Lecture 1

Prof. Ginestra Bianconi covering for the Module Organizer
Dr Subajit Jana

General Info

Lecture on Tuesdays 9am - 11am
4pm - 6pm.

Office hours: Support Learning Hours. Tuesdays 1pm - 2pm
MB G27.

Assessment: Two assessed courseworks.

1) Week 6
10%.

2) Week 12
10%

3) Final exam 80%

After the lecture Handwritten notes will be uploaded on QM+
Compare with typed lecture notes.

Main refs. 1) Lecture notes (in QM+)

Additional refs. 1) Higher Arithmetics (Davenport)
2) Introduction to the theory of numbers
(Hardy - Wright).

Motivation

Chapter 0

1) Number theory is one of the oldest subject in the history of mankind

a) Find sol^n in $\mathbb{Q}^2 \ni (x,y)$ so that

$$x^2 + y^2 = 1$$

b) Find sol^n in $\mathbb{Q} \ni x$ so that

$$x^2 = 2$$

Both theses problems are reallyreally old (1000 BC)

2) There are many problems that are so elementary to formulate, but we have no clue on how to solve them.

c) Can you write ~~inctor~~ any even integer $2n$ as a sum of two primes p_1 & p_2 so that

$$2n = p_1 + p_2 \; ? \quad \text{(Goldbach conjecture)}$$

True for all integers $\leq 4 \cdot 10^8$.

3) There are many harmless looking problems that give rise to very deep mathematics.

a) The equation $x^n + y^n = 1$ has infinitely many sol^n $(x,y) \in \mathbb{Q}^2$ if $n = 2$

but has <u>NO</u> solution for $n \geq 3$ (Fermat's last theorem)

This problem is intimately related to

i) Elliptic curves (Azithmetic Geometry)

ii) Langland program (Representation theory)

This problem was solved by Andrew Wiles, Richard Taylor.. (1990-2000) after inventing a lot of new mathematics.

See the lecture notes for other intriguing examples.

Some sample (and spoilers!) of the topics in this module

1) Quadratic reciprocity

Given two integers $a, b \in \mathbb{Z}$ can we find $x \in \mathbb{Z}$ so that

"b divides $a - x^2$" ?

For example $b = 3$ then $a = 22$

$$22 - (1)^2 = 21 \quad \text{divedes } 3.$$

(22 = a, 1 = x)

$a = 21$ " "

$$21 - 0^2 = 21$$

(21 = a, 0^2 = x^2)

but $a = 23$

$23 - x^2$ is NOT divisible by 3 for any x! (check)

What is the general way to answer this sort of question

2) Diophantine approximation

How closely can one "approximate" $\sqrt{2}$ by a rational number?

$$\sqrt{2} = \frac{141421}{100000}$$

also $$\sqrt{2} = \frac{1393}{985}$$

How "good" are these approximations?

How to measure "goodness"?

3) Pell's equation

a) Let p be a prime. Can we always find a sol^n $x, y \in \mathbb{Z}$ so that

$$x^2 - py^2 = 1 \; ?$$

b) What about $p = x^2 + y^2$?

Chapter 1

Notation: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

$\mathbb{N} = \{1, 2, 3, 4, \dots\}$

$\mathbb{Z}$ integers $\mathbb{N}$ natural numbers / positive numbers

\# For $a, b \in \mathbb{Z}$ we write $b \mid a$ if and only if

$$a = qb \quad \text{for some} \quad q \in \mathbb{Z}.$$

Euclid's algorithm

Given a pair $a, b \in \mathbb{Z}$ with $b > 0$ there exist a unique pair $r, q \in \mathbb{Z}$ with $0 \le r < b$ such that

$$a = qb + r$$

q is usually called the "quotient"

r is usually called the "remider" or "residue"

If $r = 0 \implies a = qb$ then $b \mid a$.

Examples : 1) $a = 12$

$b = 2$

$12 = 6 \times 2 + 0$ $\quad 2 \mid 12$

$a \quad q \quad b \quad r$

$0 \le r < b = 2$

2) $a = -25$

$b = 11$

You might guess $-25 = -2 \times 11 + (-3)$ but ~~$r < 0$~~ $r < 0$

$a \quad q \quad b \quad r$

$-25 = (-3) \times 11 + 8$ $\quad 0 \le r = 8 < 11 = b$

"Proof of Euclid's algorithm" (Non-examinable)

Given $a, b \in \mathbb{Z}$ with $b > 0$ there exist a unique pair $r, q \in \mathbb{Z}$ with $0 \leq r < b$ such that

$$a = qb + r$$

Exist

Consider $S = \{ a + zb \mid z \in \mathbb{Z},\ a + zb \geq 0 \}$

$S \neq \phi$: Choose $z \in \mathbb{Z}$ such that $z \geq -\frac{a}{b}$ $\Rightarrow$ S has a minimal element

Call that $r \geq 0$

So $\exists z = z^*$ s.t. $r = a + z^* b$ call $z^* = -q \in \mathbb{Z}$

$r = a - qb$

$\Rightarrow$ $a = qb + r$ $\quad r \geq 0$

Let us show that $r < b$ as well.

If $r \geq b$ then

$$0 \leq r - b = \underbrace{a - qb}_{= r} - b = a - (q+1)b < a - qb = r$$

$\Rightarrow$ Contradicts the minimality of r.

$0 \leq r < b$. $\Rightarrow$ There exist at least a pair $r, q \in \mathbb{Z}$ s.t. $a = qb + r$. with $0 \leq r < b$

Uniqueness Let $a = qb + r = q'b + r'$ $\quad 0 \le r < b$, $0 \le r' < b$

By minimality $0 \le r \le r'$ $\quad r' \in S$

$\Rightarrow r' - r = (q - q')b \ge 0$ $\quad \Rightarrow q - q' \ge 0$

If $q > q'$

$r' = r + (q - q')b \ge b$ $\Rightarrow$ Contradiction

If $q = q'$ we get trivially

$r' = r$

$\Rightarrow$ The pair $r, q \in \mathbb{Z}$ with $0 \le r < b$ s.t. $a = qb + r$

is <u>unique</u>

Exercise : Prove that

$$GCD(a,b) = GCD(-a,b) = GCD(a,-b) = GCD(-a,-b).$$

What is the $d = GCD(n,0)$? with $n \neq 0$

$d \mid 0$ if $0 = qd$ $q \in \mathbb{Z}$ $\Rightarrow q = 0$

$d \mid n$ if $n = q'd$ $q' \in \mathbb{Z}$

$\boxed{GCD(n,0) = n}$

This theorem helps reducing the "complexity" of $GCD(a,b)$

Lemma Let $a = qb + r$, $0 \leq r < b$

the $GCD(a,b) = GCD(b,r)$

Proof Let $d : GCD(a,b)$ $e : GCD(b,r)$

$d \mid a$ & $d \mid b$ $\Rightarrow d \mid a - qb = r$

$\Rightarrow d \mid b$ & $d \mid r$ $\Rightarrow d \leq e$

$e \mid b$ & $e \mid r$ $\Rightarrow e \mid a = qb + r$

$\Rightarrow e \mid a$ & $e \mid b$ $\Rightarrow e \leq d$

$\boxed{d = e}$

□

Examples

$GCD(99, 72) =$

$= GCD(27, 72)$

$= GCD(27, 18)$

$= GCD(9, 18)$

$= 9$

$99 = 72 \cdot 1 + 27$

~~$72 = 27 \cdot 4 + 45$~~

$72 = 27 \cdot 2 + 18$

$27 = 18 \cdot 1 + 9$

$18 = 9 \cdot 2$

$GCD(123, 87)$

$= GCD(36, 87)$

$= GCD(36, 15)$

$= GCD(6, 15)$

$= GCD(6, 3) = 3$

$123 = 87 \cdot 1 + 36$

$87 = 36 \cdot (2) + 15$

$36 = 15 \cdot (2) + 6$

$15 = 6 \cdot 2 + 3$

Proposition 2 Bezout's identity

Let $a, b \in \mathbb{Z}$ then there exist $r, s \in \mathbb{Z}$ such that

$$ar + bs = GCD(a, b)$$

Example 1) $GCD(6,5) = 1$

$GCD(6,5) = GCD(1,5) = 1$

$6 = 5 \cdot 1 + 1$

$1 = 6 \cdot 1 + 5(-1)$

$a \quad b$

$r = 1$

$s = -1$

2) $GCD(12,20) =$

$= GCD(12,8)$

$= GCD(4,8) = 4$

$20 = 12 \cdot 1 + 8$

$12 = 8 \cdot 1 + 4$

$4 = 12 - 8 \cdot 1$

$= 12 - (20 - 12)$

$= 12 \times 2 + 20(-1) = GCD(a,b)$

$a \quad r \quad b \quad s$