EUCLID'S DIVISION LEMMA AND G.C.D.

Here I give proofs of Euclid's Division Lemma, and the existence and uniqueness of $g.c.d.(a,b)$, and the existence of integers x and y such that

$$g.c.d(a,b) = ax + by.$$

These are the proofs which I gave in class. These proofs differ from those given in the book.

All arguments are based on the following proposition.

Proposition 1. *Every non-empty bounded below set of integers contains a unique minimal element.*

This proposition looks *obvious*, and we take it for granted. In fact, this proposition is equivalent to the principle of mathematical induction, and one can easily prove it by an inductive argument.

Note, however, that this *obvious* proposition becomes *false* if one speaks about rational numbers instead of reals. Indeed, the set $\mathbb{Q}^+ = \{x \in Q \mid x > 0\}$ of positive rational numbers does not contain a minimal element. Indeed, no element is minimal because for every $x \in \mathbb{Q}^+$, also $x/2 \in \mathbb{Q}^+$, and, since $x/2 < x$, no x can be the minimal element of $\mathbb{Q}^+$.

We start with Euclid's Division Lemma (Theorem 2-1 from the textbook).

Theorem. *For any positive integer k and integer j, there exist unique integers q and r such that*

$$0 \leq r < k$$

and

$$j = qk + r$$

Proof. We start with the uniqueness clause. Assume that we have two presentations

$$j = qk + r = q'k + r'$$

with with integers q and q', and both $0 \leq r, r' < k$. Thus

$$r - r' = (q' - q)k.$$

Note that, since $0 \leq r < k$ and $0 \leq r' < k$, we have that

$$|r - r'| < k.$$

We thus have that

$$k > |r - r'| = |q' - q|k \geq k,$$

and this would lead us to an absurd conclusion $k > k$ unless

$$r - r'| = |q' - q| = 0,$$

which proves the uniqueness.

We now address the existence. Consider the set

$$S = \{j - xk \mid x \in \mathbb{Z},\ j - xk \geq 0\}$$

of all integers of the form $j - xk$ with an integer x which happen to be non-negative. This is a bounded below set of integers, but we still must verify that S is non-empty in order to apply Proposition 1. That is simple: if $j \geq 0$, then $j \in S$ (just take $x = 0$), while if $j < 0$, then take $x = j$ and find that $j(1 - k) \in S$.

Now Proposition 1 guarantees that S has a minimal element, call it

$$r = j - qk.$$

We claim that

$$0 \leq r = j - qk < k.$$

Indeed, we have that $0 \leq r$ because, by construction, $r \in S$, and all elements of S are non-negative. It is also easy to see that, if $r \geq k$, then S would contain $r - k < r$, because

$$0 \leq r - k = j - qk - k = j = (q + 1)k \in S,$$

and r would not be the minimal element of S. □

We will now apply Proposition 1 in order to give an alternative proof of Theorem 2-2 and Corollary 2-1 from the textbook.

We start with the definition of the greatest common divisor. Let a and b be two integers, not both zeros.

Definition 1. *An integer d is called the greatest common divisor of a and b is the following three conditions are satisfied.*

(i) $d > 0$

(ii) $d|a$ *and* $d|b$ *(common divisor)*

(iii) *if* $d'|a$ *and* $d'|b$*, then* $d'|d$ *(the greatest)*

It easy to derive from the definition that $g.c.d.(a, b)$ is unique if it exists. Indeed, assume that both d_1 and d_2 are the greatest common divisors of a and b. Then condition (iii) of the definition implies that both $d_1|d_2$ and $d_2|d_1$. It follows that there are positive integers g and h such that

$$gd_1 = d_2 \quad \text{and} \quad hd_2 = d_1.$$

We easily conclude that $gh = 1$, and since both g and h are positive integers, we must have $g = h = 1$, therefore $d_1 = d_2$.

It is more difficult to prove that $g.c.d.(a, b)$ exists and can be represented as an integral linear combination of a and b. In order to do that, we prepare a construction.

Consider that set

$$S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}$$

of all integral linear combinations of a and b which happen to be positive. Set S is non-empty because $a^2 + b^2 \in S$ (pick $m = a$ and $n = b$, and recall that a and b are not both zeros). Clearly, set S is bounded below (by zero). We thus can apply Proposition 1, which guarantees the existence of a minimal element in S.

Theorem. *The minimal element of S is the greatest common divisor of a and b.*

This theorem implies both the existence of $g.c.d.(a, b)$, and the fact that it can be represented as an integral linear combination of a and b (since any element of S can). Moreover, this theorem gives an alternative characterization of $g.c.d.(a, b)$ as

the smallest positive integral linear combination of a and b However, this theorem does not provide an immediate algorithm of calculation of $g.c.d.(a, b)$.

Proof. Let d be the minimal element of S. We need to show that d satisfies conditions (i),(ii), and (iii) from the definition.

Condition (i) is obviously satisfied: by construction, $d \in S$, and all elements of S are positive.

Condition (iii) is also easy to verify. Indeed, we have that

$$d = ax + by$$

for some integers x and y. If d' divides both a and b, then

$$a = d'u \quad \text{and} b = d'v$$

with some integers u and v. We thus have that

$$d = ax + by = d'ux + d'vy = d'(ux + vy),$$

and thus $d'|d$.

We now verify condition (ii). We prove only that $d|a$ because $d|b$ can be shown by the same token. Euclid's Division Lemma (see above) guarantees the existence of q and r such that

$$a = dq + r$$

with

$$0 \leq r < d,$$

and we want to show that in fact $r = 0$. We have that non-negative integer r can be represented as an integral linear combination of a and b:

$$r = a - dq = a - q(ax + by) = a(1 - qx) + b(qy).$$

Thus it cannot happen that $r > 0$: if this was the case, then $r \in S$, but $r < d$ so d would not be the minimal element of S. It follows that $r = 0$, and thus $d|a$ as required. □