MATH 433

Applied Algebra

Lecture 2:
Euclidean algorithm.

Division of integer numbers

Let a and b be integers and $a > 0$. Suppose that $b = aq + r$ for some integers q and r such that $0 \leq r < a$. Then r is the **remainder** and q is the **quotient** of b by a.

Theorem 1 Let a and b be integers and $a > 0$. Then the remainder and the quotient of b by a are well-defined.

Division of integer numbers

Theorem 2 Let a and b be integers and $a > 0$. Then the remainder and the quotient of b by a are uniquely determined.

Proof: Suppose that $b = aq_1 + r_1$ and $b = aq_2 + r_2$, where q_1, r_1, q_2, r_2 are integers and $0 \leq r_1, r_2 < a$. We need to show that $q_1 = q_2$ and $r_1 = r_2$.

We have $aq_1 + r_1 = aq_2 + r_2$, which implies that $r_1 - r_2 = aq_2 - aq_1 = a(q_2 - q_1)$. Adding inequalities $0 \leq r_1 < a$ and $-a < -r_2 \leq 0$, we obtain $-a < r_1 - r_2 < a$. Consequently, $-1 < (r_1 - r_2)/a < 1$. On the other hand, $(r_1 - r_2)/a = q_2 - q_1$ is an integer. Therefore $(r_1 - r_2)/a = q_2 - q_1 = 0$ so that $q_1 = q_2$ and $r_1 = r_2$.

Greatest common divisor

Given two natural numbers a and b, the **greatest common divisor** $\gcd(a, b)$ of a and b is the largest natural number that divides both a and b.

Lemma 1 If a divides b then $\gcd(a, b) = a$.

Lemma 2 If $a \nmid b$ and r is the remainder of b by a, then $\gcd(a, b) = \gcd(r, a)$.

Proof: We have $b = aq + r$, where q is an integer.
Let $d|a$ and $d|b$. Then $a = dn$, $b = dm$ for some $n, m \in \mathbb{Z}$
$\implies r = b - aq = dm - dnq = d(m - nq) \implies d$ divides r.
Conversely, let $d|r$ and $d|a$. Then $r = dk$, $a = dn$ for some $k, n \in \mathbb{Z} \implies b = dnq + dk = d(nq + k) \implies d$ divides b.
Thus the pairs a, b and r, a have the same common divisors.
In particular, $\gcd(a, b) = \gcd(r, a)$.

Euclidean algorithm

Theorem Given $a, b \in \mathbb{Z}$, $0 < a < b$, there is a decreasing sequence of positive integers $r_1 > r_2 > \cdots > r_k$ such that $r_1 = b$, $r_2 = a$, r_i is the remainder of r_{i-2} by r_{i-1} for $3 \le i \le k$, and r_k divides r_{k-1}. Then $\gcd(a, b) = r_k$.

Example. $a = 1356$, $b = 744$. $\gcd(a, b) = ?$

We obtain

$$\begin{aligned}
&1356 = 744 \cdot 1 + 612,\\
&744 = 612 \cdot 1 + 132,\\
&612 = 132 \cdot 4 + 84,\\
&132 = 84 \cdot 1 + 48,\\
&84 = 48 \cdot 1 + 36,\\
&48 = 36 \cdot 1 + 12,\\
&36 = 12 \cdot 3.
\end{aligned}$$

Thus $\gcd(1356, 744) = 12$.

Problem. Find an integer solution of the equation $1356m + 744n = 12$.

Let us use calculations done for the Euclidean algorithm applied to 1356 and 744.

$1356 = 744 \cdot 1 + 612$

$\implies 612 = 1 \cdot 1356 - 1 \cdot 744$

$744 = 612 \cdot 1 + 132$

$\implies 132 = 744 - 612 = -1 \cdot 1356 + 2 \cdot 744$

$612 = 132 \cdot 4 + 84$

$\implies 84 = 612 - 4 \cdot 132 = 5 \cdot 1356 - 9 \cdot 744$

$132 = 84 \cdot 1 + 48$

$\implies 48 = 132 - 84 = -6 \cdot 1356 + 11 \cdot 744$

$84 = 48 \cdot 1 + 36$

$\implies 36 = 84 - 48 = 11 \cdot 1356 - 20 \cdot 744$

$48 = 36 \cdot 1 + 12$

$\implies 12 = 48 - 36 = -17 \cdot 1356 + 31 \cdot 744$

Thus $m = -17$, $n = 31$ is a solution.

Problem. Find an integer solution of the equation $1356m + 744n = 12$.

Let us consider a partitioned matrix $\left(\begin{array}{cc|c} 1 & 0 & 1356 \\ 0 & 1 & 744 \end{array}\right)$.

This is the augmented matrix of the system $\begin{cases} x = 1356, \\ y = 744. \end{cases}$

We are going to apply elementary row operations to this matrix until we get 12 in the rightmost column.

$$\left(\begin{array}{cc|c} 1 & 0 & 1356 \\ 0 & 1 & 744 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 612 \\ 0 & 1 & 744 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 612 \\ -1 & 2 & 132 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 5 & -9 & 84 \\ -1 & 2 & 132 \end{array}\right) \to \left(\begin{array}{cc|c} 5 & -9 & 84 \\ -6 & 11 & 48 \end{array}\right) \to \left(\begin{array}{cc|c} 11 & -20 & 36 \\ -6 & 11 & 48 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 11 & -20 & 36 \\ -17 & 31 & 12 \end{array}\right) \to \left(\begin{array}{cc|c} 62 & -113 & 0 \\ -17 & 31 & 12 \end{array}\right)$$

Thus $m = -17$, $n = 31$ is a solution.

Theorem Let a and b be positive integers. Then $\gcd(a, b)$ is the smallest positive number represented as $na + mb$, $m, n \in \mathbb{Z}$ (that is, as an **integral linear combination** of a and b).

Proof: Let $L = \{x \in \mathbb{P} \mid x = na + mb \text{ for some } m, n \in \mathbb{Z}\}$. The set L is not empty as $b = 0a + 1b \in L$. Hence it has the smallest element c. We have $c = na + mb$, $m, n \in \mathbb{Z}$.

Consider the remainder r of a by c. Then $r = a - cq$, where q is the quotient of a by c. It follows that
$r = a - (na + mb)q = (1 - nq)a + (-mq)b$.
Since $r < c$, it cannot belong to the set L. Therefore $r = 0$.
That is, c divides a. Similarly, one can prove that c divides b.

Let $d > 0$ be another common divisor of a and b.
Then $a = dk$ and $b = dl$ for some $k, l \in \mathbb{Z}$
$\implies c = na + mb = ndk + mdl = d(nk + ml)$
$\implies d$ divides $c \implies d \leq c$.

Corollary $\gcd(a, b)$ is divisible by any other common divisor of a and b.