18.781 - Theory of Numbers, Spring 2012

Massachusetts Institute of Technology

taught by Prof. Abhinav Kumar

Lecture 1
Introduction, Diophantine Equations, Divisibility, GCD

Introduction - First, what is number theory? At the most basic level, it's the study of the properties of the integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ or the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$. A few reasons to study number theory:

1. In some ways the most basic piece of mathematics, for you can build everything else from natural numbers.

$$\mathbb{N} \xrightarrow{\text{negation}} \mathbb{Z} \xrightarrow{\text{division}} \mathbb{Q} \xrightarrow{\text{real analysis, Dedekind cuts}} \mathbb{R} \xrightarrow{\sqrt{-1}} \mathbb{C}$$

   From there you can get to calculus, topology, etc.

   > God made the integers, all the rest is the work of man.
   >
   > –Leopold Kronecker (1823-1891)

2. Some of the most elegant mathematics!

   > Mathematics is the queen of sciences and number theory is the queen of mathematics. She often condescends to render service to astronomy and other natural sciences, but in all relations she is entitled to the first rank.
   >
   > –Carl Friedrich Gauss (1777-1855)

   Number theory uses techniques from algebra, analysis, geometry and topology, logic and computer science, and often drives development in these fields.

3. Has some great applications - eg., RSA public key cryptography, construction of expander graphs, coding theory, etc.
4. It's a great place to learn how to read and write proofs
5. It's a rich source of conjecture which are easy to state and VERY hard to prove

Diophantine Equations - Given some equation, look for integer solutions.

Eg. The Pythagorean Theorem

$$a^2 + b^2 = c^2$$

results in triples (3, 4, 5), (5, 12, 13), (7, 24, 25), (8, 15, 17), etc. This can also be generalized to Fermat's Last Theorem,

$$a^n + b^n = c^n$$

or to the open question of the existence of a perfect cuboid, where $a^2 + b^2 + c^2, a^2 + b^2, a^2 + c^2$, and $b^2 + c^2$ are all squares, with integer a, b, c.

Basic Properties of $\mathbb{N}$

1. **Successor Operation** - Fundamental operation for natural numbers:

$$s(n) = n + 1$$

   - Addition then becomes repeated applications of successor, multiplication is repeated addition

2. **Principle of Mathematical Induction (PMI)** - For property $p(n)$ true or false, if 1. $p(1)$ true and 2. "$p(n) \Rightarrow p(n+1)$", then $p(n)$ true for all natural numbers
3. **Well Ordering Principle (WOP)** - Every nonempty subset of natural numbers has a smallest element

   - PMI and WOP are equivalent - each follows from the other

4. **Divisibility** - Say $a|b$ if $b = ax$ for $a, b, x \in \mathbb{Z}$ and $a \neq 0$
   (a) $\forall\, n \in \mathbb{N}, n|0$
   (b) $a|b, b|c \implies a|c$
   (c) $a|b, a|c \implies a|bx + cy \,\forall\, x, y \in \mathbb{Z}$

Theorem 1 (Division with Remainder)**.** *Given $a, b \in \mathbb{Z}$ with $a > 0$, $\exists\, q, r \in \mathbb{Z}$ such that $b = aq + r, 0 \leq r < a$*

Proof. Let set $S = \{b + ka : k \in \mathbb{Z}, b + ka \geq 0\}$.

$$S \text{ is nonempty: } \begin{cases} b > 0 & \text{then } b + 0a \in S \\ b < 0 & \text{then adding } a \text{ enough times makes it positive} \end{cases}$$

We can make this rigorous by another application of WOP - since S is nonempty, it has a smallest element $r = b + ka$ for some k. Setting $q = -k$ results in $r = b - qa$. $r \geq 0$ because its in S, and $r < a$ because if not, then $b + (k-1)a$ would be smallest element in S instead ($\lightning$). ■

Note: $a|b$ iff $r = 0$

(Definition): If a and b are not both 0, then $\gcd(a, b)$ or (a, b) is the **greatest common divisor** of a and b

Theorem 2. *Let $g = (a, b)$. Then $\exists\, v_0, y_0 \in \mathbb{Z}$ such that $g = ax_0 + by_0$.*

Proof. Let set $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$, and assume a, b not both 0.

$$S \text{ is nonempty (wlog, assume } a \neq 0\text{): } \begin{cases} a > 0, a \in S \\ a < 0, -a \in S \end{cases}$$

Since S is nonempty, it has a smallest element $g = ax + by$. To prove theorem, show that $g|a,\ g|b$, and g is largest common divisor (if another common divisor d, then $d|g$).

$g|a$ ***by contradiction (assume*** $g \nmid a$***).***

$$\begin{aligned} a &= gq + r, 0 < r < g \\ r &= a - gq \\ &= a - q(ax + by) \\ &= a(1 - qx) - b(qy) \\ &\Rightarrow r \in S, \text{ but } r < g, \text{ so } g \text{ isn't smallest } \lightning \end{aligned}$$

g ***is largest common.*** If $d|a$ and $d|b$, then $d|ax + by = g$

Since $g|a,\ g|b$, and g is largest common divisor, then g is gcd of a, b. ■

(Definition) Co-Prime, Relatively Prime: If $(a, b) = 1$, then a and b are **co-prime**, or **relatively prime**.

Corollary 3. *If* $(a, m) = 1$ *and* $(b, m) = 1$*, then* $(ab, m) = 1$

Proof.

$$\begin{aligned} 1 &= ax + my, ax = 1 - my \\ 1 &= bx' + my', bx' = 1 - my' \\ abxx' &= (1 - my)(1 - my') \\ &= 1 - my - my' + m^2yy' \\ &= 1 + m(-y - y' + myy') \\ 1 &= ab(xx') + m(y + y' - myy') \end{aligned}$$

■

Corollary 4. *If* $c|ab$ *and* $(c, a) = 1$*, then* $c|b$

Proof.

$$\begin{aligned} (a, c) = 1 &\Rightarrow 1 = ax + cy \\ &\Rightarrow b = abx + bcy \\ c|ab,\ c|bc &\Rightarrow c|(abx + bcy) = b \end{aligned}$$

■

18.781 Theory of Numbers
Spring 2012