Part IV. Chapter 17. Consequences of the Euclidean algorithm

An important consequence of the Euclidean algorithm is that the greatest common divisor of integers $a$ and $b$ can be written as an ‘integral linear combination’ of $a$ and $b$, i.e., as a linear combination of $a$ and $b$ using integer coefficients.

**Theorem 1 (Eccles 17.1.1)** If $a, b \in \mathbb{Z}$, where at least one of them is nonzero, then there exist $m, n \in \mathbb{Z}$ such that

$$\gcd(a, b) = am + bn.$$ 

The idea of the proof is to apply the Euclidean algorithm to $a$ and $b$ to find their gcd. Then reversing the algorithm, we may express $\gcd(a, b)$ as an integral linear combination of $a$ and $b$. We do not discuss the rigorous proof in this course.

*Example.* $a = 4199$ and $b = 1748$. Here, $\gcd(4199, 1748) = 19$ and we saw that

$$19 = 5 \cdot 4199 + (-12) \cdot 1748.$$ 

**Definition 2 (Eccles 11.3.2)** Integers $a$ and $b$, not both zero, are **coprime** if $\gcd(a, b) = 1$.

An important consequence of Theorem 17.1.1 is:

**Proposition 3 (Eccles 17.3.1)** Nonzero integers $a$ and $b$, are coprime if and only if $1$ can be written as an integral linear combination of $a$ and $b$.

In other words,

**Equivalent Proposition** Nonzero integers $a$ and $b$ satisfy $\gcd(a, b) = 1$ if and only if there exist $m, n \in \mathbb{Z}$ such that $1 = am + bn$.

**Proof.** ($\Rightarrow$) This is the statement:

*If $\gcd(a, b) = 1$, then there exist $m, n \in \mathbb{Z}$ such that $1 = am + bn$.*

This is a special case of Theorem 17.1.1.

($\Leftarrow$) This is the statement:
If there exist $m, n \in \mathbb{Z}$ such that $1 = am + bn$, then $\gcd(a, b) = 1$.

Suppose there exist $m, n \in \mathbb{Z}$ such that $1 = am + bn$. Let $c$ be any positive common divisor of $a$ and $b$. Since $c$ divides $a$ and $b$, we have $c$ divides $am + bn$. This and $am + bn = 1$ implies $c$ divides $1$. This and $c > 0$ implies $c = 1$. Since any positive common divisor of $a$ and $b$ equals $1$, we conclude that $\gcd(a, b) = 1$. ■

Example. Euclidean algorithm applet:

http://people.math.sc.edu/sumner/numbertheory/euclidean/euclidean.html

gcd(17, 83) = 1 and

$$1 = (-39) \cdot 17 + 8 \cdot 83.$$ 

Theorem 4 (Eccles 17.3.2) Suppose $a, b, c \in \mathbb{Z}^+$ and $a$ and $b$ are coprime. If $a$ divides $bc$, then $a$ divides $c$.

Intuitively the statement says that if $a$ goes completely into the product of $b$ and $c$ while $a$ has nothing to do with $b$, then $a$ must go completely into $c$.

On the other hand, if as above but $a$ has something to do with $b$, such as $a = 6$ and $b = 15$ (here, $a$ and $b$ are not coprime). Then we can take for example $c = 14$ (an even number) and we get that

$$a = 6 \text{ divides } b \cdot c = 15 \cdot 14 = 210$$

but $a = 6$ does not divide $c = 14$. What happens is that part of $6$ (namely $3$) goes into $b = 15$ whereas the other part of $6$ (namely $2$) goes into $c = 14$.

Proof. The idea is to use $a$ and $b$ are coprime. By Proposition 17.3.1, there exist $m, n \in \mathbb{Z}$ such that

$$1 = am + bn.$$ 

The key is to link this to $c$. The idea is simply to multiply this equation by $c$ to get

$$c = cam + cbn.$$ 

Now $a$ clearly divides $cam$ since $a \cdot cm = cam$. On the other hand, since $a$ divides $bc$ by hypothesis, we have that $a$ divides $cbn$ since $cbn = bc \cdot n$. Hence $a$ divides the sum $cam + cbn$. Since $cam + cbn = c$, we conclude that $a$ divides $c$. ■

This is an elegant and important proof.