Chapter 27 Modular Arithmetic

Def Let $m, n \in \mathbb{Z}$ be integers not both 0. Then their **greatest common divisor** is an integer $d \in \mathbb{Z}^+$ such that (1) $d \mid m$ and $d \mid n$ (common divisor)

(2) if $s \in \mathbb{Z}^+$ and $s \mid m$ and $s \mid n$, then $s \mid d$.

(greatest common divisor)

We denote d by $\gcd(m,n)$. We say m and n are **relatively prime** if $\gcd(m,n) = 1$.

Example Find $\gcd(-16, 40)$, $\gcd(0, 45)$, $\gcd(-30, -27)$.

$= 8$ $= 45$ $= 3$

Theorem Let $m, n \in \mathbb{Z}$ be integers not both 0. Then their greatest common divisor exists, is unique, and $\gcd(m,n) = km + ln$ for some $k, l \in \mathbb{Z}$.

Proof Let $A = \{ xm + yn : x, y \in \mathbb{Z} \text{ and } xm + yn > 0 \}$.

We claim A is nonempty. Indeed, $m^2 + n^2 \in A$ since $m^2 + n^2 > 0$ and $m^2 + n^2 = xm + ny$ when $x = m$ and $y = n$. Since $A \subseteq \mathbb{N}$ is non-empty, by the Well-Ordering Principle of $\mathbb{N}$, it has a minimum.

Let $d = \min A$. Since $d \in A$, $d = km + ln$ for some

$k, l \in \mathbb{Z}$. We claim $d = \gcd(m,n)$. First note $d \in \mathbb{Z}^+$ since $d \in A$. Next we must show $d \mid m$ and $d \mid n$.

By the division algorithm, $m = qd + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < d$. We claim $r = 0$.

Suppose not. Then $r > 0$ and

$$\begin{aligned} r &= m - qd \\ &= m - q(km + ln) \\ &= (1 - qk)m + (-ql)n, \end{aligned}$$

which implies $r \in A$. However since $r < d$, this contradicts the fact that $d = \min A$.

So since $r = 0$, $m = qd$, which means $d \mid m$.

The same argument shows $d \mid n$. Next we must show that if $s \in \mathbb{Z}^+$ such that $s \mid m$ and $s \mid n$, then $s \mid d$. Exercise Prove that if $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$ and use this here.

Finally, we must show uniqueness: if $t \in \mathbb{Z}^+$ satisfies properties (1) and (2) of the gcd definition, then $t = d$.

Exercise Prove that if $a, b \in \mathbb{Z}^+$ such that $a \mid b$ and $b \mid a$, then $a = b$ and use this here.

Euclidean Algorithm Let $m, n \in \mathbb{Z}^+$ and suppose $m > n$.

Repeatedly apply the division algorithm:

$$m = q_1 n + r_1$$
$$n = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$r_2 = q_4 r_3 + r_4$$
$$\vdots$$
$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$$
$$r_{k-2} = q_k r_{k-1} + r_k$$
$$r_{k-1} = q_{k+1} r_k + 0.$$

Eventually you'll get a remainder of 0 since $n > r_1 > r_2 > \dots \geq 0$. Then $r_k = \gcd(m, n)$.

Example Use the Euclidean Algorithm to compute $\gcd(35, 20)$ and $\gcd(86, 24)$.

$35 = 1 \cdot 20 + 15$
$20 = 1 \cdot 15 + 5$
$15 = 3 \cdot 5 + 0$

$\Rightarrow \gcd(35, 20) = 5$

$86 = 3 \cdot 24 + 14$
$24 = 1 \cdot 14 + 10$
$14 = 1 \cdot 10 + 4$
$10 = 2 \cdot 4 + 2$
$4 = 2 \cdot 2 + 0$

$\gcd(86, 24) = 2.$

Why the algorithm works:

① $r_k \mid r_{k-1}$ since $r_{k-1} = q_{k+1} r_k$

$\Rightarrow r_k \mid r_{k-2}$ since r_{k-2} is a linear combination of r_{k-1} and r_k and $r_k \mid r_{k-1}$ and $r_k \mid r_k$.

$\ldots \Rightarrow r_k \mid m$ and $r_k \mid n$.

So $r_k \mid \gcd(m,n)$.

② Let $d = \gcd(m,n)$. Then $d \mid m$ and $d \mid n$

and $r_1 = m - q_1 n \Rightarrow d \mid r_1$

Since $d \mid n$ and $d \mid r_1$ and $r_2 = n - q_2 r_1$

$\Rightarrow d \mid r_2$.

$\ldots \quad d \mid r_k$.

So $d \mid r_k$ and $r_k \mid d \Rightarrow r_k = d$.