

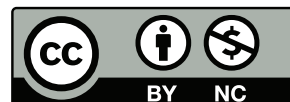
# MAT246: Concepts in Abstract Mathematics:

Lecture 0101 Notes

Tianyu Du

October 2, 2018

This work is licensed under a Creative Commons  
“Attribution-NonCommercial 4.0 International” li-  
cense.



## Contents

<b>1</b>	<b>Lecture 1 Sep. 7 2018</b>	<b>2</b>
<b>2</b>	<b>Lecture 2 Sep. 10 2018</b>	<b>2</b>
<b>3</b>	<b>Lecture 3 Sep. 12 2018</b>	<b>3</b>
<b>4</b>	<b>Lecture 4 Sep. 14 2018</b>	<b>4</b>
<b>5</b>	<b>Lecture 5 Sep. 17 2018</b>	<b>5</b>
<b>6</b>	<b>Lecture 6 Sep. 19 2018</b>	<b>7</b>
<b>7</b>	<b>Lecture 7 Sep. 21 2018</b>	<b>8</b>
<b>8</b>	<b>Lecture 8 Sep. 24 2018</b>	<b>9</b>
<b>9</b>	<b>Lecture 9 Sep. 26 2018</b>	<b>11</b>
<b>10</b>	<b>Lecture 10 Sep. 28 2018</b>	<b>13</b>
<b>11</b>	<b>Lecture 11 Oct. 2 2018</b>	<b>15</b>
	11.1 Rational and Irrational Numbers . . . . .	15

## 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

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

*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

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

*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  $T = \mathbb{N} \setminus S$

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

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

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*<sup>1</sup> of prime numbers.

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

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

then

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

*Proof of Lemma.* Let  $S \subseteq \mathbb{N}$  for which the lemma is true,

Want to show:  $S = \mathbb{N} \setminus \{1\}$

(Base Case) For 2 it's a product of prime. Thus  $2 \in S$

(Inductive Step) Suppose  $\{2, 3, \dots, k\} \subseteq S$

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.

---

<sup>1</sup>Product could mean the product of a single number.

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,  $\{2, 3, \dots\} \subseteq S$ . ■

**Theorem 3.2.** There is no largest prime number.

*Proof.* (By contradiction)

Assume there is a largest prime  $p$ ,

then  $\{2, 3, 5, \dots, p\}$  is the set of all primes

Let  $M := (2 * 3 * 5 * \dots * p) + 1 \in \mathbb{N}$

$M$  is either prime or not.

Suppose  $M$  is not a prime, then by Lemma 3.1,  $\exists p'$  dividing  $M$ .

Obviously  $\forall i \in \{2 * 3 * 5 * \dots * p\}$ ,  $i \nmid M$ .

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  $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_{\ell}$  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  $m = p_1(p_2p_3 \dots p_k - q_2q_3 \dots q_\ell)$   
 Also  $m = (q_1 - p_1)(q_2q_3 \dots q_\ell)$   
 $\implies m = p_1 \dots p_k = q_2q_3 \dots q_\ell(q_1 - p_1)$   
 $\implies p_1 | m$  also notices that  $p_1 \nmid q_2q_3 \dots q_\ell$   
 $\implies p_1 | (q_1 - p_1) \implies p_1 | q_1 \implies p_1 = q_1$   
 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  $2^2 \equiv 4 \pmod{7}$  and  $2^3 \equiv 1 \pmod{7}$ .

$$\implies (2^3)^9 \equiv 1^9 \pmod{7}$$

$$\implies 2^{27} \equiv 1 \pmod{7}$$

$$\implies 2^{29} \equiv 4 \pmod{7}$$

$$\text{Also } 3 \equiv 3 \pmod{7}$$

$$\implies 2^{29} + 3 \equiv 4 + 3 \pmod{7}$$

$$\implies 2^{29} + 3 \equiv 7 \pmod{7}$$

$$\implies 7 | 2^{29} + 3. \quad \blacksquare$$

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

$$1. a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}$$

$$2. a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$$

*Proof.* Let  $a, b, c, d \in \mathbb{Z}$  and  $m \in \mathbb{N}$ ,

suppose  $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$

by definition of congruence,  $\exists p, q \in \mathbb{Z}$  s.t.  $(a - b) = pm \wedge (c - d) = qm$

$$\implies (a + c - b - d) = (p + q)m, (p + q) \in \mathbb{Z}$$

$$\implies a + c \equiv b + d \pmod{m}$$

$$\text{And } a = b + pm \wedge c = d + qm$$

$$ac - bd = (b + pm)(d + qm) - bd$$

$$= bd + dpm + qbm + pqm^2 - bd$$

$$= (dp + qb + pqm)m$$

$$\implies m | ac - bd$$

$$\implies ac \equiv bd \pmod{m} \quad \blacksquare$$

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

$$a \equiv b \pmod{m} \implies a + c \equiv b + c \pmod{m}$$

and

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

## 6 Lecture 6 Sep. 19 2018

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

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

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

*Solution.* Notice  $3^2 \equiv 1 \pmod{8}$

Therefore,  $(3^2)^{101} \equiv 1^{101} \pmod{8}$

That's,  $3^{202} \equiv 1 \pmod{8}$

Also  $5^2 \equiv 1 \pmod{8}$

$\implies (5^2)^4 \equiv 1^4 \pmod{8}$

$\implies 5^9 \equiv 5 \pmod{8}$

$\implies 3^{202} + 5^9 \equiv 1 + 5 \pmod{8}$

$\implies$  the remainder is 6.

(Notice that  $3^{202} + 5^9 \equiv 6 \equiv 14 \equiv 22 \equiv \dots \pmod{8}$ , and the remainder is the smallest integer satisfying above relation.) ■

**Theorem 6.2.** Let  $M \in \mathbb{Z}$  and  $M = d_N \dots d_2 d_1 d_0$ ,  $d_i \in \{0, 1, \dots, 9\}$ <sup>2</sup>, then

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

*Proof.* Notice  $10 \equiv 1 \pmod{3}$ ,  $100 \equiv 1 \pmod{3}$  and so on,

(Fact)  $10^k \equiv 1 \pmod{3}$ ,  $\forall k \in \mathbb{Z}_{\geq 0}$

Then  $d_i 10^i \equiv d_i \pmod{3}$ ,  $\forall i$

Therefore,  $\sum_{i=0}^N 10^i d_i \equiv \sum_{i=0}^N d_i \pmod{3}$

Therefore  $\sum_{i=0}^N 10^i d_i \equiv 0 \pmod{3} \iff \sum_{i=0}^N d_i \equiv 0 \pmod{3}$  ■

**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  $10^i \equiv (-1)^i \pmod{11}$

Therefore  $10^i d_i \equiv (-1)^i d_i$

Thus,  $\sum_{i=0}^N 10^i d_i \equiv \sum_{i=0}^N (-1)^i d_i \pmod{11}$

Then,  $\sum_{i=0}^N 10^i d_i \equiv 0 \pmod{11} \iff \sum_{i=0}^N (-1)^i d_i \equiv 0 \pmod{11}$  ■

---

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

## 7 Lecture 7 Sep. 21 2018

**Theorem 7.1.** Suppose  $p$  is a prime and  $a, b \in \mathbb{N}$ , if  $p|ab$  then  $p|a \vee p|b$ .

*Proof.* If  $a = 1 \vee b = 1$ , then done. And for the case  $a = b = 1$ , the proposition is vacuously true.

Let  $a, b > 1$ ,

By the fundamental theorem of arithmetic, we can write  $a, b$  as their unique prime factorization

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \alpha_j \geq 1 \text{ and } b = q_1^{\beta_1} \dots q_\ell^{\beta_\ell}, \beta_j \geq 1$$

then  $ab = p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_\ell^{\beta_\ell}$  is the unique prime factorization of  $ab$ .

Since  $p \in \mathbb{P}$ , therefore,  $p = p_j \vee p = q_j \implies p|a \vee p|b$

■

**Remark 7.1.** We have shown that  $a \equiv b \pmod{m} \implies ca \equiv cb \pmod{m}$ . But notice that

$$ca \equiv cb \pmod{m} \not\Rightarrow a \equiv b \pmod{m}$$

**Definition 7.1.** Let  $a, b \in \mathbb{Z}$ , then we say  $a$  and  $b$  are **relatively prime** if they have no prime factor in common.

**Theorem 7.2.** Suppose  $p$  is a prime and  $a \in \mathbb{Z}$  and  $p \nmid a$ , then  $ax \equiv ay \pmod{p} \implies x \equiv y \pmod{p}$ .

*Proof.* Let  $x, y, a \in \mathbb{N}$  and  $p \in \mathbb{P}$ .

Suppose  $ax \equiv ay \pmod{p}$

Then  $p|a(x - y)$

By theorem 7.1,  $p|a \vee p|(x - y)$

But by our assumption,  $p \nmid a$ , therefore  $p|(x - y)$

Thus  $x \equiv y \pmod{p}$

■

**Theorem 7.3** (Generalization of Theorem 7.2). Let  $m \in \mathbb{N}$  and  $a \in \mathbb{Z}$  and  $a$  and  $m$  are relatively prime. Then

$$ax \equiv ay \pmod{m} \implies x \equiv y \pmod{m}$$

*Proof.* Suppose  $ax \equiv ay \pmod{m}$

Then  $m|a(x - y)$

Therefore  $m|a \vee m|(x - y)$

For  $m$  to divide  $a$ , all of  $m$ 's prime factors have to be in the prime factorization of  $|a|$ .



But  $m$  and  $a$  are relatively prime, therefore  $m \nmid a$ .

Therefore  $m \mid (x - y)$  and that's  $x \equiv y \pmod{m}$

■

**Theorem 7.4.** Any integer  $a$  is congruent to mod  $m$  to exactly one of  $\{0, 1, \dots, m - 1\}$ .

**Theorem 7.5** (Fermat's Little Theorem). If  $p$  is a prime and  $p \nmid a$  (i.e.  $a$  and  $p$  are relatively prime), then

$$a^{p-1} \equiv 1 \pmod{p}$$

*Proof.* Let  $S := \{a1, a2, \dots, a(p-1)\}$

Notice that if  $ax_i \equiv ax_j \pmod{p}$ , since  $p \nmid a$ ,  $x_1 \equiv x_2 \pmod{p}$ .

Since  $1 \leq x_i, x_j \leq p - 1$ , then  $x_i = x_j$ .

Therefore all elements in  $S$  are distinct with mod  $p$

i.e.  $x_i \not\equiv x_j \pmod{p}$ ,  $\forall (i, j) \in \mathbb{Z}^2$ .

Since  $p \nmid a \wedge p \nmid m$ ,  $\forall m \in \{1, 2, \dots, (p-1)\}$

So no element in  $S$  is congruent to  $0 \pmod{p}$ .

Thus,  $S$  contains  $p - 1$  numbers and no two of them are congruent mod  $p$ .

Also none of them are congruent to  $0 \pmod{p}$ .

By theorem 7.4, each element in  $S$  is congruent to one corresponding element in set  $\{1, 2, \dots, p - 1\}$ .

Therefore  $(a1)(a2) \dots (a(p-1)) \equiv 1 * 2 * \dots * (p-1) \pmod{p}$

That's  $a^{p-1} (1 * 2 * \dots * (p-1)) \equiv 1 * 2 * \dots * (p-1) \pmod{p}$

Clearly  $p \nmid (1 * 2 * \dots * (p-1))$ , since if a prime divides a product of natural numbers, the prime must divide at least one of elements in the product.

Therefore  $a^{p-1} \equiv 1 \pmod{p}$

■

## 8 Lecture 8 Sep. 24 2018

**Definition 8.1.** Let  $p \in \mathbb{N}$  and  $a \in \mathbb{Z}$ . The **multiplicative inverse** mod  $p$  of  $a$  is an integer  $b$  such that

$$ab \equiv 1 \pmod{p}$$

**Remark 8.1.** Notice that the multiplicative inverse is generally not unique but unique up to mod  $p$ .

**Corollary 8.1.** Let  $p \in \mathbb{P}$ ,  $a \in \mathbb{N}$  and  $p \nmid a$ . Then

$$\exists b \in \mathbb{Z}, \text{ s.t. } ba \equiv 1 \pmod{p}$$

*Proof.* Let  $p \in \mathbb{Z}$  and  $a \in \mathbb{Z}$

Suppose  $p \nmid a$ , then by Fermat's little theorem,

$$a^{p-1} \equiv 1 \pmod{p} \implies a^{p-2}a \equiv 1 \pmod{p}$$

Take  $b = a^{p-2} \in \mathbb{Z}$  and  $ab \equiv 1 \pmod{p}$  ■

**Example 8.1.** Let  $a = 8$  and  $p = 5$ . Obviously  $p \nmid a$ . By corollary above,

$$\exists b \in \mathbb{Z}, \text{ s.t. } 8b \equiv 1 \pmod{5}$$

Notice  $b = 2$  satisfies above equation.

**Remark 8.2.** Corollary 8.1 requires  $p$  to be a prime.

**Corollary 8.2** (Generalization). Let  $a$  and  $m \in \mathbb{N}$  and  $a$  and  $m$  are relatively prime, then

$$\exists b \in \mathbb{Z}, \text{ s.t. } ab \equiv 1 \pmod{m}$$

**Theorem 8.1** (Wilson's Theorem). Let  $p \in \mathbb{P}$  then

$$(p-1)! \equiv -1 \pmod{p}$$

*Proof.* Let  $p \in \mathbb{P}$

if  $p = 2 \vee p = 3$ , then  $1! \equiv -1 \pmod{2}$  and  $2! \equiv -1 \pmod{3}$ .

Otherwise, suppose  $p > 3$ ,

Consider, let  $S := \{2, 3, 4, \dots, p-2\}$

Notice that none of  $S$  is divisible by  $p$ .

Therefore  $p$  is relatively prime to all elements in  $S$ .

Then by Corollary 8.1,  $\exists b_i \in \mathbb{Z}$  s.t.  $b_i s_i \equiv 1 \pmod{p}$ ,  $\forall s_i \in S$ .

Notice that 0 has no multiplicative inverse and

$$(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \pmod{p}$$

That's, 1 and  $(p-1)$  have themselves as their multiplicative inverse.

Also notice that for any  $s_i \in S$ ,  $s_i$  does not have itself as its multiplicative inverse.

If  $a \in S$  has itself as its multiplicative inverse, then

$$\begin{aligned} a^2 &\equiv 1 \pmod{p} \\ \implies a^2 - 1 &\equiv 0 \pmod{p} \\ \implies (a+1)(a-1) &\equiv 0 \pmod{p} \\ \implies p &\mid (a+1)(a-1) \end{aligned}$$

Notice that at last one of  $(a + 1)$  and  $(a - 1)$  is in set  $S$  since  $p > 3 \implies S \neq \emptyset$ .

This contradicts what we argued above, *none of  $S$  is divisible by  $p$* .

That's

$$s_i s_i \not\equiv 1 \pmod{p}, \forall s_i \in S$$

*Note that if  $y$  is a multiplicative inverse of  $x$ , then  $x$  is a multiplicative inverse of  $y$ .*

Notice that for any  $s_i \in S$ , by Corollary 8.1,

there exists an integer  $b_i$  s.t.  $s_i b_i \equiv 1 \pmod{p}$

And the multiplicative inverse is unique up to  $\pmod{p}$ ,

Thus  $s_i(b_i \pmod{p}) \equiv 1 \pmod{p}$  and  $(b_i \pmod{p}) \in S$ .

And for all elements in  $S$  has one of their multiplicative inverse in  $S$ ,

That's

$$s_i s_j \equiv 1 \pmod{p}, i \neq j$$

Notice  $p > 3$  implies  $p$  is odd, so  $|S|$  is even.

Match every pair of multiplicative inverses in  $S$  and they collapse to  $1 \pmod{p}$

Therefore

$$\begin{aligned} 2 \cdot 3 \cdot 4 \cdots (p-2) &\equiv 1 \pmod{p} \\ \implies 2 \cdot 3 \cdot 4 \cdots (p-2) \cdot (p-1) &\equiv (p-1) \pmod{p} \\ \implies (p-1)! &\equiv -1 \pmod{p} \end{aligned}$$

■

## 9 Lecture 9 Sep. 26 2018

**Remark 9.1.** Recall that an integer  $n$  is even iff  $n \equiv 0 \pmod{2}$  and is odd iff  $n \equiv 1 \pmod{2}$ .

**Theorem 9.1.** There are infinitely many primes of the form  $4k + 3$ , where  $k \in \mathbb{Z}$ .

*Proof.* Note that odd numbers  $n$  can be classified as  $n \equiv 1 \pmod{4}$  and  $n \equiv 3 \equiv -1 \pmod{4}$

(Suppose 1) there are only finitely many primes in the form  $4k + 3$ .

Let finite set  $S := \{p_1, p_2, \dots, p_m\}$  denotes the collection of them.

And notice that  $p_i \equiv -1 \pmod{4}, \forall p_i \in S$ .

Let

$$M := (p_1 \cdot p_2 \cdots p_m)^2 + 2$$

and  $M \equiv 1 + 2 \equiv 3 \equiv -1 \pmod{4}$ .

Therefore  $M$  is an odd natural number.

By the Fundamental Theorem of Arithmetic,  $M$  can be factorized into product of

primes.

$$M = \prod_{i=1}^{\ell} q_i$$

and since  $M$  is odd,  $q_i \neq 2 \forall i$ . Thus all  $q_i$  are odd.

(Suppose 2) All  $q_i \equiv 1 \pmod{4}$ .

Then  $M \equiv 1 \pmod{4}$ .

Contradict the fact that  $M \equiv -1 \pmod{4}$ . Thus (Suppose 2) is false.

Therefore  $\exists i$ , s.t.  $q_i \equiv -1 \pmod{4}$ .

From (Suppose 1),  $S$  is the collection of all primes that  $\equiv -1 \pmod{4}$ .

Therefore  $q_i = p_j$  for some  $j$ .

Therefore  $p_j | M$ .

Also note that  $p_j | (p_1 \cdot p_2 \cdots p_m) \implies p_j | (p_1 \cdot p_2 \cdots p_m)^2$   
 $\implies p_j | 2 \implies p_j = 2$  contradicts the fact that  $p_j$  is odd.

Therefore (Suppose 1) is false, there are infinitely many primes taking the form  $4k + 3$ . ■

**Example 9.1.** Find  $7^{20^{30}} \pmod{5}$ .

*Solution.* Let  $n := 20^{30}$ .

Notice that  $7^4 \equiv 1 \pmod{5}$ .

And if  $n \equiv r \pmod{4}$  where  $r \in \mathbb{Z}$ ,

$n = 4k + r$  and  $7^n \equiv 7^{4k+r} \equiv (7^4)^k \times 7^r \equiv 1^k \times 7^r \equiv 7^r \pmod{5}$ .

Notice that  $20 \equiv 0 \pmod{4} \implies 20^{30} \equiv 0 \pmod{4}$ .

Thus  $r = 0$ .

Therefore  $7^n \equiv 7^0 \equiv 1 \pmod{5}$ .

Thus  $7^{20^{30}} \pmod{5} = 1$ . ■

**Example 9.2.** Find  $10^{3^{30}} \pmod{7}$ .

*Solution.* Notice that  $10^6 \equiv 1 \pmod{7}$ .

And  $3 \equiv 3 \pmod{6}, 3^2 \equiv 3 \pmod{6}, 3^3 \equiv 3 \pmod{6} \dots$

Using induction, we can show that

$$3^k \equiv 3 \pmod{6}, \forall k \in \mathbb{Z}_{\geq 0}$$

Therefore  $3^{30} \equiv 3 \pmod{6}$ .

That's  $3^{30} = 6k + 3$  for some  $k$ .

Thus  $10^{3^{30}} \equiv (10^6)^k \times 10^3 \equiv (1)^k \times 10^3 \equiv -1 \equiv 6 \pmod{7}$ .

So  $10^{3^{30}} \pmod{7} = 6$ . ■

## 10 Lecture 10 Sep. 28 2018

**Example 10.1.** Find  $8^{9^{10^{11}}} \bmod 5$ .

*Solution.* Let  $n := 9^{10^{11}}$

And notices that  $8^4 \equiv 1 \pmod{5}$ .

Then find  $n \bmod 4$

Note that  $9 \equiv 1 \pmod{4} \implies 9^{10^{11}} \equiv 1 \pmod{4}$ .

Thus  $n = 4k + 1$ .

Therefore  $8^{9^{10^{11}}} \equiv (8^4)^k \cdot 8 \equiv 1 \cdot 3 \pmod{5}$ .

That's  $8^{9^{10^{11}}} \bmod 5 = 3$ . ■

**Definition 10.1** (Euler  $\phi$ -function). Let  $m \in \mathbb{N}$  and  $\phi(m) : \mathbb{N} \rightarrow \mathbb{N}$  is defined as *the number of elements in  $\{1, 2, \dots, m-1\}$  that are relatively prime to  $m$ .*

**Example 10.2.** For  $m = 8$ , note that  $\{1, 3, 5, 7\} \subset \{1, 2, \dots, 7\}$  are relatively prime with 8, therefore  $\phi(8) = 4$ .

And for  $m = 11$ , since  $m$  is a prime, then every integer between 1 and  $m-1$  are relatively prime with 11. Therefore  $\phi(11) = 10$ .

And notice that  $\phi(p) = p-1$  if  $p \in \mathbb{P}$ . (Fermat's Little Theorem)

**Proposition 10.1.** Let  $p, q$  be two distinct primes, then

$$\phi(pq) = (p-1)(q-1)$$

*Proof.* Let  $S := \{1, 2, \dots, pq-1\}$ .

WLOG, assume  $p < q$ .

We need find all elements in  $S$  that with either  $p$  or  $q$  in their prime factorization to find elements in  $S$  that are not relatively prime to  $pq$ .

And those elements are multiples of  $p$  and multiples of  $q$ .

And since  $pq \notin S$ , the largest multiple of  $p$  in  $S$  is  $(q-1)p$  and the largest multiple of  $q$  in  $S$  is  $p(q-1)$ .

And since there is no multiple of both  $p$  and  $q$  in set  $S$ , therefore there's no overlapping between multiples of  $p$  and multiples of  $q$ .

Therefore exists  $(p-1) + (q-1)$  elements that are not relatively prime to  $pq$ .

Therefore  $\phi(pq) = (pq-1) - (p-1) - (q-1)$

$$= pq - p - q + 1$$

$$= (p-1)(q-1)$$
 ■

**Proposition 10.2.** For any natural number  $m \in \mathbb{N}$ . Therefore  $m$  can be expressed as

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Then

$$\phi(m) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$$

And

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1)$$

Therefore

$$\phi(m) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1})$$

**Example 10.3.**

$$\begin{aligned} \phi(6) &= \phi(2^1 3^1) \\ &= \phi(2^1)\phi(3^1) \\ &= (2^1 - 2^0)(3^1 - 3^0) \\ &= (2 - 1)(3 - 1) = 2 \end{aligned}$$

**Example 10.4.**

$$\begin{aligned} \phi(8) &= \phi(2^3) \\ &= (2^3 - 2^2) = 4 \end{aligned}$$

**Theorem 10.1** (Euler's Theorem). Suppose  $m \in \mathbb{N} \setminus \{1\}$ . And  $a \in \mathbb{N}$ <sup>3</sup> Assume  $a$  and  $m$  are relatively prime, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

**Remark 10.1.** This theorem is a generalization of Fermat's Little Theorem. When  $m \in \mathbb{P}$ , it becomes Fermat's Little Theorem.

*Proof.* Let  $S := \{r_1, r_2, \dots, r_{\phi(m)}\}$  be the set of all elements in  $\{1, 2, \dots, m - 1\}$  that are relatively prime to  $m$ .

Let  $T := \{ar_1, ar_2, \dots, ar_{\phi(m)}\}$ .

(Observation 1) that no two elements in  $S$  are congruent to each other  $\pmod{m}$ . Since all elements are in the range  $[1, m - 1]$  and they are the remainder while  $r_i$  is divided by  $m$ .

---

<sup>3</sup>Also true for  $a \in \mathbb{Z}$

Also notice that elements in  $T$  are not congruent to each other  $\pmod m$ .

Since, suppose

$$ar_i \equiv ar_j \pmod m$$

for some  $(i, j)$ .

Since  $a$  and  $m$  are relatively prime, therefore we could use cancellation law.

$$r_i \equiv r_j \pmod m$$

This would contradict our observation 1

(Observation 2) elements in  $T$  are not congruent to each other  $\pmod m$ .

Therefore elements in  $S$  are congruent to elements in  $T \pmod m$  in some order.

Therefore

$$r_1 r_2 r_3 \cdots r_{\phi(m)} \equiv a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \pmod m$$

And notice  $r_1 r_2 r_3 \cdots r_{\phi(m)}$  is a product of natural numbers relatively prime to  $m$ .

Therefore  $r_1 r_2 r_3 \cdots r_{\phi(m)}$  is relatively prime to  $m$ .

And by cancellation law, we have

$$a^{\phi(m)} \equiv 1 \pmod m$$



## 11 Lecture 11 Oct. 2 2018

### 11.1 Rational and Irrational Numbers

**Definition 11.1.** A **rational number** is an expression in form

$$\frac{m}{n}, m, n \in \mathbb{Z}, n \neq 0$$

**Definition 11.2.** Two rational numbers  $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in \mathbb{Q}$  are **equal** if and only if  $m_1 n_2 = m_2 n_1$ .

**Definition 11.3.** Arithmetic on  $\mathbb{Q}$  are defined as

- **Addition**  $+$  :  $\frac{m_1}{n_1} + \frac{m_2}{n_2} := \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}$
- **Multiplication**  $\times$  :  $\frac{m_1}{n_1} \times \frac{m_2}{n_2} := \frac{m_1 m_2}{n_1 n_2}$
- **Subtraction**  $-$  :  $\frac{m_1}{n_1} - \frac{m_2}{n_2} := \frac{m_1 n_2 - m_2 n_1}{n_1 n_2}$
- **Division**