MAT246: Concepts in Abstract Mathematics:
Lecture 0101 Notes

Tianyu Du

December 5, 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. $n_0, n_0 + 1, \dots, k \in S \implies k + 1 \in S, \ \forall k \geq n_0$

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: $S = \mathbb{N} \backslash \{1\}$
(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.
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 $\{2, 3, 5, \cdots, p\}$ is the set of all primes
Let $M := (2 * 3 * 5 * \cdots * p) + 1 \in \mathbb{N}$
M is either prime or not.

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

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 $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$ 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 $m = p_1(p_2 p_3 \dots p_k - q_2 q_3 \dots q_\ell)$
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 $p_1 \nmid q_2 q_3 \dots q_\ell$
$\implies p_1 | (q_1 - p_1) \implies p_1 | q_1 \implies p_1 = q_1$
Contradicts the assumption that $p_1 < q_1$
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 $1, 2, 3, \ldots, k \in T$, 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 $1, 2, 3, \ldots k \in T \implies k + 1 \in T$.
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

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

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

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

■

7 Lecture 7 Sep. 21 2018

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

Proof. If $a = 1 \lor b = 1$, 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, $p = p_j \lor p = q_j \implies p|a \lor p|b$

■

Remark 7.1. We have shown that $a \equiv b \mod m \implies ca \equiv cb \mod m$. But notice that

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

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 $\underline{p \text{ is a prime}}$ 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, $p|a \lor p|(x - y)$
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 $m|a \lor m|(x - y)$
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 $m \not| a$.
Therefore $m|(x-y)$ and that's $x \equiv y \mod m$

$\blacksquare$

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 $p \not| a$ (i.e. a and p are relatively prime), then

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

Proof. Let $S := \{a1, a2, \dots a(p-1)\}$
Notice that if $ax_i \equiv ax_j \mod p$, since $p \not| a$, $x_1 \equiv x_2 \mod p$.
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 $p \not| a \wedge p \not| m$, $\forall m \in \{1, 2, \dots, (p-1)\}$
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 $\{1, 2, \dots, p-1\}$.
Therefore $(a1)(a2)\dots(a(p-1)) \equiv 1 * 2 * \dots * (p-1) \mod p$
That's $a^{p-1}(1 * 2 * \dots * (p-1)) \equiv 1 * 2 * \dots * (p-1) \mod p$
Clearly $p \not| (1 * 2 * \dots (p-1))$, since if a prime divides a product of natural numbers, the prime must divide at least one of elements in the product.
Therefore $a^{p-1} \equiv 1 \mod p$

$\blacksquare$

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 $p \not| a$. 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 $p \not| a$, 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 $ab \equiv 1 \mod p$ $\blacksquare$

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 <u>relatively prime</u>, 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 $p = 2 \vee p = 3$, 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 $S := \{p_1, p_2, \dots p_m\}$ 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

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

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

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.
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 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 $2 \nmid m$, then m is odd, then $2 \nmid m^2$.
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. ($\mathbb{R} \setminus \mathbb{Q}$)

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

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

Proof. Let $m = q_1 q_2 \ldots q_\ell$ be the unique prime factorization.
Suppose $p \nmid m$, then $p \notin \{q_1, q_2, \ldots, q_\ell\}$.
Obviously, $m^2 = q_1^2 q_2^2 \ldots q_\ell^2$ 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.

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

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

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

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

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

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

Suppose

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

The prime factor 2 has power of 2 or $2 + 3\alpha_j$ 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,

$$a_0 + a_1 x + x_2 x^2 + \cdots + a_k x^k,\ a_i \in \mathbb{Z}$$

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

$$a_0 n^k + a_1 m n^{k-1} + a_2 m^2 n^{k-2} + \cdots + a_k m^k = 0$$

And

$$-a_0 n^k = a_1 m n^{k-1} + a_2 m^2 n^{k-2} + \cdots + a_k m^k$$

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

$$-a_k m^k = a_0 n^k + a_1 m n^{k-1} + a_2 m^2 n^{k-2} + \cdots + a_{k-1} m^{k-1} n$$

Which implies $n | a_k m^k$ 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 $\{p_1, \dots p_k\} = \{\text{prime factors of } m\} \cup \{ \text{ prime factors of } n \}$. And $\alpha_i, \beta_i \geq 0$. 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 $0 \le M < N$ 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 $d \ge 0$ 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 $\{1, 2, \ldots N\}$ 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

$$\begin{cases} 1 \equiv x_2 m_2 \mod m_1 \\ 1 \equiv x_1 m_1 \mod m_2 \end{cases}$$

Consider

$$x = a x_2 m_2 + b x_1 m_1$$

Clearly

$$\begin{aligned} x - a &= a(x_2 m_2 - 1) + b x_1 m_1 \\ m_1 | (x_2 m_2 - 1) \wedge m_1 | b x_1 m_1 &\implies m_1 | x - a \\ &\implies x \equiv a \mod m_1 \end{aligned}$$

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

$$x = a x_2 m_2 + b x_1 m_1 = 5 \times 8 \times 1 + 13 \times 7 \times 7 = 677$$

■

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.

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

■

18 Lecture 18 Oct. 19 2018 Complex Numbers

Definition 18.1. The **division** on complex numbers is equivalent to multiplying a complex number by its inverse, and is defined as

$$\frac{c + id}{a + id} = (c + id)\frac{a - ib}{a^2 + b^2}$$

Notation 18.1. The set of all complex numbers is denoted as

$$\mathbb{C} = \{a + ib : a, b \in \mathbb{R}, i^2 = -1\}$$

Remark 18.1. Notice that $\mathbb{C}$ is closed under the 4 basic operations of arithmetics.

Definition 18.2. An algebraic structure on which the four basic arithmetic operations are defined and closed under the four operations is called a **field**.

Example 18.1. The irrational set $\mathbb{Q}^c$ is *not* a field.

Definition 18.3. The **complex conjugate** of a complex number $a + ib$ is defined as

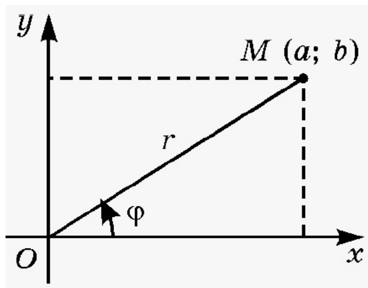
$$a - ib$$

Definition 18.4. The **modulus** of a complex number $a + ib$ is defined as

$$|a + ib| = \sqrt{a^2 + b^2} \in \mathbb{R}_{\geq 0}$$

18.1 The Geometric Representation of Complex Numbers

Any complex could be represented as a vector in a 2-dimensional coordinate, with real line on the x axis and imaginary line on the y axis.



Remark 18.2 (Geometrical Interpretation)**.** The **modulus** is the *distance* from the point to the origin.

Remark 18.3 (Geometrical Interpretation)**.** The **conjugate** is the *reflection* of the point about the real (x) axis.

18.2 Polar Coordinates

18.2.1 Coordinate Conversion

Consider a complex number represented by (a, b) in Cartesian coordinate and (r, θ) in polar coordinate.

Cartesian	Polar
(a, b)	$(\sqrt{a^2 + b^2}, \arctan(\frac{b}{a}))$
$(r\cos(\theta), r\sin(\theta))$	(r, θ)

Remark 18.4. $\arctan(\frac{b}{a})$ gives multiple solutions due to the periodicity of tan. We need to use the signs of real and imaginary values to determine which value of $\arctan\frac{b}{a}$ to take.

Example 18.2. Consider $1+i$, it could be represented as $(1, 1)$ in Cartesian coordinate. Converting it into polar coordinates gives $(\sqrt{2}, \frac{\pi}{4})$. Converting back gives

$$\begin{aligned}1 + i &= \sqrt{2}(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})) \\ &= \sqrt{2}(\cos(\frac{\pi}{4} + 2\pi k) + i\sin(\frac{\pi}{4} + 2\pi k)),\ \forall k \in \mathbb{Z}\end{aligned}$$

18.2.2 Multiplication in Polar Coordinates

Consider the product of two complex numbers $r_1(\cos(\theta_1) + i\sin(\theta_1))$ and $r_2(\cos(\theta_2) + i\sin(\theta_2))$:

$$r_1(\cos(\theta_1) + i\sin(\theta_1)) \times r_2(\cos(\theta_2) + i\sin(\theta_2))$$
$$= r_1 r_2\Big[\Big(\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)\Big) + i\Big(\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)\Big)\Big]$$
$$\text{By triangle inequality}$$
$$= r_1 r_2\Big(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)\Big)$$

Example 18.3. Every complex number has a square root. (Generalized idea: complex field is algebraically closed.)

Proof. Let $z = r(\cos(\theta) + i\sin(\theta)) \in \mathbb{C}$.
Consider $w = \sqrt{r}(\cos(\frac{\theta}{2}) + i\sin(\frac{\theta}{2}))$
By above result, we could easily verify that $w^2 = z$.
Notice that, $w = \sqrt{r}\Big(\cos(\frac{\theta}{2} + \pi) + i\sin(\frac{\theta}{2} + \pi)\Big)$ is also a square root of z. ∎

19 Lecture 19 Oct. 22 2018

19.1 De Moivre's Theorem

Theorem 19.1. (De Moivre's Theorem) Let $z = r[\cos(\theta) + i\sin(\theta)] \in \mathbb{C}$, and the n^{th} power of z is given by

$$(r[\cos(\theta) + i\sin(\theta)])^n = r^n[\cos(n\theta) + i\sin(n\theta)], \ \forall n \in \mathbb{N}$$

Proof. (By induction)
Base Case for $n = 1$, obviously $z^1 = z$
Inductive Step let $k \in \mathbb{N}$,
suppose $z^k = r^k[\cos(k\theta) + i\sin(k\theta)]$
Consider z^{k+1},

$$r^{k+1} = r^k[\cos(k\theta) + i\sin(k\theta)] \times r[\cos(\theta) + i\sin(\theta)]$$
$$= r^{k+1}\Big[(\cos(k\theta)\cos(\theta) - \sin(k\theta)\sin(\theta)) + i(\cos(k\theta)\sin(\theta) + \sin(k\theta)\cos(\theta))\Big]$$
$$\text{By Triangle Identity}$$
$$= r^{k+1}[\cos((k+1)\theta) + i\sin((k+1)\theta)]$$

We could then conclude what the theorem stated by principle of mathematical induction. ∎

Example 19.1. Calculate $(1 + i)^8$.

Solution. $1 + i$ can be written as $(1, 1)$ in Cartesian coordinate.
Then it can be converted into Polar coordinate as

$$\sqrt{2}\Big(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})\Big)$$

Then by De Moivre's theorem,

$$\begin{aligned}
&\Big(\sqrt{2}\Big(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})\Big)\Big)^8 \\
&= (\sqrt{2})^8\Big(\cos(\frac{\pi}{4}\times 8) + i\sin(\frac{\pi}{4}\times 8)\Big) \\
&= 16\times\Big(\cos(2\pi) + i\sin(2\pi)\Big) \\
&= 16(\cos(0) + i\sin(0)) \\
&= 16
\end{aligned}$$

∎

Geometrically Interpretation rotates the vector anti-clockwise by $(n-1)\theta$-radius and enlarge the magnitude by factor of n.

19.2 Roots of Unity

Example 19.2. Find all roots of $z^2 = 1$, where $z \in \mathbb{C}$.

Solution. In polar coordinates, let $z = r(\cos\theta + i\sin\theta)$.
Thus by De Moivre's Theorem, $z^2 = r^2(\cos(2\theta) + i\sin(2\theta))$.
And $1 = 1(\cos(0 + 2k\pi) + \sin(0 + 2k\pi)),\ k \in \mathbb{Z}$ in polar coordinate.
Solving the equation $z^2 = 1$ gives

$$\begin{cases} r^2 = 1 \\ 2\theta = 2k\pi,\ k \in \mathbb{Z} \end{cases}$$

We can conclude that $r = 1$ since it represents a *distance* and $r \in \mathbb{R}_{\geq 0}$.

- $k = 0:\quad r = 1,\ \theta = 0 \to 1(\cos(0) + i\sin(0)) = 1$
- $k = 1:\quad r = 1,\ \theta = \pi \to 1(\cos(\pi) + i\sin(\pi)) = -1$
- $k = 2:\quad r = 1,\ \theta = 2\pi \to 1(\cos(2\pi) + i\sin(2\pi)) = 1$

∎

From the repeating pattern we can conclude that $\forall k \in \mathbb{Z}$ [5]

$$z = 1(\cos(\pi k) + i\sin(\pi k)) = \pm 1$$

[5] The case $k < 0$ is covered by symmetry.

Example 19.3. Find all roots of $z^n = 1$

Solution.

$$
\begin{aligned}
z^n &= r^n[\cos(n\theta) + i\sin(n\theta)] \\
1 &= 1(\cos(2k\pi) + i\sin(2k\pi)) \\
&\implies r = 1 \\
\wedge n\theta = 2k\pi &\iff \theta = k\frac{2\pi}{n}
\end{aligned}
$$

Consider cases

- $k = 0: \quad r = 1,\ \theta = 0$
- $k = 1: \quad r = 1,\ \theta = \frac{2\pi}{n}$
- $k = 2: \quad r = 1,\ \theta = 2\frac{2\pi}{n}$
- $k = 3: \quad r = 1,\ \theta = 3\frac{2\pi}{n}$

Until $k = n$, we have $r = 1 \wedge \theta = n\frac{2\pi}{n} = 2\pi$, where $z|_{k=n} = z|_{k=0}$ and the root starts repeating.
There are n roots in total,

$$
z = \cos(k\frac{2\pi}{n}) + \sin(k\frac{2\pi}{n}),\ k \in \{0, 1, \ldots, n-1\}
$$

∎

Example 19.4. Solve $z^3 = 1$

Example 19.5. Solve $z^4 = 1$

Geometrically Interpretation Divides the unit ball into n equal slices.

Example 19.6. Solve $z^3 = 2 + 2i$

Solution. In polar coordinate,

$$
2 + 2i = \sqrt{8}\Big(\cos(\frac{\pi}{4} + 2k\pi) + i\sin(\frac{\pi}{4} + 2k\pi)\Big)
$$

We have to solve

$$
\begin{aligned}
3\theta &= \frac{\pi}{4} + 2k\pi,\ k \in \mathbb{Z} \\
\implies \theta &= \frac{\pi}{12} + k\frac{2\pi}{3},\ k \in \mathbb{Z}
\end{aligned}
$$

And clearly $r = \sqrt{2}$. And roots are fond by plugging in k with $0, 1, 2$.

$$
\begin{cases}
z_1 = \sqrt{2}(\cos(\frac{\pi}{12}) + i\sin(\frac{\pi}{12})) \\
z_2 = \sqrt{2}(\cos(\frac{\pi}{12} + \frac{2\pi}{3}) + i\sin(\frac{\pi}{12} + \frac{2\pi}{3})) \\
z_3 = \sqrt{2}(\cos(\frac{\pi}{12} + \frac{4\pi}{3}) + i\sin(\frac{\pi}{12} + \frac{4\pi}{3}))
\end{cases}
$$

∎

20 Lecture 20. Oct. 24 2018

Theorem 20.1 (The Fundamental Theorem of Algebra)**.** Every *non-constant* polynomial (with complex coefficients) has a complex root. i.e. for

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0, \quad a_i \in \mathbb{C},\ n \geq 1$$

there exists $r \in \mathbb{C}$ such that $p(r) = 0$.

Example 20.1. Let $p(x) = x^3 - 3x^2 - 9x + 27$, $p(x) = (x-3)^2(x+3)$.
Interpretation *Linear polynomials (polynomials of degree 1) are building blocks of all polynomials.*

Theorem 20.2 (Long Division)**.** Suppose $p(z)$ is a non-constant polynomial and $r \in \mathbb{C}$, there exists a polynomial $q(z) \in \mathcal{P}$ and $c \in \mathbb{C}$ such that

$$p(z) = q(z)(z - r) + c$$

where c is the *reminder* of long division.

Definition 20.1. A polynomial $f(z)$ is a **factor** of another polynomial $p(z)$ if

$$\exists q(z) \in \mathcal{P},\ s.t.\ p(z) = f(z)q(z)$$

Theorem 20.3 (Factor Theorem)**.** A complex number r is a root of a polynomial $p(z)$ if and only if $(z - r)$ is a factor of $p(z)$.

Proof. ($\Longleftarrow$) Suppose $(z - r)$ is a factor.
By definition of factor, $\exists q(z) \in \mathcal{P}$ such that $p(z) = q(z)(z - r)$.
Plugging in r gives $p(r) = q(r)(r - r) = 0$ and suggests r is a root of $p(z)$.
($\Longrightarrow$) Suppose r is a root of $p(z)$.
By the theorem of long division, $\exists q(z) \in \mathcal{P}$ and $c \in \mathbb{C}$ satisfying
$p(z) = q(z)(z - r) + c$.
Plugging in $z = r$ gives $p(r) = q(r)(r - r) + c = 0$, which implies $c = 0$.
That's $p(z) = q(z)(z - r)$. ∎

Theorem 20.4 (Extended Fundamental Theorem of Algebra)**.** A non-zero[6] polynomial of degree n has exactly n roots, counting multiplicities.

Proof. Let $p(z) \in \mathcal{P}$ with degree $n \geq 0$ and suppose $p(z)$ is non-zero.
Case 1: $n = 0$, then $p(z)$ has 0 roots.
Case 2: $n \geq 1$, by the fundamental theorem of algebra,
$p(z)$ has a root $r_1 \in \mathbb{C}$.
By factor theorem, $\exists q_1(z) \in \mathcal{P}(\mathbb{C}),\ s.t.\ p(z) = (z - r_1)q_1(z)$.
Note that $q_1(z)$ has degree of $n - 1$.
If $n - 1 \geq 1$, repeating above argument and we have
$\exists r_2 \in \mathbb{C},\ \exists q_2(z) \in \mathcal{P}(\mathbb{C}),\ s.t.\ q_1(z) = (z - r_2)q_2(z)$.
Note that $q_2(z)$ has degree of $n - 2$.

[6] For zero polynomial, it has infinitely many roots.

Equivalently $p(z) = (z - r_1)(z - r_2)q_2(z)$.
Iterating till $q_i(z)$ has degree 0 (i.e. constant), this will be achieved after exactly n iterations.
Aggregately, we can factorize $p(z)$ into

$$p(z) = (z - r_1)(z - r_2)\dots(z - r_n)q_n$$

where q_n is a constant.
Obviously there are n (possibly repeating) roots, namely $r_1, r_2, \dots, r_n$. ■

21 Lecture 21. Oct. 29 2018

Lemma 21.1 (Triangle Inequality)**.**

$$|z_1 + z_2| \leq |z_1| + |z_2|, \ \forall z_1, z_2 \in \mathbb{C}$$

Lemma 21.2 (Extended version of triangle inequality)**.**

$$|\sum_{i=1}^{n} z_i| \leq \sum_{i=1}^{n} |z_i|, \ \forall (z_i) \in \mathbb{C}^n$$

Definition 21.1. A **closed curve in the plane** is a continuous function mapping from $[0, 2\pi]$ to $\mathbb{C}$ such that its values at 0 and 2π are the same.

Definition 21.2. If $\phi(t) : [0, 2\pi] \to \mathbb{C}$ is a closed curve that does not go through the origin, its **winding number** is the number of times a vector from the origin to a point on the curve winds around the origin as t goes from 0 to 2π.

Example 21.1. Consider

$$\phi(t) = f(t) + i(g)$$

where $f, g : [0, 2\pi] \to \mathbb{R}$ are continuous. Then $\phi(t)$ is continuous.

Example 21.2. Consider

$$\phi(t) = \cos(t) + i\sin(t)$$

the function above is a closed curve with winding nunber +1.

Remark 21.1. If points on the curve go around the origin *anti-clockwise* as t goes from 0 to 2π, then we consider the winding number to be *negative*.

Example 21.3. Curve $\phi(t) = \cos(3t) + i\sin(3t)$ has winding number +3.

Example 21.4. Curve $\phi(t) = 27\cos(4t) + 27i\sin(4t)$ has winding number +4.

Example 21.5. Curve $\phi(t) = \sin(t) + i\cos(t)$ has winding number −1.

Example 21.6. A non-zero constant (e.g. $\phi(t) = 3 + 4i$) is closed and not passing the origin, it has winding number 0.

Remark 21.2. The notation of winding number only apply to closed curves that do **not** passes the origin.

21.1 Proof of the Fundamental Theorem of Algebra

Proof. Idea: prove by contradiction.
Suppose $p(z)$ is a non-constant polynomial with no roots.
i.e.

$$p(z) \neq 0, \ \forall z \in \mathbb{C}$$

and degree of $p(z) = n > 0$.
For each radius $R > 0$ define

$$\phi_R(t) := R(\cos(t) + i\sin(t))$$

Then for each $R > 0$, let

$$p_R(t) := p(\phi_R(t))$$

note that $p_R(t) : [0, 2\pi] \to \mathbb{C}$ and it's a closed curve.
Also note that since $p_R(t) \neq 0 \ \forall t \in [0, 2\pi]$, $p_R(t)$ does not go through the origin.
We will show that

1. If R is large enough then the winding number of $p_R(t) = deg(p(z))$.
2. If R is small enough then the winding number of $p_R(t) = 0$.

But the winding number of $p_R(t)$ is a continuous function of R and it has co-domain of integers. Then it must be the case that $p_R(t)$ is constant, but this contradicts our assumption that $deg(p(z)) > 0$. ■

22 Lecture 22. Oct. 31 2018

Recall the outline of proving the Fundamental Theorem of Algebra.
Suppose $p(z)$ is a non-=constant polynomial with no roots. i.e.

$$p(z) \neq 0 \quad \forall z \in \mathbb{C}$$

Let

$$p_R(t) := p(\phi_R(t))$$

where $\phi(t) : [0, 2\pi] \to \mathbb{C} = R(\cos(t) + i\sin(t))$.
And we well show

1. R is large $\implies$ winding number of $p_R(t) = degree(p(z))$
2. R is small $\implies$ winding number of $p_R(t) = 0$.

Proof. Let $q(z) = z^n$, where n is the degree of polynomial $p(z)$.
Let $L_R(t) = q(\phi_R(t))$.
Note that

$$\begin{aligned} L_R(t) &= q(\phi_R(t)) \\ &= q(R(\cos(t) + i\sin(t))) \\ &= R^n(\cos(nt) + i\sin(nt)) \end{aligned}$$

so $L_R(t)$ has winding number n.

Lemma 22.1. Let $L(t)$ and $M(t)$ be 2 closed curves not passing through the origin. Suppose

$$|L(t) - M(t)| < |L(t)| \quad \forall t \in [0, 2\pi]$$

then $L(t)$ and $M(t)$ have the same winding number.

*We are **not** going to prove this lemma.*

Proof. Proposition 1. Since $L_R(t) = \phi_R(t)^n$,
Suppose

$$p(\phi_R(t)) = a_n z^n + a_{n-1} z^{z-1} + \cdots + a_1 z + a_0$$

WLOG, assume $a_n = 1$.
Then

$$p_R(t) = \phi_R(t)^n + a_{n-1}\phi_R(t)^{n-1} + \cdots + a_1\phi_R(t) + a_0$$

and

$$\begin{aligned}
|L_R(t) - p_R(t)| &= |a_{n-1}\phi_R(t)^{n-1} + \cdots + a_1\phi_R(t) + a_0| \\
&\leq |a_{n-1}\phi_R(t)^{n-1}| + \cdots + |a_0| \\
&= |a_{n-1}||\phi_R(t)|^{n-1} + |a_{n-2}||\phi_R(t)|^{n-2} + \cdots + |a_1||\phi_R(t)| + |a_0| \\
&= |a_{n-1}|R^{n-1} + |a_{n-2}|R^{n-2} + \cdots + |a_1|R + |a_0| \\
&\text{Choosing } R > \max\{1, \sum_{i=1}^{n-1} |a_i|\} \\
&< |a_{n-1}|R^{n-1} + |a_{n-2}|R^{n-1} + \cdots + |a_1|R^{n-1} + |a_0|R^{n-1} \\
&= R^{n-1} \sum_{i=1}^{n-1} |a_i| \\
&< R^n = |L_R(t)|
\end{aligned}$$

Thus we have shown that

$$|L_R(t) - p_R(t)| < |L_R(t)|, \quad \forall t \in [0, 2\pi]$$

by choosing R large enough. By previous lemma, we conclude that $p_R(t)$ has the same winding number as $L_R(t)$, which is n.

∎

Proof. Proposition 2. Note $p(0) = a_0 \neq 0$ since we assumed p has no roots.
Since $p(z)$ is a polynomial so its continuous. (of course near 0)

$$\forall \epsilon > 0, \ \exists \delta > 0 \ s.t. \ 0 < |z - 0| < \delta \implies |p(z) - p(0)| < \epsilon$$

Since $p(0) \neq 0$ and the quadrant(excluding axes) containing a_0 is open.
There exists ϵ such that all points z in $\mathcal{B}(\epsilon, a_0)$ are in that quadrant.
There exists $\delta > 0$ satisfying the continuity definition above and we choose

$$R = \frac{\delta}{2}$$

Then all z in set $\{\phi_R(t) : t \in [0, 2\pi]\}$ are mapped into $\epsilon, \dashv,$, and of course in the quadrant containing a_0.
Therefore the winding number of $p_R(t)$ is 0. ■

altogether with the fact that winding number of $p_R(t)$ is a continuous function from $R_{>0}$ to integers, we conclude that $p_R(t)$ is constant.
This conclusion contradicts our assumption that $p(z)$ is non-constant, i.e. $n \neq 0$.
Thus $p(z)$ has root. ■

23 Lecture 23. Nov. 2 2018

Proposition 23.1. The winding number transformation of $p_R(t) = p(\phi_R(t))$, $W : \mathbb{R}_{>0} \to \mathbb{Z}$ is continuous in R.

Proof. For small enough $\epsilon > 0$,
Consider

$$|p_{R+\epsilon}(t) - p_R(t)| < |p_R(t)|, \ \forall t \tag{1}$$

we will show (1) is true for sufficiently small $\epsilon > 0$.
By lemma 22.1, $p_{R+\epsilon}(t)$ and $p_R(t)$ have the same winding number.
Let

$$p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 \tag{2}$$

Then

$$\begin{aligned}
\left|p_{R+\epsilon}(t) - p_R(t)\right| &= \left|(\phi_{r+\epsilon}(t)^n + a_{n-1}\phi_{r+\epsilon}(t)^{n-1} + \dots) - (\phi_R(t)^n + \dots)\right| &(3)\\
&= \left|(\phi_{r+\epsilon}(t)^n - \phi_R(t)^n) + a_{n-1}(\phi_{r+\epsilon}(t)^{n-1} - \phi_R(t)^{n-1}) + \dots\right| &(4)\\
&= \left|[(R+\epsilon)^n - R^n]e^{int} + a_{n-1}[(R+\epsilon)^{n-1} - R^{n-1}]e^{i(n-1)t} + \dots\right| &(5)\\
&\leq \left|(R+\epsilon)^n - R^n\right|\left|e^{int}\right| + \left|a_{n-1}\right|\left|(R+\epsilon)^{n-1} - R^{n-1}\right|\left|e^{i(n-1)t}\right| + \cdots + \left|a_1\right|\left|e^{it}\right| &(6)
\end{aligned}$$

note that

$$\left|e^{ijt}\right| = 1, \quad \forall j \in \{1, 2, \dots, n\} \tag{7}$$

Thus

$$\left|p_{R+\epsilon}(t) - p_R(t)\right| \leq \sum_{j=1}^{n} \left|(R+\epsilon)^j - R^j\right| \tag{8}$$

Note that we can make $\left|(R+\epsilon)^k - R^k\right|$ as small as we want by specifying a sufficiently small ϵ since x^k is continuous.

■

Definition 23.1. A set S is **finite** if there exists some $n \in \mathbb{N}$ such that the elements of S can be paired with the elements in set $\{1, 2, \dots, n\}$. Equivalently, we can label the elements of S as $s_1, s_2, \dots s_n$.

Definition 23.2. A set is **infinite** if it is not finite.

Definition 23.3. Two sets S and T [7] have the same **cardinality** if and only if there exists a *bijection* between them. Written as $\left|S\right| = \left|T\right|$.

24 Lecture 24. Nov 12. 2018

Example 24.1 (Infinite Sets with Same Cardinality)**.** Let $S = \mathbb{N}$ and $T = \{2, 4, 6, \dots\}$, easy to construct a bijective mapping $f : S \to T$ defined as $f(n) = 2n$ to show S and T have the same cardinality.

Example 24.2 (Infinite Sets with Same Cardinality)**.** Let $S = \mathbb{N}$ and $T = \{2, 3, 4, \dots\}$, easy to construct a bijective mapping $f : S \to T$ defined as $f(n) = n + 1$ to show S and T have the same cardinality.

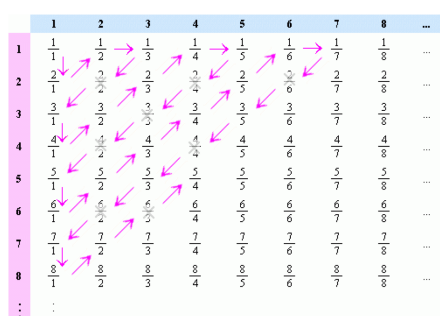
Remark 24.1 (How to prove a set has the same cardinality as natural numbers)**.** If $\left|\mathbb{N}\right| = \left|T\right|$, then $\exists$ bijection $f : \mathbb{N} \to T$. That's we can *enumerate* elements in T with $f(n)$:

$$t_1 = f(1),\ t_2 = f(2), \dots \quad \forall t_i \in T$$

Definition 24.1. Let T be a set, if $\left|T\right| = \left|\mathbb{N}\right|$, then T is **countably infinite** and written as $\left|T\right| = \aleph_0$.

Definition 24.2. A set is **countable** if it is either finite or countably infinite.

Theorem 24.1. Set $S = \mathbb{Q}^+$ is countable infinite.



Proof. ■

[7] S and T are **not** necessarily finite.

Proof. (alternative.) Note that the Cartesian product of countably infinite sets is countably infinite.
Then, for all $\frac{p}{q} \in \mathbb{Q}^+$, where $p, q \in \mathbb{N}$ and p, q are relatively prime.
Setup bijection $\phi : \mathbb{Q}^+ \to \mathbb{N}^2$, defined as $\phi(\frac{p}{q}) = (p, q)$.
So $\left|\mathbb{Q}^+\right| = \left|\mathbb{N}^2\right|$.
Thus $\mathbb{Q}^+$ is countably infinite. ∎

Theorem 24.2. Let $[0, 1]$ be the set of all real numbers between 0 and 1. $[0, 1]$ is not infinitely countable.

Proof. (Prove by contradiction)
Suppose we can list all real numbers between 0 and 1 as

$$\begin{aligned} a_1 &= 0.a_{11}a_{12}a_{13}\ldots \\ a_2 &= 0.a_{21}a_{22}a_{23}\ldots \\ a_3 &= 0.a_{31}a_{32}a_{33}\ldots \\ &\vdots \end{aligned}$$

Consider another real number in $[0, 1]$ constructed as following

$$x = 0.x_1x_2x_3\ldots \text{ where } x_i = \begin{cases} 6 \text{ if } a_{ii} = 5 \\ 5 \text{ otherwise} \end{cases}$$

Note that the first decimal of $x(x_1)$ is not the same as the first decimal of $a_1(a_{11})$, so $x \neq a_1$.
Similarly, the second decimal of $x(x_2)$ is not the same as the second decimal of $a_2(a_{22})$, so $x \neq a_2$,
It is easy to show that $x \neq a_i,\ \forall i$. So x is a real number between 0 and 1 not included in the table above.
Contradicting the assumption that we could list all real numbers between 0 and 1 in a table.
Thus $[0, 1]$ is not infinitely countable. ∎

25 Lecture 25. Nov. 14 2018

Notation 25.1 (the Cardinality of continuum)**.** $\left|[0, 1]\right| = C$

Definition 25.1. $|S| \leq |T|$ if there exists a subset $T_0 \subseteq T$ such that $|T_0| = |S|$. Or, equivalently, there exists an injection maps from S to T.

Definition 25.2. $|S| < |T|$ if $|S| \leq |T|$ and $|S| \neq |T|$.

Proposition 25.1. $|\mathbb{N}| < |[0, 1]|$ (i.e. $\aleph_0 < C$)

Proof. We've already shown that $|\mathbb{N}| \neq |[0, 1]|$.
Consider injection $f : \mathbb{N} \to [0, 1]$ defined as $f(n) = \frac{1}{n}$.

Therefore $|\mathbb{N}| \leq |[0,1]|$.
Or equivalently the subset of $[0,1]$ defined as $\{\frac{1}{n} : n \in \mathbb{N}\}$ has the same cardinality as $\mathbb{N}$.
Thus, by definition, $|\mathbb{N}| < |[0,1]|$. ■

Theorem 25.1 (Schödre-Bernstein-Cantor Theorem)**.** Let S and T be two sets then

$$|S| \leq |T| \wedge |S| \geq |T| \implies |S| = |T|$$

Proof. ■

Proposition 25.2. Let $a, b, c, d \in \mathbb{R}$ satisfying $a < b$ and $c < d$, then

$$|[a,b]| = |[c,d]| = C$$

Every closed interval has the same cardinality.

Proof. Consider mapping $f(x) = (d-c)\frac{x-a}{b-a} + c$.
Obviously, $f : [a,b] \to [c,d]$ and bijective.
And therefore it's inverse is a bijection from $[c,d]$ to $[a,b]$.
Thus those two closed intervals have the same cardinality. ■

Proposition 25.3. $|\mathbb{R}| = |(-\frac{\pi}{2}, \frac{\pi}{2})|$.

Proof. Consider bijection $f(x) := \tan(x)$. ■

Proposition 25.4. $|[0,1]| = |(0,1)|$.

Proof. Step 1. Consider bijection $f(x) := x$ and obviously $|(0,1)| \leq |[0,1]|$.
Step 2. As shown before, all closed interval have the same cardinality. Thus $|[0,1]| = |[\frac{1}{4}, \frac{1}{2}]|$. And clearly $[\frac{1}{4}, \frac{1}{2}] \subsetneq (0,1)$.
So $|[0,1]| = |[\frac{1}{4}, \frac{1}{2}]| \leq |(0,1)|$.
By Schödre-Bernstein-Cantor theorem, $|[0,1]| = |(0,1)|$ ■

Proposition 25.5. Above result can be generalized to arbitrary open and closed intervals, i.e.

$$|[a,b]| = |(c,d)|$$

26 Lecture 26 Nov. 16 2018

Theorem 26.1 (A Countable Union of Countable Sets is Countable)**.** If $|S_i| = \aleph_0,\ \forall i \in \mathcal{I}$ where $|\mathcal{I}| = \aleph_0$, then

$$|\cup_{i\in\mathcal{I}} S_i| = \aleph_0$$

Proof. The proof involving finite union or all finite sets is trivial, here we consider countable as infinitely countable.
Since $S_1 \subseteq \cup_{i\in\mathcal{I}} S_i \implies |S_1| \leq |\cup_{i\in\mathcal{I}} S_i| \implies |\cup_{i\in\mathcal{I}} S_i| \geq \aleph_0$.
Then use the snake argument (count along the diagonal) we can easily prove that the set $\cup_{i\in\mathcal{I}} S_i$ is countable. ■

Example 26.1. $|\mathbb{Q}| = \aleph_0$.

Proof. Obviously, $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$.
Also we've shown that $|\mathbb{Q}^+| = \aleph_0$.
A bijection can be set up between $\mathbb{Q}^+$ and $\mathbb{Q}^-$.
And $\{0\}$ is finite.
So $\mathbb{Q}$ is a finite (countable) union of three countable sets.
Therefore $|\mathbb{Q}| = \aleph_0$. ∎

Example 26.2. $|\mathbb{N}^2| = \aleph_0$

Proof. Note that $\mathbb{N}^2 = \cup_{i\in\mathbb{N}}\{(i, j) : j \in \mathbb{N}\}$, which is a countable union of countable sets.
So $\mathbb{N}^2$ is countable. ∎

Corollary 26.1. As a generalization of above example, the Cartesian product of countable sets is countable.

Theorem 26.2. A countable union of sets with cardinality c also have cardinality c.

$$|S_i| = c,\ \forall i = 1, 2, 3\cdots \implies |\cup_{i=1}^{\infty} S_i| = c$$

Proof. $S_1 \subseteq \cup_{i=1}^{\infty} S_i \implies c = |S_1| \leq \cup_{i=1}^{\infty} S_i$.
WLOG, assume all sets S_i are disjoint.
(Otherwise, we could construct a new collection of disjoint sets by defining $S'_1 = S_1$ and $S'_j = S_j \backslash \cup_{i=1}^{j-1} S_i$)
Since $|S_i| = c$, $|S_i| = |(i, i + 1)|$.
Therefore, for every S_i, there's a bijection between it and open interval $(i, i + 1)$.
Easy to shown that there exists a bijection between $\cup_{i=1}^{\infty} S_i$ and $\cup_{i=1}^{\infty}(i, i + 1) \subseteq \mathbb{R}$.
So, $|\cup_{i=1}^{\infty} S_i| = |\cup_{i=1}^{\infty} (i, i + 1)| \leq |\mathbb{R}| = c$.
Thus $|\cup_{i=1}^{\infty} (i, i + 1)| \leq c$.
By SBC, $|\cup_{i=1}^{\infty} (i, i + 1)| = c$.
∎

Example 26.3. Consider the unit square $S = [0, 1]\times[0, 1]$. S is an uncountably infinite union of uncountably infinite sets.
Claim $|S| = c$.

Proof. $S = \cup_{x\in[0,1]}\{(x, y) : y \in [0, 1]\}$.
Consider $\{(x, 0) : x \in [0, 1]\} \subseteq S$, which has cardinality c.
Therefore $|S| \geq c$.
Consider the function $f : S \to \{(x, 0) : x \in [0, 1]\}$
Consider $(x, y) \in S$ with $x = 0.x_1x_2x_3\ldots$, $y = 0.y_1y_2y_3\ldots$.
Defined f as $f(x, y) = (0.x_1y_1x_2y_2x_3y_3\ldots, 0)$.
f is injective, therefore $|S| \leq c$.
Thus by SBC, $|S| = c$. ∎

Corollary 26.2.

$$|\mathbb{R}^n| = c$$

27 Lecture 27. Nov. 19 2018

Theorem 27.1. Let S be the power set of real numbers, $\mathcal{P}(\mathbb{R})$, then $|S| > c$. [8]

Proof. **Part 1** Consider an injection $f : R \to S$ defined as $f(x) = \{x\}$.
Clearly f is injective but not surjective.
Therefore $c = |\mathbb{R}| \leq S$.
Part 2 we are going to show $|S| \neq |\mathbb{R}|$ by contradiction.
Suppose $|S| = |\mathbb{R}|$, then there must exists a bijection $g : \mathbb{R} \to S$.
Define the set

$$T := \{x \in \mathbb{R} : x \notin g(x)\} \subseteq S$$

We claim that g cannot be surjective by showing that $T \notin g(\mathbb{R})$.
($g(\mathbb{R})$ is the image of g on $\mathbb{R}$.)
Suppose g is surjective, then $\exists z \in \mathbb{R}$ s.t. $g(z) = T$.
Case 1: $z \in g(z) \implies z \notin T \implies z \notin g(z)$.
Case 2: $z \notin g(z) \implies z \in T \implies z \in g(z)$.
Therefore such z cannot exist.
Thus g is not surjective or bijective.
So we cannot construct any bijective transformation between $\mathbb{R}$ and S,
Consequently, $|\mathbb{R}| \neq |S|$. ■

Notation 27.1. For cardinality of $\mathcal{P}(\mathbb{R})$ is denoted as 2^c.

Remark 27.1. Note that $\aleph_0 < c < 2^c$.

Theorem 27.2 (10.3.27)**.** For every set S, $|S| < |\mathcal{P}(S)|$.

Proof. Proof is similar to the proof above, the key is to consider set

$$T = \{x \in S : x \notin g(x)\} \in \mathcal{P}(S)$$

and setup contradiction. ■

Corollary 27.1. There is no largest cardinality.

Definition 27.1 (10.3.14)**.** Let $\mathcal{S}$ and $\mathcal{T}$ be any sets. We will say that $\mathcal{T}$ **can be labelled** by set $\mathcal{S}$ is there is a way of assigning a finite sequence of elements of $\mathcal{S}$ to each element of $\mathcal{T}$ so that each finite sequence corresponds to at most one element of $\mathcal{T}$. (i.e. injective assigning)

Theorem 27.3 (Enumeration Principle)**.** The set of finite sequences of (elements from) a countable set is countable.

Theorem 27.4 (Enumeration Principle)**.** Every set that can be labelled by a countable set is countable.

Example 27.1. The set of all finite sequence of $\mathbb{N}$ is countable.

[8]The **power set** of a set S is defined as the collection of all subsets of set S, including S itself and $\emptyset$.

Proof. The set can be expressed as

$$\cup_{i=0}^{\infty}\{\text{sequence of } \mathbb{N} \text{ with length} = i\} = \cup_{i=0}^{\infty}\mathbb{N}^i$$

Note that we regard $\mathbb{N}^0 = \emptyset$
which is a (infinitely) countable union of countable sets, and consequently countable. ■

Example 27.2. $\mathbb{Q}^+$ is countable.

Proof. Express positive rationals as

$$\mathbb{Q}^+ = \{\frac{m}{n} : m, n \in \mathbb{N}, m, n \text{ are relatively prime.}\}$$

Setup injection $f : \mathbb{Q}^+ \to \mathbb{N}^2$ defined as $f(\frac{m}{n}) = (m, n)$.
Since $\mathbb{N}^2$ can be considered as a set of tuples(finite sequences of length 2) from $\mathbb{N}$,
i.e. $\mathbb{Q}^+$ can be labelled using finite sequences from countable set $\mathbb{N}$.
By enumeration principle, $\mathbb{Q}^+$ is countable, i.e. $|\mathbb{Q}^+| \leq \aleph_0$. ■

28 Lecture 28 Nov. 21 2018

Example 28.1. We've already shown that $|[0, 1]| = |(0, 1]|$ by

$$\begin{aligned}
(0, 1] \subseteq [0, 1] &\implies |(0, 1])| \leq |[0, 1]| \\
|[0, 1]| = |[\frac{1}{2}, 1]| \wedge [\frac{1}{2}, 1] \subseteq (0, 1] &\implies |[0, 1]| \leq |(0, 1]| \\
&\implies |[0, 1]| = |(0, 1]|
\end{aligned}$$

Now construct a bijection between $[0, 1]$ and $(0, 1]$.

$$f(x) = \begin{cases} 1 & \text{if } x = 0 \\ \frac{1}{n+1} & \text{if } \exists n \in \mathbb{N},\ s.t.\ x = \frac{1}{n} \\ x & \text{otherwise} \end{cases} \tag{9}$$

Lemma 28.1. If S is a infinite set, then S contains a countably infinite That's,

$$|S| \geq \aleph_0$$

for all infinite set S. And $\aleph_0$ is the smallest infinite cardinality.

Proof. Let SS be infinite,
Pick $s_1 \in S$ and $S\backslash\{s_1\}$ is still infinite.
Pick $s_2 \in S\backslash\{s_1\}$ and $S\backslash\{s_1, s_2\}$ is still infinite.
⋮
Pick $s_k \in S \backslash \cup_{i=1}^{k-1} \{s_i\}$ and $S \backslash \cup_{i=1}^{k} \{s_i\}$ is still infinite.
We've constructed an infinite (countable) list $\{s_1, s_2, \dots\} \subset S$.
Note that, by construction, there's no repeated elements in the constructed list. ■

Theorem 28.1. Suppose S is an uncountable (infinite) set and $S_0 \subseteq S$ is a countably infinite subset of S, then

$$|S \backslash S_0| = |S|$$

Proof. If $S \backslash S_0$ is finite or countable, then $(S \backslash S_1) \cup S_0 = S$ is also countable as a countable union of countable sets, which contradicts our assumption that S is uncountable.
So $S \backslash S_0$ is uncountably infinite.
By lemma above, we know there exists a countably infinite set $S_1 \subseteq S \backslash S_0$.
The union $S_0 \cup S_1$ is countably infinite, that's,

$$|S_0 \cup S_1| = |S_1| = \aleph_0$$

So there exists a bijection $g : S_0 \cup S_1 \to S_1$.
Define function $f : S \to S \backslash S_0$ as

$$f(x) = \begin{cases} g(x) & \text{if } x \in S_0 \cup S_1 \\ x & \text{otherwise} \end{cases}$$

Note that in the first case, bijection $g(S) = S_1$ and in the second case bijection $y(x) = x$ has range $S \backslash S_1$.
Therefore the domains and ranges of the two pieces in piece-wise function $f(x)$ are all disjoint.
So $f(x)$ is bijective, therefore $|S \backslash S_0| = |S|$. ∎

29 Lecture 29 Nov. 23 2018

Theorem 29.1. A set S is infinite if and only if it has a proper subset with same cardinality as S.

Proof. ($\implies$)
Suppose S is infinite, it has a countable subset $S_0 = \{s_1, s_2, \dots\}$.
Note that $S = (S \backslash S_0) \cup S_0$.
Let $T := S \backslash \{s_1\} \subsetneq S$.
Consider function $f : T \to S$

$$f(x) = \begin{cases} s_{i+1} & \text{if } x \in S_0 \\ x & \text{if } x \in S \backslash S_0 \end{cases}$$

Note that f is a piece-wise function and $f(S_0) \cap f(S \backslash S_0) = \emptyset$.
($\impliedby$)
If S is finite, then any proper subset T would have $|T| < |S|$.
The converse part can be shown by showing its contraposition. ∎

Theorem 29.2. The set of all subset of $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, has cardinality c.

$$2^{\aleph_0} = c$$

Definition 29.1. Let S be a set and the **characteristic function** of set $S_0 \subseteq S$ is a function $f : S \to \{0, 1\}$ defined as

$$f_S(n) = \begin{cases} 1 & \text{if } n \in S_0 \\ 0 & \text{if } n \notin S_0 \end{cases}$$

proof. of above theorem. Obviously, we can construct a characteristic function f_S for any set $S \subseteq \mathbb{N}$ and such a constructor is bijective.
There exists a bijection $\phi : \mathcal{P}(\mathbb{N}) \to \{char.\ func.\} = T$.
Therefore $|\mathcal{P}(\mathbb{N})| = |\{char.\ func.\}| = |T|$
We are going to show $|\mathcal{P}(\mathbb{N})| = c$ by showing $|T| = c$.
Define $\varphi : T \to \mathbb{R}$ as $\varphi(f) := 0.f(1)f(2)f(3)\ldots$,
φ is obviously injective.
Therefore $|T| \leq |\mathbb{R}| = c$.

Consider function $\psi : [0, 1] \to T$ defined in the following way,
for any $x \in [0, 1]$, the binary representation of x is

$$x = \sum_{i=0}^{\infty} b_i 2^{-i} = (b_0 b_1 b_2 b_3 \ldots)_2$$

Defined the image $\psi(x)$ as f such that
$f(i) :=$ the i^{th} element in the binary representation of x.
Consider $x_1, x_2 \in [0, 1]$, suppose $\psi(x_1) = \psi(x_2)$, then x_1 and x_2 have identical binary representation.
Since conversion between binary and decimal representations is bijective, we conclude that $\psi(x_1) = \psi(x_2) \implies x_1 = x_2$.
So that $\psi : [0, 1] \to T$ is injective, and $|T| \geq |[0, 1]| = c$.
By SBC, we conclude $|T| = c$.
Consequently, $\mathcal{P}(\mathbb{N}) = c$. ■

Definition 29.2. A real number is **algebraic** if there exists a non-zero polynomial with integer coefficients that has this number as a root. The set of all algebraic numbers is denoted as $\mathcal{A}$.

Theorem 29.3. Any rational number is algebraic. i.e.

$$\mathbb{Q} \subseteq \mathcal{A}$$

Proof. Let $\frac{m}{n} \in \mathbb{Q}$, where $m, n \in \mathbb{Z}$. Obviously it's a root of polynomial $nx - m$. ■

Theorem 29.4.

$$|\mathcal{A}| = \aleph_0$$

Therefore

$$\mathcal{A} \subsetneq \mathbb{R}$$

Definition 29.3. Real numbers that are not algebraic are called **transcendental**, can be denoted as $\mathbb{R} \backslash \mathcal{A}$.

Example 29.1. π and e are transcendental numbers.

30 Lecture 30. Nov 26 2018

Theorem 30.1.

$$|\mathcal{A}| = \aleph_0$$

Proof. **General idea**: we can label each $a \in \mathcal{A}$ using a finite sequence of integers capturing the coefficients of polynomial having a as a root, altogether with a natural number representing the position order of a as a root. Then $\mathcal{A}$ can be labelled using countable sets then it's countable.
Note that $\mathcal{A}$ can be written as

$$\mathcal{A} = \cup_{i\in\mathbb{N}}\mathcal{A}_i$$

where $\mathcal{A}_i$ denotes the set of $x \in \mathbb{R}$ where x is a root of a polynomial with integer coefficients and degree i.
Note that for any polynomial of degree n

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

can be written as a $(n + 1)$-tuple:

$$(a_n, a_{n-1}, a_{n-2}, \ldots, a_1, a_0) \in \mathbb{Z}^{n+1}$$

By the fundamental theorem of algebra, a polynomial of degree i has i roots, including the multiplicities and complex roots.
For each polynomial of degree i, list its roots in some order and append the index of each root $j \in \{1, 2, \ldots, i\}$ to the $(i + 1)$-tuple representing the polynomial.
So that

$$(a_n, \ldots, a_1, a_0, j) \in \mathbb{Z}^{i+1} \times \{1, 2, \ldots, i\}$$

provides an unique label (i.e. a bijection) to locate every root of every polynomial with integer coefficients and degree i.
i.e.

$$\begin{aligned}&|\{\text{all roots, including complex and duplicates, of polynomials of degree } i\}|\\ &= |\mathbb{Z}^{i+1} \times \{1, 2, \ldots, i\}|\end{aligned}$$

And note that algebraic numbers are all real, so we have to exclude those complex roots from our locator system.
Also, we have to drop the duplicate roots from above label system.
Since $\mathbb{Z}$ and $\{1, 2, \ldots, i\}$ are countable,

$$|\mathbb{Z}^{i+1} \times \{1, 2, \ldots, i\}| = \aleph_0$$

So that

$$|\mathcal{A}_i| \leq |\mathbb{Z}^{i+1} \times \{1, 2, \ldots, i\}| = \aleph_0$$

Lastly, since we've shown that all rational numbers are algebraic and the set of rational numbers is countable.

$$\aleph_0 = |\mathbb{Q}| \leq |\mathcal{A}|$$

Consequently,

$$|\mathcal{A}_i| = \aleph_0, \ \forall i \in \mathbb{N}$$

and $\mathcal{A}$ is a countable union of countable $\mathcal{A}_i$, so

$$|\mathcal{A}| = \aleph_0$$

$\blacksquare$

Notation 30.1. $\mathbb{R} \backslash \mathcal{A}$ denotes the set of **transcendental** numbers.

Theorem 30.2. The set of transcendental numbers has cardinality c.

$$|\mathbb{R} \backslash \mathcal{A}| = c$$

Proof. Since $|\mathbb{R}| = c$ and $|\mathcal{A}| = \aleph_0$,
Taking element since $\mathcal{A}$ has the same cardinality of $\mathbb{N}$.
Consider $\mathbb{R} \backslash \mathbb{N}$, obviously $(-1, 0) \subseteq \mathbb{R} \backslash \mathbb{N}$.
And the open interval in $\mathbb{R}$ has cardinality c.
So

$$c = |(-1, 0)| \leq |\mathbb{R} \backslash \mathbb{N}|$$

and $\mathbb{R} \backslash \mathbb{N} \subseteq \mathbb{R}$ implies

$$|\mathbb{R} \backslash \mathbb{N}| \leq |\mathbb{R}| = c$$

therefore

$$|T| \equiv |\mathbb{R} \backslash \mathcal{A}| = c$$

$\blacksquare$

30.1 Number Fields

Definition 30.1. Any subset of $\mathbb{R}$ which contained $\{0, 1\}$ and closed under the four basic operations of arithmetic, $+, -, \times, \div$, is called a **number field**.

Example 30.1. $\mathbb{R}$, $\mathbb{Q}$, and $\mathcal{A}$ are all number fields.

Example 30.2.

$$\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

is a number field.

Proof. Obviously $\{0, 1\} \subseteq \mathbb{Q}(\sqrt{2})$.
Let $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
Closed under addition and subtraction:

$$(a_1 + b_1\sqrt{2}) \pm (a_2 + b_2\sqrt{2}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Closed under multiplication:

$$(a_1 + b_1\sqrt{2}) \times (a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Closed under division: this can be shown by showing that

$$z \in \mathbb{Q}(\sqrt{2}) \implies \frac{1}{z} \in \mathbb{Q}(\sqrt{2})$$

Let $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$,

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} &= \frac{1}{a+b\sqrt{2}}\frac{a-b\sqrt{2}}{a-b\sqrt{2}} \\ &= \frac{a-b\sqrt{2}}{a^2-2b^2} \\ &= (\frac{a}{a^2-2b^2}) + (\frac{-b}{a^2-2b^2})\sqrt{2} \in \mathbb{Q}(\sqrt{2})\end{aligned}$$

■

31 Lecture 31. Nov. 28 2018

Definition 31.1. The set of points that can be marked on a line, which has zero and one, using straight edge and compass is called **constructible points/numbers**, denoted as C.

Example 31.1. $\mathbb{Z} \in C$

Remark 31.1. If $a, b \in C$, i.e. a and b are constructible, then,

1. $a \pm b \in C$.
2. $\frac{a}{b} \in C$.
3. $a \cdot b \in C$.

Proposition 31.1. From above remark, it's obvious that

1. $C \subseteq \mathbb{R}$,
2. $\{0, 1\} \subseteq C$,
3. and C is closed under four basic arithmetic operations.

So C is a <u>number field</u>.

Remark 31.2. A *number field* is certainly a field, and we add the *number* prefix to emphasize it's a subset of real numbers.

Example 31.2. $\mathbb{Q} \in C$

Proposition 31.2. Let $\mathcal{F}$ be a number field, and exists $0 < r \in \mathcal{F}$ such that $\sqrt{r} \notin \mathcal{F}$. $\mathcal{F}(\sqrt{r})$, called <u>$\mathcal{F}$ adjoin $\sqrt{r}$</u>, is a number field.

Proof. Easy to show $\mathcal{F}(\sqrt{r}) \subseteq \mathbb{R}$ and it contains $\{0, 1\}$.
Let $a, b, r > 0 \in \mathcal{F}$, so $a + b\sqrt{r} \in \mathcal{F}(\sqrt{r})$.
Easy to verify $\mathcal{F}(\sqrt{r})$ is closed under addition, subtraction and multiplication.
To check the division closure, consider the closure under inverse operation:

$$\frac{1}{a+b\sqrt{r}} = \frac{1}{a+b\sqrt{r}}\frac{a-b\sqrt{r}}{a-b\sqrt{r}}$$
$$\frac{a}{a^2-rb^2} - \frac{b}{a^2-rb^2}\sqrt{r} \in \mathcal{F}(\sqrt{r})$$

Note: Given $a + b\sqrt{r} \in \mathcal{F}(\sqrt{r})$, $a - b\sqrt{r}$ is guaranteed to be non-negative.
If $a - b\sqrt{r} = 0$, then $\sqrt{r} = \frac{a}{b} \in \mathcal{F}$, which contradicts our assumption that $\sqrt{r} \notin \mathcal{F}$. So we will not encounter zero division exception while examining closure. ∎

Example 31.3. $\mathbb{Q}(\sqrt{3})$ is a number field.

32 Lecture 32. Nov. 30 2018

Recall $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are number field. And set

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) := \{a + 3b : a, b \in \mathbb{Q}(\sqrt{2})\}$$

is also a number field.

Definition 32.1. A <u>**tower** of number fields</u> is a <u>finite</u> collection of number fields, each obtained from previous one by adjoining a square root.

$$\mathcal{F}_0 \text{ is a field, and,}$$
$$\mathcal{F}_1 := \mathcal{F}_0(\sqrt{r_1}), \quad 0 < r_1 \in \mathcal{F}_0 \wedge \sqrt{r_1} \notin \mathcal{F}_0$$
$$\mathcal{F}_2 := \mathcal{F}_1(\sqrt{r_2}), \quad 0 < r_2 \in \mathcal{F}_1 \wedge \sqrt{r_2} \notin \mathcal{F}_1$$

Example 32.1. The collection $\{\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{2})(\sqrt{3})\}$ is a tower.

Theorem 32.1. Suppose $r \in C$ and $r > 0$, then $\sqrt{r} \in C$.

Remark 32.1.
$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{r_1}) \subseteq \mathbb{Q}(\sqrt{r_1})(\sqrt{r_2}) \subseteq \cdots \subseteq C$$

Theorem 32.2. The union of all towers of number fields equals C.

Proposition 32.1. We cannot trisect a 60-degree angle with compass and straight edge.

Proof. We can easily construct a 60-degree angle.
Note that an angle θ (assuming it's acute) is constructible if and only if $\cos(\theta)$ is constructible.

Recall

$$\cos(A+B) = \cos(A)\cos(B) - \sin(A)\sin(B)$$
$$\sin(A+B) = \sin(A)\cos(B) + \sin(B)\cos(A)$$
$$\cos(2A) = \cos^2(A) - \sin^2(B) = 2\cos^2(A) - 1$$
$$\sin(2A) = 2\sin(A)\cos(A)$$
$$\begin{aligned}\cos(3A) &= \cos(A+2A) = \cos(A)\cos(2A) - \sin(A)\sin(2A)\\ &= \cos(A)(2\cos^2(A)-1) - 2\sin^2(A)\cos(A)\\ &= 2\cos^3(A) - \cos(A) - 2(1-\cos^2(A))\cos(A)\\ &= 4\cos^3(A) - 3\cos(A)\end{aligned}$$

Therefore

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$$

Suppose $\theta = 20 - deg$, then

$$\begin{aligned}\cos(60) = \frac{1}{2} &= 4\cos^3(20) - 3\cos(20)\\ \implies 8\cos^3(20) &- 6\cos(20) - 1 = 0\\ \iff (2\cos(20))^3 &- 3(\cos(20)) - 1 = 0\end{aligned}$$

$\cos(20)$ is constructible if and only if polynomial $x^2 - 3x - 1$ has constructible roots.

Theorem 32.3. If any polynomial with integer coefficients has constructible roots, then all of its roots are rational.

By rational root theorem, if the polynomial has rational roots $\frac{m}{n}$, then it must be ± 1. Easy to verify the polynomial x^2-3x-1 has no rational roots by rational root theorem. Thus it has no constructible roots so $2\cos(20)$ and $\cos(20$ are not constructible.
So 20-deg angle is not constructible and we cannot trisect 60-degree angles with compass and straight edge only. ∎

33 Lecture 33. Dec. 3 2018

Theorem 33.1. If a cubic polynomial with rational coefficients has constructible root(s), then is also have rational root(s).

Lemma 33.1. For any cubic polynomials with rational coefficients, sum of its three roots is also rational.

Proof. WLOG, assuming the leading coefficient of the polynomial is 1.
By the fundamental theorem of algebra, the polynomial has three roots in $\mathbb{C}$.

Let $r_1, r_2, r_3 \in \mathbb{C}$ denote the roots of the polynomial.
The polynomial can therefore, be written as

$$\begin{aligned}&(x - r_1)(x - r_2)(x - r_3)\\ &= x^3 - (r_1 + r_2 + r_3)x^2 + \dots\end{aligned}$$

Obviously, the coefficient of x^2 is a rational number by assumption, so is the sum of roots. ■

Definition 33.1. Let $\mathcal{F}(\sqrt{2})$ be a number field and $a + b\sqrt{r} \in \mathcal{F}(\sqrt{2})$, the **conjugate** of $a + b\sqrt{r}$ is defined as

$$\overline{a + b\sqrt{r}} \equiv a - b\sqrt{r}$$

Lemma 33.2. Let $\mathcal{F}(\sqrt{2})$ be a number field, and $z_1, z_2 \in \mathcal{F}(\sqrt{2})$. Then for any $k \in \mathbb{N}$,

$$\begin{cases}\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}\\ \overline{z_1} \times \overline{z_2} = \overline{z_1 \times z_2}\\ (\overline{z_1})^k = \overline{(z_1)^k}\end{cases}$$

Theorem 33.2. If p is a polynomial with rational coefficients and $p(a+b\sqrt{r}) = 0$, then

$$p(a - b\sqrt{r}) = 0$$

i.e. the conjugate of any root of such polynomial is also a root of this polynomial.

Proof. (Trivial.) ■

proof. of theorem 33.1. Assuming C = the union of all towers of number fields starting with $\mathbb{Q}$ (defined as **surd**).
Suppose root $x_0 = a + b\sqrt{r_k}$ in some tower $\mathcal{F}_k$, where

$$\mathbb{Q} \subset \mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_k$$

and suppose $\mathcal{F}_k$ is the shortest tower containing x_0.
So that $b \neq 0$ (otherwise, $x_0 \in \mathcal{F}_{k-1}$.
Note that $x_1 = a - b\sqrt{r_k}$ is also a root the cubic polynomial.
Let q denote the third root of the cubic polynomial, so that

$$x_0 + x_1 + q = 2a + q \in \mathbb{Q}$$

by above lemma.
Let $s = 2a + q \in \mathbb{Q}$, and $q = s - 2a \in \mathcal{F}_{k-1}$ since $s \in \mathbb{Q} \subset \mathcal{F}_{k-1}$
So if the cubic polynomial has roots in some towers $\mathcal{F}_k \neq \mathbb{Q}$, we can show that this polynomial also have root in $\mathcal{F}_{k-1}$.
By applying above argument recursively, we can show that all roots of this cubic polynomial must be rational. ■

34 Lecture 3 Dec. 5 2018

Example 34.1. Given a constructible angle θ such that $\cos(\theta) = \frac{2}{3}$, show that θ cannot be trisected.

Proof. Recall that $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$.
Therefore $\cos(\theta) = 4\cos^3(\frac{\theta}{3}) - 3\cos(\frac{\theta}{3})$.
Then if θ can be trisected, then $\frac{\theta}{3}$ and $\cos(\frac{\theta}{3})$ are constructible.
So equation $4x^3 - 3x = \frac{2}{3}$ has constructible solutions.
So polynomial $12x^3 - 9x - 2$ has constructible roots.
Therefore it also has rational roots.
Easy to check with rational root theorem, it has no rational roots.
The contradiction suggests $\frac{\theta}{3}$ and $\cos(\frac{\theta}{3})$ cannot be constructed.
Thus θ cannot be trisected. ■

Proposition 34.1. A point with coordinates (a, b) in a plane if constructible if and only if both a and b are constructible.

Definition 34.1. Constructions consist of

1. Join 2 constructible points with a line.
2. Draw a circle centred at a constructible point with constructible radius.
3. Taking intersection of constructed objects above.

Theorem 34.1. The union of all surds, S, is equal to the set of all constructible numbers C.

Proof. We've already shown that $S \subseteq C$.
Now showing $C \subseteq S$.
We show that if you start with points whose coordinates are in S, then any construction produce points whose coordinate is also in S.
Easy to verify constructions above preserve the property of being surds.
Clearly $0, 1 \in \mathbb{Q} \subseteq S$,
therefore, any constructible numbers have the property of being surds. ■