**3.1.3 Greatest Common Divisor**

The greatest common divisor of *a* and *b* is the largest positive integer dividing both a and *b* and is denoted by either *gcd(a, b)* or by *(a, b)*. In this book, we shall use the first notation.

**Examples:** *gcd(6, 4) = 2*, gcd(5, 7) = 1, gcd(24, GO) = 12.

We say that *a* and *b* are relatively prime if *gcd(a, b) = 1*. There are two standard ways for finding the gcd:

1. If you can factor a and b into primes, do so, For each prime number, look at the powers that it appears in the factorizations of a and b. Take the smaller of the two. Put these prime powers together to get the gcd. This is easiest to understand by examples:

576 = 2632, 135 = 33\*5, gcd(576,135) = 32 = 9

gcd(253472, 22537) = 22305071 = 227 = 28.

Note that if a prime does not appear in a factorization, then it cannot appear in the gcd.

1. Suppose a and b are large numbers, so it might not be easy to factor them. The gcd can be calculated by a procedure known as the Euclidean algorithm. It goes back to what everyone learned in grade school: division with remainder. Before giving a formal description of the algorithm, let’s see some examples.

**Example**. Compute gcd(482, 1180).

**Solution:** Divide 482 into 1180. The quotient is 2 and the remainder is 216. Now divide the remainder 216 into 482. The quotient is 2 and the remainder is 50. Divide the remainder 50 into the previous remainder 216. The quotient is 4 and the remainder is 16. Continue this process of dividing the most recent remainder into the previous one. The last nonzero remainder is the gcd, which is 2 in this case:

1180 = 2 \* 482 + 216

482 = 2 \*216 + 50

216 = 4 \* 50 + 16

50 = 3 \* 16 + 2

16 = 8 \* 2 + 0

Notice how the numbers are shifted:

Remainder —» divisor —> dividend —> ignore.

Here is another example:

12345 = 1 \* 11111+ 1234

11111 = 9 \* 1234 + 5

1234 = 246 \* 5 + 4

5 = 1 \* 4 + 1

4 = 4 \* 1 + 0.

Therefore, gcd(12345,11111) = 1.

Using these examples as guidelines, we can now give a more formal description of the **Euclidean algorithm**. Suppose that *a* is greater than b. If not, switch a and b. The first step is to divide a by b, hence represent a in the form

a = q1b + r1.

If r1 = 0, then b divides a and the greatest common divisor is b. If r1!= 0, then continue by representing b in the form

b = q2r1 + r2.

Continue in this way until the remainder that is zero, giving the following sequence of steps:

a = q1b + r1

b = q2r1 + r2

r1 = q3r2 + r3

……..

rk-2 = qkrk-1 + rk

rk-1 = qk+1rk.

The conclusion is that

gcd(a, b) = rk.

There are two important aspects to this algorithm:

1. It does not require factorization of the numbers.
2. It is fast

For a proof that it actually computes the gcd, see Exercise 28.

The Euclidean algorithm allows us to prove the following fundamental result.

**Theorem.** Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a, b). Then there exist integers x, y such that ax + by = d. In particular, if a and b are relatively prime, then there exist integers x, y, with ax + by = 1.

*Proof.* More generally, we’ll show that if rj is a remainder obtained during the Euclidean algorithm, then there are integers xj, yj such that rj = axj + byj. Start with j = 1, Taking x1 = 1 and y1 = -q1, we find that r1 = ax1+by1. Similarly, r2 = a(-q2)+b(1+q1q2). Suppose we have ri = axi+ byi, for all i < j. Then

rj = rj-2 - qjrj -1 = axj-2 + byj-2 – qj(axj-1 + byj-1)

Rearranging yields

rj = - a( xj-2 – qjxj-1) + b(yj-2 - qjyj-1)

Continuing, we obtain the result for all j, in particular for j = k. Since rk = gcd (a, b), we are done.

As a corollary, we deduce the lemma we needed during the proof of the uniqueness of factorization into primes.

**Corollary**. If p is a prime and p divides a product of integers ab, then either p|a or p|b. More generally, if a prime p divides a product ab…z, then p must divide one of the factors a ,b ,...,z .

*Proof*. First, let’s work with the case p|ab. If p divides a, we are done. Now assume p|a . We claim p|b. Since p is prime, gcd(a,p) = 1 or p. Since p|a , the gcd cannot be p. Therefore, gcd(a, p) = 1, so there exist integers x ,y with ax + py = 1. Multiply by b to obtain abx + pby = b. Since p|ab and p|p, we have p|abx +pby, so p|b, as claimed.

If p |ab…z, then p|a or p|b…z. If p|a, we're done. Otherwise, p|b…z. We now have a shorter product. Either p|b, in which case we're done, or p divides the product of the remaining factors. Continuing in this way, we eventually find that p divides one of the factors of the product.

The property of primes stated in the corollary holds only for primes. For example, if we know a product ab is divisible by 6, we cannot conclude that q or b is a multiple of 6. The problem is that 6 = 2 \* 3, and the 2 could be in a while the 3 could be in b, as seen in the example 60 = 4 \*15. More generally, if n = ab is any composite, then n|ab but n|a and n|b. Therefore, the primes, and 1, are the only integers with the property of the corollary.