and  $-60$  by 7 with a remainder:

$$60 = 7 \cdot 8 + 4 \quad -60 = 7 \cdot (-9) + 3$$

**Theorem 0.3.** *There are infinitely many primes.*

*Proof.* (Euclid) Suppose, on the contrary, there are finitely many primes and write out the list of all primes:

$$p_1, p_2, p_3, \dots, p_k.$$

Consider now

$$N = p_1 \cdot p_2 \cdots p_k + 1$$

This number is not prime (it is not on the list). If it were composite, it would have been divisible by one of the primes, but it's not (the remainder is 1). Contradiction. Hence our assumption that there are finitely many primes was erroneous.  $\square$

**Definition 0.4.** If  $a$  and  $b$  are integers, then  $a$  is a **divisor** of  $b$  if there is an integer  $d$  with  $b = ad$ . We also say that  $a$  **divides**  $b$  or that  $b$  is a multiple of  $a$ , and we denote this by

$$a \mid b.$$

**Definition 0.5.** A **common divisor** of integers  $a$  and  $b$  is an integer  $c$  with  $c \mid a$  and  $c \mid b$ . The **greatest common divisor**,  $\gcd(a, b)$  is defined by

$$\gcd(a, b) = \begin{cases} 0 & \text{if } a = b = 0 \\ \text{the largest common divisor of } a \text{ and } b & \text{otherwise} \end{cases}$$

Note that the gcd is always nonnegative, as if  $c$  is a common divisor then so is  $-c$ .

**Example 2.**  $\gcd(84, 105) = 21$

**Proposition 0.6.** *If  $p$  is prime and  $b$  is any integer, then*

$$\gcd(p, b) = \begin{cases} p & \text{if } p \mid b \\ 1 & \text{otherwise} \end{cases}$$

*Proof.* A common divisor of  $p$  and  $b$  has to divide  $p$ . Hence the gcd is either  $p$ , if  $p$  divides  $b$ , or 1 otherwise.  $\square$

**Definition 0.7.** A **linear combination** of integers  $a$  and  $b$  is an integer of the form

$$sa + tb,$$

where  $s$  and  $t$  are integers.

**Example 3.** 3 is not a linear combination of 2 and 6. Indeed,

$$3 = 2s + 6t$$

is impossible as 3 is odd and  $2s + 6t = 2(s + 3t)$  is even. But 1 is a linear combination of 7 and 9:

$$1 = 4 \cdot 9 + (-5) \cdot 7$$

**Theorem 0.8.** *If  $a$  and  $b$  are integers, then their gcd is a linear combination of  $a$  and  $b$ .*

*Proof.* We can assume that one of  $a, b$ , say  $a$ , is nonzero (if  $a = b = 0$  the conclusion of the theorem is obvious). Consider the set of all linear combinations of  $a$  and  $b$

$$I = \{sa + tb : s, t \in \mathbb{Z}\}$$

Both  $a$  and  $b$  are in  $I$  ( $a = 1 \cdot a + 0 \cdot b, b = 0 \cdot a + 1 \cdot b$ ), and so are  $-a$  and  $-b$ . Hence  $I$  contains some positive integers (either  $a$  or  $-a$  is positive). Let  $d$  be the smallest positive integer in  $I$ .

**Claim:**  $d = \gcd(a, b)$ .

Since  $d$  is in  $I$ , there exist integers  $s$  and  $t$  such that

$$d = sa + tb.$$

To show that  $d$  is the gcd we need to check that it is a common divisor of  $a$  and  $b$  and it is the largest among all common divisors. First, let's check it's a common divisor. Divide  $a$  by  $d$  with a remainder:

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

We have

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b$$

is a linear combination of  $a$  and  $b$  and hence lies in  $I$ . If  $r$  were positive it would contradict the minimality of  $d$ . Hence  $r = 0$ . Similarly,  $d \mid b$ . Hence  $d$  is a common divisor of  $a$  and  $b$ .

It remains to check that  $d$  is the largest among all common divisors. Let  $c$  be a positive common divisor of  $a$  and  $b$ . Then  $c$  divides  $d$  as  $d = sa + tb$  and hence  $c \leq d$ .  $\square$

In particular, this theorem implies

**Proposition 0.9.** *Let  $a$  and  $b$  be integers. A nonnegative common divisor  $d$  is their gcd if and only if every common divisor of  $a$  and  $b$  divides  $c$ .*

**Theorem 0.10. (Euclid's Lemma)** *If  $p$  is prime and  $p \mid ab$  then either  $p \mid a$  or  $p \mid b$ . More generally, if  $p \mid a_1 \cdots a_n$  then  $p \mid a_i$  for some  $i = 1 \dots n$ .*

*Proof.* Assume that  $p \nmid a$ , we will show  $p \mid b$ . Now  $\gcd(a, p) = 1$  hence 1 can be written as a linear combination of  $a$  and  $p$

$$1 = sa + tp.$$

Multiply this by  $b$

$$b = s(ab) + tpb.$$

We see that  $p$  divides the right-hand side (recall  $p \mid ab$ ) and hence  $p \mid b$ . The second statement follows by induction.  $\square$

**Definition 0.11.** We call integers  $a$  and  $b$  **relatively prime** if their gcd equals 1.

Here is a generalization of Euclid's lemma.

**Proposition 0.12.** *Let  $a, b, c$  be integers and  $(a, c) = 1$ . Then if  $c \mid ab$  then  $c \mid b$ .*

*Proof.* Since  $\gcd(a, c) = 1$ , 1 can be written as a linear combination of  $a$  and  $c$

$$1 = sa + tc.$$

Multiply this by  $b$

$$b = s(ab) + tcb.$$

We see that  $c$  divides the right-hand side (recall  $c \mid ab$ ) and hence  $c \mid b$ .  $\square$

A rational number can be written as a ratio of two integers  $r = a/b$ . If  $r$  is nonzero we can assume it is written in lowest terms and  $(a, b) = 1$ .

**Theorem 0.13.**  $\sqrt{2}$  is irrational.

Suppose, on the contrary, that  $\sqrt{2}$  is rational, that is,

$$\sqrt{2} = \frac{a}{b}.$$

We can assume that this fraction is written in lowest terms. Square both sides and multiply the result by  $b^2$ , get

$$2b^2 = a^2.$$

Then  $2 \mid a^2$ , which implies  $2 \mid a$  (this follows from Euclid's lemma or can be proved directly — if  $a$  were odd then  $a^2$  would have been odd as well). Hence  $a = 2m$  for some integer  $m$ . We get

$$2b^2 = (2m)^2 = 4m^2$$

and hence

$$b^2 = 2m^2$$

which implies  $2 \mid b^2$  and  $2 \mid b$ . Hence both  $a$  and  $b$  are even, which contradicts  $(a, b) = 1$  and our assumption that  $\sqrt{2}$  is rational was erroneous.