MATH 433

Applied Algebra

Lecture 1:
Division of integers.
Greatest common divisor.

Integer numbers

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

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 $\boxed{a \text{ **divides** } b}$ or that $\boxed{b \text{ **is divisible by** } a}$ 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 $\gcd(a, b) = \gcd(r, a)$.

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