Chapter 17 – Consequences of the Euclidean Algorithm

Def^n: Given integers a and b, we say that $c \in \mathbb{Z}$ is an integer linear combination of a and b if $\exists\, m,n \in \mathbb{Z}$ s.t.

$$c = ma + nb.$$

Theorem 17.1.1: Let $a,b \in \mathbb{Z}$, not both zero. Then $\exists\, m,n \in \mathbb{Z}$ s.t.

$$\gcd(a,b) = ma + nb.$$

That is, $\gcd(a,b)$ is an integer linear combination of a and b.

Before we do the proof, let's consider an example: (or two)

Example: Let $a = 72$ and $b = 30$.
We use the Euclidean algorithm to find $\gcd(72,30)$.

$$72 = 30 \times 2 + 12 \quad \longrightarrow \quad 12 = 72 - 30 \times 2$$
$$30 = 12 \times 2 + \boxed{6} \quad \longrightarrow \quad 6 = 30 - 12 \times 2$$
$$12 = 6 \times 2 + 0$$

$$\longrightarrow \gcd(72,30) = 6.$$

We can "reverse" the Euclidean algorithm to express $\gcd(a,b)$ as an integer linear combination of a and b.

We calculate

$$\begin{aligned} 6 &= 30 - 12\times 2 \\ &= 30 - (72 - 30\times 2)\times 2 \\ &= 30 - 72\times 2 + 30\times 4 \\ &= (-2)\times 72 + 5\times 30 \end{aligned}$$

Another Example: Let $a = 232$ and $b = 136$.

Euclidean algorithm:

$$\begin{aligned} 232 &= 136\times 1 + 96 \quad &\longrightarrow\ 96 &= 232 - 136\times 1 \\ 136 &= 96\times 1 + 40 \quad &\longrightarrow\ 40 &= 136 - 96\times 1 \\ 96 &= 40\times 2 + 16 \quad &\longrightarrow\ 16 &= 96 - 40\times 2 \\ 40 &= 16\times 2 + \boxed{8} \quad &\longrightarrow\ 8 &= 40 - 16\times 2 \\ 16 &= 8\times 2 + 0 \end{aligned}$$

$\longrightarrow \gcd(232, 136) = 8.$

use these formulae one after the other in reverse order

Working backwards:

$$\begin{aligned} 8 &= 40 - 16\times 2 \\ &= 40 - (96 - 40\times 2)\times 2 \\ &= 40\times 5 - 96\times 2 \\ &= (136 - 96\times 1)\times 5 - 96\times 2 \\ &= 136\times 5 - 96\times 7 \\ &= 136\times 5 - (232 - 136\times 1)\times 7 \\ &= 136\times 12 - 232\times 7 \\ &= (-7)\times 232 + 12\times 136. \end{aligned}$$

Remark: Note that this calculation is easy to check:

$$(-7)\times 232 + 12\times 136 = -1624 + 1632 = 8.$$

Proof of Theorem 17.1.1:

We first prove the case where $a, b \geq 0$.

Note that the case $a = b$ is trivial. Suppose, without loss of generality, that $a > b$.

Let $a_0, a_1, \ldots, a_n$ be the numbers generated by the Euclidean Algorithm ($a_0 = a$, $a_1 = b$, $a_n = \gcd(a,b)$).

"finite induction" → We prove by induction on $k \in \{1, \ldots, n\}$ that each of the numbers $a_0, \ldots, a_n$ can be expressed as an integer linear combination of a and b.

Base case ($k = 0, 1$): $a_0 = a = 1 \times a + 0 \times b$ and $a_1 = b = 0 \times a + 1 \times b$, so the base case holds.

Inductive step: Let $k \in \{1, \ldots, n-1\}$ and suppose that each of the numbers $a_0, \ldots, a_k$ can be expressed as an integer linear combination of a and b (we are using strong induction). Then for $i \in \{0, \ldots, k\}$ we have $a_i = m_i a + n_i b$ where $m_i, n_i \in \mathbb{Z}$. By the definition of a_{k+1}, we have

k^{th} step in the Euclidean Algorithm →

$$a_{k-1} = a_k q_k + a_{k+1}$$

for some $q_k \in \mathbb{Z}$. Hence

$$\begin{aligned} a_{k+1} &= a_{k-1} - a_k q_k \\ &= m_{k-1} a + n_{k-1} b - q_k (m_k a + n_k b) \\ &= \underbrace{(m_{k-1} - q_k m_k)}_{\text{integer}} a + \underbrace{(n_{k-1} - q_k n_k)}_{\text{integer}} b, \end{aligned}$$

as required.

It follows by induction that each of the numbers $a_0, \ldots, a_n$ can be expressed as an integer linear combination of a and b. In particular, $\exists m, n \in \mathbb{Z}$ s.t. $a_n = \gcd(a,b) = ma + nb$, as required.

The cases where one or both of a and b are negative then follow from the above applied to $|a|$ and $|b|$. For example, if $a<0$ and $b \geq 0$ then $\exists\, m,n \in \mathbb{Z}$ s.t.

$$\gcd(-a,b) = m(-a) + nb$$

($-a$ ↑ $|a|$, b ↑ $|b|$)

$\gcd(-a,b) = \gcd(a,b)$

equivalently,

$$\gcd(a,b) = (-m)a + nb. \qquad \square$$

Corollary: Let $a,b \in \mathbb{Z}$, not both zero. If $c \in \mathbb{Z}$ is a common divisor of a and b, then c divides $\gcd(a,b)$.

Proof: Suppose $c \in \mathbb{Z}$ divides a and b. Since $\exists\, m,n \in \mathbb{Z}$ s.t. $\gcd(a,b) = ma + nb$, it follows that c divides $\gcd(a,b)$. $\square$

Corollary 17.2.1: Let $a,b \in \mathbb{Z}$, not both zero. Then

$$D(a,b) = D(\gcd(a,b)).$$

($D(a,b)$: the set of all common divisors of a and b; $D(\gcd(a,b))$: the set of all divisors of $\gcd(a,b)$)

Proof: If $c \in D(a,b)$, then by the previous corollary $c \in D(\gcd(a,b))$. So $D(a,b) \subseteq D(\gcd(a,b))$. On the other hand if $c \in D(\gcd(a,b))$ then since $c \mid \gcd(a,b)$ and $\gcd(a,b) \mid a$ we have $c \mid a$. Similarly c must divide b, so $c \in D(a,b)$. Hence $D(\gcd(a,b)) \subseteq D(a,b)$. This proves the result. $\square$

Coprime Pairs:

Def^n: Let $a,b \in \mathbb{Z}$, not both zero. We say that a and b are coprime (or relatively prime) if $\gcd(a,b) = 1$.

Example: $30 = 2\times3\times5$ and $77 = 7\times11$ are coprime. (They have no prime factors in common.)

Proposition 17.3.1: Integers $a,b \in \mathbb{Z} - \{0\}$ are coprime if and only if $\exists\, m,n \in \mathbb{Z}$ s.t.

$$ma + nb = 1.$$

Proof: Let $a,b \in \mathbb{Z} - \{0\}$.

Forward implication: If a,b are coprime then $\gcd(a,b) = 1$, so $\exists m,n \in \mathbb{Z}$ s.t. $ma+nb=1$.

Reverse implication: Suppose $\exists m,n \in \mathbb{Z}$ s.t. $ma+nb=1$. It follows that if $d \in \mathbb{Z}$ divides a and b, then d divides $1 = ma+nb$. Hence the only common divisors of a and b are ± 1, and hence $\gcd(a,b) = 1$, i.e. a and b are coprime. □

$d \mid 1$ implies $d \leq 1$

Theorem: Suppose $a, b, c \in \mathbb{N}$ and $\gcd(a,b) = 1$. Then

$$a \mid bc \iff a \mid c.$$

Proof: Let $a, b, c \in \mathbb{N}$ with $\gcd(a,b) = 1$.

The reverse implication is clear.

Forward implication: Suppose $a \mid bc$. Then $\exists q \in \mathbb{Z}$ s.t. $qa = bc$. Moreover, since $\gcd(a,b) = 1$, $\exists m, n \in \mathbb{Z}$ s.t. $ma + nb = 1$.

multiply this by c on both sides

Hence

$$\begin{aligned} c = c \times 1 &= c(ma + nb) \\ &= cma + ncb \\ &= cma + nqa \\ &= (\underbrace{cm + nq}_{\text{integer}})\, a. \end{aligned}$$

It follows that $a \mid c$. □

An Application:

Observe that if p is a prime number then

$$D(p) = \{-p, -1, 1, p\}.$$

Hence if $a \in \mathbb{N}$ and p does not divide a, then $p \notin D(a)$ and hence $p \notin \underbrace{D(p,a)}_{= D(p) \cap D(a)}$.

Thus $\gcd(p,a) = 1$.

We make use of this in the following.

Theorem: Suppose p is a prime number and $a, b \in \mathbb{N}$. Then

$$p \mid ab \iff (p \mid a \text{ or } p \mid b).$$

Proof: Let p be a prime, and $a, b \in \mathbb{N}$.

The reverse implication is clear.

Forward implication: Suppose $p \mid ab$. To prove that $p \mid a$ or $p \mid b$ we suppose that p does not divide a and prove that $p \mid b$. So suppose p does not divide a. Then $\gcd(p, a) = 1$, so by the previous theorem $p \mid b$. □

Remark: Sometimes this property is used to define the prime numbers. That is, a natural number $p > 1$ is said to be prime if, for natural numbers a, b,

$$p \mid ab \implies (p \mid a \text{ or } p \mid b).$$

Corollary: Suppose p is a prime number and $a_1, \ldots, a_n \in \mathbb{N}$. If $p \mid \underbrace{a_1 \cdot \cdots \cdot a_n}_{\text{product}}$ then p divides a_i for some $i \in \{1, \ldots, n\}$.

With this fact established we may now prove the uniqueness of prime factorizations.

Theorem 23.3.1 (The Fundamental Theorem of Arithmetic):

Every positive integer greater than 1 can be written uniquely as a product of prime numbers, up to the order of the factors.

↑ the order of the factors can be fixed by requiring that the factors appear in "non-decreasing" order, e.g., as in $60 = 2 \times 2 \times 3 \times 5$

Proof: Let $n \in \mathbb{Z}$, $n > 1$. We have already seen that n may be written as a product of primes (see the notes on Chapter 5).

To prove uniqueness of the prime factorization we suppose, with a view to obtaining a contradiction, that n has two different prime factorizations

$$n = p_1 \cdot \cdots \cdot p_r \quad , \quad \text{and}$$
$$n = q_1 \cdot \cdots \cdot q_s$$

where $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are primes and $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$. Cancelling any primes which appear on both sides of the expression $p_1 \cdot \cdots \cdot p_r = q_1 \cdot \cdots \cdot q_s$ we obtain an expression of the form

$$(*) \qquad p'_1 \cdot \cdots \cdot p'_{r'} = q'_1 \cdot \cdots \cdot q'_{s'}$$

not all of the primes can cancel since the two prime factorizations differ

where $\{p_1', \ldots, p_{r'}'\} \subseteq \{p_1, \ldots, p_r\}$, $\{q_1', \ldots, q_{s'}'\} \subseteq \{q_1, \ldots, q_r\}$ and the sets $\{p_1', \ldots, p_{r'}'\}$ and $\{q_1', \ldots, q_{s'}'\}$ are disjoint.

But then, since p_1' divides $p_1' \cdot \ldots \cdot p_{r'}'$, (*) implies that p_1' divides $q_1' \cdot \ldots \cdot q_{s'}'$.

Hence p_1' divides q_i' for some $i \in \{1, \ldots, s'\}$, which contradicts the fact that $p_1', q_1', \ldots, q_{s'}'$ are distinct primes.

We conclude that n cannot have two different prime factorizations. This proves the result. □