Chapter 16 The Euclidean Algorithm

Recall: Let $a, b$ be two integers, at least one of which is non-zero. Then the greatest common divisor of $a$ and $b$ is the largest integer that divides both $a$ and $b$.

Notation: $\text{gcd}(a, b), (a, b)$

Lemma: Let $a, b \in \mathbb{Z}$ and $b > 0$. Then $b$ divides $a$ if and only if $\text{gcd}(a, b) = b$.

Lemma: For non-zero integers $a$ and $b$, suppose that $a = bq + r$ where $q, r \in \mathbb{Z}$. Then $\text{gcd}(a, b) = \text{gcd}(b, r)$

Eg. $72 = 30 \times 2 + 12 \Rightarrow (72, 30) = (30, 12)$

Q: Given $a, b \in \mathbb{Z}$, how to find $\text{gcd}(a, b)$?

The Euclidean Algorithm.

Q: Given $a, b \in \mathbb{Z}, a, b \neq 0, 0 < b < a$. Find $\text{gcd}(a, b)$

Step1: Use $b$ to divide $a$, find the quotient $q$ and the remainder $r_1$.

$$a = bq_1 + r_1, 0 \leq r_1 < b$$

Step2: Repeat Step1 for $b$ and $r_1$. That is, use $r_1$ to divide $b$, find the quotient $q_2$ and the remainder $r_2$

$$b = r_1q_2 + r_2, 0 \leq r_2 < r_1$$

Step 3: Repeat the division for $r_1$ and $r_2$.

$$r_1 = r_2q_3 + r_3$$

Keep doing the division until we get a remainder equal to zero. Then the last non-zero remainder is the answer $\text{gcd}(a, b)$.

Eg. $\text{gcd}(72, 30)$

$72 = 30 \times 2 + 12$

$30 = 12 \times 2 + 6$

$12 = 6 \times 2 + 0$

so $\text{gcd}(72, 30) = 6$.

Eg. Find $\text{gcd}(232, 136)$

Step1: $232 = 136 \times 1 + 96$

Step2: $136 = 96 \times 1 + 40$

Step3: $96 = 40 \times 2 + 16$

Step4: $40 = 16 \times 2 + 8$

Step5: $16 = 8 \times 2 + 0$

$\Rightarrow \text{gcd}(232, 136) = 8$
Chapter 17 Consequences of the Euclidean algorithm

Definition: Given integers $a, b$, we say that an integral linear combination of $a$ and $b$ if there exists $m, n \in \mathbb{Z}$, such that $c = am + bn$.

**Theorem** Let $a, b \in \mathbb{Z}$, and not both zero. Then $\text{gcd}(a, b)$ is an integral linear combination. That is, there exists $m, n \in \mathbb{Z}$, such that $\text{gcd}(a, b) = am + bn$.

Q: Given $a, b \in \mathbb{Z}$, how to find $m, n \in \mathbb{Z}$ such that $\text{gcd}(a, b) = ma + bn$.

Eg. Recall $6 = \text{gcd}(72, 30)$. Find $m, n \in \mathbb{Z}$ such that $6 = 72m + 30n$.

Step1: Write down the Euclidean algorithm:

\[
\begin{align*}
70 &= 30 \times 2 + 12 \\
30 &= 12 \times 2 + 6 \\
12 &= 6 \times 2 + 0
\end{align*}
\]

Step2: 

\[
\begin{align*}
6 &= 30 - 12 \times 2 \\
&= 30 - (72 + 30 \times (-2)) \times 2 \\
&= 72 \times (-2) + 30 \times (1 + 4) \\
&= 72 \times (-2) + 30 \times 5
\end{align*}
\]

so $m = -2, n = 5$

Eg. Recall $\text{gcd}(232, 136) = 8$

Find $m, n \in \mathbb{Z}$ such that $8 = 232m + 136n$.

Step1: Write down the Euclidean algorithm:

\[
\begin{align*}
232 &= 136 \times 1 + 96 \\
136 &= 96 \times 1 + 40 \\
96 &= 40 \times 2 + 16 \\
40 &= 16 \times 2 + 8 \\
16 &= 8 \times 2 + 0
\end{align*}
\]

Step2: 

\[
\begin{align*}
8 &= 40 + 16 \times (-2) \\
&= 40 + (96 + 40 \times (-2)) \times (-2) \\
&= 96 \times (-2) + 40 \times 5 \\
&= 96 \times (-2) + (136 - 96 \times 1) \times 5 \\
&= 136 \times 5 + 96 \times (-7) \\
&= 136 \times 5 + (232 - 136 \times 1) \times (-7) \\
&= 232 \times (-7) + 136 \times 12
\end{align*}
\]

so $m = -7, n = 12$
Corollary: Let $k$ be a common divisor of $a, b$, then $k$ divides $\gcd(a, b)$.

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

**Coprime Pairs**

**Definition:** Let $a, b \in \mathbb{Z}$, not both zero. They are called coprime when $\gcd(a, b) = 1$.

**Proposition:** Let $a, b \in \mathbb{Z}$, not both zero. They are coprime if and only if there exist integers $m, n$ such that

$$am + bn = 1.$$ 

**Theorem:** Suppose $a, b, c \in \mathbb{Z}^+$ and $(a, b) = 1$. Then $a|bc$ if and only if $a|c$. 