Lecture 5: The Euclidean Algorithm

Lemma 5.1 If $a=qb+r$ then $\gcd(a,b)=\gcd(b,r)$

Proof Let $d=\gcd(a,b)$

Then $d|a$ and $d|b$

Hence $d|(a-qb)$ i.e. $d|r$

Therefore d is a common divisor of both b and r

Suppose c is any arbitrary common divisor of b and r

Hence $c|(qb+r)$ i.e. $c|a$

$\Rightarrow$ c is a common divisor of a and b

$\Rightarrow$ $c \leq d$

Hence $d=\gcd(b,r)$

The Euclidean algorithm

Let $a,b \in \mathbb{Z}$. Since $\gcd(|a|,|b|)=\gcd(a,b)$, Hence we assume that $a \geq b > 0$.

Apply division algorithm to a and b. $\exists\ q_1, r_1 \in \mathbb{Z}$ such that

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

If $r_1 = 0$ then $a = q_1 b$ and hence $b|a$ and $\gcd(a,b)=b$

Next we apply division algorithm on b and r_1. $\exists\ q_2, r_2 \in \mathbb{Z}$ such that

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$ then $b = q_2 r_1$ and hence $r_1|b$ and $\gcd(a,b)=\gcd(b,r_1)$

$= r_1$

If $r_2 \neq 0$ we continue the same process: The division continues untill some zero remainder appears: say at the $(n+1)^{th}$ stage which gives us the following system of equations:

$$a = q_1 b + r_1 \qquad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \qquad 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

Lemma 5.1 gives us: $\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots$

$$\cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$$

$$= r_n$$

Exercises:

1) Find $\gcd(306, 657)$ and $\gcd(272, 1479)$ using Euclidean algorithm

2) Prove that if d is a common divisor of a, b then $d = \gcd(a,b)$ if and only if $\gcd(a/d, b/d) = 1$

3)

Example We calculate the gcd (12378, 3054) and try to express the gcd in the form of $ax+by$ where $a=12378$, $b=3054$, $x, y \in \mathbb{Z}$.

Solution:

$$12378 = 4 \cdot 3054 + 162$$

$$3054 = 18 \cdot 162 + 138$$

$$162 = 1 \cdot 138 + 24$$

$$138 = 5 \cdot 24 + 18$$

$$24 = 1 \cdot 18 + 6$$

$$18 = 3 \cdot 6 + 0$$

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

Next we will represent 6 as a linear combination of 12378 and 3054

$$6 = 24 - 18$$

$$= 24 - (138 - 5 \cdot 24)$$

$$= 6 \cdot 24 - 138$$

$$= 6 (162 - 138) - 138$$

$$= 6 \cdot 162 - 7 \cdot 138$$

$$= 6 \cdot 162 - 7 (3054 - 18 \cdot 162)$$

$$= 132 \cdot 162 - 7 \cdot 3054$$

$$= 132 \cdot (12378 - 4 \cdot 3054) - 7 \cdot 3054$$

$$\Rightarrow 6 = 132 \cdot 12378 + (-535) \cdot 3054$$

Thm 5.2 If $k>0$, then $\gcd(ka, kb) = k\gcd(a,b)$

Proof Multiply each equation appearing in Euclidean algorithm by k

$$ak = q_1(bk) + r_1k \qquad 0<r_1k<bk$$

$$bk = q_2(r_1k) + r_2k \qquad 0<r_2k<r_1k$$

$$\vdots$$

$$r_{m-2}k = q_m(r_{m-1}k) + r_mk \qquad 0<r_mk<r_{m-1}k$$

$$r_{m-1}k = q_{m+1}(r_mk) + 0$$

Note that this is the Euclidean algorithm to ka, kb

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

Corollary 5.3 For any integer $k \neq 0$ $\gcd(ka, kb) = |k|\gcd(a,b)$

Proof $k>0$ is already proved.

Suppose $k<0$. Then $-k = |k| > 0$

$$\gcd(ak, bk) = \gcd(-ak, -bk)$$

$$= \gcd(a|k|, b|k|)$$

$$= |k|\gcd(a,b)$$

Exercises:

Q) Assuming $\gcd(a,b)=1$, prove the following:

(a) $\gcd(a+b, a-b) = 1$ OR 2.

(b) $\gcd(2a+b, a+2b) = 1$ OR 3.

(c) $\gcd(a+b, a^2+b^2) = 1$ OR 2

(d) $\gcd(a+b, a^2-ab+b^2) = 1$ OR 3