

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 6.**

**Every number is an integer unless otherwise stated!**

Last time: we defined the greatest common multiple  $(a, b)$  of two integers  $a$  and  $b$ .

Today we will see three Theorems:

**Theorem 1.** *If  $a, b$  are not both zero there exist  $m, n$  with*

$$(a, b) = ma + nb.$$

Last time we stopped in the middle of the proof.

*Proof.* First we prove the **Lemma** that if  $ma + nb$  is a common divisor of  $a$  and  $b$  then  $ma + nb = (a, b)$ . This is clear since  $ma + nb$  is a common divisor, so  $ma + nb \leq (a, b)$ . But  $(a, b) | ma + nb$  so  $(a, b) \leq ma + nb$ . Hence  $ma + nb = (a, b)$ .

Now set

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

Then  $S$  contains positive elements since one of  $\pm a$  and  $\pm b$  is positive. Let  $d$  be the smallest positive element of  $S$ , and choose  $m$  and  $n$  with  $d = ma + nb$ . We will show that  $d|a$  and  $d|b$ . Suppose not, then using the division theorem,

$$a = dq + r, \quad 0 < r < d,$$

but then

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

is a smaller positive element of  $S$ . This is a contradiction so  $d|a$  and similarly  $d|b$ , so  $d = (a, b)$  by the lemma.  $\square$

**Theorem.** *If  $p$  is a prime and  $p|ab$  then  $p|a$  or  $p|b$  (or both!).*

*Proof.* If  $p$  does not divide  $a$  then since  $p$  is prime  $(a, p) = 1$ . Hence  $1 = mp + na$  for some  $m, n$ . Then  $b = bmp + nab$ , but since  $p$  divides both terms in this sum, this implies  $p|b$ .  $\square$

By induction we get that if  $p$  is a prime and  $p$  divides  $a_1, \dots, a_k$  then  $p|a_j$  for some  $j$  with  $1 \leq j \leq k$ . (Exercise)

**Theorem. (Fundamental Theorem of Arithmetic.)** *Every integer  $N > 1$  can be written as a product of primes  $N = p_1 \cdots p_k$  and this is unique up to reordering.*

We have already proved that every integer  $N$  is a prime or product of primes. The problem is to show that this is unique up to reordering. What this is saying is that if  $N = p_1 \cdots p_k = q_1 \cdots q_\ell$  where the  $p$ s and  $q$ s are all primes, then  $k = \ell$  and the list of

numbers  $p_1, \dots, p_k$  can be changed into the list of numbers  $q_1, \dots, q_\ell$  just by switching the order of the elements in the list.

Here is the idea of the proof. A student in the class noticed that this is what is going on. We could set it up as a formal induction, but if we don't it is easier to understand.

If  $N = p_1 \cdots p_k = q_1 \cdots q_\ell$  where the  $p$ s and  $q$ s are all primes. Then  $p_1 | q_1 \cdots q_\ell$  and so  $p_1 | q_j$  for one of the  $j$ s. Since  $q_j$  is prime,  $p_1 = q_j$ . We can reorder the  $q$ s so  $p_1 = q_1$ . But then dividing through by  $p_1$  we have

$$\frac{N}{p_1} = p_2 \cdots p_k = q_2 \cdots q_\ell$$

Repeating this argument with  $p_2$  and again reordering the  $q$ s we get

$$\frac{N}{p_1 p_2} = p_3 \cdots p_k = q_3 \cdots q_\ell$$

We continue in this way until either the  $p$ s or the  $q$ s are all used up. Suppose that  $k \leq \ell$  so the  $p$ s get used up first. Then we have that after reordering  $q_j = p_j$  for  $1 \leq j \leq k$  and we are left with

$$(*) \quad 1 = \frac{N}{p_1 \cdots p_k} = q_{k+1} \cdots q_\ell.$$

This is a contradiction if  $\ell > k$ , so in fact  $\ell = k$ .