Ve203 Discrete Mathematics

Runze Cai

University of Michigan - Shanghai Jiao Tong University
Joint Institute

Spring 2022

Part II

Basic Number Theory and Basic Group Theory

Table of Contents

Divisibility

Definition

Let $n, d \in \mathbb{Z}$ with $d \neq 0$, we say that d divides n, denoted by $d \mid n$, if $n = dk$, for some $k \in \mathbb{Z}$, i.e.,

$$d \mid n \Leftrightarrow (\exists k \in \mathbb{Z})(n = dk)$$

By convention, $0 \mid n$ only if $n = 0$.

The following expressions are equivalent

- d divides n.
- n is divisible by d.
- n is a multiple of d.
- d is a divisor of n.
- d is a factor of n.

Divisibility

Non-divisibility

If d does not divide n, we write $d \nmid n$. Note that

$$d \nmid n \Leftrightarrow \frac{n}{d} \notin \mathbb{Z}$$

Examples

- $n \mid 0$ for all $n \in \mathbb{Z}$.
- $1 \mid n$ for all $n \in \mathbb{Z}$.
- If $d \in \mathbb{Z}$, then $d \mid 1 \Rightarrow d = \pm 1$.
- If $d \in \mathbb{N}$ and $d \mid 2021$, then $d =?$.

Prime Numbers

Definition

A natural number $p \in \mathbb{N}$ is a prime number (or simply, a prime) if $p \geq 2$ and if p is divisible only by itself and 1.

Remark

A natural number $p \in \mathbb{N}$ is a prime number if it has exactly two distinct factors. The set of all primes is sometimes denoted by $\mathbb{P}$.

Remark

1 is NOT a prime.

For convenience, e.g.,

- Unique factorization property.
- Largest power of p dividing n.
- Riemann Zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}}$.

Famous Prime Numbers

Mersenne Primes

Mersenne Prime is a prime of the form $2^n - 1$.

- $2^2 - 1 = 3 \in \mathbb{P}$
- $2^3 - 1 = 7 \in \mathbb{P}$
- $2^5 - 1 = 31 \in \mathbb{P}$
- $2^7 - 1 = 127 \in \mathbb{P}$
- Necessary condition: $2^n - 1 \in \mathbb{P} \Rightarrow n \in \mathbb{P}$.
  - $2^{11} - 1 = 2047 = 23 \times 89$.
- Not all primes are Mersenne.
  - $5 \in \mathbb{P}$ but is not Mersenne.

Famous Prime Numbers

Fermat Numbers

$F_n = 2^{2^n} + 1$.

- $F_0 = 2^{2^0} + 1 = 3 \in \mathbb{P}$.
- $F_1 = 2^{2^1} + 1 = 5 \in \mathbb{P}$.
- $F_2 = 2^{2^2} + 1 = 17 \in \mathbb{P}$.
- $F_3 = 2^{2^3} + 1 = 257 \in \mathbb{P}$.
- $F_4 = 2^{2^4} + 1 = 65537 \in \mathbb{P}$.
- $F_5 = 2^{2^5} + 1 = 4274967297 = 641 \times 6700417$. (Euler, 1732)

The only known Fermat primes are F_0, F_1, F_2, F_3, F_4.

Famous Conjectures

Goldbach Conjecture (18th century), “1+1”

Can every even number greater than 4 be written as the sum of 2 primes?

- $4 = 2 + 2$
- $6 = 3 + 3$
- $8 = 3 + 5$
- $10 = 5 + 5$
- $20 = 7 + 13$
- $200 = 7 + 193$
- $2040 = 1019 + 1021$

Jing-run Chen, 1966, “1+2”

All sufficiently large even numbers are the sum of a prime and the product of at most two primes

$$2n = p_1 + p_2 p_3$$

Famous Conjectures

Twin Prime Conjecture

Twin primes are a pair of primes which differ by 2:

- (3, 5); (5, 7); (11, 13); (17, 19); (29, 31); (41, 43); (59, 61); (71, 73); (107, 109); (2027, 2029); (1,000,037, 1,000,039);

Are there infinitely many such pairs?

Yitang Zhang: Bounded gaps between primes, 2014

It is proved that

$$\liminf_{n\to\infty}(p_{n+1} - p_n) < 7 \times 10^7,$$

where p_n is the n-th prime.

Infinitude of Primes

Theorem

There are infinitely many primes.

Proof of Euclid.

For any finite set $\{p_1, \ldots, p_r\} \subset \mathbb{P}$, consider the number $n = p_1 p_2 \cdots p_r + 1$. Note that $p_i \nmid n$ for all $i = 1, \ldots, r$, then

- either n is a prime,
- or n has a divisor $p \notin \{p_1, \ldots, p_r\}$.

Either way a new prime is generated from the finite set, hence $\{p_1, \ldots, p_r\}$ cannot be the whole collection of all primes. $\square$

Example

- $\{2, 3, 7\} \subset \mathbb{P}$, $2 \cdot 3 \cdot 7 + 1 = 43 \in \mathbb{P}$;
- $2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \times 139$.

Euclid's Proof of the Infinity of the Number of Primes

Note that the proof does not state that $n = p_1 \cdot p_2 \cdots p_r + 1$ must be a prime. However, it is interesting to note that it often seems to be the case:

- $2 + 1 = 3$,
- $2 \cdot 3 + 1 = 7$,
- $2 \cdot 3 \cdot 5 + 1 = 31$,
- $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$,
- $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$,
- $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$, etc.

It is not known whether there are infinitely many r for which n is prime.

Infinitely Many Twin Primes?

- Euclid number: $E_n = p_1 \cdots p_n + 1$
- Euclid number of the second kind (also called Kummer number): $E_n = p_1 \cdots p_n - 1$.

Variant of Euclid's Theorem

Lemma

Given $p \in \mathbb{P}$, $k \in \mathbb{N}$, if $p \mid k^2 + 1$, then $p = 2$ or p is of the form $4m + 1$.
e.g.,

- $2^2 + 1 = 5$
- $3^2 + 1 = 2 \times 5$
- $4^2 + 1 = 17$
- $5^2 + 1 = 2 \times 13$

We'll prove this later.

Example

There are infinitely many primes of the form $4m + 1$, $m \in \mathbb{N}$. Given $\{p_1, p_2, \ldots, p_m\} \subset \mathbb{P}$, take $n = 4(p_1 \cdots p_m)^2 + 1$. Either n is a new prime, which is of the form $4m + 1$, or

- there is a new prime $p_{m+1} \mid n$,
- since $p_{m+1} \in \mathbb{P}$, and $p_{m+1} \mid n$, but $p_{m+1} \neq 2$, thus p_{m+1} is of the form $4m + 1$.

Dirichlet's Theorem

Theorem

There are infinitely many primes of the form $an + b$*, for* $n \in \mathbb{N}$*, and* a, b *coprime.*

cf., Stein, Fourier Analysis.

Table of Contents

Greatest Common Divisor

Definition

Let $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$ or simply (a, b), is the positive integer d satisfying:

- d is a common divisor of a and b, i.e.,

$$d \mid a \qquad \text{and} \qquad d \mid b$$

- If c also divides a and b, then $c \leq d$ (or $c \mid d$). In other words,

$$\forall c \in \mathbb{N}, \text{ if } c \mid a \text{ and } c \mid b, \text{ then } c \leq d.$$

Example

- $\gcd(72, 63) = 9$
- $\gcd(10^{12}, 6^{18}) = \gcd(2^{12} \cdot 5^{12}, 2^{18} \cdot 3^{18}) = 2^{12}$
- $\gcd(5, 0) = 5$
- $\gcd(0, 0) = 0$

Calculate gcd(m, n), Algorithm 1

Algorithm 1 (assuming $m \le n$)

Input: $m, n \in \mathbb{N} \setminus \{0\}$, $m \le n$
Output: Greatest common divisor of m and n

```
Function gcd(m, n):
    d ← m;
    while d ∤ n and d ∤ n do
        d ← d − 1
    end
    return d
end
```

Advantage

- Simple
- Terminates in finite steps (try $d = 1$)
- Yields the correct answer (which exists)

Disadvantage

- Slow

Calculate $\gcd(m, n)$, $m, n \in \mathbb{N} \setminus \{0\}$

Algorithm 2 (Factorization)

Factor m and n as

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

with $p_1, \ldots, p_k \in \mathbb{P}$, and $\alpha_i, \ldots \alpha_k, \beta_1, \ldots, \beta_k \in \mathbb{N}$. Then

$$\gcd(m, n) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}$$

Disadvantage

- Factorization is hard (until the foreseeable future).

Calculate $\gcd(m, n)$, $m, n \in \mathbb{N} \setminus \{0\}$

Algorithm 3 (Euclidean algorithm, assuming $m \leq n$)

Input: $m, n \in \mathbb{N} \setminus \{0\}$, $m \leq n$
Output: Greatest common divisor of m and n

```
Function gcd(m, n):
    if n mod m = 0 then
        return m
    else
        return gcd(n mod m, m)
    end
end
```

FACTS: For $m, n \in \mathbb{N} \setminus \{0\}$

- If $m \mid n$, then

$$\gcd(n, m) = m.$$

- If $n = qm + r$ with $q \geq 0$ and $0 \leq r < m$, then

$$\gcd(n, m) = \gcd(m, r).$$

Proof of Facts

FACT 1

For $m, n \in \mathbb{N} \setminus \{0\}$, if $m \mid n$, then $\gcd(n, m) = m$.

Proof.

- Since $\gcd(n, m) \mid m$, then $\gcd(n, m) \leq m$.
- Since m is a common divisor, then $m \leq \gcd(n, m)$.

Hence $\gcd(n, m) = m$ $\square$

Proof of Facts

FACT 2

For $m, n \in \mathbb{N} \setminus \{0\}$, if $n = qm + r$ with $q \geq 0$ and $0 \leq r < m$, then $\gcd(n, m) = \gcd(m, r)$

Proof.

- $\gcd(n, m) \leq \gcd(m, r)$. Let c be any common divisor of n and m, i.e., $c \mid m$ and $c \mid n$, hence there exist $k, \ell \in \mathbb{Z}$ such that $n = ck$ and $m = c\ell$. Then

$$
\begin{aligned}
& n = ck = c\ell q + r \\
\Rightarrow \quad & r = ck - c\ell q = c(k - \ell q) \\
\Rightarrow \quad & c \mid r
\end{aligned}
$$

  Take $c = \gcd(n, m)$, hence $\gcd(n, m)$ divides both m and r, so $\gcd(n, m) \leq \gcd(m, r)$.

Proof of Facts

Proof (Cont.)

- $\gcd(m, r) \leq \gcd(n, m)$. Similarly let c be any common divisor of m and r, i.e., $c \mid m$ and $c \mid r$, hence there exist $x, y \in \mathbb{Z}$ such that $m = cx$ and $r = cy$. Then

  $$n = cxq + cy = (xq + y)c$$

  hence $c \mid n$. Take $c = \gcd(m, r)$, hence $c = \gcd(m, r)$ divides both n and m, so $\gcd(m, r) \leq \gcd(n, m)$.

Combine the two results. $\square$

Division Algorithm

Theorem ((Long) Division Algorithm)

Given $m, n \in \mathbb{N} \setminus \{0\}$, there exist unique integers q and r with $q \geq 0$ and $0 \leq r < m$ so that $n = qm + r$.

Proof.

Existence by induction on n. Let

$$S = \{n \in \mathbb{N} \mid (\forall m > 0)(\exists q, r \text{ with } q \geq 0 \text{ and } 0 \leq r < m)(n = qm + r)\}$$

- $1 \in S$. ($1 = 1 \cdot 1 + 0$ for $m = 1$, and $1 = 0m + 1$ for $m > 1$)
- Let $k \in S$. Then for any $m > 0$, there exist q, r such that $k = qm + r$. Now
  - $k + 1 = qm + (r + 1)$, if $r + 1 < m$;
  - $k + 1 = (q + 1)m + 0$, if $r + 1 = m$.

  Thus $k + 1 \in S$.

Division Algorithm

Proof (Cont.)

Uniqueness.
Suppose $n = q_1 m + r_1 = q_2 m + r_2$, then $r_1 - r_2 = (q_2 - q_1)m$, thus if $q_1 \neq q_2$, then $m \mid (r_1 - r_2)$.
But $|r_1 - r_2| < m$, hence $r_1 - r_2 = 0$.
But then $q_1 = q_2$, contradiction. $\square$

Remark

Note that $(q_1 - q_2)m + (r_1 - r_2) = 0$ implies $q_1 - q_2 = 0$ and $r_1 - r_2 = 0$, which is basically applying the long division algorithm to 0.

Euclidean Algorithm

Euclidean Algorithm

Given positive integers n and m, we can repeat the division algorithm to obtain a series of equations

$$
\begin{aligned}
n &= mq_1 + r_1, && 0 < r_1 < m \\
m &= r_1 q_2 + r_2, && 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, && 0 < r_3 < r_2 \\
&\vdots \\
r_{j-2} &= r_{j-1} q_j + \color{red}{r_j}, && 0 < r_j < r_{j-1} \\
r_{j-1} &= r_j q_{j+1}
\end{aligned}
$$

Then $\gcd(n, m) = r_j$.

Remark: By induction and the two facts, the Euclidean algorithm terminates within finite number of steps and produce the correct answer.

Euclidean Algorithm

Example

$n = 42823$ and $m = 6409$

$$\begin{aligned} 42823 &= 6409 \times 6 + 4369 & &(42823, 6409) \\ 6409 &= 4369 \times 1 + 2040 & &= (6409, 4369) \\ 4369 &= 2040 \times 2 + 289 & &= (4369, 2040) \\ 2040 &= 289 \times 7 + 17 & &= (2040, 289) \\ 289 &= 17 \times 17 + 0 & &= (289, 17) = 17 \end{aligned}$$

Remark

The Euclidean algorithm provides a solution to the Diophantine equation

$$mx + ny = \gcd(m, n)$$

by back-tracking.

Euclidean Algorithm

Example (Cont.)

Consider the Diophantine equation
$42823x + 6409y = 17 = \gcd(42823, 6409)$.

Euclidean Algorithm

$$\begin{aligned}
42823 &= 6409 \times 6 + 4369 \\
6409 &= 4369 \times 1 + 2040 \\
4369 &= 2040 \times 2 + 289 \\
2040 &= 289 \times 7 + 17 \\
289 &= 17 \times 17 + 0
\end{aligned}$$

Back-Tracking

$$\begin{aligned}
17 &= 2040 - 289 \times 7 \\
&= 2040 - (4369 - 2040 \times 2) \times 7 \\
&= 2040 \times 15 - 4369 \times 7 \\
&= (6409 - 4369) \times 15 - 4369 \times 7 \\
&= 6409 \times 15 - 4369 \times 22 \\
&= 6409 \times 15 - (42823 - 6409 \times 6) \times 22 \\
&= 6409 \times (15 + 6 \times 22) - 42823 \times 22 \\
&= 6409 \times 147 - 42823 \times 22
\end{aligned}$$

Let's take $x = -22$ and $y = 147$.

Euclidean Algorithm

Example (Cont.)

$$\frac{42823}{6409} = 6 + \frac{6369}{6409} = 6 + \cfrac{1}{1 + \cfrac{2040}{4369}} = 6 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{289}{2040}}}$$

$$= 6 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{7 + \cfrac{17}{289}}}} = 6 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{7 + \cfrac{1}{17}}}}$$

Euclidean Algorithm

Example (Cont.)

$$6+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{7+\cancel{\cfrac{1}{17}}}}}=6+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{7}}}=6+\cfrac{1}{1+\cfrac{7}{15}}=6+\frac{15}{22}=\frac{147}{22}$$

Now

$$\frac{42823}{6409}=\frac{2519}{377}\lesseqgtr\frac{147}{22}?$$

Of course

$$377\times 147-2519\times 22=1$$

i.e.,

$$6409\times 147-42823\times 22=17$$

Calculate $\gcd(m, n)$, $m, n \in \mathbb{N} \setminus \{0\}$

Algorithm 4 (Binary Euclidean/GCD Algorithm)

Input: $m, n \in \mathbb{N} \setminus \{0\}$
Output: Greatest common divisor of m and n

Function $\texttt{gcd}(m, n)$**:**
  if $n = m$ **then return** m;
  else if $2 \mid m$ **and** $2 \mid n$ **then return** $2\texttt{gcd}(m/2, n/2)$;
  else if $2 \mid m$ **then return** $\texttt{gcd}(m/2, n)$;
  else if $2 \mid n$ **then return** $\texttt{gcd}(m, n/2)$;
  else if $m > n$ **then return** $\texttt{gcd}(m - n, n)$;
  else return $\texttt{gcd}(m, n - m)$;
end

FACTS:

- If $2 \mid m$ and $2 \mid n$, then $\gcd(m, n) = 2\gcd(m/2, n/2)$.
- If $2 \mid m$ and $2 \nmid n$, then $\gcd(m, n) = \gcd(m/2, n)$

Table of Contents

Groups

Definition

A group is a pair $(G, \cdot)$, where G is a set, and $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h = gh$, is a law of composition (aka group law) that has the following properties:

- The law of composition is associative: $(ab)c = a(bc)$ for all $a, b, c \in G$.
- G contains an identity element 1, such that $1a = a1 = a$ for all $a \in G$.
- Every element $a \in G$ has an inverse, an element b such that $ab = ba = 1$.

An abelian group is a group whose law of composition is commutative.

Example

- $(\mathbb{Z}, +)$
- $(\mathbb{R} \setminus \{0\}, \cdot)$
- The set of $n \times n$ invertible matrices $GL_n(\mathbb{R})$ or $GL_n(\mathbb{C})$.

Elementary Properties of Groups

Theorem

Given a group G, $a, b, c \in G$, then

- *there exists a unique identity element.*
- $ba = ca \Rightarrow b = c$ *and* $ab = ac \Rightarrow b = c$.
- *For all $a \in G$, there exists a unique element $b \in G$ such that* $ab = ba = 1$.
- $(ab)^{-1} = b^{-1}a^{-1}$.

Subgroup

Definition

A subset H of a group G is a subgroup if it has the following properties:

- Closure: If $a, b \in H$, then $ab \in H$.
- Identity: $1 \in H$.
- Inverses: If $a \in H$, then $a^{-1} \in H$.

Subgroups of the Additive Group $(\mathbb{Z}, +)$

A subset S of $(\mathbb{Z}, +)$ is a subgroup if

- Closure: If $a, b \in S$, then $a + b \in S$.
- Identity: $0 \in S$.
- Inverses: If $a \in S$, then $-a \in S$.

For $a \in \mathbb{Z}$, a subgroup of $(\mathbb{Z}, +)$ is given by

$$a\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \in \mathbb{Z}\}$$

Subgroup of $(\mathbb{Z}, +)$

Subgroups of the Additive Group $(\mathbb{Z}, +)$

A subset S of $(\mathbb{Z}, +)$ is a subgroup if

- Closure: $a, b \in S \Rightarrow a + b \in S$.
- Identity: $0 \in S$.
- Inverses: $a \in S \Rightarrow -a \in S$.

For $a \in \mathbb{Z}$, a subgroup of $(\mathbb{Z}, +)$ is given by integers divisible by a as,

$$a\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \in \mathbb{Z}\}$$

Remark

We write $H \leq G$ if H is subgroup of G.

Example

- $a = 0$ yields the trivial group $(\{0\}, +)$.
- $a = 1$ yields the whole of $(\mathbb{Z}, +)$.

Subgroup of $(\mathbb{Z}, +)$

Theorem

Let S be a subgroup of the additive group $(\mathbb{Z}, +)$, then

- *either S is the trivial subgroup $(\{0\}, +)$,*
- *or it has the form $a\mathbb{Z}$, where a is the smallest positive integer in S.*

Proof.

Let S be a subgroup of $(\mathbb{Z}, +)$, then $0 \in S$. If $S = \{0\}$, then we are done. Otherwise, $\exists n \in \mathbb{Z} \cap S - \{0\}$, then $\pm n \in S$ by subgroup property of S, hence either n or $-n$ is a positive integer.

Next we show $S = a\mathbb{Z}$, where a is the smallest positive integer of S.

- $a\mathbb{Z} \subset S$. Let $z \in a\mathbb{Z}$, then $z = ka$ for some $k \in \mathbb{Z}$. Suppose $z > 0$, since $a \in S$, then $ka \in S$ for $k \in \mathbb{N}$ by induction and closure. Also $-ka \in S$ by the inverse property. Similar goes for $z < 0$. If $z = 0 \in a\mathbb{Z}$, then also $z = 0 \in S$.

Subgroup of $(\mathbb{Z}, +)$

Proof (Cont.)

- $a\mathbb{Z} \supset S$. Take $n \in S$, then $n = qa + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < a$. Now since $qa \in a\mathbb{Z} \subset S$, and $n \in S$, then $r = n - qa \in S$. But a is the smallest positive integer in S, hence $r = 0$. Therefore $n = qa$ for some $q \in \mathbb{Z}$, thus $n \in a\mathbb{Z}$.

Therefore $a\mathbb{Z} = S$. □

Definition

Given $a, b \in \mathbb{Z}$, then the subgroup S generated by a and b, denoted by

$$S = a\mathbb{Z} + b\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ra + sb \text{ for some integers } r, s\}$$

It is also the smallest subgroup that contains both a and b.

Remark

Since $S \subset \mathbb{Z}$ is a subgroup, then $S = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.

Subgroup of $(\mathbb{Z}, +)$

Theorem

Let $a, b \in \mathbb{Z}$, not both zero, and let d be the positive integer that generates the subgroup $S = a\mathbb{Z} + b\mathbb{Z}$, i.e., $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Then

1. *$d \mid a$ and $d \mid b$.*
2. *For $e \in \mathbb{Z}$, if $e \mid a$ and $e \mid b$, then $e \mid d$.*
3. *There are integers r and s such that $d = ra + sb$.*

Note that $d = \gcd(a, b)$.

Proof.

1. $a \in \mathbb{Z}d$ and $b \in \mathbb{Z}d$.
3. $d \in \mathbb{Z}a + \mathbb{Z}b$.
2. Let $d = ra + sb$, then $e \mid a$ and $e \mid b$ implies $e \mid (ra + sb)$, therefore $e \mid d$. $\square$

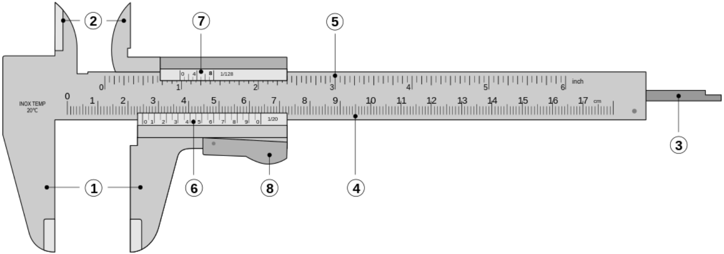
Subgroup of $(\mathbb{Z}, +)$

Corollary (Bézout Identity)

Given $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$, i.e., a and b relatively prime or coprime iff there exist $r, s \in \mathbb{Z}$ such that $ra + sb = 1$.

Remark

The proof is just by letting $d = 1$. In this case $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.



Vernier Caliper

Subgroup of $(\mathbb{Z}, +)$

Corollary

Let p be prime, and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof.

Suppose $p \nmid a$, then $\gcd(a, p) = 1$. Therefore $\exists r, s \in \mathbb{Z}$ such that $ra + sp = 1$. Hence $rab + spb = b$. Note that $p \mid rab$ and $p \mid spb$, thus $p \mid b$. $\square$

Remark

By induction, given $p \in \mathbb{P}$, and $a_1, \ldots, a_n \in \mathbb{Z}$, if $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some factor a_i of the product.

Corollary

If $c \mid ab$ and $\gcd(b, c) = 1$, then $c \mid a$.

Fundamental Theorem of Arithmetic

Theorem

Every positive integer can be written uniquely (up to order) as a product of primes (with possibly only one factor).

Remark

Convention: 1 is the product of empty set of primes

Proof.

- Existence: If $n > 1$, then either n is prime, or can be factored into, say $n = p \cdot (n/p)$ for some prime p, continue by induction.
- Uniqueness: Suppose $n = p_1 \cdots p_r = q_1 \cdots q_s$, with p_i, q_i primes. Then $p_1 \mid (q_1 \cdots q_s)$, thus $p_1 = q_i$ for some i. Cancel p_1 and q_i and continue by induction. $\square$

Fundamental Theorem of Arithmetic

Other versions of Fundamental Theorem of Arithmetic

- Integers. (allow negative primes and -1).
- Polynomials over a field. (Factor into irreducible polynomials)

Examples of Non-uniqueness

- Positive integers of the form $4n+1$. Consider 1, 5, 9, 13, 17, 21, $25 (= 5^2)$, 29, 33, 37, 41, $45 (= 5 \cdot 9)$, 49, ...

$$21 \cdot 21 = 9 \cdot 49.$$

- Consider numbers of the form $m + n\sqrt{-5}$, $m, n \in \mathbb{Z}$, then

$$2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Fundamental Theorem of Arithmetic

Riemann Zeta Function

Euler discovered that (equivalent to fundamental theorem of arithmetic)

$$\begin{aligned}\zeta(s) &= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \frac{1}{1-7^{-s}} \cdots \\ &= \prod_{p \in \mathbb{P}} \frac{1}{1-p^{-s}}\end{aligned}$$

Let $s = 1$, then by divergence of the harmonic series, there are infinitely many primes.

Theorem (Dirichlet)

If $u, v \in \mathbb{Z}$ are chosen at random, the probability that $\gcd(u, v) = 1$ is $\zeta(2)^{-1} = 6/\pi^2 \approx 0.60793$.

Fundamental Theorem of Arithmetic

Example

To illustrate $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1-p^{-s}}$, consider

$$
\begin{aligned}
&\frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \frac{1}{1-7^{-s}} \cdots \\
&\quad = (1 + 2^{-s} + (2^{-s})^2 + (2^{-s})^3 + \cdots) \\
&\qquad (1 + 3^{-s} + (3^{-s})^2 + (3^{-s})^3 + \cdots) \\
&\qquad\quad (1 + 5^{-s} + (5^{-s})^2 + (5^{-s})^3 + \cdots) \\
&\qquad\qquad (\cdots)
\end{aligned}
$$

Note that, for example,

$$(2^{-s})^3 \cdot (3^{-s}) \cdot (5^{-s})^2 = \frac{1}{(2^3 \cdot 3 \cdot 5^2)^s} = \frac{1}{600^s}$$

Fundamental Theorem of Arithmetic

Also by Euler, $p \in \mathbb{P}$,

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p} \approx \log\log p \text{ “}\approx 3\text{”}$$

n	$\log\log n$
10^3	1.9
10^9	2.6
10^9	3.0
10^{12}	3.3
10^{15}	3.5

Least Common Multiple

Theorem

*Let $a, b \in \mathbb{Z} \setminus \{0\}$, and let $m = \operatorname{lcm}(a, b)$ be their **least common multiple** — the positive integer that generates the subgroup $S = a\mathbb{Z} \cap b\mathbb{Z}$, i.e., $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Then*

- *$a \mid m$ and $b \mid m$.*
- *$a, b \mid n$ for some $n \in \mathbb{Z}$, then $m \mid n$.*

Proof.

Note that $a\mathbb{Z} \cap b\mathbb{Z}$ is a nontrivial subgroup of $(\mathbb{Z}, +)$. □

Remark

Again by induction, if n is any common multiple of $a_1, \ldots, a_n \in \mathbb{Z}$, then $\operatorname{lcm}(a_1, \ldots, a_n) \mid n$.

Greatest Common Divisor and Least Common Multiple

Corollary

Given $a, b \in \mathbb{N} \setminus \{0\}$*, let* $d = \gcd(a, b)$ *and* $m = \operatorname{lcm}(a, b)$*, then* $ab = dm$*.*

Proof.

- Since $b/d \in \mathbb{Z}$, then $ab/d \in a\mathbb{Z}$, and similarly $ab/d \in b\mathbb{Z}$. Therefore $ab/d \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, thus $ab \in md\mathbb{Z}$, i.e., $md \mid ab$.
- Since $m/b \in \mathbb{Z}$, and $a \mid m$, then

$$a \,\bigg|\, b \cdot \frac{m}{b} \Leftrightarrow \frac{a}{d} \,\bigg|\, \frac{m}{b} \Leftrightarrow ab \mid dm$$

Therefore $ab = dm$. □

Table of Contents

Cyclic Groups

Definition

A group is ***cyclic*** if it can be ***generated by*** a single element.

Example

In multiplication notation, The cyclic subgroup $H \leq G$ generated by $x \in G$ is the set of all elements that are powers of x,

$$\begin{aligned} H &:= \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\} \\ &= \{x^m \mid m \in \mathbb{Z}\} \end{aligned}$$

This is the ***smallest subgroup*** of G containing x, (often) denoted by $\langle x \rangle$. If there exists a smallest $m \in \mathbb{N} - \{0\}$ such that $x^m = 1$, we say m is the ***order*** of x, denoted by $m = |x|$. Similarly, the ***order*** of a group G, denoted $|G|$, is given by the number of elements of G.

Remark

The powers x^n may represent distinct elements, or not. For example, given $-1 \in \mathbb{R}^\times$, then $\{(-1)^m \mid m \in \mathbb{Z}\} = \{\pm 1\}$.

Cyclic Groups

Theorem

Let $\langle x \rangle$ be the cyclic subgroup of a group G generated by an element x, and let $S := \{k \in \mathbb{Z} \mid x^k = 1\}$, then

1. *The set S is a subgroup of the additive group $(\mathbb{Z}, +)$.*
2. *For $r, s \in \mathbb{Z}$, $x^r = x^s$ iff $x^{r-s} = 1$, i.e., $r - s \in S$.*
3. *Suppose $S \neq \{0\}$, then $S = n\mathbb{Z}$ for some $n \in \mathbb{N} \setminus \{0\}$. The powers 1, x, x^2, $\dots$, x^{n-1} are distinct elements of the subgroup $\langle x \rangle$, and $|\langle x \rangle| = n$, i.e., the order of $\langle x \rangle$ is n.*

Proof.

1. We check the properties of S
   - Let $k, \ell \in S$, then $x^k = x^\ell = 1$, hence $x^{k+\ell} = x^k x^\ell = 1$, therefore $k + \ell \in S$.
   - $x^0 = 1$, hence $0 \in S$.
   - If $k \in S$, i.e., $x^k = 1$, then $x^{-k} = (x^k)^{-1} = 1$, hence $-k \in S$.

Cyclic Groups

Proof (Cont.)

2. By straightforward calculation (cancellation law).
3. If $S \neq \{0\}$, then since S is a subgroup of $(\mathbb{Z}, +)$, then $S = n\mathbb{Z}$ for some smallest positive integer $n \in S$. For any $k \in \mathbb{Z}$, $k = qn + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < n$. Thus $x^k = x^{qn+r} = x^{nq}x^r = x^r$. Note that $1, x, x^2, \ldots, x^{n-1}$ are distinct since n is the smallest power such that $x^n = 1$. $\square$

Remark

- If $|x| = \infty$, then $x^r = x^s$ iff $r = s$ (since $r - s \in \{0\}$).
- If $|x| < \infty$, say, $|x| = n \in \mathbb{N}$, then $x^r = x^s$ iff $n \mid r - s$, i.e., $r \equiv s \pmod{n}$ (since $r - s \in n\mathbb{Z}$).
- $|x| = |\langle x \rangle|$.
- If $|x| = n$ and $x^k = 1$, then $n \mid k$.

Cyclic Groups

Examples

- $(\mathbb{Z}, +)$
- $\mathbb{Z}/8\mathbb{Z} = \langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle$.
- $\langle r \mid r^n = 1 \rangle$, where r represents counterclockwise rotation of $2\pi/n$.
- $\{e^{2\pi ik/n} \mid k \in \mathbb{Z}\} = \langle e^{2\pi i/n} \rangle$, $n \in \mathbb{N} \setminus \{0\}$.
- $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv$, where $a \equiv b$ if $n \mid a - b$, i.e., $a - b \in n\mathbb{Z}$, for given $n \in \mathbb{N} \setminus \{0\}$.

Nonexamples

- The Klein four group $V = \left\{ \begin{bmatrix} \pm 1 & \\ & \pm 1 \end{bmatrix} \right\}$.
- The quaternion group $H = \{\pm \mathbf{1}, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}$, where

$$\mathbf{1} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \quad \boldsymbol{i} = \begin{bmatrix} i & \\ & -i \end{bmatrix}, \quad \boldsymbol{j} = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}, \quad \boldsymbol{k} = \begin{bmatrix} & i \\ -i & \end{bmatrix}$$

Cyclic Group

Theorem

Let $n, k \in \mathbb{N} \setminus \{0\}$. Given group G and $x \in G$ with $|x| = n \in \mathbb{N} \setminus \{0\}$, then $\langle x^k \rangle = \langle x^{\gcd(n,k)} \rangle$ and $|x^k| = n/\gcd(n,k)$.

Proof.

Note that since $|x| = n$, we have

$$\begin{aligned}
\langle x^k \rangle &= \{(x^k)^t \mid t \in \mathbb{Z}\} = \{x^{kt+ns} \mid t, s \in \mathbb{Z}\} \\
&= \{x^d \mid d \in k\mathbb{Z} + n\mathbb{Z}\} = \{x^d \mid d \in \gcd(n,k)\mathbb{Z}\} \\
&= \{(x^{\gcd(n,k)})^r \mid r \in \mathbb{Z}\} = \langle x^{\gcd(n,k)} \rangle
\end{aligned}$$

Next note that for $m \in \mathbb{Z} \setminus \{0\}$, $a \mid b$ iff $ma \mid mb$. Let $t := |x^k|$, then $t = |x^k| = |\langle x^k \rangle| = |\langle x^{\gcd(n,k)} \rangle| = |x^{\gcd(n,k)}|$. Thus

- $(x^{\gcd(n,k)})^t = 1 \Rightarrow n \mid \gcd(n,k)t \Rightarrow n/\gcd(n,k) \mid t$;
- $(x^{\gcd(n,k)})^{n/\gcd(n,k)} = x^n = 1 \Rightarrow t \mid n/\gcd(n,k)$. □

Cyclic Groups

Remark

- Let $|\langle x\rangle| < \infty$, then $y \in \langle x\rangle \Rightarrow |y|$ divides $|\langle x\rangle|$.
- Let $|x| = n \in \mathbb{N} \setminus \{0\}$, then

  $$\langle x^i\rangle = \langle x^j\rangle \Leftrightarrow |x^i| = |x^j| \Leftrightarrow \mathrm{gcd}(n,i) = \mathrm{gcd}(n,j)$$

  In particular,

  $$\langle x\rangle = \langle x^j\rangle \Leftrightarrow |x| = |x^j| \Leftrightarrow \mathrm{gcd}(n,j) = 1$$

  For example,

  $$\langle k\rangle = \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \mathrm{gcd}(n,k) = 1$$

Cyclic Groups

Theorem (Fundamental Theorem of Cyclic Groups)

- *Every subgroup of a cyclic group is cyclic.*
- *If* $|\langle x\rangle| = n \in \mathbb{N} \setminus \{0\}$*, then the order of any subgroup of* $\langle x\rangle$ *divides* n*.*
- *For each* $k \mid n$ *with* $k > 0$*, the group* $\langle x\rangle$ *has exactly one subgroup of order* k*, i.e.,* $\langle x^{n/k}\rangle$*.*

Proof.

- Suppose $G = \langle x\rangle$ is cyclic, i.e., $G = \{x^t \mid t \in \mathbb{Z}\}$. If $H \leq G$, then $H = \{x^t \mid t \in S \leq \mathbb{Z}\}$, where $S = m\mathbb{Z}$, $m \in \mathbb{N}$. (Verify this!) Hence $H = \{x^t \mid t \in m\mathbb{Z}, m \in \mathbb{N}\} = \{(x^m)^t \mid t \in \mathbb{Z}\} = \langle x^m\rangle$, which is cyclic.
- Consider $H \leq \langle x\rangle$, then $H = \langle x^m\rangle$ for some $m \in \mathbb{N} \setminus \{0\}$. Now $|\langle x^m\rangle| = |x^m| = n/\gcd(n, m)$, which divides n.
- For uniqueness, if $|\langle x^m\rangle| = k = n/\gcd(n, m)$, then $\langle x^m\rangle = \langle x^{\gcd(n,m)}\rangle = \langle x^{n/k}\rangle$. For existence, note that $|\langle x^{n/k}\rangle| = n/(n/k) = k$. $\square$

Applications of Cyclic Groups

Euler's Totient Function

The ***Euler's Totient Function***, or the ***Euler phi function***, denoted $\varphi(n)$ or $\phi(n)$ counts the number of positive integers less than n and relatively prime to n, i.e.

$$\varphi(n) = |\{k \in \mathbb{N} \mid \gcd(k, n) = 1, 1 \leq k \leq n\}|$$

In particular, given $p \in \mathbb{P}$,

- $\varphi(p) = p - 1$.
- $\varphi(p^k) = p^k - p^{k-1}$ for $k \in \mathbb{N} \setminus \{0\}$. Since the numbers

  $$1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p^{k-1} \cdot p$$

  are NOT relatively prime to p.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Applications of Cyclic Groups

Lemma

Given a cyclic group C with order $|C| = n$, if $d > 0$ and $d \mid n$, then the number of elements of order d in C is given by $\varphi(d)$.

Proof.

Since the group has exactly one subgroup of order d, which is also cyclic. Denote this subgroup by $C_d = \langle x \rangle$ for some $x \in C$ with $x^d = 1$. Now, since $\langle x^k \rangle = \langle x \rangle$ iff $|x^k| = |x| = d$ iff $\gcd(d, k) = 1$, hence the number of elements of order d is given by $\varphi(d)$. □

Remark

Note that $\varphi(d)$ is independent of n in the lemma above.

Divisor Sum (Gauss)

Given $n \in \mathbb{N} \setminus \{0\}$, then

$$\sum_{d \mid n} \varphi(d) = n$$

where the sum is over all positive divisor d of n.

Applications of Cyclic Groups

Proof 1 (Counting generators).

Consider the cyclic group of order n, denoted by C_n. Since C_n can be partitioned into disjoint sets each containing generators of order d with $d \mid n$, each block of size $\varphi(d)$, therefore the equality follows. □

Proof 2.

Consider the set of n fractions $\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\}$, and put each fraction in lowest terms of the form $\frac{c}{d}$ where d is a positive divisor of n, and $\gcd(c, d) = 1$. For each denominator d there are $\varphi(d)$ relatively prime numerators. The total number of fractions is given by $\sum_{d|n} \varphi(d)$.
For example, consider $n = 20$, then we have

$$\frac{1}{20}, \frac{2}{20}, \frac{3}{20}, \frac{4}{20}, \frac{5}{20}, \frac{6}{20}, \frac{7}{20}, \frac{8}{20}, \frac{9}{20}, \frac{10}{20}, \frac{11}{20}, \frac{12}{20}, \frac{13}{20}, \frac{14}{20}, \frac{15}{20}, \frac{16}{20}, \frac{17}{20}, \frac{18}{20}, \frac{19}{20}, \frac{20}{20}$$

which can be put into lowest terms as

$$\frac{1}{20}, \frac{1}{10}, \frac{3}{20}, \frac{1}{5}, \frac{1}{4}, \frac{3}{10}, \frac{7}{20}, \frac{2}{5}, \frac{9}{20}, \frac{1}{2}, \frac{11}{20}, \frac{3}{5}, \frac{13}{20}, \frac{7}{10}, \frac{3}{4}, \frac{4}{5}, \frac{17}{20}, \frac{9}{10}, \frac{19}{20}, \frac{1}{1}$$

□

Euler's Totient Function

A function $f : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ is ***multiplicative*** if $f(1) = 1$ and $f(m_1 m_2) = f(m_1) f(m_2)$ for $\gcd(m_1, m_2) = 1$.

Theorem

The Euler's Totient Function φ is multiplicative.

This is a consequence of the following more general fact.

Theorem

If f is any function such that the sum

$$g(m) = \sum_{d|m} f(d)$$

is multiplicative, the f is itself multiplicative. (The converse is also true. cf., Graham, Knuth, & Patashnik, Concrete Mathematics, 2ed)

Proof.

Induction on m.

base case ($m = 1$): True because $f(1) = g(1) = 1$.

Euler's Totient Function

Proof (Cont.)

inductive case ($m > 1$): assume the inductive hypothesis that $f(m_1 m_2) = f(m_1)f(m_2)$ if $\gcd(m_1, m_2) = 1$ and $m_1 m_2 < m$. Now if $m = m_1 m_2$ and $\gcd(m_1, m_2) = 1$, then

$$g(m_1 m_2) = \sum_{d|m_1 m_2} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2)$$

where $\gcd(d_1, d_2) = 1$ since all divisors of m_1 are relatively prime to divisors of m_2. By induction hypothesis, $f(d_1 d_2) = f(d_1)f(d_2)$ except possibly when $d_1 = m_1$ and $d_2 = m_2$. Thus

$$g(m_1 m_2) = \sum_{d_1|m_1} f(d_1) \sum_{d_2|m_2} f(d_2) - f(m_1)f(m_2) + f(m_1 m_2)$$

But we also have $g(m_1 m_2) = g(m_1)g(m_2)$, hence $f(m_1 m_2) = f(m_1)f(m_2)$. $\square$

Symmetric Group

Symmetric Group S_n

Given $n \in \mathbb{N} \setminus \{0\}$, we have the following ***symmetric group of degree*** n,

$$\begin{aligned} S_n &= \{\text{All permutations on } n \text{ letters/numbers}\} \\ &= \mathrm{Sym}\{1, 2, 3, \dots, n\} \\ &= \{f : [n] \to [n] \mid f \text{ bijective}\} \end{aligned}$$

Note that it is a finite group of order $n!$, i.e., $|S_n| = n!$.

Examples

- $S_1 = \{e\}$.
- $S_2 = \{e, \tau\}$, where $e, \tau : [2] \to [2]$, with

$$\begin{aligned} e(1) = 1, \quad e(2) = 2 \\ \tau(1) = 2, \quad \tau(2) = 1 \end{aligned}$$

$\circ$	e	τ
e	e	τ
τ	τ	e

Observe that $\tau \circ \tau = e$, i.e., $\tau = \tau^{-1}$.

Symmetric Group

Examples

- $S_3 = \{e, \tau, \tau', \tau'', \sigma, \sigma'\}$.

Use cycle notation, such that

$$
\begin{aligned}
e &= () = \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right) & \tau &= (12) = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)\\
\sigma &= (123) = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) & \tau' &= (23) = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)\\
\sigma' &= (132) = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right) & \tau'' &= (13) = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)
\end{aligned}
$$

Abbreviate $\tau \circ \sigma$ as $\tau\sigma$,

$$
\begin{aligned}
\tau\sigma(1) &= \tau(\sigma(1)) = \tau(2) = 1\\
\tau\sigma(2) &= \tau(\sigma(2)) = \tau(3) = 3\\
\tau\sigma(3) &= \tau(\sigma(3)) = \tau(1) = 2
\end{aligned}
$$

Hence $\tau\sigma = \tau'$.

Symmetric Group

Similarly, we have the following multiplication table

$\circ$	e	τ	τ'	τ''	σ	σ'
e	e	τ	τ'	τ''	σ	σ'
τ	τ	e	σ	σ'	τ'	τ''
τ'	τ'	σ'	e	σ	τ''	τ
τ''	τ''	σ	σ'	e	τ	τ'
σ'	σ'	τ'	τ''	τ	e	σ
σ	σ	τ''	τ	τ'	σ'	e

Corollary

The group S_n is nonabelian for $n \geq 3$.

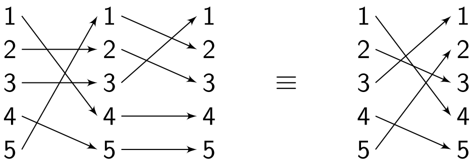
Proof.

Consider the subgroup $S_3 \subset S_n$. $\square$

Facts About General Permutations

Cycle Notation

- Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.
- If the pair of cycles $\alpha = (a_1 a_2 \cdots a_m)$ and $\beta = (b_1 b_2 \cdots b_n)$ have no entries in common, i.e., α and β are ***disjoint***, then $\alpha\beta = \beta\alpha$. (Such α is called a ***cycle of length*** m or an m-***cycle***.)
- The order of a permutation of a finite set written in disjoint cycle form is the **least common multiple** of the lengths of the cycles.
  - $|(132)(45)| = 6$
  - $|(1432)(56)| = 4$
  - $|(123)(456)(78)| = 6$
  - $|(123)(145)| = |(14523)| = 5$



Facts About General Permutations

Cycles and Transpositions

A permutation of the form (ab) where $a \neq b$ is called a ***transposition***.

- Every permutation in S_n, $n > 1$, is a product of transpositions.
- If $e = \beta_1\beta_2 \cdots \beta_r$, where β_i's are transpositions, then r is even.

Even and Odd Permutations

A permutation that can be expressed as a product of an even/odd number of transpositions is called an ***even/odd*** permutation. (Note that this parity is well-defined.) For each permutation σ, define

$$\operatorname{sgn}(\sigma) = \begin{cases} +1, & \text{if } \sigma \text{ is an even permutation.} \\ -1, & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

- The set of even permutations in S_n forms a subgroup of S_n, denoted A_n, is called the ***alternating group of degree*** n.
- $|A_n| = n!/2$ for $n > 1$.

The Determinant

Definition

Given a matrix $A \in M_n(\mathbb{C})$, the ***determinant*** function is given by

$$\begin{aligned} \det : M_n(\mathbb{C}) &\to \mathbb{C} \\ (a_{ij}) &\mapsto \det(a_{ij}) \coloneqq \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \end{aligned}$$

where S_n is the set of all permutations of the set $\{1, \ldots, n\} \subset \mathbb{N}$, and $\operatorname{sgn}(\sigma)$ the sign of the permutation σ.

The Determinant

An equivalent definition of the determinant is as follows.

Definition

The determinant $\det : M_n(\mathbb{C}) \cong \underbrace{\mathbb{C}^n \times \cdots \times \mathbb{C}^n}_{n \text{ times}} \to \mathbb{C}$ is the ***unique*** function satisfiying,

(i) ***alternating***, for all $v \in \mathbb{C}^n$, $\det(v_1, \ldots, v, \ldots, v, \ldots, v_n) = 0$, or equivalently ***skew-symmetric***, i.e.,

$$\det(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_{j-1}, v_j, v_{j+1}, \ldots, v_n) \\ = -\det(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_n)$$

(ii) ***multilinear***, i.e., for all $\lambda, \mu \in \mathbb{C}$, $v_i, u \in \mathbb{C}^n$, $i = 1, \ldots, n$,

$$\det(v_1, \ldots, v_{i-1}, \lambda v_i + \mu u, v_{i+1}, \ldots, v_n) \\ = \lambda \det(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n) \\ + \mu \det(v_1, \ldots, v_{i-1}, u, v_{i+1}, \ldots, v_n)$$

(iii) ***unitary***, i.e., $\det I_n = 1$.

Table of Contents

Homomorphism

Definition

Given groups G, G', a homomorphism is a map $f : G \to G'$ such that for all $x, y \in G$,

$$f(xy) = f(x)f(y)$$

Examples

- Trivial homomorphism $f : G \to G'$, $x \mapsto 1_{G'} \in G'$.
- Inclusion map $\iota : H \hookrightarrow G$, $x \mapsto x$, when H is a subgroup of G.
- The determinant function $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$.
- The sign homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$.
- The exponential map $\exp : (\mathbb{R}, +) \to \mathbb{R}^\times$, $x \mapsto e^x$.
- The absolute value map $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$.
- $f : \mathbb{Z} \to S_2$, even number $\mapsto e$, odd number $\mapsto \tau$.

Homomorphism

Example

$\mathrm{sgn} = \det \circ \varphi$.

$$
\begin{tikzcd}
S_3 \arrow[r, "\varphi", "\sim"'] \arrow[rr, bend left, "\mathrm{sgn}"] & GL_3(\mathbb{R}) \arrow[r, "\det"] & \mathbb{R}^\times = GL_1(\mathbb{R})
\end{tikzcd}
$$

$$
\begin{array}{ccccc}
1 & \mapsto & \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} & \mapsto & 1 \\
(123) & \mapsto & \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} & \mapsto & 1 \\
(132) & \mapsto & \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix} & \mapsto & 1 \\
(12) & \mapsto & \begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix} & \mapsto & -1 \\
(23) & \mapsto & \begin{pmatrix} 1 & & \\ & & 1 \\ & 1 & \end{pmatrix} & \mapsto & -1 \\
(31) & \mapsto & \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} & \mapsto & -1
\end{array}
$$

Homomorphism

Theorem

Let $f : G \to G'$ be a group homomorphism, then

- *If $a_1, \ldots, a_k \in G$, then $f(a_1 \cdots a_k) = f(a_1) \cdots f(a_k)$.*
- $f(1_G) = 1_{G'}$.
- $f(a^{-1}) = f(a)^{-1}$ *for* $a \in G$.

Proof.

- Induction.
- $f(1_G) \cdot f(1_G) = f(1_G \cdot 1_G) = f(1_G)$, thus $f(1_G) = 1_{G'}$ by cancellation.
- $f(a^{-1})f(a) = f(a^{-1}a) = f(1_G) = 1_{G'}$. □

Image and Kernel of Homomorphisms

A group homomorphism determines two important ***subgroups***: its image and its kernel.

Definition

The ***image*** of a homomorphism $f : G \to G'$, often denoted by $\operatorname{im} f$, or $f(G)$, is simply the image of as a map of sets:

$$\operatorname{im} f = \{x \in G' \mid x = f(a) \text{ for some } a \in G\}$$

The ***kernel*** of f, denoted by $\ker f$, is the set of elements of G that are mapped to the identity in G':

$$\ker f = \{a \in G \mid f(a) = 1_{G'}\}.$$

Examples

- The determinant function $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$. $\ker \det = SL_n(\mathbb{R})$.
- The sign homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. $\ker \operatorname{sgn} = A_n$.

Cosets

Definition

Given a group G, if $H \leq G$ is a subgroup and $a \in G$, the notation aH will stand for the set of all products ah with $h \in H$,

$$aH = \{g \in G \mid g = ah \text{ for some } h \in H\}$$

This set is called a ***left coset*** of H in G

Example

- $1H = \{1, (12)\} = H$.
- $(12)H = \{(12), (12)(12)\} = \{(12), 1\} = H$.
- $(23)H = \{(23), (23)(12)\} = \{(23), (132)\} = (132)H$.
- $(31)H = \{(31), (31)(12)\} = \{(31), (123)\} = (123)H$.
- $(123)H = \{(123), (123)(12)\} = \{(123), (31)\} = (31)H$.
- $(132)H = \{(132), (132)(12)\} = \{(132), (23)\} = (23)H$.

Hence the left coset of $\langle (12) \rangle$ in S_3 is $\{H, (23)H, (31)H\}$.

Homomorphisms

Theorem

Let $f : G \to G'$ be a group homomorphism, and let $a, b \in G$. Let $K = \ker f$. TFAE,

(i) $f(a) = f(b)$ (ii) $a^{-1}b \in K$ (iii) $b \in aK$ (iv) $aK = bK$

Proof.

- (i) $\Leftrightarrow$ (ii). Note that $f(a) = f(b)$ iff

$$f(a^{-1}b) = f(a^{-1})f(b) = f(a)^{-1}f(b) = 1_{G'}$$

  iff $a^{-1}b \in \ker f = K$.
- (ii) $\Leftrightarrow$ (iii). By definition of left coset.
- (iii) $\Leftrightarrow$ (iv). Check the cosets of K in G are equivalence classes. (on this later) $\square$

Homomorphisms

Corollary

A homomorphism $f : G \to G'$ is injective iff $\ker f = \{1_G\}$.

Proof.

- $(\Leftarrow)$. Suppose $\ker f = \{1_G\}$, then by previous theorem $f(a) = f(b) \Rightarrow a^{-1}b \in \ker f \Rightarrow a^{-1}b = 1_G$, i.e., $a = b$.
- $(\Rightarrow)$. Since $\ker f \leq G$, it is always true that $1_G \in \ker f$, i.e., $\{1_G\} \subset \ker f$. It is sufficient to show that $\ker f \subset \{1_G\}$, i.e., the only element in $\ker f$ is 1_G. Indeed, Suppose that $a, b \in \ker f$, then $f(a) = f(b) = 1_{G'}$, hence $a = b$ by injectivity. Therefore $\ker f = \{1_G\}$. □

Isomorphisms

Definition

Given groups G and G', an ***isomorphism*** $f : G \to G'$ is a bijective group homomorphism, i.e., a bijection such that $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Examples

- $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$, $x \mapsto e^x$.
- $f : S_n \to n \times n$ permutation matrices.
- $f : G \to f(G) = \operatorname{im} f$ is an isomorphism if f is injective.

Check if $f : G \to G'$ is an isomorphism

Verify $\ker f = \{1_G\}$ and $\operatorname{im} f = G'$.

Isomorphisms

Theorem

If $f : G \to G'$ is an isomorphism, its inverse map $f^{-1} : G' \to G$ is also an isomorphism.

Proof.

Since the inverse of a bijection is also a bijection, we only need to verify that f^{-1} is a homomorphism, that is,

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y) \text{ for all } x, y \in G'$$

Indeed. Note that f is bijective, then for $x, y \in G'$,

$$\begin{aligned} f(f^{-1}(xy)) &= (f \circ f^{-1})(xy) = xy = (f \circ f^{-1})(x)(f \circ f^{-1})(y) \\ &= f(f^{-1}(x))f(f^{-1}(y)) = f(f^{-1}(x) \cdot f^{-1}(y)) \end{aligned}$$

Again, since f is bijective and we are done. $\square$

Cosets

Given a subgroup H of G, then the cosets of H are equivalence classes. Denote $a \equiv b$ if $b \in aH$. Indeed,

- Reflexivity. $a = a \cdot 1$ and $1 \in H$, hence $a \equiv a$.
- Symmetry. Suppose $a \equiv b$, then $b \in aH$ hence $b = ah$ for some $h \in H$. Hence $a = bh^{-1}$, but $h^{-1} \in H$. Therefore $a \in bH$, i.e., $b \equiv a$.
- Transitivity. Suppose $a \equiv b$ and $b \equiv c$, then $b = ah$ and $c = bh'$ for some $h, h' \in H$. Therefore $c = ahh'$. Note that $hh' \in H$ (since H is a subgroup), hence $c \in aH$, i.e., $c \equiv a$.

Corollary

The left cosets of a subgroup H of a group G partition the group.

Remark

The subgroup H is a particular ***left*** coset since $H = 1 \cdot H$.

Cosets

Example

Let $S_3 = \left\langle \tau, \sigma \mid \tau^2 = \sigma^3 = 1, \tau\sigma\tau = \sigma^{-1} \right\rangle$. Then

- $H \coloneqq \langle \tau \rangle = \{1, \tau\} = \tau H$,
- $\sigma H = \{\sigma, \sigma\tau\} = \sigma\tau H$,
- $\sigma^2 H = \{\sigma^2, \sigma^2\tau\} = \sigma^2\tau H$,

form a partition of S_3. Similarly

- $K \coloneqq \langle \sigma \rangle = \{1, \sigma, \sigma^2\} = \sigma K = \sigma^2 K$,
- $\tau K = \{\tau, \tau\sigma, \tau\sigma^2\} = \tau\sigma K = \tau\sigma^2 K$,

also form a partition of S_3.

Cosets

Definition

The number of ***left cosets*** of a subgroup is called the ***index*** of H in G. The index is denoted by $[G : H]$ (which could be infinite if $|G| = \infty$).

Example

1	(12)
(132)	(23)
(123)	(13)

$[S_3 : \langle (12) \rangle] = 3.$

1	(12)
(132)	(23)
(123)	(13)

$[S_3 : \langle (123) \rangle] = 2.$

Cosets

Lemma

*All left cosets aH of a subgroup H of a group G have the **same** order.*

Proof.

The map $h \mapsto ah$ induces a bijective map

$$\begin{aligned} H &\mapsto aH \\ a^{-1}(aH) &\leftarrow aH \end{aligned}$$

□

Counting Formula

Note that the cosets all have the same order, and since they ***partition*** the group, then we have the ***Counting Formula***

$$|G| = |H| \cdot [G : H]$$

$$(\text{order of } G) = (\text{order of } H) \cdot \begin{pmatrix} \text{number of left} \\ \text{cosets of } H \end{pmatrix}$$

Lagrange's Theorem

Theorem (Lagrange's Theorem)

Let H be a subgroup of a finite group G. The order of H divides the order of G.

Proof.

By applying the counting formula. $\square$

Corollary

The order of an element of a finite group divides the order of the group.

Proof.

Let $g \in G$, then $H := \langle g \rangle \leq G$, and recall

$$H = \langle g \rangle = \{1, g, g^2, \ldots, g^{m-2}, g^{m-1}\}$$

where $|H| = m =$ order of g. $\square$

Lagrange's Theorem

Corollary

Given a group G, with $|G| = p$ prime. Let $g \in G$, $g \neq 1$, then $G = \langle g \rangle$ which is cyclic.

Proof.

Let $g \in G$ and $g \neq 1$, note that the order of g divides $|G| = p$, which is prime, hence the order of g is p. Therefore $|\langle g \rangle| = p$. Note that $\langle g \rangle \subset G$, with $|\langle g \rangle| = |G| = p$, hence $G = \langle g \rangle$, which is cyclic. $\square$

Remark

- Let G be a finite group, then $g^{|G|} = 1_G$ for all $g \in G$.
- Let G be a finite group of prime order, the only subgroups of G are the trivial group $\{1_G\}$ and the group G itself.
- This classifies groups of prime order p. They form ***one*** isomorphism class, the class of the cyclic groups of order p.

Lagrange's Theorem

Example

Given group G of order 6, then

- G contains an element of order 3. Indeed, if G has an element of order 6, then it is cyclic, so contains an element of order 3. If G does not have elements of order 3 or 6, then all non-identity elements of G have order 2. In this case, for all $x, y \in G$ we have $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, hence G is abelian. Then for $x, y \in G$ with $x \neq y$, $\{1, a, b, ab\}$ form a subgroup of G of order 4, but this contradicts Lagrange's theorem. Therefore G must contain an element of order 3.
- G contains an element of order 2. Indeed, if it did not, then all non-identity elements would have order 3. But elements of order 3 come in pairs (e.g., x and x^{-1}), but there are are odd number of non-identity elements (i.e., 5), which is a contradiction. hence there must be an element of order 2.

Lagrange's Theorem

Corollary

Let G, G' be finite groups, and $f : G \to G'$ a homomorphism. Then

1. $|G| = |\ker f| \cdot |\operatorname{im} f|$,
2. $|\ker f|$ *divides* $|G|$,
3. $|\operatorname{im} f|$ *divides both* $|G|$ *and* $|G'|$.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "q"'] & \operatorname{im} f \\ G/\ker f \arrow[ur, dashed, "\sim", "\tilde{f}"'] & \end{tikzcd}$$

Proof.

1. Note that $\ker f$ is a subgroup, then $\tilde{f} : G/\ker f \to \operatorname{im} f$ is a set-theoretc bijection between cosets of $\ker f$ and elements of $\operatorname{im} f$. Thus we have the counting formula

$$[G : \ker f] = |\operatorname{im} f|$$

2. Follows from counting formula.
3. Follows from counting formula and Lagrange's theorem (Note that $\operatorname{im} f \leq G'$). $\square$

Lagrange's Theorem

Compare the previous theorem with the following result in linear algebra.

Remark (Rank-Nullity Theorem)

Given $T : V \to W$ a linear map, then

$$\dim V = \dim \ker T + \dim \operatorname{im} T$$

$$\begin{array}{c}
\overleftrightarrow{\qquad\qquad \dim V \text{ columns} \qquad\qquad} \\
\begin{bmatrix}
* & * & * & * & * & * & * & * \\
0 & * & * & * & * & * & * & * \\
0 & 0 & 0 & * & * & * & * & * \\
0 & 0 & 0 & 0 & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \\
\begin{array}{cccccccc}
\uparrow & \uparrow & & \uparrow & \uparrow & & &
\end{array}
\end{array}$$

Right Cosets

Definition

The right cosets of a subgroup $H \leq G$ are the sets

$$Ha := \{ha \mid h \in H\}$$

Example

Consider $\langle(12)\rangle \leq S_3$.

1	(12)
(132)	(23)
(13)	(123)

Left cosets of $\langle(12)\rangle$.

1	(12)
(132)	(23)
(13)	(123)

Right cosets of $\langle(12)\rangle$.

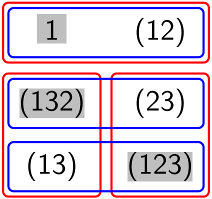
Group Transversals

Definition

Given a group G, and subgroup $H \leq G$. A subset $S \subset G$ is a left/right transversal for H in G if every left/right coset of H contains exactly one element of S.

Theorem

Common transversal always exists for subgroups of finite groups.

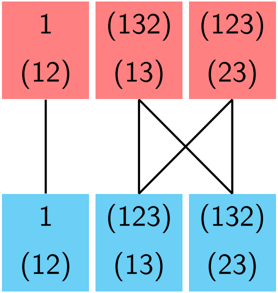


e.g., $\{1, (123), (132)\}$ is a common transversal for $\langle (12) \rangle$ in S_3.

Group Transversals

Proof.

Suppose $G = \bigcup_{k=1}^{n} x_k H = \bigcup_{k=1}^{n} Hy_k$. We define the partial order on $P = \{x_1 H, \ldots, x_n H\} \cup \{Hy_1, \ldots, Hy_n\}$ where $x < y$ if $x \in \{x_1 H, \ldots, x_n H\}$, $y \in \{Hy_1, \ldots, Hy_n\}$, and $x \cap y \neq \varnothing$. We know that the width of the poset is at least n (e.g., $\{x_1 H, \ldots, x_n H\}$ is an antichain.) Suppose there exsits a subset $Q \subset P$ containing $n+1$ pairwise disjoint sets, then the size of their union exceedes the size of G, which is impossible. The rest follows from Dilworth theorem. □



Normal Subgroup

Definition

Given group G, and $a, g \in G$, the element $gag^{-1} \in G$ is called the ***conjugate of a by g***.

Definition

A subgroup N of G is a ***normal subgroup***, denoted by $N \trianglelefteq G$, if for all $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Theorem

Given groups G, G', and $f : G \to G'$ a homomorphism, then $\ker f \trianglelefteq G$.

Proof.

Let $a \in \ker f$ and $g \in G$, then

$$f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g) \cdot 1_{G'} \cdot f(g)^{-1} = 1_{G'} \qquad \square$$

Normal Subgroup

Examples

- $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.
- $A_n \trianglelefteq S_n$.
- Every subgroup of an abelian group is normal.
- The ***center*** of a group G, denoted by Z, is the set of elements that commute with every element of G:

$$Z := \{z \in G \mid zx = xz \text{ for all } x \in G\}$$

  The center is always a normal subgroup. ($zx = xz \Leftrightarrow x = zxz^{-1}$.)

Normal Subgroup

Theorem

Let $H \leq G$, TFAE

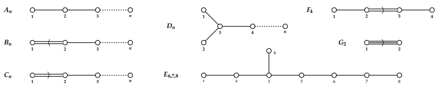
1. $H \trianglelefteq G$, *i.e.,* $ghg^{-1} \in H$ *for all* $h \in H, g \in G$.
2. $gHg^{-1} = H$ *for all* $g \in G$.
3. $gH = Hg$ *for all* $g \in G$.
4. *Every left coset of* H *is a right coset.*
5. $H = \ker f$ *for some homomorphism* $f : G \to X$.
6. *The quotient group* G/H *exists.*

Definition

A group is ***simple*** if its only normal subgroup are the identity subgroup and the group itself.

The Periodic Table Of Finite Simple Groups

Dynkin Diagrams of Simple Lie Algebras



$0, C_1, \mathbb{Z}_1$ 1 1

Alternating	Classical Chevalley	Chevalley	Chevalley	Chevalley	Chevalley	Chevalley	Steinberg	Steinberg	Suzuki	Ree / Tits	Ree	Classical Chevalley	Classical Chevalley	Classical Chevalley	Classical Steinberg	Classical Steinberg
$A_1(4), A_1(5)$ A_5 60	$A_2(2)$ $A_1(7)$ 168											$^2A_3(4)$ $B_2(3)$ 25 920	$C_3(3)$ 4 585 351 680	$D_4(2)$ 174 182 400	$^2D_4(2^2)$ 197 406 720	$G_2(2)'$ $^2A_2(9)$ 6 048
$A_1(9), B_2(2)'$ A_6 360	$^2G_2(3)'$ $A_1(8)$ 504											$B_2(4)$ 979 200	$C_3(5)$ 228 501 000 000 000	$D_4(3)$ 4 952 179 814 400	$^2D_4(3^2)$ 10 151 968 619 520	$^2A_2(16)$ 62 400
A_7 2 520	$A_1(11)$ 660	$E_6(2)$ 214 841 575 522 005 575 270 400	$E_7(2)$ 7 997 476 042 075 799 759 100 487 262 680 802 918 400	$E_8(2)$ 337 804 753 143 634 806 261 388 190 614 085 595 079 991 692 242 467 651 576 160 959 909 068 800 000	$F_4(2)$ 3 311 126 603 366 400	$G_2(3)$ 4 245 696	$^3D_4(2^3)$ 211 341 312	$^2E_6(2^2)$ 76 532 479 683 774 853 939 200	$^2B_2(2^3)$ 29 120	Tits* $^2F_4(2)'$ 17 971 200	$^2G_2(3^3)$ 10 073 444 472	$B_3(2)$ 1 451 520	$C_4(3)$ 65 784 756 654 489 600	$D_5(2)$ 23 499 295 948 800	$^2D_5(2^2)$ 25 015 379 558 400	$^2A_2(25)$ 126 000
$A_3(2)$ A_8 20 160	$A_1(13)$ 1 092	$E_6(3)$ 7 257 703 347 541 463 210 028 258 395 214 643 200	$E_7(3)$ 1 271 375 236 818 136 742 240 479 751 139 021 644 554 379 203 770 766 254 617 395 200	$E_8(3)$ [illegible]	$F_4(3)$ 5 734 420 792 816 671 844 761 600	$G_2(4)$ 251 596 800	$^3D_4(3^3)$ 20 560 831 566 912	$^2E_6(3^2)$ 14 636 855 916 969 695 633 965 120 680 532 377 600	$^2B_2(2^5)$ 32 537 600	$^2F_4(2^3)$ 264 905 352 699 586 176 614 400	$^2G_2(3^5)$ 49 825 657 439 340 552	$B_2(5)$ 4 680 000	$C_3(7)$ 273 457 218 604 953 600	$D_4(5)$ 8 911 539 000 000 000 000	$^2D_4(4^2)$ 67 536 471 195 648 000	$^2A_3(9)$ 3 265 920
A_9 181 440	$A_1(17)$ 2 448	$E_6(4)$ 85 528 710 781 342 640 103 833 619 055 142 765 466 746 880 000	$E_7(4)$ 111 131 458 114 940 385 379 597 233 477 884 941 280 664 199 527 155 056 307 251 745 263 504 588 800 000 000	$E_8(4)$ [illegible]	$F_4(4)$ 19 009 825 523 840 945 451 297 669 120 000	$G_2(5)$ 5 859 000 000	$^3D_4(4^3)$ 67 802 350 642 790 400	$^2E_6(4^2)$ 85 696 576 147 617 709 485 896 772 387 584 983 695 360 000 000	$^2B_2(2^7)$ 34 093 383 680	$^2F_4(2^5)$ 1 318 633 155 799 591 447 702 161 609 782 722 560 000	$^2G_2(3^7)$ 239 189 910 264 352 349 332 632	$B_2(7)$ 138 297 600	$C_3(9)$ 54 025 731 402 499 584 000	$D_5(3)$ 1 289 512 799 941 305 139 200	$^2D_4(5^2)$ 17 880 203 250 000 000 000	$^2A_2(64)$ 5 515 776
A_n $\frac{n!}{2}$	$PSL_{n+1}(q), L_{n+1}(q)$ $A_n(q)$ $\frac{q^{n(n+1)/2}}{(n+1,q-1)}\prod_{i=1}^{n}(q^{i+1}-1)$	$E_6(q)$ $\frac{q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)}{(3,q-1)}$	$E_7(q)$ $\frac{q^{63}}{(2,q-1)}\prod_{i=1, i\neq 2,8}^{9}(q^{2i}-1)$	$E_8(q)$ $q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$	$F_4(q)$ $q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	$G_2(q)$ $q^6(q^6-1)(q^2-1)$	$^3D_4(q^3)$ $q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	$^2E_6(q^2)$ $\frac{q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)}{(3,q+1)}$	$^2B_2(2^{2n+1})$ $q^2(q^2+1)(q-1)$	$^2F_4(2^{2n+1})$ $q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	$^2G_2(3^{2n+1})$ $q^3(q^3+1)(q-1)$	$O_{2n+1}(q), \Omega_{2n+1}(q)$ $B_n(q)$ $\frac{q^{n^2}}{(2,q-1)}\prod_{i=1}^{n}(q^{2i}-1)$	$PSp_{2n}(q)$ $C_n(q)$ $\frac{q^{n^2}}{(2,q-1)}\prod_{i=1}^{n}(q^{2i}-1)$	$O_{2n}^{+}(q)$ $D_n(q)$ $\frac{q^{n(n-1)}(q^n-1)}{(4,q^n-1)}\prod_{i=1}^{n-1}(q^{2i}-1)$	$O_{2n}^{-}(q)$ $^2D_n(q^2)$ $\frac{q^{n(n-1)}(q^n+1)}{(4,q^n+1)}\prod_{i=1}^{n-1}(q^{2i}-1)$	$PSU_{n+1}(q)$ $^2A_n(q^2)$ $\frac{q^{n(n+1)/2}}{(n+1,q+1)}\prod_{i=2}^{n+1}(q^i-(-1)^i)$

Cyclic
C_2 2
C_3 3
C_5 5
C_7 7
C_{11} 11
C_{13} 13
$\mathbb{Z}_p$ C_p p

- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Suzuki Groups
- Ree Groups and Tits Group*
- Sporadic Groups
- Cyclic Groups

Alternates† Symbol Order‡

M_{11} 7 920	M_{12} 95 040	M_{22} 443 520	M_{23} 10 200 960	M_{24} 244 823 040	$J(1), J(11)$ J_1 175 560	HJ J_2 604 800	HJM J_3 50 232 960	J_4 86 775 571 046 077 562 880	HS 44 352 000	McL 898 128 000	F_7, HHM, HTH He 4 030 387 200	Ru 145 926 144 000
Sz Suz 448 345 497 600	$O'NS, O\text{–}S$ $O'N$ 460 815 505 920	$\cdot 3$ Co_3 495 766 656 000	$\cdot 2$ Co_2 42 305 421 312 000	$\cdot 1$ Co_1 4 157 776 806 543 360 000	F_5, D HN 273 030 912 000 000	LyS Ly 51 765 179 004 000 000	F_3, E Th 90 745 943 887 872 000	$M(22)$ Fi_{22} 64 561 751 654 400	$M(23)$ Fi_{23} 4 089 470 473 293 004 800	$F_{3+}, M(24)'$ Fi_{24}' 1 255 205 709 190 661 721 292 800	F_2 B 4 154 781 481 226 426 191 177 580 544 000 000	F_1, M_1 M 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

*The Tits group $^2F_4(2)'$ is not a group of Lie type, but is the (index 2) commutator subgroup of $^2F_4(2)$. It is usually given honorary Lie type status.

†For sporadic groups and families, alternate names in the upper left are other names by which they may be known. For specific non-sporadic groups these are used to indicate isomorphims. All such isomorphisms appear on the table except the family $B_n(2^m) \cong C_n(2^m)$.

The groups starting on the second row are the classical groups. The sporadic suzuki group is unrelated to the families of Suzuki groups.

‡Finite simple groups are determined by their order with the following exceptions:
$B_n(q)$ and $C_n(q)$ for q odd, $n > 2$;
$A_8 \cong A_3(2)$ and $A_2(4)$ of order 20160.

Table of Contents

Modular Arithmetic

Definition

Given $a, b \in \mathbb{Z}$, a and b are said to be ***congruent modulo*** n, i.e.,

$$a \equiv b \pmod{n}$$

if $n \mid b - a$, i.e., $b = a + nk$ for some $k \in \mathbb{Z}$.

Remark

This is an equivalence relation. The equivalence classes are called ***congruence classes***.

- $a \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$.
- If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
- If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Modular Arithmetic

Congruence Classes

Let $H = n\mathbb{Z} \trianglelefteq \mathbb{Z}$, then the cosets of H, i.e., the congruence classes, are given by

$$[a]_n = \overline{a} = a + H = a + n\mathbb{Z} = \{a + kn \mid k \in \mathbb{Z}\}$$

The integers $0, 1, \ldots, n-1$ are representatives for the n congruence classes.

Notation

	Multiplicative Notation	Additive Notation
Operation:	ab	$a+b$
Identity:	e or 1	0
Inverse:	a^{-1}	$-a$
Exponents:	$a^n = aa\cdots a$ (n factors)	$na = a + a + \cdots + a$ (n summands)
	$a^{-n} = a^{-1}\cdots a^{-1}$	$(-n)a = -a - a - \cdots - a$
	$a^m a^n = a^{m+n}$	$(ma) + (na) = (m+n)a$
	$(a^m)^n = a^{mn}$	$n(ma) = (mn)a$
Cosets:	aH	$a + H$

Modular Arithmetic

In an attempt to prove Fermat's Last Theorem,

Theorem (Schur, 1916)

Let $n \in \mathbb{N} \setminus \{0\}$, then for all sufficiently large primes p, there are $x, y, z \in \{1, \ldots, p-1\}$ such that $x^n + y^n \equiv z^n \pmod{p}$.

Less Dramatic Examples

Given $x, y, z \in \mathbb{Z}$, then

- $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$.
- $x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{8}$.
- $x^3 + y^3 + z^3 \equiv 0, \pm 1, \pm 2, \pm 3 \pmod{9}$.

Modular Arithmetic

Theorem

There are n congruence classes modulo n, namely, $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. The index of the subgroup $n\mathbb{Z}$ in $\mathbb{Z}$ is $[\mathbb{Z} : n\mathbb{Z}] = n$.

Proof.

Consider the function $f : \mathbb{Z} \to \{0, 1, \ldots, n-1\}$, $x \mapsto x \bmod n$. Note that f induces a bijection $\tilde{f} : \mathbb{Z}/n\mathbb{Z} \to \{0, \ldots, n-1\}$. $\square$

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "f"] \arrow[d, "q"'] & \{0, \ldots, n-1\} \\
\mathbb{Z}/n\mathbb{Z} \arrow[ur, dashed, "\sim", "\tilde{f}"'] &
\end{tikzcd}$$

Remark

- The set of congruence classes modulo n may be denoted by $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/\mathbb{Z}n$, $\mathbb{Z}_n$, or $\mathbb{Z}/(n)$.
- It is the same to say $\overline{a} = \overline{b}$, $a = b$ in $\mathbb{Z}/n\mathbb{Z}$, or $a \equiv b \pmod{n}$.

Modular Arithmetic

We can do "arithmetic" in $\mathbb{Z}/n\mathbb{Z}$, e.g.,

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

which are well-defined.

Lemma

If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

Proof.

Assume that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a' = a + rn$ and $b' = b + sn$ for some $r, s \in \mathbb{Z}$. Then

- $a' + b' = a + b + (r + s)n$, hence $a + b \equiv a' + b' \pmod{n}$.
- $a'b' = (a + rs)(b + sn) = ab + (as + rb + rns)n$, hence $ab \equiv a'b' \pmod{n}$. $\square$

Modular Arithmetic

$(\mathbb{Z}/n\mathbb{Z}, +)$ is a group

- Addition is associative. (inherited from $\mathbb{Z}$)

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b + c} = \overline{a} + (\overline{b} + \overline{c})$$

- Identity: $\overline{0}$.
- Inverses: $-\overline{a} = \overline{n - a} = \overline{-a}$.

i.e., the set of cosets of $n\mathbb{Z} \subset \mathbb{Z}$ form a (quotient) group.

Inheritance from $\mathbb{Z}$

The associative, commutative, and distributive laws hold for addition and multiplication of congruence classes. e.g.,

$$\begin{aligned}
\overline{a}(\overline{b} + \overline{c}) = \overline{a}(\overline{b + c}) &= \overline{a(b + c)} \\
&= \overline{ab + ac} \\
&= \overline{ab} + \overline{ac} = \overline{a}\overline{b} + \overline{a}\overline{c}
\end{aligned}$$

Modular Arithmetic

Multiplicative Group of Integers Modulo n

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } \overline{a} \cdot \overline{c} = \overline{1}\}$$

- Closure: product of inverses are inverse of product.
- Associtivity: inherited from $\mathbb{Z}$.
- Identity: $\overline{1}$.
- Inverses by construction.

Theorem

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$$

Proof.

- (LHS $\supset$ RHS). If $\gcd(a, n) = 1$, then $\exists r, s \in \mathbb{Z}$ such that $ar + ns = 1$, i.e., $ar - 1 \in n\mathbb{Z}$, or $\overline{a} \cdot \overline{r} = \overline{1}$, so $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- (LHS $\subset$ RHS). Consider $\overline{a} \cdot \overline{c} = \overline{1}$, then $ac - 1 = nb$ for some $b \in \mathbb{Z}$. Hence $1 = ac + nb \in a\mathbb{Z} + n\mathbb{Z} = \gcd(a, n)\mathbb{Z}$. □

Modular Arithmetic

Finding Inverses

For example, we want to solve $7x \equiv 1 \pmod{31}$.

Method I

By Euclidean algorithm, we can find integers $x = 9$, $y = -2$ such that $7x + 31y = 1$, i.e.

$$7 \times 9 + 31 \times (-2) = 1$$

hence $7 \cdot 9 \equiv 1 \pmod{31}$, i.e., $x \equiv 7^{-1} \equiv 9 \pmod{31}$.

Method II (Gauss), for prime modulus

By division algorithm (keep remainder with smallest absoute value),

$$\begin{aligned} 31 &= 7 \times 4 + 3 & \Rightarrow \quad & 7 \times 4 \equiv -3 \pmod{31} \\ 31 &= 3 \times 10 + 1 & \Rightarrow \quad & 3 \times 10 \equiv -1 \pmod{31} \end{aligned}$$

Hence $7 \cdot 4 \cdot \cancel{3} \cdot 10 \equiv \cancel{3} \cdot 1$, so $7^{-1} \equiv 4 \cdot 10 \equiv 9 \pmod{31}$.

Fermat's (Little) Theorem

Theorem (Fermat-I)

Given $a \in \mathbb{Z}$ and $p \in \mathbb{P}$, such that $(a, p) = 1$, then

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

Theorem (Fermat-II)

Given $a \in \mathbb{Z}$ and $p \in \mathbb{P}$, then

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

Remark

- (Fermat-I $\Rightarrow$ Fermat-II). Clear by multiplying a on both sides.
- (Fermat-II $\Rightarrow$ Fermat-I). Clear by multiplying a^{-1} on both sides. $a^{-1} \pmod{p}$ exsits because $(a, p) = 1$.

Fermat's (Little) Theorem

Proof of Fermat-II (Euler).

Induction on $a \in \mathbb{N}$.
base case. ($a = 0$). True.
inductive case. ($a \geq 0$). Assume the IH that $a^p \equiv a \pmod{p}$ for some $a \in \mathbb{N}$, we want to show that $(a+1)^p \equiv a+1 \pmod{p}$ also holds. Note that

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1$$

Now it is sufficient to show that $p \mid \binom{p}{k}$ for $p \in \mathbb{P}$, $1 \leq k \leq p-1$. Indeed, since

$$p! = \binom{p}{k} \cdot (p-k)!k!$$

Now note that $p \mid p!$ but $p \nmid [(p-k)!k!]$, we have $p \mid \binom{p}{k}$. $\square$

Euler's Theorem

Theorem (Euler)

For $m \in \mathbb{N} \setminus \{0\}$ *and* $a \in \mathbb{Z}$ *such that* $\gcd(a, m) = 1$*,*

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

where $\varphi(m)$ *is the number of invertible integers modulo* m*.*

Proof.

Note that $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$, which is divisible by the order of $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ by Lagrange's theorem. (In fact, $a^{|G|} = 1_G \ \forall a \in G$.) $\square$

Remark

Given $p \in \mathbb{P}$,

- Fermat's theorem becomes Euler's theorem since $\varphi(p) = p - 1$.
- $\mathbb{Z}/p\mathbb{Z}$ is cyclic due to Lagrange's theorem.
- $(\mathbb{Z}/p\mathbb{Z})^\times$ is also cyclic, but NOT due to Lagrange's theorem.

Fermat's Theorem

Theorem

Given $p \in \mathbb{P}$, if $p \mid n^2+1$, then $p = 2$ or $p \equiv 1 \pmod 4$.

n	1	2	3	4	5	6	7	8
n^2+1	2	5	10	17	26	37	50	65
p	2	5	$2, 5$	17	$2, 13$	37	$2, 5$	$5, 13$

Proof.

If p is odd, then $p \mid n^2+1 \Leftrightarrow n^2 \equiv -1 \pmod p$, hence the order of n is not 1 or 2. (Note that $1 \not\equiv -1 \pmod p$ since p is odd.) But since $n^4 \equiv 1 \pmod p$, we know that the order of n divides 4, hence the order of n is exactly 4. Also note that $\gcd(n, p) = 1$, hence by Fermat's theorem, we have $n^{p-1} \equiv 1 \pmod p$, so the order of n divides $p-1$, that is, $4 \mid p-1$, i.e., $p \equiv 1 \pmod 4$. $\square$

Euler's Theorem

Example

For $\varphi(8) = 4$, by Euler's theorem

$$a^4 \equiv 1 \pmod 8, \qquad \text{for all } a \in \mathbb{Z} \text{ s.t. } \gcd(a, 8) = 1$$

Note that $\gcd(a, 8) = 1$ leads to $a = 1, 3, 5, 7$. In fact,

$$a^2 \equiv 1 \pmod 8$$

Example

Let $m = 35 = 5 \times 7$, then by Fermat's theorem

- $a^6 \equiv 1 \pmod 7$
- $a^4 \equiv 1 \pmod 5$

Hence $a^{\mathrm{lcm}(4,6)} = a^{12} \equiv 1 \pmod{5, 7}$, i.e., $a^{12} \equiv 1 \pmod{35}$.
By Euler's Theorem, $a^{\varphi(35)} = a^{24} \equiv 1 \pmod{35}$.

Fermat Primes

When is $2^n + 1$ prime? $(n > 0)$

- If $n > 1$, odd, then NO. (since $3 \mid (2^n + 1)$)
- If $n = ab$, b odd, also NO. (since $(2^a + 1) \mid (2^n + 1)$)

Therefore $n = 2^m$, $m \in \mathbb{N}$.

Fermat Primes

$F_n = 2^{2^n} + 1$.

- $F_0 = 2^{2^0} + 1 = 3 \in \mathbb{P}$.
- $F_1 = 2^{2^1} + 1 = 5 \in \mathbb{P}$.
- $F_2 = 2^{2^2} + 1 = 17 \in \mathbb{P}$.
- $F_3 = 2^{2^3} + 1 = 257 \in \mathbb{P}$.
- $F_4 = 2^{2^4} + 1 = 65537 \in \mathbb{P}$.
- $F_5 = 2^{2^5} + 1 = 4274967297 = 641 \times 6700417$. (Euler, 1732)

FACT

If m is odd, then $(-1)^m + 1 = 0$, thus $x^m + 1$ is divisible by $x + 1$. By long division, we have

$$x^m+1 = (x+1)(x^{m-1} - x^{m-2} + \cdots + 1)$$

Testing Fermat Primes

Check $F_4 = 2^{2^4} + 1 = 65537$ is prime

Suppose $p \mid 65537$, $p \leq \sqrt{65537}$, that is, $p \mid 2^{16} + 1$, hence

$$2^{16} \equiv -1 \pmod{p}$$
$$2^{32} \equiv 1 \pmod{p}$$

Hence the order of 2 divides 32 but not 16, that is, the order of 2 is 32.
On the other hand, by Fermat's theorem, we have $2^{p-1} \equiv 1 \pmod{p}$, thus

$$p \equiv 1 \pmod{32}$$

Note that $p \leq \sqrt{65537}$, possible p's are listed as follows

$$\cancel{33}, \quad \cancel{65}, \quad 97, \quad \cancel{129}, \quad \cancel{161}, \quad 193, \quad \cancel{225}$$

Among which we only need to check 97 and 193.

Primality Testing of General Numbers

Fermat Primality Test

Given $n \in \mathbb{N}$, calculate $2^n \pmod{n}$,

- If $2^n \not\equiv 2 \pmod{n}$, then n is COMPOSITE.
- If $2^n \equiv 2 \pmod{n}$, then n is PROBABLY prime. (Try other numbers next.)

Such test is called ***probabilistic test***.

Task: Calculate $2^n \pmod{n}$

n is usually large, e.g., $n \sim 10^{100}$

- 2^n is rediculously large.
- Takes spatial and temporal resources to calculate.
- Mod n after each multiplication of 2 is still slow.

Fast Modular Exponentiation

Calculate a^b mod m

1. Write b in binary, i.e.,

$$b = (b_{k-1} \cdots b_0)_2 = \sum_{j=0}^{k-1} b_j 2^j = b_{k-1} 2^{k-1} + \cdots + b_1 \cdot 2 + b_0,$$

   with $b_0, \ldots, b_{k-1} \in \{0, 1\}$, then

$$a^b = \prod_{j=0}^{k-1} a^{b_j 2^j} = a^{b_{k-1} 2^{k-1}} \times a^{b_{k-1} 2^{k-1}} \times \cdots \times a^{b_1 \cdot 2} \times a^{b_0}$$

2. Calculate a^{2^j} mod m for $j = 0, \ldots, k-1$, by noting that $a^{2^{j+1}} = (a^{2^j})^2$
3. Multiply the terms for which $b_k = 1$.

Such ***square and multiply*** method is also known as ***repeated squaring***.

Fast Modular Exponentiation

Example: Test if 35 is prime.

Note that $35 = (100011)_2 = 2^5 + 2^1 + 2^0$, then

$$2^{35} = 2^{32} \times 2^2 \times 2^1$$

Next calculate

- $2^1 \equiv 2 \pmod{35}$.
- $2^2 \equiv 2^2 \equiv 4 \pmod{35}$.
- $\cancel{2^4 \equiv 4^2 \equiv 16 \pmod{35}}$
- $\cancel{2^8 \equiv 16^2 \equiv 256 \equiv 11 \pmod{35}}$
- $\cancel{2^{16} \equiv 11^2 \equiv 121 \equiv 16 \pmod{35}}$
- $2^{32} \equiv 16^2 \equiv 11 \pmod{35}$.

Now $2^{35} \equiv 2^{32} \times 2^2 \times 2^1 \equiv 11 \times 4 \times 2 \equiv 18 \not\equiv 2 \pmod{35}$.
Hence 35 is NOT prime.

Fast Modular Exponentiation and Egyptian/Ethiopian/Russian Multiplication

Example: $2^{35} \pmod{35}$

HALVING	SQUARING
35	$2 \pmod{35}$
17	$4 \pmod{35}$
~~8~~	~~$16 \pmod{35}$~~
~~4~~	~~$256 \equiv 11 \pmod{35}$~~
~~2~~	~~$121 \equiv 16 \pmod{35}$~~
1	$256 \equiv 11 \pmod{35}$

$2^{35} \equiv 2 \cdot 4 \cdot 11 \pmod{35}$.

Example: 35×27

HALVING	DOUBLING
35	27
17	54
~~8~~	~~108~~
~~4~~	~~216~~
~~2~~	~~432~~
1	864

$35 \times 27 = 27 + 54 + 864 = 945$.

Carmichael Numbers

Fermat Primality Test

Given $n \in \mathbb{N}$, calculate $a^n \pmod{n}$, $a < n$ (in general for many a)

- If $a^n \not\equiv a \pmod{n}$, then n is COMPOSITE. Such a is called a ***Fermat witness***.
- If $a^n \equiv a \pmod{n}$, then
  - n is prime.
  - n is composite, such a is called a Fermat Liar.

Definition

A ***Carmichael number*** is a ***composite*** number n for which

$$a^n \equiv a \pmod{n} \text{ for all } a \in \mathbb{Z}.$$

Remark

Carmichael numbers have ***NO*** Fermat witnesses.

Carmichael Numbers

The first few Carmichael numbers are 561, 1105, 1729, 2465, 2821, 6601, 8911,...

Example

Let $n = 561 = 3 \times 11 \times 17$, note that by Fermat's Theorem, for a coprime to 561,

- $a^{3-1} \equiv 1 \pmod 3$
- $a^{11-1} \equiv 1 \pmod{11}$
- $a^{17-1} \equiv 1 \pmod{17}$

Now note that $\operatorname{lcm}(3-1, 11-1, 17-1) = 80$ which divides $560 = 561 - 1$. Therefore for a coprime to 561,

$$a^{561-1} \equiv 1 \pmod{3, 11, 17}$$

hence (why?)

$$a^{561} \equiv a \pmod{561} \text{ for all } a \in \mathbb{Z}$$

Carmichael Numbers

For 100-digit numbers, less than 1 in 1030 are Carmichael numbers. For 200-digit numbers, the chances are even less.

Remark

- If we randomly choose a 200-digit number n, and test ≈ 100 different values of a without getting a Fermat witness, then we can be almost certain that n is prime.
- There are infinitely many Carmichael numbers.
- There are infinitely many Carmichael numbers of the form $km + a$, where $\gcd(a, m) = 1$.

Table of Contents

Sunzi's Problem

Sunzi asks:

> *There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?*

今有物不知其数，三三数之剩二，五五数之剩三，
七七数之剩二，问物几何？

In Language of Congruences

Find x such that

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}, \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

Sunzi's Problem

Solution Algorithm

三人同行七十希，五树梅花廿一支，
七子团圆正半月，除百零五便得知。

Solution in modern mathematical language

$$x \equiv 2 \times 70 + 3 \times 21 + 2 \times 15 = 233 \equiv 23 \pmod{105}$$

Remark

- $70 \equiv 1 \pmod 3$, $70 \equiv 0 \pmod 5$, $70 \equiv 0 \pmod 7$;
- $21 \equiv 0 \pmod 3$, $21 \equiv 1 \pmod 5$, $21 \equiv 0 \pmod 7$;
- $15 \equiv 0 \pmod 3$, $15 \equiv 0 \pmod 5$, $15 \equiv 1 \pmod 7$;
- $105 \equiv 0 \pmod 3$, $105 \equiv 0 \pmod 5$, $105 \equiv 0 \pmod 7$.

Sunzi's Problem

General Form

Given $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, r$, $a_1, \ldots, a_r \in \mathbb{Z}$, and $m_1, \ldots, m_r$ are pairwise relatively prime. The unique solution is given by

$$x = a_1 y_1 + a_2 y_2 + \cdots + a_r y_r \pmod{m}$$

where $m = m_1 \cdots m_r$ and $y_i = \delta_{ij} \pmod{m_j}$, e.g., $y_i = (m/m_i)^{\varphi(m_i)}$.

Lagrange interpolation (also cf., Green's function, matrix inverse)

Given a set of $k+1$ data points $(x_0, y_0), (x_1, y_1), \ldots, (x_k, y_k)$, with distinct x_j's. The ***interpolation polynomial in the Lagrange form*** is a linear combination $L = y_0 \ell_0 + \cdots + y_k \ell_k$, with ℓ_i satisfying $\ell_i(x_j) = \delta_{ij}$, e.g.,

$$\ell_j(x) := \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m} = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

Sunzi's Problem

Matrix Inverse

Given an $n \times n$ invertible matrix A, its inverse A^{-1} can be found by solving

$$Ax_1 = e_1, \qquad Ax_2 = e_2, \qquad \ldots, \qquad Ax_n = e_n$$

where

$$e_k = \begin{array}{c} \\ \begin{bmatrix} 0 & 0 & \cdots & 0 & \overset{\substack{k\text{-th}\\ \downarrow}}{1} & 0 & \cdots & 0 \end{bmatrix}^\top \end{array}$$

Now the general solution to $Ax = b$ can be solved by first recognizing that $b = \sum_{k=1}^{n} b_k e_k$, then

$$x = A^{-1}b = A^{-1}\left(\sum_{k=1}^{n} b_k e_k\right) = \sum_{k=1}^{n} b_k A^{-1} e_k = \sum_{k=1}^{n} b_k x_k$$

Remark

Recall the procedure of finding matrix inverse by Gauss-Jordan elimination: $[A|I_n] \rightsquigarrow [I_n|B]$, then $B = A^{-1}$.

Sunzi's Problem

Green's Function

Given a differential equation $Lu = f$ with boundary condition $Bu = 0$ over certain domain D, we first solve the following equation

$$Lg(x;\xi) = \delta(x-\xi), \qquad Bg(x;\xi) = 0$$

where the solution $g(x;\xi)$ is known as the ***Green's function***. Now the solution to original equation is given by

$$u(x) = \int_D g(x;\xi) f(\xi)\, d\xi$$

If the differential operator L is time-invariant, then the solution is given by a convolution

$$u(x) = \int_D g(x-\xi) f(\xi)\, d\xi = (g * f)(x)$$

where $g(x) = g(x;0)$ and $Lg(x) = \delta(x)$.

Sunzi's Problem

Find the smallest $x \in \mathbb{N}$ (or all $x \in \mathbb{Z}$) such that

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

Remark

- No constraints on the remainders $a_1, \ldots, a_r$.
- The moduli $m_1, \ldots, m_r$ are pairwise relatively prime. (This is NOT equivalent to $\gcd(m_1, \ldots, m_r) = 1$.)

Product Group

Definition

Given groups G and G', the product group $(G \times G', \cdot_\times)$ is the set $G \times G'$ equipped with the group law

$$\begin{aligned}\cdot_\times : (G \times G') \times (G \times G') &\to G \times G' \\ ((g, g'), (h, h')) &\mapsto (g, g') \cdot_\times (h, h') = (gh, g'h')\end{aligned}$$

Remark

- The identity element of $(G \times G', \cdot_\times)$ is given by $(1_G, 1_{G'})$.
- The inverse of (g, g') is (g^{-1}, g'^{-1}).
- Associativity is inherited from G and G'.

Chinese Remainder Theorem

Let $m, n \in \mathbb{N} \setminus \{0\}$ and $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_n$. ($C_n$ is the cyclic group of order n.) Note that $C_4 \ncong C_2 \times C_2$.

Chinese Remainder Theorem

Theorem

$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *if* $\gcd(m, n) = 1$.

Proof.

Consider the mapping

$$\begin{aligned} f : \mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x &\mapsto (x, x) \end{aligned}$$

which is obviously a homomorphisms. We show that it is bijective.

- Injectivity. We need to show $f(x) = (0, 0) \Rightarrow x \equiv 0 \pmod{mn}$. Indeed, since if $m, n \mid x$, and $\gcd(m, n) = 1$, then $mn \mid x$.
- Surjectivity. By dimension count (basically pigeonhole). $\square$

Chinese Remainder Theorem (General Form)

Theorem

$\mathbb{Z}/m_1 \cdots m_r\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ *if* $\gcd(m_i, m_j) = 1$ *for* $i \neq j$. (Induction on r.)

Lemma (Base case for induction)

Given the system $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ with $\gcd(m, n) = 1$, the solution can be found as follows,

1. Find u and v such that $mu + nv = 1$.
2. Then $t = bmu + anv \bmod mn$ is a solution.

Example

Consider $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$. We can apply the Euclidean algorithm (or by guessing),

- Then consider the first two, we have $x \equiv 8 \pmod{15}$.
- Combine with the third one, we have $x \equiv 23 \pmod{105}$.

Chinese Remainder Theorem (General Form)

Example (Cont.)

We first solve $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, that is,

$$x = 2 + 3y = 3 + 5z \Rightarrow 3y - 5z = 1 \Rightarrow (y, z) = (7, 4)$$

thus $x = 2 + 3 \cdot 7 = 23 \equiv 8 \pmod{15 = 3 \times 5}$.
Next we solve $x \equiv 8 \pmod{15}$, $x \equiv 2 \pmod 7$, that is,

$$\begin{aligned} x = 8 + 15t = 2 + 7t &\Rightarrow 7t - 15s = 6 \\ &\Rightarrow (t, s) = (6 \cdot 13, 6 \cdot 6) = (78, 36) \end{aligned}$$

thus $x = 8 + 15 \cdot 36 \equiv 23 \pmod{105 = 15 \times 7}$.

Solution of a System in an Elementary Fashion

Example

We solve the congruency

$$17x \equiv 9 \pmod{276}.$$

Instead of solving it directly, we note that $276 = 3 \cdot 4 \cdot 23$, so the congruency is equivalent to the system

$$\begin{aligned} 17x &\equiv 9 \pmod{3}, & 17x &\equiv 9 \pmod{4}, & 17x &\equiv 9 \pmod{23}. \\ x &\equiv 0 \pmod{3}, & x &\equiv 1 \pmod{4}, & 17x &\equiv 9 \pmod{23}. \end{aligned}$$

The first congruence gives $x = 3k$, $k \in \mathbb{Z}$. Plugging into the second one,

$$3k \equiv 1 \pmod{4}$$

The modular inverse of $a = 3$ is $a^{-1} = 3$, so we obtain $k \equiv 3 \pmod{4}$.

Solution of a System in an Elementary Fashion

Example (Cont.)

We then have

$$x = 3 \cdot (3 + 4j) = 9 + 12j, \qquad j \in \mathbb{Z}.$$

Inserting into the last congruence,

$$17 \cdot (9 + 12j) \equiv 9 \pmod{23}$$

or

$$204j \equiv -144 \pmod{23}.$$

Hence, $j = 2 + 23t$, $t \in \mathbb{Z}$ and hence

$$x = 33 + 276t$$

or simply $x \equiv 33 \pmod{276}$.

Euler's Phi Function

Theorem
$\varphi(mn) = \varphi(m)\varphi(n)$ *if* $\gcd(m, n) = 1$.

Proof.
Recall the isomorphism $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $x \mapsto (x, x)$. Similarly consider $f^\times : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, $x \mapsto (x, x)$. Obviously $f^\times$ is a homomorphism. We want to show that $f^\times$ is an isomorphism, hence $|(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times|$, i.e., $\varphi(mn) = \varphi(m)\varphi(n)$.

- Injectivity. Note that $f^\times$ is f restricted to the subset $(\mathbb{Z}/mn\mathbb{Z})^\times \subset \mathbb{Z}/mn\mathbb{Z}$, then $f^\times$ is injective since f is.
- Surjectivity. Given $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, by Chinese remainder theorem, we know that there exists $c \in \mathbb{Z}/mn\mathbb{Z}$ such that $f(c) = (a, b)$. We show that $c \in (\mathbb{Z}/mn\mathbb{Z})^\times$. Indeed, if $c = a \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $m \in (\mathbb{Z}/c\mathbb{Z})^\times$. Similarly $n \in (\mathbb{Z}/c\mathbb{Z})^\times$, thus $mn \in (\mathbb{Z}/c\mathbb{Z})^\times$, so $c \in (\mathbb{Z}/mn\mathbb{Z})^\times$. (Be careful with representatives and abuse of notation.)

$\square$

Chinese Remainder Theorem

Corollary

By fundamental theorem of arithmetic, if $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots$ *, then*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \mathbb{Z}/p_3^{k_3}\mathbb{Z} \times \cdots$$

and

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^\times \times (\mathbb{Z}/p_3^{k_3}\mathbb{Z})^\times \times \cdots$$

Theorem (Gauss)

The group $(\mathbb{Z}/n\mathbb{Z})^\times$ *is cyclic if and only if* n *is* 1, 2, 4, p^k, *or* $2p^k$, *where* p *is an odd prime and* $k > 0$.

Table of Contents

RSA (Rivest–Shamir–Adleman) Cryptography

Goal

Transfer information from A (Alice) to B (Bob).

Trapdoor Function

Want to find a (bijective) trapdoor function $f : S \to S$, S a HUGE set, such that

- Easy to compute.
- HARD to invert.
- Unless one has the secret key.

Example (Discrete Logarithm)

Having the inverse of $e \bmod \varphi(n)$, the Euler's totient function of n, is the trapdoor: $f(x) = x^e \pmod{n}$.
If the factorization is known, $\varphi(n)$ can be computed, hence $e^{-1} \bmod \varphi(n)$ can be computed. Its hardness follows from RSA assumption.

RSA Example

1. (Alice) Choose 2 (large) distinct primes, e.g., $p = 17$, $q = 19$.
2. (Alice) Let $n = pq = 17 \times 19 = 323$.
3. (Alice) Let $A = \varphi(n) = (p-1)(q-1) = 16 \times 18 = 288$. (Keep private!)
4. (Alice) Pick[3] $E < \varphi(n)$ such that $\gcd(E, \varphi(n)) = 1$, say, $E = 95$. Publish public key $(n, E) = (323, 95)$, with (public) encryption function e (for Bob)

$$y = e(x) = x^E \pmod{n}, \qquad e.g.,\ y = e(x) = x^{95} \pmod{323}$$

5. (Alice) Compute private key, $D = E^{-1} \pmod{A}$. Then the decryption function d is given by

$$d(y) = y^D = x^{ED} \equiv x \pmod{n}, \qquad e.g.,\ d(y) = y^{191} \pmod{323}$$

3. usually choose $E = 65537$

RSA Correctness

Theorem

Given distinct primes p, q, let $n = pq$ and $ed \equiv 1 \pmod{(p-1)(q-1)}$. Then if $x < n$ with $\gcd(x, n) = 1$, then $x^{ed} \equiv x \pmod{n}$.

Proof.

Since $\gcd(x, n) = 1$, we have $x^{(p-1)(q-1)} \equiv 1 \pmod{n}$.
Therefore $ed = 1 + k(p-1)(q-1)$ for some $k \in \mathbb{Z}$, then

$$\begin{aligned} x^{ed} &= x^{1+k(p-1)(q-1)} \\ &= x \cdot x^{k(p-1)(q-1)} \\ &= x \cdot (x^{(p-1)(q-1)})^k \\ &\equiv x \pmod{n} \end{aligned}$$

□

RSA Correctness

Theorem (Stronger, cf., Gallier, p. 316)

For any two distinct prime numbers p and q, if e and d are any two positive integers such that

1. $1 < e, d < (p-1)(q-1)$,
2. $ed \equiv 1 \pmod{(p-1)(q-1)}$,

then for every $x \in \mathbb{Z}$ we have

$$x^{ed} \equiv x \pmod{pq}$$

Remark

The proof does NOT rely on Euler's theorem (no coprimeness condition).