MAT246: Concepts in Abstract Mathematics:
Lecture 0101 Notes

Tianyu Du

September 20, 2018

Contents

1 Lecture 1 Sep. 7 2018

Definition 1.1. Let $\mathbb{N} := \{1, 2, 3, \dots\}$ be the set of **natural numbers**.

Theorem 1.1 (Principle of Mathematical Induction)**.** Suppose S is a set of natural numbers, $S \subseteq \mathbb{N}$. If

1. $1 \in S$
2. $k \in S \implies k + 1 \in S, \ \forall k \in \mathbb{N}$

then, $S = \mathbb{N}$

Example 1.1. Show that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \ \forall n \in \mathbb{N}$$

Proof. ■

2 Lecture 2 Sep. 10 2018

Theorem 2.1 (Extended Principle of Mathematical Induction)**.** Suppose set $S \subseteq \mathbb{N}$ and let $n_0 \in \mathbb{N}$ fixed, if

1. $n_0 \in S$
2. $\forall k \geq n_0, k \in S \implies k + 1 \in S$

then $\{n_0, n_0 + 1, n_0 + 2, \dots\} \subseteq S$

Example 2.1. Show that

$$n! \geq 3^n \ \forall n \geq 7$$

Proof. ■

Theorem 2.2 (Well-Ordering Principle)**.** Every non-empty subset of natural number has a smallest element.

Proof. (Principle of Mathematical Induction)
Let $S \subseteq \mathbb{N}$
Suppose $1 \in S \wedge (k \in S \implies k + 1 \in S, \forall k \in \mathbb{N})$
Show: $S = \mathbb{N}$
Let $T = \mathbb{N} \backslash S$

Suppose $T \neq \emptyset$
By Well-Ordering Principle, there exists a smallest element of T, denoted as $t_0 \in \mathbb{N}$.
Since $1 \in S$, therefore $t_0 \neq 1$.
Therefore $t_0 > 2$.
Thus $t_0 - 1 \in \mathbb{N}$ and since $t_0 = \min T$, $t_0 - 1 \notin T$
Therefore $t_0 - 1 \in S$, then, $t_0 - 1 + 1 = t_0 \in S$,
Contradict the assumption that $t_0 \in T$.
Thus $T = \emptyset$ and $S = \mathbb{N}$.

■

Remark 2.1. We can use principle of Mathematical Induction to prove Well-Ordering Principle as well.

3 Lecture 3 Sep. 12 2018

Definition 3.1. Let $a, b \in \mathbb{N}$ and a **divides** b, written as $a|b$ if

$$\exists c \in \mathbb{N} \ s.t. \ b = ac$$

And a is a **divisor** of b.

Definition 3.2. A natural number p (except 1) is called **prime** if the only divisors of p are 1 and p.

Lemma 3.1 (Prime numbers are building blocks of natural numbers)**.** Every natural number other than 1 is a *product*[1] of prime numbers.

Theorem 3.1 (Principle of Complete Induction)**.** Suppose $S \subseteq \mathbb{N}$ and if

1. $n_0 \in S$
2. $n_0, n_0 + 1, \ldots, k \in S \implies k + 1 \in S, \ \forall k \geq n_0$

then

$$\{n_0, n_0 + 1, \ldots\} \subseteq S$$

Proof of Lemma. Let $S \subseteq \mathbb{N}$ for which the lemma is true,
Want to show: $S = \mathbb{N} \backslash \{1\}$
(Base Case) For 2 it's a product of prime. Thus $2 \in S$
(Inductive Step) Suppose $\{2, 3, \ldots k\} \subseteq S$

[1]Product could mean the product of a single number.

Consider $k+1$, if $k+1$ is a prime then $k+1$ can be written as a product of itself, as a product of one single prime.
Else, if $k+1$ is not a prime, then $\exists 1 < m, n < k+1$ $s.t.$ $k+1 = mn$.
By induction hypothesis of strong induction, m, n can both be written as product of primes.
$m = \prod_{i=1}^{\ell} p_i,\ n = \prod_{i=1}^{t} q_i$ where p_i, q_i are all primes.
and $k+1 = \prod_{i=1}^{t} q_i \prod_{i=1}^{\ell} p_i$
thus $k+1 \in S$
by principle of strong induction, $\{2, 3, \ldots, \} \subseteq S$. ■

Theorem 3.2. There is no largest prime number.

Proof. (By contradiction)
Assume there is a largest prime p,
then $\{2, 3, 5, \cdots, p\}$ is the set of all primes
Let $M := (2 * 3 * 5 * \cdots * p) + 1 \in \mathbb{N}$
M is either prime or not.
Suppose M is not a prime, then by Lemma 3.1, $\exists p'$ dividing M.
Obviously $\forall i \in \{2 * 3 * 5 * \cdots * p\},\ i \not| M$.
There is no prime dividing M, which contradict Lemma 3.1
Thus M is a prime, and $M > p$, which contradicts assumption
Therefore there is no largest prime. ■

4 Lecture 4 Sep. 14 2018

Theorem 4.1 (the Fundamental Theorem of Arithmetic)**.** Every natural (except 1) is a product of prime(s), and the prime(s) in the product are unique including multiplicity except for the order.

Proof. We have already proven that the existential parts of this theorem in Lemma 3.1.
(Proof for the uniqueness part) Suppose there exists natural number (not 1) has 2 different prime factorizations.
By well ordering principle, there is a smallest n, which has two distinct prime factorizations.
Say $n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_\ell$ where p_i, q_i are all primes.
Notice that $p_i \neq q_j$ for any combination of (i, j) since if so $\frac{n}{p_i} = \frac{n}{q_j}$ is a natural number smaller than n having 2 distinct prime factorization, which contradicts our assumption above.
Specifically, $p_1 \neq q_1$.

(Case 1: $p_1 < q_1$)
Let $m := n - p_1 q_2 \dots q_\ell \in \mathbb{N}$
Notice $m = p_1(p_2 p_3 \dots p_k - q_2 q_3 \dots q_\ell)$
Also $m = (q_1 - p_1)(q_2 q_3 \dots q_\ell)$
$\implies m = p_1 \dots p_k = q_2 q_3 \dots q_\ell (q_1 - p_1)$
$\implies p_1 | m$ also notices that $p_1 \not| \, q_2 q_3 \dots q_\ell$
$\implies p_1 | (q_1 - p_1) \implies p_1 | q_1 \implies p_1 = q_1$
Contradicts the assumption that $p_q < q_1$
The other case goes a similar proof. ■

Definition 4.1. A natural number n is called **composite** if it's not 1 or a prime number.

Remark 4.1. Natural numbers are partitioned into 3 categories, 1, prime and composite numbers.

Example 4.1. Find 20 consecutive composite numbers.

$$(21!) + 2, (21!) + 3, \dots, (21!) + 21$$

Example 4.2. Find k consecutive composite numbers.

$$(k + 1!) + 2, (k + 1)! + 3, \dots, (k + 1!) + k + 1$$

5 Lecture 5 Sep. 17 2018

Definition 5.1. Let $a, b \in \mathbb{Z}$, and let $m \in \mathbb{N}$. If $m | a - b$ then we say "a and b are congruent modulo m"

Remark 5.1. Regular Induction $\iff$ Complete Induction $\iff$ Well-Ordering Principle

Proof. (WTS: Complete Induction $\implies$ Well-Ordering Principle)
Let $S \subseteq \mathbb{N}$ and $S \neq \emptyset$
(WTS, S has the smallest element)
Assume S does not have the smallest element.
Let $T := S^c$
Clearly $1 \in T$ (prop 1)
Since other wise 1 could be the smallest element of S.
Let $k \in \mathbb{N}$.
Suppose $1, 2, 3, \dots, k \in T$, if $k + 1 \notin T$, then $k + 1 \in S$ and $k + 1$ becomes the smallest element of S and contradicts our assumption above.

Therefore $1, 2, 3, \dots k \in T \implies k+1 \in T$.
By principle of strong induction, $T = \mathbb{N}$.
Thus, $S = \emptyset$, and contradicts our definition of S.
Therefore $\forall S \subseteq \mathbb{N}$ *s.t.* $S \neq \emptyset$, S has the smallest element (Well-Ordering Principle). ∎

Example 5.1 (Application 2)**.** Is $2^{29} + 3$ divisible by 7?

Solution. Notice $2^2 \equiv 4 \mod 7$ and $2^3 \equiv 1 \mod 7$.
$\implies (2^3)^9 \equiv 1^9 \mod 7$
$\implies 2^{27} \equiv 1 \mod 7$
$\implies 2^{29} \equiv 4 \mod 7$
Also $3 \equiv 3 \mod 7$
$\implies 2^{29} + 3 \equiv 4 + 3 \mod 7$
$\implies 2^{29} + 3 \equiv 7 \mod 7$
$\implies 7 | 2^{29} + 3$. ∎

Theorem 5.1 (Rules on computing congruence)**.** Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

1. $a \equiv b \mod m \land c \equiv d \mod m \implies a + c \equiv b + d \mod m$
2. $a \equiv b \mod m \land c \equiv d \mod m \implies ac \equiv bd \mod m$

Proof. Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$,
suppose $a \equiv b \mod m \land c \equiv d \mod m$
by definition of congruence, $\exists p, q \in \mathbb{Z}$ *s.t.* $(a - b) = pm \land (c - d) = qm$
$\implies (a + c - b - d) = (p + q)m, \ (p + q) \in \mathbb{Z}$
$\implies a + c \equiv b + d \mod m$
And $a = b + pm \land c = d + qm$
$ac - bd = (b + pm)(d + qm) - bd$
$= bd + dpm + qbm + pqm^2 - bd$
$= (dp + qb + pqm)m$
$\implies m | ac - bd$
$\implies ac \equiv bd \mod m$ ∎

Proposition 5.1 (Corollary from theorem 5.1)**.**

$$a \equiv b \mod m \implies a + c \equiv b + c \mod m$$

and

$$a \equiv b \mod m \implies a^k \equiv b^k \mod m, \ \forall k \in \mathbb{Z}_{\geq 0}$$

6 Lecture 6 Sep. 19 2018

Theorem 6.1. Let $a, b \in \mathbb{Z}$,

$$a = b \implies a \equiv b \mod m \; \forall m \in \mathbb{N}$$

Example 6.1. What is the reminder when $3^{202} + 5^9$ is divided by 8

Solution. Notice $3^2 \equiv 1 \mod 8$
Therefore, $(3^2)^{101} \equiv 1^{101} \mod 8$
That's, $3^{202} \equiv 1 \mod 8$
Also $5^2 \equiv 1 \mod 8$
$\implies (5^2)^4 \equiv 1^4 \mod 8$
$\implies 5^9 \equiv 5 \mod 8$
$\implies 3^{202} + 5^9 \equiv 5 + 1 \mod 8$
$\implies$ the reminder is 6.
(Notice that $3^{202} + 5^9 \equiv 6 \equiv 14 \equiv 22 \equiv \dots \mod 8$, and the reminder is the smallest integer satisfying above relation.) ■

Theorem 6.2. Let $M \in \mathbb{Z}$ and $M = d_N \dots d_2 d_1 d_0,\; d_i \in \{0, 1, \dots, 9\}$ [2], then

$$3|M \iff 3 \mid \sum_{i=0}^{N} d_i$$

Proof. Notice $10 \equiv 1 \mod 3$, $100 \equiv 1 \mod 3$ and so on,
(Fact) $10^k \equiv 1 \mod 3,\; \forall k \in \mathbb{Z}_{\geq 0}$
Then $d_i 10^i \equiv d_i \mod 3,\; \forall i$
Therefore, $\sum_{i=0}^{N} 10^i d_i \equiv \sum_{i=0}^{N} d_i \mod 3$
Therefore $\sum_{i=0}^{N} 10^i d_i \equiv 0 \mod 3 \iff \sum_{i=0}^{N} d_i \equiv 0 \mod 3$

■

Theorem 6.3. Let $M \in \mathbb{Z}$ and $M = d_N \dots d_2 d_1 d_0,\; d_i \in \{0, 1, \dots, 9\}$, then

$$11|M \iff 11 \mid \sum_{i=0}^{N} (-1)^i d_i$$

Proof. Notice $10^i \equiv (-1)^i \mod 11$
Therefore $10^i d_i \equiv (-1)^i d_i$
Thus, $\sum_{i=0}^{N} 10^i d_i \equiv \sum_{i=0}^{N} (-1)^i d_i \mod 11$
Then, $\sum_{i=0}^{N} 10^i d_i \equiv 0 \mod 11 \iff \sum_{i=0}^{N} (-1)^i d_i \equiv 0 \mod 11$

■

[2] This means the integer M is constructed from digits d_i. For example, $M = 256$, then $d_0 = 6, d_1 = 5, d_2 = 2$