MATH 433

Applied Algebra

Lecture 1:
Greatest common divisor.
Euclidean algorithm.

Integer numbers

Positive integers: $\mathbb{P} = \{1, 2, 3, \dots\}$
Natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
Integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Arithmetic operations: addition, subtraction, multiplication, and division.

Addition and multiplication are well defined for the natural numbers $\mathbb{N}$. Subtraction is well defined for the integers $\mathbb{Z}$ (only partially defined on $\mathbb{N}$). Division by a nonzero number is well defined on the set of *rational numbers* $\mathbb{Q}$ (only partially defined on $\mathbb{Z}$ and $\mathbb{N}$).

Division of integer numbers

Let a and b be integers and $a \neq 0$. We say that $\boxed{a\ \textbf{divides}\ b}$ or that $\boxed{b\ \textbf{is divisible by}\ a}$ if $b = aq$ for some integer q. The integer q is called the **quotient** of b by a.

Notation: $a \mid b$ (a divides b)
$a \nmid b$ (a does not divide b)

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 (partial) **quotient** of b by a.

Note that $a \mid b$ means that the remainder is 0.

Ordering of integers

Integer numbers are ordered: for any $a, b \in \mathbb{Z}$ we have either $a < b$ or $b < a$ or $a = b$.

One says that an integer c lies between integers a and b if $a < c < b$ or $b < c < a$.

Well-ordering principle: any nonempty set of natural numbers has the smallest element.

As a consequence, any decreasing sequence of natural numbers is finite.

Remark. The well-ordering principle does not hold for all integers (there is no smallest integer).

Division theorem

Theorem Let a and b be integers and $a > 0$. Then the remainder and the quotient of b by a are well-defined. That is, $b = aq + r$ for some integers q and r such that $0 \leq r < a$.

Proof: First consider the case $b \geq 0$.
Let $R = \{x \in \mathbb{N} : x = b - ay \text{ for some } y \in \mathbb{Z}\}$.

The set R is not empty as $b = b - a0 \in R$. Hence it has the smallest element r. We have $r = b - aq$ for some $q \in \mathbb{Z}$.

Consider the number $r - a$. Since $r - a < r$, it is not contained in R. But $r - a = (b - aq) - a = b - a(q + 1)$.
It follows that $r - a$ is not natural, i.e., $r - a < 0$.
Thus $b = aq + r$, where q and r are integers and $0 \leq r < a$.

Now consider the case $b < 0$. In this case $-b > 0$.
By the above $-b = aq + r$ for some integers q and r such that $0 \leq r < a$. If $r = 0$ then $b = -aq = a(-q) + 0$.
If $0 < r < a$ then $b = -aq - r = a(-q - 1) + (a - r)$.

Greatest common divisor

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

Notation: $\gcd(a, b)$ or simply (a, b).

Example 1. $a = 12,\ b = 18$.

Natural divisors of 12 are $1, 2, 3, 4, 6$, and 12.
Natural divisors of 18 are $1, 2, 3, 6, 9$, and 18.
Common divisors are $1, 2, 3$, and 6.
Thus $\gcd(12, 18) = 6$.

Notice that $\gcd(12, 18)$ is divisible by any other common divisor of 12 and 18.

Example 2. $a = 1356,\ b = 744.$ $\gcd(a, b) = ?$

Euclidean algorithm

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

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 $3 \leq i \leq k$, and r_k divides r_{k-1}. Then $\gcd(a,b) = r_k$.

Example 2. $a = 1356$, $b = 744$. $\gcd(a, b) = ?$

First we divide 1356 by 744: $1356 = 744 \cdot 1 + 612$.
Then divide 744 by 612: $744 = 612 \cdot 1 + 132$.
Then divide 612 by 132: $612 = 132 \cdot 4 + 84$.
Then divide 132 by 84: $132 = 84 \cdot 1 + 48$.
Then divide 84 by 48: $84 = 48 \cdot 1 + 36$.
Then divide 48 by 36: $48 = 36 \cdot 1 + 12$.
Then divide 36 by 12: $36 = 12 \cdot 3$.

Thus $\gcd(1356, 744) = \gcd(744, 612)$
$= \gcd(612, 132) = \gcd(132, 84) = \gcd(84, 48)$
$= \gcd(48, 36) = \gcd(36, 12) = 12$.

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 $L = \{x \in \mathbb{P} : x = na + mb$ 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 $c \implies d \leq c$.

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

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.