4. Greatest Common Divisor

Definition 4.1. *For $a, b \in \mathbb{Z}$, not both zero, we call $d \in \mathbb{Z}$ their* **greatest common divisor** *and write $d = \gcd(a, b)$ if:*

1. *$d > 0$;*
2. *$d \mid a$ and $d \mid b$;*
3. *if $c \in \mathbb{Z}$ is such that $c \mid a$ and $c \mid b$, then $c \leq d$.*

We say that a, b are **coprime** *if $\gcd(a, b) = 1$.*

Lemma 4.2. *Let $a, b \in \mathbb{Z}$, such that $a \neq 0$ and $a \mid b$. Then $\gcd(a, b) = |a|$.*

Proof: Clearly $|a| > 0$ and $|a|$ divides both a and b. Furthermore if $c \in \mathbb{Z}$ is such that $c \mid a$ and $c \mid b$, then by Lemma 3.3(5), we get that $c \leq |a|$. In particular $\gcd(a, b) = |a|$.

□

Theorem 4.3. *For $a, b \in \mathbb{Z}$, not both zero, $\gcd(a, b)$ exists and is the minimal element of $S := \{sa + tb \mid s, t \in \mathbb{Z}, sa + tb > 0\}$.*

Proof: Note that $|a|, |b| \in S$ and so S is a non-empty set of natural numbers. Then S has a minimal element $d = sa + tb$. Clearly $d > 0$. Next we show that $d \mid a$. Assume it does not. By the Division Algorithm there are $q, r \in \mathbb{Z}$ such that $a = qd + r$, with $0 \leq r < d$. As $d \nmid a$ we must have $0 < r$. Now

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b.$$

But then $r \in S$ and $r < d$, which contradicts the minimality of d. Hence $d \mid a$. Likewise one shows that $d \mid b$.

Finally let $c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$. If $c \leq 0$, then surely $c < d$. Hence assume that $c > 0$. By Lemma 3.3 (7) we get $c \mid d$, that is, $ct = d$, for some $t \in \mathbb{Z}$. By Lemma 3.1 we have $t > 0$, as otherwise $d < 0$. Hence $d = c(1 + (t - 1)) = c + c(t - 1)$. Now either $t - 1 = 0$, in which case $d = c$ or $t - 1 > 0$, in which case $c < d$. In all cases we have $c \leq d$. Over all this shows that $d = \gcd(a, b)$.

□

Corollary 4.4. *Let a, b be integers, not both zero. Then*

1. *a and b are coprime if and only there exist integers s, t such that $1 = sa + tb$.*
2. *If $d = \gcd(a, b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Corollary 4.5 (Euclid's Lemma)**.** *Suppose that a, b are coprime integers and that $a \mid bc$, for some integer c. Then $a \mid c$.*

Example 4.6. *(1) Note that $-2 \mid 16 = (-2) \cdot (-8)$. Hence, by Lemma 4.2, we have that $\gcd(-2, 16) = 2$.*

(2) We have $3 \cdot 17 + (-5) \cdot 10 = 1$. Hence 17 and 10 are coprime. Furthermore $3 \cdot 34 + (-5) \cdot 20 = 2$ and as $2 \mid 34$ and $2 \mid 20$ we must have that $\gcd(34, 20) = 2$.

Theorem 4.7. *(The Euclidean Algorithm) Let $a, b \in \mathbb{Z}$, not both zero and $b \nmid a$. Set $r_{-1} := a$ and $r_0 := b$ and apply the division algorithm successively to r_{k-1} and r_k, for $k \geq 0$ to obtain integers q_k and r_{k+1}, where $0 \leq r_{k+1} < |r_k|$, until $r_{n+1} = 0$, for some $n \geq 0$. That means we have*

$$\begin{array}{lll}
r_{-1} & = q_0 r_0 + r_1, & \textit{where } 0 < r_1 < |r_0| \\
r_0 & = q_1 r_1 + r_2, & \textit{where } 0 < r_2 < r_1 \\
r_1 & = q_2 r_2 + r_3, & \textit{where } 0 < r_3 < r_2 \\
\vdots & \quad \vdots & \\
r_{n-2} & = q_{n-1} r_{n-1} + r_n, & \textit{where } 0 < r_n < r_{n-1} \\
r_{n-1} & = q_n r_n + r_{n+1}, &
\end{array}$$

Then $\gcd(a, b) = r_n$.

Proof: As the sequence $(r_k)_{k \geq 1}$ is positive and decreasing, the above process must terminate eventually. In particular r_n exists and $r_n > 0$, by construction. Working through the equations in reverse order one checks that r_n divides both a and b. Finally working through the equations in forward order one checks that every $c \in \mathbb{Z}$ which divides a and b, also divides r_n. In particular $c \leq r_n$, by Lemma 3.3(5). Overall it follows that $\gcd(a, b) = r_n$.

□

Corollary 4.8. (1) $\gcd(a, b) = \gcd(r_k, r_{k+1})$*, for $k \geq 0$.*

(2) *There are $x_i, y_i \in \mathbb{Z}$ such that $r_i = x_i a + y_i b$, for all $i = -1, 0, 1 \ldots, n$, such that $x_{-1} = y_0 = 1$, $y_{-1} = x_0 = 0$ and*

$$x_{i+1} = x_{i-1} - q_i x_i, \qquad \textit{and} \qquad y_{i+1} = y_{i-1} - q_i y_i,$$

for all $i = 0, 1, \ldots, n-1$. In particular $\gcd(a, b) = x_n a + y_n b$.

Example 4.9. *Compute* $\gcd(7128, 5148)$.

i	q_i	r_i	x_i	y_i
-1		7128	1	0
0	1	5148	0	1
1	2	1980	1	-1
2	1	1188	-2	3
3	1	792	3	-4
4	2	396	-5	7
5		0		

Thus $\gcd(7128, 5148) = 396$ *and* $396 = (-5) \cdot 7128 + 7 \cdot 5148$. *Furthermore* $\gcd(1980, 1188) = 396$

Remark 4.10. *A* **Diophantine equation** *is an equation in one or more unknowns with integer coefficients, where we are only interested in integer solutions. Let* $a, b, c \in \mathbb{Z}$ *be given. Then* $ax + by = c$ *is a Diophantine equation with two unknown* x *and* y*. For example one can see that* $6x + 4y = 10$ *has a solution* $(x, y) = (1, 1)$*, while* $6x + 4y = 5$ *has no integer solutions.*

Theorem 4.11. *Set* $d = \gcd(a, b)$*. The equation* $ax + by = c$ *is has integer solutions if and only if* $d \mid c$*. If* (x_0, y_0) *is any solution, then the solution set is*

$$\{(x_0 + (b/d)t, y_0 - (a/d)t) : t \in \mathbb{Z}\}.$$

Example 4.12. *Consider the equation* $7128x + 5148y = 792$*. In Example 4.9 we found that* $\gcd(7128, 5148) = 396$*. As* $396 \mid 792 = 2 \cdot 396$*, our equation has a integer solution. Furthermore in the example we found that*

$$396 = (-5) \cdot 7128 + 7 \cdot 5148,$$

and thus $x = -10, y = 14$ *is a solution for our equation. As* $7128/396 = 18$ *and* $5148/396 = 13$*, the set of all solutions is given by*

$$\{(-10 + 13t, 14 - 18t) : t \in \mathbb{Z}\}$$

That means, for $t = -2$ *we get* $(x, y) = (-36, 50)$*, which then is also a solution to our equation.*

In fact, let us find all solutions (x, y) *such that* $15 < x + y < 25$*. As* $x = -10 + 13t$ *and* $y = 14 - 18t$ *we have* $x + y = 4 - 5t$*. Now*

$$15 < x + y < 25 \Leftrightarrow 15 < 4 - 5t < 25 \Leftrightarrow t \in \{-3, -4\}.$$

Hence $(x, y) \in \{(-49, 68), (-62, 86)\}$.