

### 3 Greatest common divisor

**Definition 3.1.** The *greatest common divisor* of two positive integers  $a, b$  is defined to be the largest integer  $d$  which divides both  $a$  and  $b$ .

The greatest common divisor is denoted by  $(a, b)$ . However, this is also the notation for the *ideal generated by  $a$  and  $b$* . So, to avoid confusion, I was writing  $\gcd(a, b)$  for the number and  $(a, b)$  for the set

$$(a, b) = \{na + mb \mid n, m \in \mathbb{Z}\}$$

of all integer linear combinations of  $a$  and  $b$ .

**Theorem 3.2.** *The greatest common divisor of  $a$  and  $b$  is the smallest positive integer  $d$  which can be written in the form*

$$d = na + mb$$

for some  $n, m \in \mathbb{Z}$ .

This theorem can be restated as follows:  $\gcd(a, b)$  is the smallest positive integer in the ideal  $(a, b)$ .

*statement of logic.* Let  $d$  be the smallest positive integer in the set  $(a, b)$ . Then we will show that  $d$  is the greatest common divisor of  $a$  and  $b$ . To show that  $d = \gcd(a, b)$  we need to show

1.  $d$  divides both  $a$  and  $b$  and
2.  $d$  is  $\geq$  any other number  $d'$  which divides both  $a$  and  $b$ .

We prove (1) by contradiction. [end of statement of logic]

Suppose that  $d$  does not divide  $a$ . Then  $a = dq + r$  where  $0 < r < d$ . But  $d = na + mb$  by assumption (since all elements of  $(a, b)$  have that form). Therefore,

$$r = a - dq = a - dna - dmb = (1 - dn)a - dmb.$$

This is a linear combination of  $a$  and  $b$  which is positive but less than  $d$  which contradicts the choice of  $d$ . Therefore,  $d$  divides  $a$  and a similar argument shows that  $d$  divides  $b$ .

For (2) suppose that  $d'$  divides both  $a$  and  $b$ . Then it divides  $d = na + mb$  so we must have  $d' \leq d$  which is what we needed to prove. The conclusion is that  $d = \gcd(a, b)$  which proves the theorem.  $\square$

Homework: p.56 # 1.46, 51, 55.