Week 2, lecture 1: Modular arithmetic

MA180/185/190 Algebra

Angela Carnevale

Introduction to Modular Arithmetic

Modular arithmetic

Applications

Recap & example

Let's find $\gcd(69,35)$

$69 = 35 \cdot 1 + 34$

$35 = 34 \cdot 1 + \underline{\underline{1}}$ The last non-zero remainder is $\gcd(69,35)$

$34 = 1 \cdot 34 + 0$ so $\gcd(69,35) = 1$ They are <u>COPRIME</u>

This helps us find $x, y \in \mathbb{Z}$ such that $69x + 35y = 1$

$$1 = 35 + 34 \cdot (-1)$$

$$= 35 + (69 - 35) \cdot (-1) = 35 + 69 \cdot (-1) + 35 = 69 \cdot \underbrace{(-1)}_{x} + 35 \cdot \underbrace{2}_{y}$$

Applications: linear equations with integer solutions

The formal result is called Bézout's Theorem and tells us the following

Bézout's Theorem

Let a and b be natural numbers. Then there are integers x and y such that

$$ax + by = \gcd(a, b).$$

This tells us that as long as c divides $\gcd(a, b)$, we are able to find a pair of integers x, y satisfying

$$ax + by = c.$$

Our method of back substitution from Euclid's algorithm gives us a practical way to compute one such pair. Let's use this to try and solve one of our initial problems.

Back to one of our challenges

Recall one of our challenges from the first lecture

We buy apples and oranges. Each apple costs 69 cents and each orange costs 35 cents. We spend €2.78. How many apples and how many oranges did we buy?

The problem can be restated more formally as follows: find **non-negative integers** x (the number of apples) and y (the number of oranges) such that

$$69x + 35y = 278.$$

Thanks to the Euclidean algorithm, we found two **integers** that solve the following related equation:

$$69x + 35y = 1,$$

namely $x = -1$ and $y = 2$.

Resolving one of our challenges

Multiplying both sides of the previous identity by 278, we find

$$69 \cdot (-278) + 35 \cdot (2 \cdot 278) = 278.$$

But the numbers of apples and oranges should be non-negative, so we're not quite done…

It's negative!

Linear equations with integer solutions

We will use the following theorem, which was already known to Indian mathematician Brahmagupta around the 7th century:

Theorem (integer solutions to $ax + by = c$)

Let $a, b, c \in \mathbb{N}$. Then the equation

$$ax + by = c$$

has an integer solution (x, y) if and only c is a multiple of $\gcd(a, b)$. If (x_0, y_0) is any particular solution, then all numbers of the form

$$x = x_0 + \frac{bn}{\gcd(a,b)}, \; y = y_0 - \frac{an}{\gcd(a,b)}, \quad n \in \mathbb{Z}$$

are also integer solutions to the same equation.

Linear equations with integer solutions

We can easily verify this result. Our **hypothesis** is that (x_0, y_0) is an integer solution to $ax + by = c$. Let's denote $d = \gcd(a, b)$.

Our **thesis** (to be verified) is that for any integer n, the pair of numbers $x_0 + bn/d$ and $y_0 - an/d$ is also an integer **and** a solution to the same equation.

1. $x_0 + \frac{bn}{d}$ is an integer because $d \mid b$

   $y_0 - \frac{an}{d}$ is an integer because $d \mid a$

2. Is it true that x, y as above are a soln to our eqn?

by hypothesis

$$a\left(x_0 + \frac{bn}{d}\right) + b\left(y_0 - \frac{an}{d}\right) = ax_0 + by_0 + \cancel{\frac{abn}{d}} - \cancel{\frac{abn}{d}} \overset{?}{=} c$$

Solution to our challenge

We can finally solve our problem about apples and oranges. Our equation is

$$69x + 35y = 278,$$

and a first solution is given by $x_0 = -278$ and $y_0 = 556$.

We now apply the previous theorem to find a solution that gives us two positive integers. This solution should be of the form

Recall: $\gcd(69,35)=1$ so we are dividing by 1

$$x = -278 + 35 \cdot n, \quad y = 556 - 69 \cdot n, \text{ for some } n \in \mathbb{Z}.$$

e.g. for $n=1$ $x=-278+35$ and $y=556-69$ are a solution, but x is still negative...

Note that for $n=8$ we get

$x = -278 + 35 \cdot 8 = -278 + 280 = 2$ and $y = 556 - 69 \cdot 8 = 556 - 552 = 4$

How to find positive integer solutions to $ax + by = c$

(1) Does $\gcd(a,b)$ divide c? → If not, there is no such solution.

→ If yes, go to (2)

(2) Use Euclid's algorithm backwards to find x_0', y_0' (not necessarily positive) such that $ax_0' + by_0' = \gcd(a,b)$ (*)

(3) If $c \neq \gcd(a,b)$, multiply (*) on both sides by a suitable number to get x_0, y_0 such that $ax_0 + by_0 = c$

(4) If x_0, y_0 are both positive, we're done. If not, find a suitable $n \in \mathbb{Z}$ such that $x = x_0 + \frac{bn}{\gcd(a,b)}$ and $y = y_0 - \frac{an}{\gcd(a,b)}$ are both positive.

Brief summary

Some takeaways so far:

- Notion of divisibility, greatest common divisor
- Prime numbers, coprime numbers
- **Remainder theorem**
- How to use the Euclidean algorithm to find **gcd**s
- How to use the Euclidean algorithm (backwards) to find an integer solution to $ax + by = \gcd(a, b)$
- Bézout's theorem
- How to find more solutions to $ax + by = c$

Congruences

We can now formalise the concept of "clock arithmetic" or **modular arithmetic**. Its foundation is the Remainder Theorem from last week. We start with the following definition.

Definition

Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$.
We say that "a is **congruent** to b **modulo** m", written

$$a \equiv b \pmod{m}$$

if $a - b$ is an integer multiple of m (equivalently, if $m | (a - b)$). The number m is called the **modulus**.

tells us: we're working on an "m-hour" clock

Congruences

We can now formalise the concept of "clock arithmetic" or **modular arithmetic**. Its foundation is the Remainder Theorem from last week. We start with the following definition.

Definition

Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$.
We say that "a is **congruent** to b **modulo** m", written

$$a \equiv b \pmod{m}$$

if $a - b$ is an integer multiple of m (equivalently, if $m | (a - b)$). The number m is called the **modulus**.

Examples.

- $9 \equiv 4 \pmod{5}$ Indeed, $9-4=5$ is an integer multiple of 5
- $29 \equiv 7 \pmod{11}$ $29-7=22=2 \cdot 11$ ✓
- $69 \equiv 34 \pmod{35}$

Congruences

Note that

- $a \equiv a \pmod{m}$
- if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$
- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

Because the above properties hold, we also say that **congruence modulo** m is an **equivalence relation**[1]**.**

[1] you will see more on equivalence relations in Semester 2.