Math 414: Number Theory.

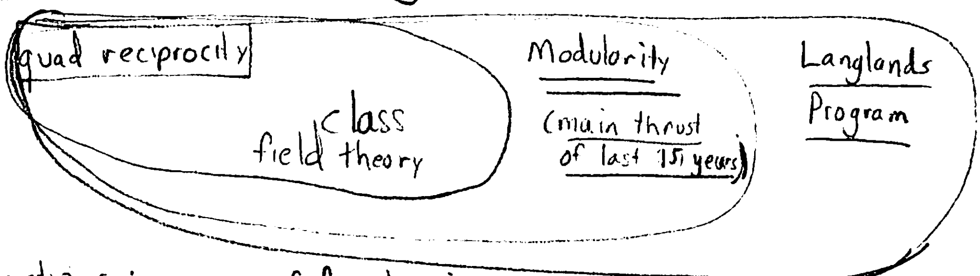
Lecture 1: Prime Factorization

1. Handout Syllabus and go over it, (~10 min)
wave around [my book], mention topics. Questions.

2. Course Overview

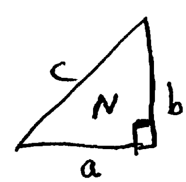
Main Topics of Course:

- Prime numbers: factorization, distribution (Riemann Hypothesis)
  - most famous and central unsolved problem in math?
  - Please read "What ... "
- Modular arithmetic: foundation of cryptography
- Quadratic Reciprocity: deep surprising theorem;



- Continued Fractions: powerful algorithmic tool; makes some computations surprisingly easy:
  - e.g. × write $p = a^2 + b^2$ (p prime)
  - × find "best" rational approx. to 3.1415
- Elliptic Curves:
  - central to solving equations
  - Birch & Swinnerton-Dyer Conjecture: Clay Problem
  - Congruent number problem: oldest unsolved problem in math...

(976)
Problem: Is there an algorithm that determines whether or not an integer N is the area of a rational right triangle?

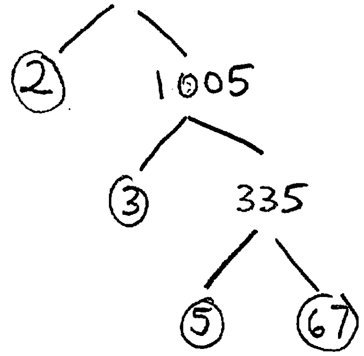


$a, b, c \in \mathbb{Q}$
fractions.

- Algorithm for factoring integers.

3. Prime Factorization

$2010 = 2\times 3\times 5\times 67$



Natural numbers:

$\mathbb{N} = \{1,2,3,\ldots\}$

Integers

$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$

Defn: $a,b \in \mathbb{Z}$ a divides b if there exists $c\in\mathbb{Z}$ with $ac=b$.

$2 \mid 6$ since $2\times 3=6$

$3 \nmid 7$ "does not divide"

Defn: $n>1$ is prime if its only positive divisors are $1, n$.

otherwise, n is composite.

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ..., 97

"if you like to memorize, this is a useful list of numbers to memorize".

Theorem ("Fundamental Theorem of Arithmetic"):

Every $n \in \mathbb{N}$ can be written uniquely as a product of primes.

Our main goal: Prove this.

Theorem: Every $n \in \mathbb{N}$ can be written as a product of primes.

Proof: We proceed by induction.

Case $n=1$: $n =$ empty product.

(also as sanity check case $n=2, 3, 4=2\times 2, 5, 6=2\times 3, \ldots$ etc. holds)

Case $n>1$: Suppose theorem true for all $m<n$.

If n is prime, done.

If n not prime, there is a divisor $b \mid n$ so $bc=n$.

By induction b, c are products of primes so $n=bc$ is also. ◻

But what about uniqueness? This is much harder. Why?

Consider: $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a,b\in\mathbb{Z}\}$

6 factors in two different ways:

$$6 = 2\times 3 = (1+\sqrt{-5})\times(1-\sqrt{-5}) \qquad !!!$$

Plan: Use Euclidean algorithm to prove

(*) $\boxed{p \mid ab \Rightarrow p \mid a \text{ or } p \mid b}$. ← seems obvious, but is not.

Then use this to cancel from both sides to get uniqueness:

$$p_1 p_2 \cdots p_r = n = q_1 q_2 \cdots q_s.$$

To prove (*) we introduce gcd:

Defn: $a,b\in\mathbb{Z}$. $\gcd(a,b) = \begin{cases} \max\{d\in\mathbb{Z} : d\mid a \text{ and } d\mid b\}, \\ 0 \text{ if } a=b=0. \end{cases}$

Examples: $\gcd(12,27)=3$, $\gcd(0,0)=0$,
$\gcd(6,35)=1$, $\gcd(-24,100)=4$, ($-24 = -8\cdot 3$, $100 = 4\cdot 25$)
$\gcd(0,10)=10$, $\gcd(-12,-27)=3$.

compute by factoring. — slow when numbers big!

Lemma: $\gcd(a,b) = \gcd(b,a) = \gcd(\pm a, \pm b) = \gcd(a, b-a) = \gcd(a, b+a)$

Proof: For class only prove $\gcd(a,b) = \gcd(a, b-a)$:

If $d \mid a$ and $d \mid b$ then $dc_1 = a$, $dc_2 = b$ so $b-a = dc_2 - dc_1 = d(c_2 - c_1)$.
Thus $d \mid a$ and $d \mid b-a$.

If $d \mid a$ and $d \mid b-a$ then $dc_1 = a$ and $dc_2 = b-a$ so

$$b = b-a+a = dc_2 + dc_1 = d(c_2+c_1)$$

so $d \mid a$ and $d \mid b$.

So (same sets)

$$\gcd(a,b) = \max\{d : d \mid a \text{ and } d \mid b\} = \max\{d : d \mid a \text{ and } d \mid b-a\} = \gcd(a, b-a)$$

$\blacksquare$

Lemma: Suppose $a, b, n \in \mathbb{Z}$.

$$\gcd(a,b) = \gcd(a, b-na)$$

Proof: $\gcd(a,b) = \underbrace{\gcd(a, b-a) = \cdots}_{n \text{ times}} = \gcd(a, b-na)$

Recall: Long Division.

Given integers $a, b \in \mathbb{Z}$ there exists unique q, r with

$$\boxed{a = bq + r, \quad 0 \le r < |b|}.$$

Proof:
- A nice inductive argument — see Prop 1.1.11 in book.
- Algorithm — grade school long division

```
    143 R4
 7 )1005
    7
    30
    28
     25
     21
      4
```

so $\boxed{1005 = 7 \cdot 143 + 4}$

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

Finish proof next time ...