Elementary Number Theory **Mathematics Dept.,**
Course I - High Diploma Students **Edu. College for Pure Sciences**
Asst. Prof. Dr. Ruma Kareem K. Ajeena **University of Babylon**
ruma.usm@gmail.com

Lecture 3: The Euclidean Algorithm

2.1 The Euclidean algorithm

The Euclidean algorithm can be described as follows:

Theorem 2.1.1 (The Euclidean algorithm). Let a and b be two integers whose greatest common divisor is desired. Because gcd(|a|,|b|) = gcd(a,b), with $a \geq b > 0$. The first step is to apply the division algorithm to a and b to get

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

If it happens that $r_1 = 0$, then b|a and gcd(a,b)=b.

When $r \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying $b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$. If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain $r_1 = q_3 r_2 + r_3$, $0 \leq r_3 < r_2$ This division process continues until some zero remainder appears, say, at the (n+1)th stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers). The result is the following system of equations:

$$a = q_1 b + r_1, \quad 0 < r_1 < b$$
$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3 \quad 0 < r_3 < r_2$$
$$\ldots$$
$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0.$$

With r_n, the last nonzero remainder that appears in this manner, is equal to gcd(a,b).

This proof is based on the following lemma:

Lemma 2.1.1. If $a = qb + r$, then gcd(a,b)=gcd(b,r).

Proof. If d =gcd(a,b), then the relations d|a and d|b together imply that d|(a−qb), or d|r. Thus, d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then c|(qb+r), whence c|a. This makes c a common divisor of a and b, so that $c \leq d$. It now follows from the definition of gcd(b,r) that d =gcd(b,r).

Using the result of this lemma, we simply work down the displayed system of equations, obtaining

$$\gcd(a,b)=\gcd(b, r_1)=\cdots=\gcd(r_{n-1}, r_n)=\gcd(r_n,0)= r_n.$$

Theorem 2.1.1 asserts that gcd(a,b) can be expressed in the form ax+by, but the proof of the theorem gives no hint as to how to determine the integers x and y. For this, we fall back on the Euclidean Algorithm. Starting with the next-to-last equation arising from the algorithm, we write $r_n = r_{n-2} - q_n r_{n-1}$.

Now solve the preceding equation in the algorithm for r_{n-1} and substitute to obtain

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) =(1+q_n q_{n-1}) r_{n-2} +(-q_n) r_{n-3}.$$

This represents r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing backward through the system of equations, we successively eliminate the remainders $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ until a stage is reached where $r_n = \gcd(a,b)$ is expressed as a linear combination of a and b.

Example 2.3. Let us see how the Euclidean Algorithm works in a concrete case by calculating, say, gcd(12378, 3054). Applying the Division Algorithm produce the equations

$$12378=4\cdot 3054+162$$
$$3054=18\cdot 162+138$$
$$162=1\cdot 138+24$$
$$138=5\cdot 24+18$$
$$24=1\cdot 18+6$$
$$18=3\cdot 6+0.$$

The last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

$$6=\gcd(12378,3054).$$

To represent 6 as a linear combination of the integers 12378 and 3054, we start with the next-to-last of the displayed equations and successively eliminate the remainders
18, 24, 138, and 162:

$$6= 24-18$$
$$= 24-(138-5\cdot 24)$$
$$= 6\cdot 24-138$$
$$= 6(162-138)-138$$
$$= 6\cdot 162-7\cdot 138$$
$$= 6\cdot 162-7(3054-18\cdot 162)$$
$$=132\cdot 162-7\cdot 3054$$
$$=132(12378-4\cdot 3054)-7\cdot 3054$$
$$=132\cdot 12378 + (-535)3054.$$

Thus, we have 6=gcd(12378,3054)=12378x +3054y, where x =132and y =−535. Note that this is not the only way to express the integer 6 as a linear combination of 12378 and 3054; among other possibilities, we could add and subtract 3054·12378 to get

$$6=(132+3054)12378+(-535-12378)3054 =3186\cdot 12378+(-12913)3054.$$

Theorem 2.7. If $k > 0$, then gcd(ka,kb)=k gcd(a,b).
Proof. If each of the equations appearing in the Euclidean Algorithm for a and b is multiplied by k, we obtain

$$ak = q_1(bk) + r_1k, \quad 0 < r_1k < bk$$
$$bk = q_2(r_1k) + r_2k, \quad 0 < r_2k < r_1k$$
$$\cdots$$
$$r_{n-2}k = q_n(r_{n-1}k) + r_nk, \quad 0 < r_nk < r_{n-1}k$$
$$r_{n-1}k = q_{n+1}(r_nk) + 0.$$

But this is clearly the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder r_nk; that is,

$$\gcd(ka,kb) = r_nk = k\gcd(a,b)$$

as stated in the theorem.
Corollary. For any integer $k \neq 0$, $\gcd(ka,kb)=|k|\gcd(a,b)$.
Proof. It suffices to consider the case in which $k < 0$. Then $-k = |k| > 0$ and, by Theorem 2.7,

$$\gcd(ak,bk) = \gcd(-ak,-bk) = \gcd(a|k|,b|k|) = |k|\gcd(a,b).$$

An alternate proof of Theorem 2.7 runs very quickly as follows: gcd(ak,bk) is the smallest positive integer of the form $(ak)x + (bk)y$, which, in turn, is equal to k times the smallest positive integer of the form $ax+by$; the latter value is equal to k gcd(a,b). By way of illustrating Theorem 2.7, we see that

$$\gcd(12,30) = 3\gcd(4,10) = 3\cdot 2\gcd(2,5) = 6\cdot 1 = 6.$$

There is a concept parallel to that of the greatest common divisor of two integers, known as their least common multiple; but we shall not have much occasion to make use of it. An integer c is said to be a common multiple of two nonzero integers a and b whenever $a|c$ and $b|c$. Evidently, zero is a common multiple of a and b. To see there exist common multiples that are not trivial, just note that the products ab and $-(ab)$ are both common multiples of a and b, and one of these is positive. By the Well-Ordering Principle, the set of positive common multiples of a and b must contain a smallest integer; we call it the least common multiple of a and b. For the record, here is the official definition.
Definition 2.4. The least common multiple of two nonzero integers a and b, denoted by lcm(a,b), is the positive integer m satisfying the following:
(a) $a|m$ and $b|m$.
(b) If $a|c$ and $b|c$, with $c > 0$, then $m \leq c$.
As an example, the positive common multiples of the integers -12 and 30 are 60, 120, 180,..., hence, 1cm(−12,30)=60. The following remark is clear from our discussion: given nonzero integers a and b, lcm(a,b) always exists and $\text{lcm}(a,b) \leq |ab|$. There is a relationship between the ideas of greatest

common divisor and least common multiple.

Theorem 2.8. For positive integers a and b $\gcd(a,b)\,\mathrm{lcm}(a,b)=ab$

Proof. Suppose $d=\gcd(a,b)$. $a=dr$, $b=ds$ for integers r and s. If $m=ab/d$, then $m=as=rb$, the effect of which is to make m a (positive) common multiple of a and b. Now let c be any positive integer that is a common multiple of a and b; say, for definiteness, $c=au=bv$.

Thus, there exist integers x and y satisfying $d=ax+by$. In consequence,

$c/m = cd/ab = c(ax+by)/ab =(c/b)x +(c/a)y =vx+uy$.

This equation states that $m|c$, allowing us to conclude that $m \le c$. Thus, in accordance with Definition 2.4, $m=\mathrm{lcm}(a,b)$; that is,

$$\mathrm{lcm}(a,b)= ab/d = ab/\gcd(a,b)$$

which is what we started out to prove.

Theorem 2.8 has a corollary that is worth a separate statement.

Corollary. For any choice of positive integers a and b, $\mathrm{lcm}(a,b)=ab$ if and only if $\gcd(a,b)=1$.

When considering the positive integers 3054 and 12378, for instance, we found that $\gcd(3054, 12378)=6$; whence, $\mathrm{lcm}(3054,12378)= 3054\cdot 12378/6 =6300402$.