Euclidean Algorithm (self-study notes)

Recall that the **greatest common divisor** (GCD) of two or more integers, which are not all zero, is **the largest positive integer that divides each of the integers**. For example, the GCD of 8 and 12 is 4.

Consider the following property[1]:

Proposition 1. Let a and b be natural numbers such that $a \geq b$. Then $GCD(a, b) = GCD(b, r)$, where r is the remainder of the division $a \div b$.

Proof. Recall the following well-known equality:

$$a = q \cdot b + r, \tag{1}$$

where q is the **quotient** of the division $a \div b$ (in other words, DIVIDEND = QUOTIENT $\times$ DIVISOR + REMAINDER).

Denote by D_a be the set of positive divisors of a and by D_b the set of positive divisors of b. We will prove the following equality of sets:

$$D_a \cap D_b = D_b \cap D_r.$$

Let us prove the inclusion $D_a \cap D_b \subseteq D_b \cap D_r$:

Take an arbitrary element $x \in D_a \cap D_b$. Then x is a divisor of a and b at the same time. Since x divides a, there exists a natural number k_1 such that $a = k_1 x$. Similarly, there exists a natural number k_2 such that $b = k_2 x$. Replacing a and b in Equality (1):

$$k_1 x = q k_2 x + r \;\Rightarrow\; r = (k_1 - q k_2)x,$$

concluding that x is a divisor of r. Since x is also a divisor of b, we have that $x \in D_b \cap D_r$. This finishes the proof of the inclusion $D_a \cap D_b \subseteq D_b \cap D_r$.

Let us prove, now, the inclusion $D_b \cap D_r \subseteq D_a \cap D_b$:

[1] You can skip its proof, if you are not interested in.

Take an arbitrary element $x \in D_b \cap D_r$. Then x is a divisor of b and r at the same time. Since x divides b, there exists a natural number s_1 such that $b = s_1 x$. Similarly, there exists a natural number s_2 such that $r = s_2 x$. Replacing b and r in Equality (1):

$$a = qs_1 x + s_2 x \;\Rightarrow\; a = (qs_1 + s_2)x,$$

concluding that x is a divisor of a. Since x is also a divisor of b, we have that $x \in D_a \cap D_b$. This finishes the proof of the inclusion $D_b \cap D_r \subseteq D_a \cap D_b$.

Since $D_a \cap D_b = D_b \cap D_r$ we have that the set of common positive divisors of a and b coincides with the set of common positive divisors of b and r. Therefore:

$$GCD(a, b) = GCD(b, r).$$

□

In order to understand this property, let us consider the following example: take $a = 20$ and $b = 6$. Considering the Euclidean division $a \div b$ we see that the quotient is $q = 3$ and the remainder is $r = 2$. The above property says that $GCD(20, 6) = GCD(6, 2)$.

This property gives rise to an extremely important algorithm: the **Eulidean Algorithm**. It allows us to compute, in a very easy way, the greatest common divisor of two integers.

Euclidean Algorithm:

Since $GCD(a, b) = GCD(|a|, |b|)$ we can assume that both, a and b, are positive numbers (if not, take absolute values). Moreover, we assume that $a \geq b$.

- Compute the Euclidean division $a \div b$ and take the quotient q_1 and the remainder r_1:

$$a = q_1 \cdot b + r_1.$$

  ↪ If $r_1 = 0$, then b divides a and $GCD(a, b) = b$.

  ↪ If $r_1 \neq 0$,

  - Compute the Euclidean division $b \div r_1$ ($b = q_2 \cdot r_1 + r_2$).

    ↪ If $r_2 = 0$, then r_1 divides b and, applying the above property, $GCD(a, b) = GCD(b, r_1) = r_1$.

    ↪ If $r_2 \neq 0$,

    * Compute the Euclidean division of the previous divisor (r_1) by the previous remainder ($r_1 = q_3 \cdot r_2 + r_3$)... *and continue the process*

Since the each remainder is strictly less than the corresponding divisor, we have that $b > r_1 > r_2 > \cdots > r_n \geq 0$ (that is, the sequence of remainders is strictly decreasing). Therefore, at some step, the obtained remainder r_k will be zero and the process will finish. Then, applying the above property, we have that $GCD(a, b)$ **is the last non-zero remainder** that is obtained when we apply the Euclidean Algorithm.

Let us see an example. Assume that we want to compute $GCD(689, 234)$ by applying Euclidean Algorithm. Then, we will compute the division $689 \div 234$ and, after each step, we will compute the division of the **previous divisor** by **the previous remainder**. We will stop then the division be exact. The GCD will be *the last non-zero remainder*:

1. Divide $a = 689$ by $b = 234$: $\begin{array}{ll} 689 & |\underline{234} \\ 221 & 2 \end{array}$
2. Divide the divisor by the remainder: $\begin{array}{ll} 234 & |\underline{221} \\ 13 & 1 \end{array}$
3. Divide the new divisor by the new remainder: $\begin{array}{ll} 221 & |\underline{13} \\ 0 & 17 \end{array}$

The last non-zero remainder is 13. Therefore $GCD(689, 234) = 13$.

Obsevation:

Let us consider the **least common multiple** of several integers, that is, the minimum of the set of positive common multiples (denoted by LCM). We have the following well-known property:

Proposition 2. If a and b are integers, then

$$LCM(a, b) \cdot GCD(a, b) = |a||b|.$$

Applying this property we have that $GCD(689, 234) \cdot LCM(689, 234) = 689 \cdot 234$. Terefore, we can compute also the least common multiple of 689 and 234 from the Euclidean Algorithm:

$$LCM(689, 234) = 689 \cdot 234/13 = 12402.$$

Let us see a different example. Let us compute $GCD(54321, 50)$:

$$\begin{array}{ll} 54321 & |\underline{50} \\ 21 & 1056 \end{array} \qquad \begin{array}{ll} 50 & |\underline{21} \\ 8 & 2 \end{array} \qquad \begin{array}{ll} 21 & |\underline{8} \\ 5 & 2 \end{array}$$

$$\begin{array}{ll} 8 & |\underline{5} \\ 3 & 1 \end{array} \qquad \begin{array}{ll} 5 & |\underline{3} \\ 2 & 1 \end{array} \qquad \begin{array}{ll} 3 & |\underline{2} \\ 1 & 1 \end{array} \qquad \begin{array}{ll} 2 & |\underline{1} \\ 0 & 2 \end{array}$$

Since the last non-zero remainder is 1 we have that $GCD(54321, 50) = 1$.

Moreover:

$$LCM(54321, 50) = 54321 \cdot 50/GCD(54321, 50) = 2716050.$$

Exercise 1. Compute the GCD and the LCM of the following pairs of integers by using the Eucidean Algorithm:

(a) 29341, 1739.

(b) 10285, 9009.