Discrete Mathematics, Section 001, Fall 2016

Lecture 18: First steps in number theory.

Zsolt Pajor-Gyulai

zsolt@cims.nyu.edu

Courant Institute of Mathematical Sciences

November 16, 2016

Outline

Division with remainder

Theorem

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist integers q and r such that

$$a = qb + r \qquad 0 \leq r < |b|$$

Moreover, there is only one such pair of integers (q, r).

$$q : \text{quotient} \qquad r : \text{remainder}$$

Example

Let $a = -37$ and $b = 5$. Then $q = -8$ and $r = 3$ because

$$-37 = -8 \times 5 + 3 \qquad \text{and} \qquad 0 \leq 3 < 5.$$

Division with remainder

Theorem

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist integers q and r such that

$$a = qb + r \qquad 0 \leq r < |b|$$

Moreover, there is only one such pair of integers (q, r).

Things to prove:

- There is such a pair (q, r):
  - $a = qb + r$
  - $0 \leq r < |b|$
- There is at most one such pair.

Idea of the proof for $b > 0$: Keep substracting multiples of b from a, then the smallest natural number we can get like this will be r:

$$a - qb = r$$

Existence proof when $b > 0$

There is a pair (q, r):

- $a = qb + r$
- $0 \leq r < b$

Let

$$B = \{a - bk : k \in \mathbb{Z}, a - bk \geq 0\} \subseteq \mathbb{N}$$

and note that $B \neq \emptyset$ as

1. if $a \geq 0$, then $a \in B$ (choose $k = 0$),
2. if $a < 0$, then choose $k < \frac{a}{b}$.

Thus, the Well-Ordering Principle states that there is a least element $r \in B$. Since $r \in B$, there is a $q \in \mathbb{Z}$ such that

$$r = a - bq$$

Thus $a = qb + r$ and $r \geq 0$. It remains to show that $r < b$.
[...]

Existence proof when $b > 0$

There is a pair (q, r):

- $a = qb + r$
- $0 \leq r < b$

[...]
For the sake of contradiction, suppose that $r \geq b$. Then

$$a - qb = r \geq b$$

and therefore

$$r' = r - b = (a - qb) - b = a - (q + 1)b \geq 0.$$

This implies $r' \in B$, but $r' < r$ and r was the least element of B. $\Rightarrow\Leftarrow$. This finishes the existence proof.

Uniqueness proof

There is at most one pair (q, r) such that

- $a = qb + r$
- $0 \leq r < |b|$

Suppose, for the sake of contradiction, that there are two different pairs of numbers (q, r) and (q', r') that satisfies the conditions; that is

$$\begin{array}{cc} a = qb + r & 0 \leq r < |b| \\ a = q'b + r' & 0 \leq r' < |b| \end{array}$$

Combining these

$$qb + r = q'b + r' \qquad \Rightarrow \qquad r - r' = (q' - q)b.$$

and therefore $b | r - r'$. But $0 \leq r, r' < |b|$ and therefore

$$r = r'.$$

[...]

Uniqueness proof

There is at most one pair (q, r) such that

- $a = qb + r$
- $0 \leq r < |b|$

[...]
Thus

$$qb + r = a = q'b + r' = q'b + r \qquad \Rightarrow \qquad qb = q'b$$

and since $b > 0$, this implies $q = q'$. This means that

$$(q, r) = (q', r')$$

and therefore the two pairs weren't different. $\Rightarrow\Leftarrow$. Therefore, the quotient and remainder are unique. This finishes the proof of the theorem.

A simple corollary

Corollary

Every integer is either even or odd, but not both

Proof.

Let $n \in \mathbb{Z}$. We can find $q, r \in \mathbb{Z}$ such that $n = 2q + r$ where $r = 0, 1$. If $r = 0$ then n is even and if $r = 1$ then n is odd. $\square$

Div and Mod

Definition

Let $a, b \in \mathbb{Z}$ with $b > 0$ and let $q, r \in \mathbb{Z}$ be the unique integers such that $a = qb + r$ and $0 \leq r < b$. Then we say

$$a \operatorname{div} b = q, \qquad a \bmod b = r.$$

For example,

$$\begin{array}{rr} 11 \operatorname{div} 3 = 3 & 11 \bmod 3 = 2 \\ 23 \operatorname{div} 10 = 2 & 23 \bmod 10 = 3 \\ -37 \operatorname{div} 5 = -8 & -37 \bmod 5 = 3 \end{array}$$

Q: What is the connection to the earlier definition of $\bmod$?

Proposition

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then

$$a \equiv b \pmod{n} \qquad \Leftrightarrow \qquad a \bmod n = b \bmod n.$$

Outline

Definitions

Definition

Let $a, b \in \mathbb{Z}$. We call $d \in \mathbb{Z}$ a **common divisor** of a and b provided $d|a$ and $d|b$.

For example, if $a = 30$ and $b = 24$, then the common divisors are

$$-6, -3, -2, -1, 1, 2, 3, 6$$

Definition

Let $a, b \in \mathbb{Z}$. We call $d \in \mathbb{Z}$ the **greatest common divisor** of a and b, provided

(1) d is a common divisor of a and b,

(2) if e is a common divisor of a and b, then $e \leq d$.

Notation: $gcd(a, b)$

For example, $gcd(30, 24) = 6$.

Computing $gcd(a, b)$

We assume for simplicity that a and b are positive integers.
Alternative 1: Brute force

- For every positive integer k from 1 to $min(a, b)$, check whether $k|a$ and $k|b$. If so, save that number k on a list.
- Choose the largest number on the list, that is $gcd(a, b)$.

This is terribly slow.

Computing $gcd(a, b)$

Alternative 2: Euclidean algorithm.

- If $b|a$ then $gcd(a, b) = |b|$.
- If $b \nmid a$, then write

$$\begin{array}{rcl} a = bq_1 + r_1, & & 0 < r_1 < |b| \\ b = r_1 q_2 + r_2, & & 0 < r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 & & 0 < r_3 < r_2 \\ \vdots & & \vdots \\ r_{n-2} = r_{n-1} q_n + r_n & & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} & & \end{array}$$

This finishes in finite steps as the sequence of remainders decreases:

$$|b| > r_1 > r_2 > \cdots > r_{n-1} > r_n > 0$$

Then $gcd(a, b) = r_n$.

Computing $gcd(a, b)$

- For example, find $gcd(689, 234)$.

$$
\begin{aligned}
689 &= 2 \cdot 234 + 221 \\
234 &= 1 \cdot 221 + 13 \\
221 &= 17 \cdot 13
\end{aligned}
$$

  and therefore $gcd(689, 234) = 13$.

- Another example, find $gcd(431, 29)$.

$$
\begin{aligned}
431 &= 14 \cdot 29 + 25 \\
29 &= 1 \cdot 25 + 4 \\
25 &= 6 \cdot 4 + 1 \\
4 &= 4 \cdot 1
\end{aligned}
$$

  and therefore $gcd(431, 29) = 1$.

Computing $gcd(a, b)$

$$\begin{array}{rl}
a = bq_1 + r_1, & 0 < r_1 < |b| \\
b = r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 = r_2 q_3 + r_3 & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_{n-2} = r_{n-1} q_n + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} &
\end{array}$$

- r_n is a common divisor:

$$r_n | r_{n-1} \to r_n | r_{n-2} \to \cdots \to r_n | b \to r_n | a$$

- r_n is a *gcd*: Let $c|a$, $c|b$. Then

$$c|(a - bq_1) = r_1 \to c|(b - r_1 q_2) = r_2 \to \cdots \to c|(r_{n-2} - r_{n-1} q_n) = r_n$$

Both argument can be made precise by induction.

$$
\begin{array}{rcl}
a = bq_1 + r_1, & & 0 < r_1 < |b| \\
b = r_1 q_2 + r_2, & & 0 < r_2 < r_1 \\
r_1 = r_2 q_3 + r_3 & & 0 < r_3 < r_2 \\
\vdots & & \vdots \\
r_{n-2} = r_{n-1} q_n + r_n & & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} & &
\end{array}
$$

By starting the algorithm from the second line, we also proved

Proposition

Let a and b be positive integers and let $c = a \bmod b$. Then

$$gcd(a, b) = gcd(a, a \bmod b)$$

The Euclidean algorithm can be written as

$$gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_n, 0) = r_n$$

Recursive version of the Euclidean algorithm

Input: Positive integers a and b.
Output: $gcd(a, b)$

(1) Let $c = a \bmod b$.
(2) If $c = 0$, then we return b and stop.
(3) Otherwise, return $gcd(b, c)$.

Q: What about when a or b is not a positive integer?

- Note that the list of divisors for a and $-a$ are the same.
- Same for b and $-b$.

$gcd(a, b) = gcd(|a|, |b|)$

There is only one exception when this does not help: $a = b = 0$.

Theorem

Let a and b be positive integers. There are $u, v \in \mathbb{Z}$ such that

$$gcd(a,b) = ua + vb$$

First:

$$a = bq_1 + r_1 \quad \rightarrow \quad r_1 = a - bq_1$$

Second:

$$b = r_1 q_2 + r_2$$
$$\downarrow$$
$$r_2 = b - r_1 q_2 = b - q_2(a - bq_1) = a(-q_2) + b(1 + q_1 q_2)$$

and one can proceed similarly until reaching $r_n = ua + vb$.

For example, find x and y integers such that

$$431x + 29y = gcd(431, 29)(= 1)$$

Write

$$\begin{aligned} 431 &= 14 \cdot 29 + 25 \\ 29 &= 1 \cdot 25 + 4 \\ 25 &= 6 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 \end{aligned}$$

Therefore

$$25 = 431 - 14 \cdot 29$$

$$4 = 29 - 1 \cdot 25 = 29 - 431 + 14 \cdot 29 = 15 \cdot 29 - 431$$

$$1 = 25 - 6 \cdot 4 = (431 - 14 \cdot 29) - 6(15 \cdot 29 - 431) = 7 \cdot 431 - (6 \cdot 15 + 14) \cdot 29$$

and so $x = 7$ and $y = -104$.

Relative primes

Proposition

For $a, b \in \mathbb{Z}$ positive, $gcd(a, b)$ is the smallest integer of the form $ax + by$.

Proof.

Note $gcd(a, b)|(ax + by)$ and therefore $gcd(a, b) \leq ax + by$. $\square$

Definition

Let a and b be integers. We call a and b **relatively prime** provided $gcd(a, b) = 1$.

Corollary

Let a and b be integers. There exist integers x and y such that $ax + by = 1$ if and only if a and b are relatively prime.

Diophantine equations

Algebraic equations involving only integers are usually called Diophantine equations.

Theorem

Let a, b, c be integers. The equation $ax + by = c$ has integer solution if and only if $gcd(a, b)|c$.

Proof

$\Rightarrow$ Assume that the pair of integers x_0, y_0 is a solution. Then

$$gcd(a, b)|ax_0 + by_0 = c.$$

Diophantine equations

Algebraic equations involving only integers are usually called Diophantine equations.

Theorem

Let a, b, c be integers. The equation $ax + by = c$ has integer solution if and only if $gcd(a, b)|c$.

Proof

$\Leftarrow$ Assume $gcd(a, b)|c$, i.e. there is a $t \in \mathbb{Z}$, such that $gcd(a, b)t = c$. Take $u, v \in \mathbb{Z}$ such that

$$gcd(a, b) = au + bv$$

and multiply by t to get

$$c = t \cdot gcd(a, b) = a(ut) + b(vt).$$

Thus $x = ut$ and $y = vt$ is a solution. $\square$