

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 5.**

Following 2.2.2, we showed that there are infinitely many primes.

Following 2.5.1, we defined the greatest common multiple  $(a, b)$  of two integers  $a$  and  $b$ .

For example,  $(6, 9) = 3$ ,  $(7, 5) = 1$ ,  $(-6, 9) = 3$ ,  $(5, 0) = 5$ .

Note that  $(0, 0)$  is undefined and  $(0, a) = |a|$  if  $a \neq 0$ , and  $(a, b) = (-a, b)$ .

Two numbers  $a$  and  $b$  are *relatively prime* if  $(a, b) = 1$ .

**Important Lemma.** For all integers  $a, b, c$ ,

$$(a, b) = (a - bc, b).$$

In particular,

$$(a, b) = (r, b)$$

where  $r$  is the remainder when  $a$  is divided by  $b$ .

In class we showed that  $(a, b) \leq (a - bc, b)$  and  $(a - bc, b) \leq (a, b)$ . I think that the proof in the book is better. They note that any common divisor of  $a$  and  $b$  is a divisor of  $a - cb$  and  $b$ , and conversely any common divisor of  $a - bc$  and  $b$  is a divisor of  $a$  and  $b$  (note that  $a = (a - b) + b$ ). Hence the set of common divisors of  $a$  and  $b$  is the same as the set of common divisors of  $a - bc$  and  $b$  and hence greatest common divisor is the same in both cases.

**Example. Euclidean Algorithm:** Calculate  $(570, 123)$ . Solution:

$$\begin{aligned} 570 &= 123 \cdot 4 + 78, \\ 123 &= 78 + 45, \\ 78 &= 45 + 33, \\ 45 &= 33 + 12, \\ 33 &= 12 \cdot 2 + 9, \\ 12 &= 9 + 3, \\ 9 &= 3 \cdot 3 + 0, \end{aligned}$$

We see that

$$(570, 123) = (123, 78) = (78, 45) = (45, 33) = (33, 12) = (12, 9) = (3, 3) = (3, 0) = 3.$$

If  $a, b$  are non-empty integers and  $m$  and  $n$  are integers, then  $(a, b)$  divides  $ma + nb$ . We will see that in fact there exist integers  $m$  and  $n$  such that

$$(*) \quad (a, b) = ma + nb.$$

The numbers  $m$  and  $n$  can be found by reversing the Euclidean algorithm.

Now we reverse our work and write

$$\begin{aligned}
 3 &= 12 - 9 \\
 &= 12 - (33 - 12 \cdot 2) = 12 \cdot 3 - 33 \\
 &= (45 - 33) \cdot 3 - 33 = 45 \cdot 3 - 33 \cdot 4 \\
 &= 45 \cdot 3 - (78 - 45) \cdot 4 = 45 \cdot 7 - 78 \cdot 4 \\
 &= (123 - 78) \cdot 7 - 78 \cdot 4 = 123 \cdot 7 - 78 \cdot 11 \\
 &= 123 \cdot 7 - (570 - 123 \cdot 4) \cdot 11 = 123 \cdot 51 - 570 \cdot 11
 \end{aligned}$$

To prove (\*), we will assume  $a, b > 0$ . Write

$$S = \{ma + nb : m, n \in \mathbb{Z}\}.$$

Then let  $d$  be the smallest positive element of  $S$ . (the set of positive elements of  $S$  is non-empty, in particular  $a$  and  $b$  are in  $S$ .) Write  $d = ma + nb$ . We will show  $d|a$ . Indeed, if not then by the division theorem we can write  $a = dq + r$  with  $0 < r < d$ . Then

$$r = a - dq = a - (ma + nb)q = (1 - mq)r - nbq.$$

This is a positive element of  $S$  which is less than  $d$ , which is a contradiction. Hence  $d|a$  and similarly,  $d|b$ . But then  $d \leq (a, b)$ . However,  $(a, b)|ma + nb = d$ , so  $d = (a, b)$ .

Notice that in the course of the proof, we proved the lemma: for  $a, b, m, n \in \mathbb{Z}$ , if  $(ma + nb)|a$  and  $(ma + nb)|b$  then  $ma + nb = (a, b)$ .

The following great question was asked today: are  $m$  and  $n$  such that  $(a, b) = ma + nb$  unique? If we also have  $(a, b) = m'a + n'b$  then  $a(m - m') + b(n' - n) = 0$ . What are the integers  $r, s$  with  $ar = bs$ ? They are precisely the numbers

$$r = \frac{bk}{(a, b)}, \quad s = \frac{ak}{(a, b)}, \quad k \in \mathbb{Z}.$$

Hence the possible values of  $m$  and  $n$  are

$$m' = m + \frac{bk}{(a, b)}, \quad n' = n - \frac{ak}{(a, b)}, \quad k \in \mathbb{Z}.$$