MAT246: Concepts in Abstract Mathematics:

Lecture 0101 Notes

Tianyu Du

October 17, 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 $\{2, 3, \ldots k\} \subseteq S$
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.

[1] 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, $\{2, 3, \ldots, \} \subseteq S$. ∎

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 $\forall i \in \{2 * 3 * 5 * \cdots * p\},\ i \nmid M$.
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 $n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_\ell$ 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 $m := n - p_1 q_2 \ldots q_\ell \in \mathbb{N}$

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 $p_1 \not| q_2q_3 \dots q_\ell$
$\implies p_1|(q_1 - p_1) \implies p_1|q_1 \implies p_1 = q_1$
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 $2^2 \equiv 4 \mod 7$ 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. $a \equiv b \mod m \wedge c \equiv d \mod m \implies a + c \equiv b + d \mod m$
2. $a \equiv b \mod m \wedge c \equiv d \mod m \implies ac \equiv bd \mod m$

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

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 $d_0 = 6, d_1 = 5, d_2 = 2$

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
$a = p_1^{\alpha_1} \dots p_k^{\alpha_k},\ \alpha_j \geq 1$ 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 $a \equiv b \mod m \implies ca \equiv cb \mod m$. But notice that

$$ca \equiv cb \mod m \not\Longrightarrow a \equiv b \mod m$$

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 $ax \equiv ay \mod p \implies x \equiv y \mod p$.

Proof. Let $x, y, a \in \mathbb{N}$ and $p \in \mathbb{P}$.
Suppose $ax \equiv ay \mod p$
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 $x \equiv y \mod p$

■

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

$$ax \equiv ay \mod m \implies x \equiv y \mod m$$

Proof. Suppose $ax \equiv ay \mod m$
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 $m|(x-y)$ and that's $x \equiv y \mod m$

■

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

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

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

Proof. Let $S := \{a1, a2, \ldots a(p-1)\}$
Notice that if $ax_i \equiv ax_j \mod p$, since $p \nmid a$, $x_1 \equiv x_2 \mod p$.
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. $x_i \not\equiv x_j \mod p$, $\forall (i, j) \in \mathbb{Z}^2$.
Since $p \nmid a \wedge p \nmid m$, $\forall m \in \{1, 2, \ldots, (p-1)\}$
So no element in S is congruent to $0 \mod p$.
Thus, S contains $p-1$ numbers and no two of them are congruent mod p.
Also none of them are congruent to $0 \mod p$.
By theorem 7.4, each element in S is congruent to one corresponding element in set $\{1, 2, \ldots, p-1\}$.
Therefore $(a1)(a2)\ldots(a(p-1)) \equiv 1 * 2 * \cdots * (p-1) \mod p$
That's $a^{p-1}(1 * 2 * \cdots * (p-1)) \equiv 1 * 2 * \cdots * (p-1) \mod p$
Clearly $p \nmid (1 * 2 * \ldots (p-1))$, since if a prime divides a product of natural numbers, the prime must divide at least one of elements in the product.
Therefore $a^{p-1} \equiv 1 \mod p$

■

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

$$ab \equiv 1 \mod p$$

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

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

Proof. Let $p \in \mathbb{Z}$ and $a \in \mathbb{Z}$
Suppose $p \nmid a$, then by Fermat's little theorem,
$a^{p-1} \equiv 1 \mod p \implies a^{p-2}a \equiv 1 \mod p$
Take $b = a^{p-2} \in \mathbb{Z}$ and $ab \equiv 1 \mod p$ ■

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

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

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

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

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

$$(p-1)! \equiv -1 \mod p$$

Proof. Let $p \in \mathbb{P}$
if $p = 2 \lor p = 3$, then $1! \equiv -1 \mod 2$ and $2! \equiv -1 \mod 3$.
Otherwise, suppose $p > 3$,
Consider, let $S := \{2, 3, 4, \ldots, p-2\}$
Notice that none of S is divisible by p.
Therefore p is relatively prime to all elements in S.
Then by Corollary 8.1, $\exists b_i \in \mathbb{Z}\ s.t.\ b_i s_i \equiv 1 \mod p,\ \forall s_i \in S$.
Notice that 0 has no multiplicative inverse and

$$(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \mod p$$

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 it's multiplicative inverse, then

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

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

$$s_i s_i \not\equiv 1 \mod p,\ \forall s_i \in S$$

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. $s_i b_i \equiv 1 \mod p$
And the multiplicative inverse is unique up to $\mod p$,
Thus $s_i(b_i \mod p) \equiv 1 \mod p$ and $(b_i \mod p) \in S$.
And for all elements in S has one of their multiplicative inverse in S,
That's

$$s_i s_j \equiv 1 \mod p,\ i \neq j$$

Notice $p > 3$ implies p is odd, so $|S|$ is even.
Match every pair of multiplicative inverses in S and they collapse to $1 \mod p$
Therefore

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

■

9 Lecture 9 Sep. 26 2018

Remark 9.1. Recall that an integer n is even iff $n \equiv 0 \mod 2$ and is odd iff $n \equiv 1 \mod 2$.

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 $n \equiv 1 \mod 4$ and $n \equiv 3 \equiv -1 \mod 4$
(Suppose 1) there are only finitely many primes in the form $4k + 3$.
Let finite set $S := \{p_1, p_2, \ldots p_m\}$ denotes the collection of them.
And notice that $p_i \equiv -1 \mod 4,\ \forall p_i \in S$.
Let

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

and $M \equiv 1 + 2 \equiv 3 \equiv -1 \mod 4$.
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 $q_i \equiv 1 \mod 4$.
Then $M \equiv 1 \mod 4$.
Contradict the fact that $M \equiv -1 \mod 4$. Thus (Suppose 2) is false.
Therefore $\exists i,\ s.t.\ q_i \equiv -1 \mod 4$.
From (Suppose 1), S is the collection of all primes that $\equiv -1 \mod 4$.
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 $7^{20^{30}} \mod 5$.

Solution. Let $n := 20^{30}$.
Notice that $7^4 \equiv 1 \mod 5$.
And if $n \equiv r \mod 4$ where $r \in \mathbb{Z}$,
$n = 4k + r$ and $7^n \equiv 7^{4k+r} \equiv (7^4)^k \times 7^r \equiv 1^k \times 7^r \equiv 7^r \mod 5$.
Notice that $20 \equiv 0 \mod 4 \implies 20^{30} \equiv 0 \mod 4$.
Thus $r = 0$.
Therefore $7^n \equiv 7^0 \equiv 1 \mod 5$.
Thus $7^{20^{30}} \mod 5 = 1$. ■

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

Solution. Notice that $10^6 \equiv 1 \mod 7$.
And $3 \equiv 3 \mod 6, 3^2 \equiv 3 \mod 6, 3^3 \equiv 3 \mod 6 \ldots$
Using induction, we can show that

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

Therefore $3^{30} \equiv 3 \mod 6$.
That's $3^{30} = 6k + 3$ for some k.
Thus $10^{3^{30}} \equiv (10^6)^k \times 10^3 \equiv (1)^k \times 10^3 \equiv -1 \equiv 6 \mod 7$.
So $10^{3^{30}} \mod 7 = 6$.

■

10 Lecture 10 Sep. 28 2018

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

Solution. Let $n := 9^{10^{11}}$
And notices that $8^4 \equiv 1 \mod 5$.
Then find $n \mod 4$
Note that $9 \equiv 1 \mod 4 \implies 9^{10^{11}} \equiv 1 \mod 4$.
Thus $n = 4k + 1$.
Therefore $8^{9^{10^{11}}} \equiv (8^4)^k \cdot 8 \equiv 1 \cdot 3 \mod 5$.
That's $8^{9^{10^{11}}} \mod 5 = 3$.

■

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

Example 10.2. For $m = 8$, note that $\{1, 3, 5, 7\} \subset \{1, 2, \ldots, 7\}$ 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 $S := \{1, 2, \ldots, pq - 1\}$.
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 $q(p-1)$.
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 $m \in \mathbb{N}\backslash\{1\}$. And $a \in \mathbb{N}$ [3]Assume a and m are relatively prime, then

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

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 $S := \{r_1, r_2, \ldots r_{\phi(m)}\}$ be the set of all elements in $\{1, 2, \ldots, m-1\}$ that are relatively prime to m.
Let $T := \{ar_1, ar_2, \ldots ar_{\phi(m)}\}$.
(Observation 1) that no two elements in S are congruent to each other $\mod m$. Since all elements are in the range $[1, m-1]$ and they are the reminder while r_i is divided by m.

[3] Also true for $a \in \mathbb{Z}$

Also notice that elements in T are not congruent to each other $\mod m$.
Since, suppose

$$ar_i \equiv ar_j \mod m$$

for some (i, j).
Since a and m are relatively prime, therefore we could use cancellation law.

$$r_i =\equiv r_j \mod m$$

This would contradict our observation 1
(Observation 2) elements in T are not congruent to each other $\mod m$.
Therefore elements in S are congruent to elements in T $\mod m$ in some order.
Therefore

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

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

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

♥

11 Lecture 11 Oct. 1 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** $\div$: $\frac{\frac{m_1}{n_1}}{\frac{m_2}{n_2}} := \frac{m_1 n_2}{n_1 m_2}$, defined only if $m_2 \neq 0$.

Definition 11.4. The **multiplicative inverse** of a $\underline{\text{non-zero}}$ rational number $x \neq 0$ is a rational number y such that $xy = 1$.

Remark 11.1. Let $x = \frac{m}{n} \neq 0$, then the multiplicative inverse $y = \frac{n}{m}$.

Example 11.1. Claim: $\sqrt{2}$ is not rational.

Proof. Assume $\sqrt{2}$ is rational,
by definition of rational numbers, $\sqrt{2} = \frac{m}{n}$ where $m, n \in \mathbb{Z}, n \neq 0$.
Divide numerator and denominator by their common prime factors (if any).
Assume m and n have been reduced so that they are relatively prime.

$$\begin{aligned} &\implies 2 = \frac{m^2}{n^2} \\ &\iff 2n^2 = m^2 \\ &\implies 2|m^2 \end{aligned}$$

Consider if $2 \not| m$, then m is odd, then $2 \not| m^2$.
Take the contraposition, $2|m^2 \implies 2|m$.

$$\begin{aligned} &\implies 2|m \\ &\implies m = 2q, \ q \in \mathbb{Z} \\ &\implies 2n^2 = 4q^2 \\ &\implies n^2 = 2q^2 \\ &\implies 2|n^2 \\ &\implies 2|n \end{aligned}$$

That's $2|m \wedge 2|n$, which contradicts our assumption that m and n are relatively prime.
Therefore $\sqrt{2}$ cannot be rational. ∎

Definition 11.5 (non-rigorous definition)**.** **Real numbers**, denoted as $\mathbb{R}$, are numbers representing distance of points on a line from 0.

Definition 11.6. **Irrational numbers** are real numbers which are not rational. $(\mathbb{R} \backslash \mathbb{Q})$

Proposition 11.1. Let $p \in \mathbb{P}$ and $m \in \mathbb{Z}$, then

$$p|m^2 \implies p|m$$

Proof. Let $m = q_1 q_2 \dots q_\ell$ be the unique prime factorization.
Suppose $p \nmid m$, then $p \notin \{q_1, q_2, \dots, q_\ell\}$.
Obviously, $m^2 = q_1^2 q_2^2 \dots q_\ell^2$ as it's prime factorization.
Then $p \nmid m^2$. ■

Example 11.2. $\sqrt{p} \notin \mathbb{Q}$, $\forall p \in \mathbb{P}$.

Proof. Let $p \in \mathbb{P}$, Suppose $\sqrt{p} \in \mathbb{Q}$.
Therefore $\sqrt{p} = \frac{m}{n}$ where $m, n \in \mathbb{Z}$ and $n \neq 0$.
Assume $\frac{m}{n}$ has been reduced such that m and n are relatively prime.

$$\begin{gathered}
\implies pn^2 = m^2 \\
\implies p|m^2 \\
\implies p|m \\
\implies m = pr,\ r \in \mathbb{Z}. \\
\implies pn^2 = p^2 r^2 \\
\implies n^2 = pr^2 \\
\implies p|n^2 \\
\implies p|n
\end{gathered}$$

Contradicts the assumption that m and n are relatively prime. ■

12 Lecture 12 Oct. 3 2018

Definition 12.1. A natural number (other than 1) is called a **perfect square** if it is the square of some natural number.

Theorem 12.1. A natural number m is a perfect square if and only if every prime factor occurs with an even power in its prime decomposition.

Proof. ($\implies$) Suppose m is a perfect square,
Then $m = n^2, b \in \mathbb{N}$.
Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be the prime decomposition.
Then $m = p_1^{2\alpha_1} \dots p_k^{2\alpha_k}$.
Obviously all prime factors in the prime factorization occurs with an even power.

($\Longleftarrow$) Suppose $m = p_1^{2\alpha_1} \dots p_k^{2\alpha_k}$ as its prime decomposition.
Then $m = (p_1^{\alpha_1} \dots p_k^{\alpha_k})^2$ and $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \in \mathbb{N}$.
Therefore m is a perfect square. ■

Theorem 12.2 (Generalization)**.** Let $n \in \mathbb{N}$ other than 1, then [4]

$$\sqrt{n} \in \mathbb{Q} \iff n \text{ is a perfect square}$$

Proof. ($\Longleftarrow$) if n is perfect square, then $\sqrt{n} \in \mathbb{N}$.
Obviously a natural number is rational.
($\Longrightarrow$) Suppose $\sqrt{n} \in \mathbb{Q}$.
Then

$$\sqrt{n} = \frac{m}{l} \in \mathbb{Q}$$

where $m, l \in \mathbb{Z}$ and $l \neq 0$.
Since $\sqrt{n} > 0$, WLOG, assume $m, l \geq 0$.
Suppose m, l are relatively prime. (Otherwise, factorize the friction so that m and l are relatively prime.)
Then

$$m^2 = nl^2$$

(Suppose 1) $l > 1$ and p is a prime in the prime decomposition of m, i.e. $p|l$,
Thus $p|l^2$ and therefore $p|m^2$.
By proposition 11.1 (previous lecture), $p|m$
And we have $p|l \wedge p|m$ which contradicts our assumption that m, l are relatively prime.
Therefore (Suppose 1) is false and $l \leq 1$ (so that l has no prime factor).
Also notice that $l \in \mathbb{Z}$ and $l \geq 0$. therefore $l = 1$.
Therefore $n = m^2$ and n is a prefect square. ■

Example 12.1. Claim $\sqrt[3]{4}$ is irrational.

Proof. Suppose $\sqrt[3]{4}$ is rational and

$$\sqrt[3]{4} = \frac{m}{n} \implies 4 = \frac{m^3}{n^3} \implies 2^2n^3 = m^3$$

Suppose

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$
$$m = q_1^{\beta_1} \dots q_\ell^{\beta_\ell}$$

[4] The square root here denotes the positive square root.

The prime factor 2 has power of 2 or $2+\alpha_j$ on the left hand side.
And have power of $3\beta_i$ on the right hand side.
The left hand side power is congruent to 2 mod 3 and the right hand side is congruent to 0 mod 3.
It's impossible for them to be equal. Thus, contradicts the uniqueness of prime decomposition.
Therefore $\sqrt[3]{4}$ cannot be rational. ■

13 Lecture 13 Oct. 5 2018

Example 13.1. $\sqrt{3}+\sqrt{5}$ is irrational.

Proof. Suppose $\sqrt{3}+\sqrt{5}$ are rational then $\sqrt{3}+\sqrt{5}=\frac{m}{n}$.

$$\implies \sqrt{5}=\frac{m}{n}-\sqrt{3}$$

$$\implies 5=(\frac{m}{n}-\sqrt{3})^2=\frac{m^2}{n^2}-\frac{2m\sqrt{3}}{n}+3$$

$$\implies \sqrt{3}=\frac{5-3-\frac{m^2}{n^2}}{-\frac{2n}{n}}$$

Obviously the right hand side is rational, leads to contradiction.
Therefore $\sqrt{3}+\sqrt{5}\notin\mathbb{Q}$. ■

Example 13.2. Are there two irrational numbers x, y such that $x^y\in\mathbb{Q}$?

Solution. Consider $\sqrt{3}^{\sqrt{2}}$.
case 1: $\sqrt{3}^{\sqrt{2}}\in\mathbb{Q}$, then take $x=\sqrt{3}$ and $y=\sqrt{2}$.
case 2: $\sqrt{3}^{\sqrt{2}}\notin\mathbb{Q}$, then take $x=\sqrt{3}^{\sqrt{2}}$, $y=\sqrt{2}$.
And $x^y=\sqrt{3}^{\sqrt{2}\sqrt{2}}=\sqrt{3}^2=3\in\mathbb{Q}$. ■

Remark 13.1. Basic arithmetic operations on integers preserve rationality.

Theorem 13.1 (Rational Root Theorem)**.** Consider a polynomial with integer coefficients,

$$a_0+a_1x+x_2x^2+\cdots+a_kx^k,\ a_i\in\mathbb{Z}$$

If $\frac{m}{n}$ is a rational root for the polynomial and m and n are relatively prime. Then

$$m|a_0\wedge n|a_k$$

Proof. Suppose $\frac{m}{n}$ is a rational root for the polynomial,
then

$$a_0 + a_1\frac{m}{n} + a_2\frac{m^2}{n^2} + \cdots + a_k\frac{m^k}{n^k} = 0$$

Thus

$$a_0n^k + a_1mn^{k-1} + a_2m^2n^{k-2} + \cdots + a_km^k = 0$$

And

$$-a_0n^k = a_1mn^{k-1} + a_2m^2n^{k-2} + \cdots + a_km^k$$

Therefore $m|a_0n^k$ and since $m \nmid n$, thus $m|a_0$.
Similarly,

$$-a_km^k = a_0n^k + a_1mn^{k-1} + a_2m^2n^{k-2} + \cdots + a_{k-1}m^{k-1}n$$

Which implies $n|a_km^k$ and since $n \nmid m$, thus $n|a_k$.

■

14 Lecture 14 Oct. 10 2018 Euclidean Algorithm

Definition 14.1. The **greatest common divisor**(gcd) of $m, n \in \mathbb{N}$ is denoted as $gcd(m, n)$ or $(m; n)$ is the largest natural number that divides both m and n.

Example 14.1.

$$gcd(27, 15) = 3$$
$$gcd(36, 48) = 12$$
$$gcd(7, 21) = 7$$

14.1 Conventional Method

Factorize m and n into primes and in general,

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$
$$n = p_1^{\beta_1} \dots p_k^{\beta_k}$$

where $\{p_1, \dots p_k\}$ = {prime factors of m} $\cup$ { prime factors of n }. And α_i,$\beta_i \geq 0$. and gcd could be found by

$$gcd(m, n) = p_1^{\min\{\alpha_1,\beta_1\}} \dots p_k^{\min\{\alpha_k,\beta_k\}}$$

14.2 Euclidean Algorithm

Notice that $r|a, b \implies r|gcd(a, b)$.
For $a, b \in \mathbb{N}$, WLOG, assuming $a \geq b$.

$$a = q_0 b + r_0 \quad r_0, q_0 \in \mathbb{N},\ 0 \leq r_0 < b$$
$$b = q_1 r_0 + r_1 \quad r_1, q_1 \in \mathbb{N},\ 0 \leq r_1 < r_0$$
$$r_0 = q_2 r_1 + r_2$$

r_i is strictly decreasing, and it's guaranteed to be 0 after certain iterations.

$$\dots$$
$$r_{k-2} = q_k r_{k-1} + r_k$$
$$r_{k-1} = q_{k+1} r_k + 0$$

and then r_k is the greatest common divisor of a and b.

Proof. WTS: $r_k = gcd(a, b)$
Obviously $r_k | r_{k-1}$
Then, $r_k | r_{k-1} \wedge r_k | r_k \implies r_k | r_{k-2}$
Similarly, tracing upwards through the Euclidean Algorithm,
we have $r_k | b$ and $r_k | a$.
so $r_k \leq gcd(a, b)$ since r_k is a common divisor of a and b.
Since $gcd | a \wedge gcd | b$,
Therefore $gcd | r_0$,
similarly, tracing downloads in the Euclidean Algorithm,
$gcd | r_k$, so $gcd \leq r_k$.
Therefore $r_k = gcd(a, b)$ ■

Theorem 14.1. Given natural numbers a and b with the greatest common divisor d, there exists integers x and y such that

$$d = ax + by$$

Proof. This can be seen by working upwards in the sequence of equations that constitute the Euclidean Algorithm. ■

15 Lecture 15 Oct. 12 2018 Public Key Cryptography, RSA Public Key

Lemma 15.1. Let $N = pq$ where $p \neq q$ are distinct primes,
and let n and M be integers.

Then

$$n \equiv 1 \mod \phi(N) \implies M^n \equiv M \mod N$$

Proof. Note that $\phi(N) = \phi(pq) = (p-1)(q-1)$.
And suppose $\phi(N)|(n-1)$,
Then $k\phi(N) = n-1$ for some k.
That's $n = 1 + k\phi(N)$.
Therefore $M^n = M^{1+k\phi(N)} = (M^{\phi(N)})^k \cdot M$
It's sufficient to show $M^n \equiv M \mod N$
by showing $M^n \equiv M \mod p$ and $M^n \equiv M \mod q$
To show $M^n \equiv M \mod p$,
Case 1: $p|M$, then $0^n \equiv 0 \mod p$, done.
Case 2: $p \not| M$, then $M^n = (M^{\phi(N)})^k \cdot M = (M^{(p-1)})^{(q-1)k} \cdot M$
By Fermat's Little Theorem, $M^{p-1} \equiv 1 \mod p$.
Therefore $M^n \equiv 1^{(q-1)k} \times M \mod p$. ■

15.1 RSA Public Key Procedures

Procedures:

1. **Receiver:** pick two large distinct primes $p \neq q$ and calculate $N = p \times q$.

2. **Receiver:** calculate $\phi(N) = (p-1)(q-1)$ and pick e relatively prime to $\phi(N)$.

3. **Receiver:** announce N and e.

4. **Sender:** choose message $M \in \mathbb{N}$ satisfies $M < N$ (if $M \geq N$, break M into pieces.)

5. **Sender:** find $M^e \equiv R \mod N$.

6. **Sender:** announce the encoded message R.

7. **Receiver:** pick $d \geq 0$ s.t. $de + k\phi(N) = 1$ as the decoder. Such z-linear combination is guaranteed to exist.

8. **Receiver:** the original message M can be found by $R^d \equiv M \mod N$

   Proof. $R^d \equiv (M^e)^d \equiv M^{ed} \mod N$
   Since $ed \equiv 1 \mod \phi(N)$
   By lemma 15.1, $M^{ed} \equiv M \mod N$. ■

16 Lecture 16 Oct. 15 2018 RSA Cryptography Examples

16.1 Recall

1. **Receiver:** choose $p, q \in \mathbb{P}$ and computes $N = pq, \phi(N) = (p-1)(q-1)$ and choose e *s.t.* $gcd(e, \phi(N)) = 1$. Then announces e, N.

2. **Sender:** choose $0 \leq M < N$ and calculate R such that $R = M^e \mod N$.

3. **Receiver:** compute decoder d s.t. $de + k\phi(N) = 1$. And decode message $M^* = R^d \mod N$

16.2 More Examples

Example 16.1. Receiver: pick $p = 11, q = 7$. Calculate $N = 77$ and $\phi(N) = 10 * 6 = 60$. Pick $e = 13$ which is relatively prime to $\phi(N)$.
Receiver: announces $N = 77$ and $e = 13$ to sender.
Sender: pick message $M = 71 < N$ and *encodes* message by computing $71^{13} \equiv R \mod 77$.

$$
\begin{aligned}
71 &\equiv -6 \mod 77 \\
71^3 &\equiv (-6)^3 \equiv 216 \equiv 15 \mod 77 \\
(71)^6 &\equiv (71^3)^2 \equiv 15^2 \equiv 225 \equiv -6 \mod 77 \\
(71)^{12} &\equiv (71^6)^2 \equiv (-6)^2 \equiv 36 \mod 77 \\
(71)^{13} &\equiv 36 \times (-6) \equiv -216 \equiv 15 \mod 77
\end{aligned}
$$

And calculate $R = 15$ satisfies $71^{13} \equiv 15 \mod 77$.
Sender: announces $R = 15$ to the rest of world.
Receiver: find $d \geq 0$ satisfying $d \times e + k \times \phi(N) = 1$. as the *decoder*. And find that $d = 37, k = -8$.
Receiver: compute $R^d \mod 77$

$$
\begin{aligned}
15^2 &\equiv 225 \equiv -6 \mod 77 \\
15^6 &\equiv -216 \equiv 15 \mod 77 \\
15^{12} &\equiv 15^2 \equiv -6 \mod 77 \\
15^{24} &\equiv 36 \mod 77 \\
15^{36} &\equiv -216 \equiv 15 \mod 77 \\
15^{37} &\equiv 15^2 \equiv 226 \equiv -6 \equiv 71 \mod 77 \\
\implies M^* &= 15^{37} \mod 77 = 71
\end{aligned}
$$

Security of RSA For anyone knowing N but does not know $\phi(N)$. To compute the decoder d, $\phi(N)$ needs to be calculated.

1. **Method 1:** Use definition and iterating through $\{1, 2, \dots N\}$ and compute $\phi(N)$.
2. **Method 2:** Factorize N and find p and q, then calculate $\phi(N) = (p-1)(q-1)$.

Both brute force methods are impractical in terms of run-time.

Example 16.2. Receiver: pick $p = 11, q = 7$ then $N = pq = 77$ and $\phi(N) = (p-1)(q-1) = 60$ and choose $e = 13$.
Receiver: announce $N = 77$ and $e = 13$.
Sender: pick $M = 76 < 77$ and $M^{13} \equiv (-1)^13 \equiv -1 \equiv 76 \mod 77$. Announce $R = 76$.
Receiver: find *decoder* $d \geq 0$ s.t. $d \times 13 + k \times 60 = 1$. Found $d = 13$.
Receiver: Compute $R^d \mod 77$.

$$\begin{aligned} R = 76 &\equiv -1 \mod 77 \\ R^{13} \equiv (-1)^{13} &\equiv -1 \equiv 76 \mod 77 \\ \implies M^* = R^{13} &\mod 77 = 76 \end{aligned}$$

17 Lecture 17 Oct. 17 2018

Remark 17.1. In RSA, picking the *decoder* $d \geq 0$ s.t. $de + \phi(N)k = 1$ is equivalent to pick d such that

$$de \equiv 1 \mod \phi(N)$$

17.1 Chinese Reminder Theorem

Theorem 17.1 (Chinese Reminder Theorem (CRT))**.** Solve system of congruent equations, where m_1 and m_2 are relatively prime,

$$\begin{cases} x \equiv a \mod m_1 \\ x \equiv b \mod m_2 \end{cases}$$

The solution is given by

$$x = ax_2m_2 + bx_1m_1$$

where x_1 and x_2 satisfy

$$\begin{cases} x_1m_1 \equiv 1 \mod m_2 \\ x_2m_2 \equiv 1 \mod m_1 \end{cases}$$

The general solution x is the superposition of two specific solutions.

Proof. If m_1 and m_2 are relatively prime, by Theorem 14.1,

$$\exists x_1, x_2 \in \mathbb{Z} \ s.t. \ x_1m_1 + x_2m_2 = 1$$

Taking congruence with respect to mod m_1 and m_2 gives

$$\begin{cases} 1 \equiv x_2m_2 \mod m_1 \\ 1 \equiv x_1m_1 \mod m_2 \end{cases}$$

Consider

$$x = ax_2m_2 + bx_1m_1$$

Clearly

$$\begin{aligned} x - a &= a(x_2m_2 - 1) + bx_1m_1 \\ m_1|(x_2m_2 - 1) \wedge m_1|bx_1m_1 &\implies m_1|x - a \\ &\implies x \equiv a \mod m_1 \end{aligned}$$

Similarly, we can show $x \equiv b \mod m_2$.
Thus x is the solution to system of equations

$$\begin{cases} x \equiv a \mod m_1 \\ x \equiv b \mod m_2 \end{cases}$$

■

Example 17.1. Solve

$$\begin{cases} x \equiv 5 \mod 7 \\ x \equiv 13 \mod 8 \end{cases}$$

Solution. Solve

$$\begin{cases} x_1 \times 7 \equiv 1 \mod 8 \\ x_2 \times 8 \equiv 1 \mod 7 \end{cases}$$

Solve $x_1 = 7$ and $x_2 = 1$. And one solution is given by

$$x = ax_2m_2 + bx_1m_1 = 5 \times 8 \times 1 + 13 \times 7 \times 7 = 677$$

■

17.2 Complex Numbers

Definition 17.1 (9.1.3)**.** A **complex number** is an expression of the form $a + bi$ where a and b are real numbers. The real number a is called the *real part* of $a + bi$, denoted as $\Re(a + bi)$. And the real number b is called the *imaginary part* of $a + bi$, denoted as $\Im(a + bi)$.

Definition 17.2.

$$i^2 = -1$$

Remark 17.2. Shorthands for complex numbers

- $a + i0 = a$
- $0 + ib = ib$
- $0 + i0 = 0$

Remark 17.3.

$$\mathbb{C} \subset \mathbb{R}$$

Definition 17.3. Arithmetic on complex numbers are defined as following,

- **Addition**($+ : \mathbb{C}^2 \to \mathbb{C}$) is defined as

$$(a + ib) + (c + id) := (a + c) + i(b + d)$$

- **Multiplication**($\times : \mathbb{C}^2 \to \mathbb{C}$) is defined as

$$(a + ib) \times (c + id) := (ac - bd) + i(ad + bc)$$

Proposition 17.1. Let $z = a + ib \in \mathbb{C}$ be a complex number, the **multiplication inverse** of z is given by

$$\frac{1}{a + ib} = \frac{a - ib}{a^2 + b^2}$$

Proof.

$$\frac{1}{a + ib} = \frac{1}{a + ib} \times \frac{a - ib}{a - ib} = \frac{a - ib}{(a^2 + b^2) + i(ab - ab)} = \frac{a - ib}{a^2 + b^2}$$

■