MATH430 Notes

Professor: Masoud Zargar; Notetaker: Jacob Ma

November 18, 2022

Contents

Chapter 1

Week 1: Induction

1.1 Induction

Definition 1.1.1: Induction

Suppose you have a sequence of statements $S_1, S_2, S_3, \ldots$. Suppose you show that (a) S_1 is true. (b) Whenever S_k is true, S_{k+1} is also true. Then all S_n are true.

Theorem 1.1.2: Well-ordering Principle (WOP)

If $S \subseteq \mathbb{N} = \{1, 2, 3...\}$ that is nonempty, then it has a minimal element, i.e, there is $a \in S$ such that for any $b \in S$, $a \leqslant b$.
$(\{5, 6, 2, 3\} \subset \mathbb{N})$

Proof. Proof that WOP $\implies$ **Induction**
Let $S = \{k \in \mathbb{N} : S_k \text{ is true}\}$. It suffices to shows that $S = \mathbb{N}$. Assume to the contrary that $S \neq \mathbb{N}$.
Let $T := \mathbb{N}/S$. We are assuming that $T \neq \varnothing$, and we want to reach a contradiction.
By the well-ordering principle, T has a minimal element m. Since S_1 is true, $1 \in S$, and so $1 \notin T \implies m \geqslant 2$.
Consider $m - 1 \geqslant 1$. Since m is minimal in T, $m - 1 \notin T \implies m - 1 \in S \implies S_{m-1}$ is true $\implies S_m$ is true $\implies m \in S \implies m \notin T$.
But $m \in T$, so we have a contradiction. □

Proposition 1.1.3

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

Proof. Let $S_n := 1 + 2 + 3 + .. + n$. We use inductions to show that $S_n = \frac{n(n+1)}{2}$
Base Case: $n = 1, S_1 = 1, \frac{1(1+1)}{2} = 1$

If $S_k = \frac{k(k+1)}{2}$, then $S_{k+1} = \frac{(k+1)((k+1)+1)}{2}$. Indeed, we have

$$S_{k+1} = 1 + 2 + 3 + \ldots + k + (k+1) = S_k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

Induction concludes the proof. □

Proposition 1.1.4

$$I_n = \int_0^\infty t^n e^{-t}\,\mathrm{d}t = n! \text{for} n \geqslant 0$$

Proof. We use induction.

The base case is that $I_0 = 1$. Indeed,

$$I_0 = \int_0^\infty e^{-t}\,\mathrm{d}t = -e^{-t}\Big|_0^\infty = 0 - (-1) = 1$$

Now, it suffices, by induction, to show that if

$$I_k = k!, \text{ then } I_{k+1} = (k+1)!$$

We have

$$\begin{aligned} I_{k+1} &= \int_0^\infty t^n e^{-t}\,\mathrm{d}t \\ &= -t^{k+1}e^{-t}\Big|_0^\infty + \int_0^\infty (k+1)t^k e^{-t}\,\mathrm{d}t \\ &= (k+1)I_k \\ &= (k+1)(k!) \\ &= (k+1)! \end{aligned}$$

□

Chapter 2

Week 2: Strong Induction; Dyadic Induction; Backwards Induction

2.1 Induction

Example 2.1.1.

(1) Arithmetic:

$$1 + 2 + 3 + \ldots + n = \frac{n + (n+1)}{2}$$

(2) Calculus:

$$\int_0^\infty t^n e^{-t}\, \mathrm{d}t = n!$$

Proposition 2.1.2

$$S_n = 1^2 + 2^2 + \ldots + n^2 = \frac{(2n+1)(n+1)n}{6}$$

Proof. We apply induction on n

The base case is when $n = 1$. In this case,

$$S_1 = 1^2 = 1$$

and

$$\frac{1(2 * 1 + 1)(1 + 1)}{6} = 1$$

We have now show that for any k, if

$$S_k = \frac{k(2k+1)(k+1)}{6}$$

then

$$S_{k+1} = \frac{(k+1)(2(k+1)+1)((k+1)+1)}{6}$$

Indeed, we have

$$\begin{aligned} S_{k+1} &= 1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 \\ &= S_k + (k+1)^2 \\ &= \frac{k(2k+1)(k+1)}{6} + (k+1)^2 \\ &= \frac{k(2k+1)(k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)\left(k\left(2k+1\right) + 6\left(k+1\right)\right)}{6} \\ &= \frac{(k+1)(2k^2+7k+6)}{6} \\ &= \frac{(k+1)(2k+3)(k+2)}{6} \end{aligned}$$

□

Proposition 2.1.3

Suppose $n \in \mathbb{N}$ and we have a $2^n \times 2^n$ board with a corner removed. Then we can tilt it suing tiles of L-shapes blocks.

Proof. We apply induction on n.

If $n = 1$, then our board is simply L-shape.

Now suppose we have such a tiling for $2^n \times 2^n$ boards with a corner removed.

We want to show that such a tiling is possible for $2^{n+1} * 2^{n+1}$ boards with a corner removed. The L-shape can be inserted into the intersection of three other $2^n \times 2^n$ with a corner removed. Thus it will work. □

Proposition 2.1.4

$$\sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{+\ldots + \sqrt{2}}}}} = 2\cos\frac{\pi}{2^{n+1}}$$

Proof. We apply induction on n.

When $n = 1$, $f(1) = \sqrt{2}$ while $2\cos\frac{\pi}{2^{n+1}} = \sqrt{2}$ as well.

Now suppose the identity is true for k, that is

$$f(k) = 2\cos(\frac{\pi}{2^{k+1}})$$

We want to use this to show that $f(k+1) = 2\cos(\frac{\pi}{2^{k+2}})$

Note that

$$\begin{aligned} f(k+1) &= \sqrt{2+f(k)} \\ &= \sqrt{2+2\cos(\frac{\pi}{2^{k+1}})} \\ &= \sqrt{2}\sqrt{1+\cos(\frac{\pi}{2^{k+1}})} \qquad \text{Applying } 1+\cos x = 2\cos^2\left(\frac{n}{2}\right) \\ &= \sqrt{2}\sqrt{2\cdot\cos^2(\frac{\pi}{2^{k+2}})} \\ &= 2\cos\left(\frac{\pi}{2^{k+2}}\right) \end{aligned}$$

□

Proposition 2.1.5

Define the sequence

$$a_1 = \sqrt{2}, a_{n+1} = \sqrt{2}^{a_n}, \text{ for } n \geqslant 1$$

Does this sequence converge?

Claim 1. It is an increasing sequence (for every n, $a_n \leqslant a_{n+1}$). We show this by applying induction.

Base case $(n = 1)$: $a_1 \leqslant a_2$ because $\sqrt{2} \leqslant \sqrt{2}^{\sqrt{2}}$

Suppose now that $a_k \leqslant a_{k+1}$ for a give k. We want to show that this implies that that

$$a_{k+1} \leqslant a_{k+2}$$

However,

$$a_{k+1} = \sqrt{2}^{a_k} \text{ and } a_{k+2} = \sqrt{2}^{a_{k+1}}$$

We want to show that

$$\sqrt{2}^{a_k} \leqslant \sqrt{2}^{a_{k+1}}$$

Since $a_k \leqslant a_{k+1}$ and $f(x) = \sqrt{2}^x$ is an increasing function. We are done.

Claim 2. For any $n, a_n \leqslant 2$.

We apply induction on n.

Base case $(n = 1)$ $a_1 \leqslant \sqrt{2} \leqslant 2$

Suppose $a_k \leqslant 2$ for some k, then

$$a_{k+1} = \sqrt{2}^{a_k} \leqslant \sqrt{2}^2 = 2$$

By induction, $a_n \leqslant 2$ for all n.

Conclusion. So the sequence (a_n) converges to some $L \leqslant 2$

Problem 1

What is L?

We have

$$L = \lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} \sqrt{2}^{a_n} = \sqrt{2}^{\lim_{n\to\infty} a_n} = \sqrt{2}^{L}$$

Solution

The solutions to $L = \sqrt{2}^{L}$ are $L = 2$ and $L = 4$. But, using claim 2, we have

$$\because L \leqslant 2 \qquad \therefore L = 2$$

Proposition 2.1.6

Every number in the sequence

$$1007, 10017, 100117, \ldots$$

is divisible by 53.

Proof. **Base Case:**

$$1007 = 53 * 19 \implies a_1 \text{ is divisible by } 53$$

$$a_{k+1} = 10(a_k - 6) + 7 = 10a_k - 53$$

So if a_k us is divisible by 53, then a_{k+1} is also divisible by 53. □

Proposition 2.1.7

If α is a real number that

$$\alpha + \frac{1}{\alpha} \in \mathbb{Z}$$

then for every $n \in \mathbb{N}$

$$\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$$

Proof. We use **Strong Induction**.

For $n = 1$, we are given that

$$\alpha + \frac{1}{\alpha} \in \mathbb{Z}$$

Consider $n + 1$.

$$\alpha^{n+1} + \frac{1}{\alpha^{n+1}} = (\alpha^n + \frac{1}{\alpha^n})(\alpha + \frac{1}{\alpha}) - (\alpha^{n-1} + \frac{1}{\alpha^{n-1}})$$

By strong induction, since $\alpha^n + \frac{1}{\alpha^n}, \alpha + \frac{1}{\alpha}, \alpha^{n-1} + \frac{1}{\alpha^{n-1}} \in \mathbb{Z}$ by assumption, the identity implies that

$$\alpha^{n+1} + \frac{1}{\alpha^{n+1}} \in \mathbb{Z}$$

By strong induction, the conclusion follows. □

Theorem 2.1.8: Strong Induction

Suppose we have a sequence of statements

$$S_1, S_2, S_3, \ldots$$

such that

(1) S_1 is true.

(2) For every N, if S_k is true for every $k < N$, then S_N.

It then following that S_n is true for every n.

Proposition 2.1.9

For every integer $n \leqslant 1$

$$3^{n+1} \mid 2^{3^n} + 1$$

Proof. **Base Case:** For $n = 1$, we have

$$9 = 3^{1+1} \mid 2^{3^1} + 1 = 9$$

For $n + 1$, we have

$$\begin{aligned} 2^{3^{n+1}} + 1 &= (2^{3^n})^3 + 1 \\ &= (2^{3^n} + 1)((2^{3^n})^2 - 2^{3^n} + 1) \end{aligned}$$

This is using the following formula:

$$a^3 + b^3 = (a + b)\left(a^2 - ab + b^2\right)$$

Also note that

$$\left(2^{3^n}\right)^2 - 2^{3^n} + 1 \equiv \left((-1)^{3^n}\right)^2 - (-1)^{3^n} + 1 \equiv 0 \pmod 3$$

that is, $\left(2^{3^n}\right)^2 - 2^{3^n} + 1$ is always divisible by 3.

The inductive hypothesis implies that $2^{3^n} + 1$ is divisible by 3^{n+1}. Using the identity above, we obtain that $3^{n+2} \mid 2^{3^{n+1}} + 1$. Thus, the proposition holds for $n + 1$ if it is true for n.

The conclusion follows by induction. □

Proposition 2.1.10

For every $k \in \mathbb{N}$,

$$f(k) := \frac{k^7}{7} + \frac{k^5}{5} + \frac{2k^3}{3} - \frac{k}{105} \in \mathbb{Z}$$

Proof. We will solve this using induction on k.

First, note that

$$f(k) = \frac{15k^7 + 21k^5 + 70k^3 - k}{105}$$

The claim is equivalent to

$$105 \mid 15k^7 + 21k^5 + 70k^3 - k =: g(k) \qquad \text{for every } k \in \mathbb{N}$$

Base Case: $k = 1$:

$$g(1) = 15 + 21 + 70 - 1 = 105 \quad \text{is divisible by} 105$$

Suppose $105 \mid g(k)$. I claim that then $105 \mid g(k+1)$.
It suffices to show that $105 \mid g(k+1) - g(k)$
However,

$$g(k+1) - g(k) = 105k^6 + 315k^5 + 630k^4 + 735k^3 + 735k^2 + 420k + 105$$

is divisible by 105 because all coefficient are divisible by 105 and $k \in \mathbb{N}$.
The conclusion follows from induction. □

Property 2.1.11: Review on induction

(1) **Usual Induction**

$$S_1, S_2, S_3, \ldots \qquad \text{sequence of statements}$$

(1) S_1 true

(2) for any $k \in \mathbb{N}, S_k \implies S_{k+1}$

This implies that S_n is true for every n.

(2) **Strong Induction**

(1) S_1 true

(2) for any $k \in \mathbb{N}$, $(S_1, \ldots, S_n) \implies S_{k+1}$

This implies that S_n is true for every n.

Problem 2

If $\alpha \in \mathbb{R}$ such that

$$\alpha + \frac{1}{\alpha} \in \mathbb{Z},$$

the for every $n \in \mathbb{N}$,

$$\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$$

Solution

Argument relied on the identity

$$\alpha_{n+1} + \frac{1}{\alpha_{n+1}} = \left(\alpha + \frac{1}{\alpha}\right)\left(\alpha^n + \frac{1}{\alpha^n}\right) - \left(\alpha^{n-1} + \frac{1}{\alpha^{n-1}}\right)$$

Problem 3

Every natural number can be written in the form

$$\pm 1^2 + \pm 2^2 \pm 3^2 \ldots \pm n^2$$

Proof. Note that

$$1 = +1^2$$
$$2 = -1^2 - 2^2 - 3^2 + 4^2$$
$$3 = -1^2 + 2^2$$
$$4 = 1^2 - 2^2 - 3^2 + 4^2$$

Now, in order to repeat the other natural numbers, we do an induction of the form "If k can be represented in that form, so can $k+4$

This follows from the identity

$$4 = m^2 - (m+1)^2 - (m+2)^2 + (m+4)^2 \qquad \text{for every } m$$

$$4 + k = \pm 1^2 \pm \ldots \pm n^2 + (n+1)^2 - (n+2)^2 - (n+3)^2 + (n+4)^2$$

□

Problem 4

For every $N \in \mathbb{N}, N \geqslant 2$

$$\sqrt{2\sqrt{3\sqrt{\ldots\sqrt{N}}}} < 3$$

Proposition 2.1.12: Generalization of the problem 4

For every $m \in \mathbb{N}, m \leqslant N$

$$\sqrt{m\sqrt{(m+1)\sqrt{\ldots\sqrt{N}}}} < m+1$$

This is a generalization of the problem.

Proof. We do **backwards induction** on m starting from $m = N$.

Base case: $m = N$, in which case we have

$$\sqrt{N} < N + 1$$

Induction hypothesis: Now assume it is true for $m = k, m \leqslant N$, that is,

$$\sqrt{k\sqrt{(k+1)\sqrt{(k+2)\sqrt{\ldots\sqrt{N}}}}} < k + 1$$

Induction step: Using this, we deduce it for $m = k - 1$ by noting that

$$\sqrt{(k-1)\sqrt{k\sqrt{(k+1)\sqrt{\ldots\sqrt{N}}}}} < \sqrt{(k-1)(k+1)} = \sqrt{k^2-1} < k = (k-1) + 1$$

□

Theorem 2.1.13: Dyadic Induction

Supper we have sequence of statements

$$S_1, S_2, S_3, \ldots$$

Suppose

(1) S_2 is true

(2) for every k, $S_{2^k} \implies S_{2^{k+1}}$

(3) whenever S_{n+1} is true, S_n is true

It then follows that S_n is true for every n.

Theorem 2.1.14: Arithmetic mean - geometric mean ineqaulity (AM-GM Inequality)

If $x_1, .., x_n \geqslant 0$ (real) numbers, then

$$\frac{x_1 + \ldots + x_n}{n} \geqslant \sqrt[n]{x_1 \cdot \ldots \cdot x_n}$$

Proof. For $n = 2$, this is

$$\begin{aligned}
&\frac{x_1 + x_2}{2} \geqslant \sqrt{x_1 x_2} \\
\Leftrightarrow &x_1 + x_2 \geqslant 2\sqrt{x_1 x_2} \\
\Leftrightarrow &x_1 - 2\sqrt{x_1 x_2} + x_2 \geqslant 0 \\
\Leftrightarrow &\left(\sqrt{x_1} - \sqrt{x_2}\right)^2 \geqslant 0
\end{aligned}$$

Induction Hypothesis: Suppose it is true when $n = 2^k$

Induction Step: We show that this implies that it is true for $n = 2^{k+1}$. Indeed,

$$\begin{aligned}
\frac{x_1 + \ldots + x_{2^{k+1}}}{2^{k+1}} &= \frac{\frac{x_1 + \ldots + x_{2^k}}{2^k} + \frac{x_{2^k+1} + \ldots x_{2^{k+1}}}{2^k}}{2} \\
&\geqslant \frac{\sqrt[2^k]{x_1 \ldots x_{2^k}} + \sqrt[2^k]{x_{2^k+1} \ldots x_{2^{k+1}}}}{2} && \text{Applying Induction Hypothesis: inequality holds for } n = 2^k \\
&\geqslant \sqrt{\sqrt[2^k]{x_1 x_2 \ldots x_{2^{k-1}}}\ \sqrt[2^k]{x_{2^{k-1}+1} x_{2^{k-1}+2} \ldots x_{2^k}}} && \text{Applying Base Case } n = 2 \\
&= \sqrt[2^{k+1}]{x_1 x_2 \ldots x_{2^k}}
\end{aligned}$$

So we know by induction on the power k in $n = 2^k$ that inequality is true for powers of 2. It suffices then to show that if the inequality is true for $n = m + 1$, $m \in \mathbb{N}$, then it is true for $n = m$.

Consider m numbers $\geqslant 0$,

$$x_1, \ldots, x_m$$

Extend this to a sequence

$$x_1, x_2, \ldots, x_m, \sqrt[m]{x_1 \ldots x_m}$$

I now have m+1 elements.

Assuming the truth of the inequality for $n = m + 1$, we have

$$\frac{x_1 \ldots x_m + \sqrt[m]{x_1 \ldots x_m}}{m+1} \geqslant \sqrt[m+1]{x_1 \ldots x_m \sqrt[m]{x_1 \ldots x_m}} = \sqrt[m]{x_1 \ldots x_m}$$

Algebraic manipulation gives

$$x_1 + \ldots + x_m + \sqrt[m]{x_1 \ldots x_m} \geqslant (m+1) \sqrt[m]{x_1 \ldots x_m} \implies \frac{x_1 + \ldots + x_m}{m} \geqslant \sqrt[m]{x_1 \ldots x_m}$$

□

Chapter 3

Week 3: Binomial Coefficient

3.1 Comment on Problem 2

Problem 5: Problem 2 on homework

$$\sum_{k=1}^{n} k \cdot 3^k = \frac{3}{4}\left((2n-1)\cdot 3^n + 1\right)$$

$$\sum_{k=1}^{n} k \cdot x^k = x + 2x^2 + \ldots + nx^n$$

Solution

Consider

$$\sum_{k=1}^{n} x^k = \frac{x^{n+1}-1}{x-1}$$

Differentiating both sides to x, we obtain

$$1 + 2x + 3x^2 + .. + nx^{n-1} = \frac{(n+1)\,x^n}{x-1} - \frac{x^{n+1}-1}{(x-1)^2}$$

Multiplying by x, we obtain

$$\sum_{k=1}^{n} k \cdot x^k = x\left(\frac{(n+1)\,x^n}{x-1} - \frac{\left(x^{n+1}-1\right)}{(x-1)^2}\right)$$

3.2 Binomial Coefficient

Definition 3.2.1: Binomial Coefficient

Take $0 \leqslant k \leqslant n$ integers, and define

$$\binom{n}{k} = \#\left\{k\text{- element subsets of an n element set}\right\}$$

Example 3.2.2. Take the set containing $\{Frank, Casey, Emerson, Kamilah\}$

There are 6 pairs: $\{F,C\},\{F,E\},\{F,K\},\{C,E\},\{C,K\},\{E,K\}$

The first person may be chosen in 4, and the second person may be chosen in 3.

The answer is $\frac{4\cdot3}{2} = 6$. (Division by two because pairs were counted twice)

Lemma 3.2.2.1

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

Example 3.2.3.

$$\binom{4}{2} = \frac{4!}{2!\,(4-2)!} = 6$$

Proof. The first person may be chosen in n ways.

The second person in $n-1$ ways.

The k^{th} element in $(n-k+1)$ ways.

So the number of *ordered* k-element subset is $n(n-1),\ldots,(n-k+1)$

The ordering should be removed. So far each k-element subset is counted $k!$.

Therefore,

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\ldots(n-k+1)}{k!} \\ &= \frac{[n(n-1)\ldots(n-k+1)]\,[(n-k)(n-k-1)\ldots1]}{k!\,[(n-k)(n-k-1)\ldots1]} \\ &= \frac{n!}{k!\,(n-k)!}\end{aligned}$$

□

Example 3.2.4. Suppose there are 100 employees. In how many ways can we create groups with exactly 4 members?

Solution

$$\binom{100}{4} = \frac{100!}{4!96!} = \frac{100\cdot99\cdot98\cdot97}{24}$$

Lemma 3.2.4.1

$k!$ always divides the product of any k consecutive integers.

Proof. (1) We start with the situation where the largest number among the k consecutive numbers is $n \leqslant k$:

The product of these k consecutive numbers with largest number n would be:

$$n(n-1)(n-2)\dots(n-k+1)$$

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

is an integer because it is counting the number of k-element subsets of an n-element set

$\therefore k! \mid n(n-1)\dots(n-k+1)$

(2) Another situation is that the sequence of consecutive numbers contains 0 :

The statement is obviously true, $k! \mid 0$

(3) If they are all negative:

Then up to a sign, we can reduce it to the first situation.

Note. n does not have to be larger than k, because things like

$$(-2)(-3)(-4) = (-1)^3(2 \cdot 3 \cdot 4)$$

□

Theorem 3.2.5: Newton's Binomial Theorem

Suppose $n \in \mathbb{N}$, a, b variables

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Example 3.2.6.

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Proof.

$$(a+b)^n = (a+b)(a+b)\dots(a+b) \qquad \text{There are n times}$$

If I chose k of the brackets and have a coming from it, then the other $n-k$ breakers contribute b.
The number of ways of choosing k of the $(a+b)$ terms is $\binom{n}{k}$.
Also, we could have $k \in \{0, \dots, n\}$ a's, thus, the sum is from $k=0$ to $k=n$.
So

$$(a+b) = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

□

3.3 Identities regarding binomial coefficients

Property 3.3.1

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$$

Proof.

$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k} &= \sum_{k=0}^{n} \binom{n}{k} \cdot 1^k \cdot 1^{n-k} \\ &= (1+1)^n \qquad \text{(Newton's BT)} \\ &= 2^n\end{aligned}$$

□

Combinatorial Argument:

- This identity is counting the number of subsets (including the empty subset) of a set with n elements. Each element is either in the subset or not, a state with two possibilities. Therefore, the number of subsets is 2^n, which is the right hand side of the identity.

- On the other hand, we could count subsets of size k and then sum over all possible sizes k. For each such k, there are $\binom{n}{k}$ subsets of size k. Summing over all such possible k, we obtain the total number of subsets of various sizes of an n-element set, which is the left hand side of the identity.

Property 3.3.2

When $a = -1, b = 1$

$$\begin{aligned}0 &= ((-1)+1)^n \\ &= \sum_{k=0}^{n} \binom{n}{k} (-1)^k \cdot 1^{n-k} \\ &= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^{(n)} \binom{n}{n}\end{aligned}$$

Property 3.3.3

$$\binom{n}{k} = \binom{n}{n-k} \qquad \text{for } 0 \leqslant k \leqslant n$$

Proof.

$$\begin{aligned}\binom{n}{n-k} &= \frac{n!}{(n-k)!\,(n-(n-k))!} \\ &= \frac{n!}{(n-k)!k!} \\ &= \binom{n}{k}\end{aligned}$$

□

Combinatorial Argument: Whenever you choose a k-element subset of an n-element set, the complement is an $(n-k)$-element subset of the n-element set.

Property 3.3.4

For $1 \leqslant k \leqslant n$,

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$

Problem 6

Show this algebraically.

Proof. The following is a combinatorial proof. Rewrite the identity in the form

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Let's count something in two different ways.

Consider pairs (A, x), where A is a subset of size k and $x \in A$ (of an n-element set).

We can count the number of such subsets by first selecting A in $\binom{n}{k}$ and choosing $x \in A$ in k ways. There are $k\binom{n}{k}$ such pairs.

Another way of counting such pairs is selecting $x \in \{1, \ldots, n\}$ in n ways and then choosing the other $k-1$ elements to form a subset A of size k. There are $n\binom{n-1}{k-1}$ ways of doing this. □

Property 3.3.5: Pascal's Identity

For $1 \leqslant k \leqslant n$, we have

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$$1$$

$$1, 2, 1$$

$$1, 3, 3, 1$$

$$1, 4, 6, 4, 1$$

Indians had this before (as early as 500s), Yang Hui triangle in China (1050s and 1250s), Khayyam (1050s) / Al-Karaji (950s) Persians, Pascal (1650s)

Combinatorial proof: Take the set $\{1, 2, ..., n\}$ with n element.
Split the problem in two:

(1) Count the subsets of size k contain 1

(2) Count the subsets of size k not containing 1

$$\text{number of subsets of size } k \text{ not containing } 1 = \binom{n-1}{k}$$

$$\text{number of subsets of size } k \text{ containing } 1 = \binom{n-1}{k-1}$$

Therefore,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

The triangle could be written in

$$\binom{1}{0}, \binom{1}{1}$$

$$\binom{2}{0}, \binom{2}{1}, \binom{2}{2}$$

$$\binom{3}{0}, \binom{3}{1}, \binom{3}{2}, \binom{3}{3}$$

Problem 7: Vandermonde's Identity

For $1 \leqslant k \leqslant m+n$, $m, n, k \in \mathbb{N}$

$$\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$$

Proof. Suppose we want to choose k elements from a set with $m+n$ elements.
This can be done in $\binom{m+n}{k}$ ways.
I will count this in different way:
Take the set $\{1, 2, 3, ..., m, m+1, ..., m+n\}$
If i of the elements of the subset are among the first m, than the rest $(k-i)$ elements have to be among $\{m+1, ...m+n\}$.

$$\implies \binom{m}{i}\binom{n}{k-i} \text{ ways.}$$

Now, i could be

$$0, 1, ..., k$$

So summing from $i = 0$ to $i = k$, we obtain

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$$

□

Proof. Skech of alg. proof
Note that $\binom{m+n}{k}$ is the coefficient of x^k on $(1+x)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i$

On the other hand,

$$\begin{aligned}(1+x)^{m+n} &= (1+x)^m (1+x)^n \\ &= \left(\sum_{i=0}^{m}\binom{m}{i}x^i\right)\left(\sum_{j=0}^{n}\binom{n}{j}x^j\right) \qquad \text{Newton's Binomial Theorem applied twice} \\ &= \sum_{l=0}^{m+n}\left(\sum_{i+j=l}\binom{m}{i}\binom{n}{j}x^l\right) \\ &= \sum_{l=0}^{m+n}\left(\sum_{i=0}^{l}\binom{m}{i}\binom{n}{l-i}\right)x^l\end{aligned}$$

Coefficient of x^k is exactly

$$\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}$$

□

Corollary 3.3.6

When $m = k = n$, we have

$$\begin{aligned}\binom{2n}{n} &= \sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i} \\ &= \sum_{i=0}^{n}\binom{n}{i}^2 \\ &= \binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2\end{aligned}$$

Problem 8

$$\sum_{k=1}^{n} k^2\binom{n}{k} = ?$$

Solution

Suppose we have n people. If we choose k of them in $\binom{n}{k}$ ways, the King can be choosen in k ways, and the prime minister also in k ways. There are $k^2\binom{n}{k}$ ways of doing all this.
Since k can be any of $1, 2, \ldots, n$, we have a total of $\sum_{k=1}^{n} k^2\binom{n}{k}$ ways of doing this.
Let's count this is a different way.

(1) **Case 1:** King = PM.

Choose this person in n ways, and then choose a subset of the other $n-1$ people in 2^{n-1} ways.

So when King = President, we have $n2^{n-1}$ communities.

(2) **Case 2:** King $\neq$ PM

In this situation, we choose the King in n ways, and the PM in $n-1$ ways.

Then we choose the citizens in 2^{n-2} ways.

All this can be done in $n(n-1)2^{n-2}$ ways.

Thus,

$$\sum_{k=1}^{n} k^2 \binom{n}{k} = n2^{n-1} + n(n-1)2^{n-2}$$

Proof. Sketch of alg. proof.

The idea is similar to the calculus computation of

$$\sum_{k=1}^{n} k \cdot x^k$$

Consider

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n$$

differentiating once, we obtain

$$\sum_{k=0}^{n} k \binom{n}{k} x^{k-1} = n(1+x)^{n-1}$$

Multiply by x to get

$$\sum_{k=0}^{n} k \binom{n}{k} x^k = nx(1+x)^{n-1}$$

Differentiating again, we get

$$\sum_{k=0}^{n} k^2 \binom{n}{k} x^{k-1} = n\left[(1+x)^{n-1} + (n-1)x(1+x)^{n-2}\right]$$

Set $x = 1$ to get the result. □

Problem 9

Show that

$$\sum_{k=0}^{n} \binom{n+k}{k} \frac{1}{2^k} = 2^n$$

In other words

$$\sum_{k=0}^{n} \binom{n+k}{k} \cdot \frac{1}{2^{n+k}} = 1$$

Proof. We induct on $n \geqslant 0$.

If $n = 0$, then

$$\sum_{k=0}^{0} \binom{0+k}{k} \frac{1}{2^k} = \binom{0}{0} = \frac{0!}{0!0!} = 1$$

and $2^0 = 1$ Suppose it is true for n. We show it for $n+1$. Let

$$f(n) := \sum_{k=0}^{n} \binom{n+k}{k} \frac{1}{2^k}$$

Then

$$
\begin{aligned}
f(n+1) &= \sum_{k=0}^{n+1} \binom{n+1+k}{k} \frac{1}{2^k} \\
&= 1 + \sum_{k=1}^{n} \left[\binom{n+k}{k} + \binom{n+k}{k-1} \right] \frac{1}{2^k} + \binom{2n+2}{n+1} \frac{1}{2^{n+1}} && \text{Pascal's Identity} \\
&= \underbrace{1 + \sum_{k=1}^{n} \binom{n+k}{k} \frac{1}{2^k}}_{f(n)} + \sum_{k=1}^{n} \binom{n+k}{k-1} \frac{1}{2^k} + \binom{2n+2}{n+1} \frac{1}{2^{n+1}} \\
&= f(n) + \sum_{k=1}^{n} \binom{n+k}{k-1} \frac{1}{2^k} + \binom{2n+2}{n+1} \frac{1}{2^{n+1}}
\end{aligned}
$$

Do a change of variables, let $i = k - 1$

$$
\begin{aligned}
&= f(n) + \frac{1}{2} \binom{2n+2}{n+1} \frac{1}{2^n} + \frac{1}{2} \sum_{i=0}^{n-1} \binom{n+1+i}{i} \frac{1}{2^i} && \text{Pascal's Identity on the second term} \\
&= f(n) + \frac{1}{2} \sum_{i=0}^{n-1} \binom{n+1+i}{i} \frac{1}{2^n} + \frac{1}{2} \left[\binom{2n+1}{n} \frac{1}{2^n} + \binom{2n+1}{n+1} \frac{1}{2^n} \right]
\end{aligned}
$$

We know $\binom{(n+1)+n}{n+1} \frac{1}{2^n} = \binom{n+1+(n+1)}{n+1} \frac{1}{2^{n+1}} \Leftrightarrow \binom{2n+1}{n} = \binom{2n+2}{n+1} \frac{1}{2}$ Applying $\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$

$$
\begin{aligned}
&= f(n) + \frac{1}{2} \underbrace{\sum_{i=0}^{n+1} \binom{n+1+i}{i} \frac{1}{2^i}}_{f(n+1)} \\
&= f(n) + \frac{1}{2} f(n+1)
\end{aligned}
$$

We have shown that

$$f(n+1) = f(n) + \frac{1}{2} f(n+1) \implies f(n+1) = 2f(n)$$

By assumption, $f(n) = 2^n \implies f(n+1) = 2^{n+1}$ □

Chapter 4

Week 4: Division Algorithm; Divisibility

4.1 Division algorithm

Theorem 4.1.1

Suppose $a, b \in \mathbb{Z}, b > 0$. Then there are unique integers q and r such that

$$a = bq + r, \quad 0 \leqslant r < b$$

Example 4.1.2. Suppose $b = 4$. Then this is saying that given $a \in \mathbb{Z}$, it can be uniquely written as

$$a = 4q + r, \quad \text{where } r \in \{0, 1, 2, 3\}$$

Proof. We use the Well Ordering Principle. Consider the set

$$S := \{a - bx \mid a - bx \geqslant 0, x \in \mathbb{Z}\}$$

$S \neq \varnothing$ because if $x = -|a|$, we obtain

$$a - b(-|a|) = a + b|a| \geqslant a + |a| \geqslant 0$$

By the well ordering principle, there is a $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that

$$r = a - bq \geqslant 0$$

and r is minimal.

Lemma 4.1.2.1

$$0 \leqslant r < b$$

Every element in S is $\geqslant 0$, and $r \in S \implies r \geqslant 0$.

Assume to the contrary that $r \geqslant b$.

Then take $x = q + 1 \implies$

$$a - b(q + 1) = (a - bq) - b = r - b \geqslant 0.$$

However, this would imply that $0 \leqslant r - b \in S$.

But $r - b < r$, contradicting the minimality of r in S.

This means that we have found $q, r \in \mathbb{Z}$, $0 \leqslant r < b$ such that $a = bq + r$.

Lemma 4.1.2.2

$q, r \in \mathbb{Z}$ such that $a = bq + r$, $0 \leqslant r < b$ must be unique.

Suppose that we have another pair $q_1, r_1 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1, \quad 0 \leqslant r < b$$

In order to show uniqueness, it suffices to show that

$$q_1 = q \text{ and } r_1 = r$$

Consider

$$a = bq + r \qquad (1)$$
$$a = bq_1 + r_1 \qquad (2)$$

$(1) - (2)$:

$$0 = b(q - q_1) + (r - r_1) \implies r_1 - r = b(q - q_1)$$

Take absolute values

$$\implies |r_1 - r| = b|q - q_1| \qquad (3)$$

$$0 \leqslant r_1, r < b \implies |r_1 - r| < b \implies b|q - q_1| < b \implies 0 \leqslant |q - q_1| < 1$$

However, $q, q_1 \in \mathbb{Z} \implies |q - q_1| \in \mathbb{Z}$.

Therefore, $|q - q_1| = 0 \implies q_1 = q$

This also implies, by (3), that

$$|r - r_1| = b|q - q_1| = 0 \implies r_1 = r.$$

□

4.2 Application of Division Algorithm

Problem 10

What are the possible remainder when a perfect square is divided by 3?

Solution

Suppose our perfect square is $n^2, n \in \mathbb{Z}$.

By the division algorithm,

$$n = 3k \quad \text{or} \quad 3k + 1 \quad 3k + 2 \quad \text{for some } k \in \mathbb{Z}$$

(1) $n = 3k$:

Then $n^2 = 9k^2$ divisible by $3 \implies$ remainder $= 0$.

(2) $n = 3k + 1$:

Then

$$\begin{aligned} n^2 &= 9k^2 + 6 + 1 \\ &= 3\left(3k^2 + 2k\right) + 1 \\ &\implies \text{remainder} = 1. \end{aligned}$$

(3) $n = 3k + 2$:

Then

$$\begin{aligned} n^2 &= 9k^2 + 12k + 4 \\ &= 3\left(3k^2 + 4k + 1\right) + 1 \implies \text{remainder} = 1 \end{aligned}$$

Thus, only 0 and 1 are possible remainders.

Problem 11

What are the possible remainders when a perfect square is divided by 4?

Solution

We get a rough sense of the answer by writing out perfect square from 0 to 3, find only 0 and 1 are possible remainders. Below is the formal reasoning:
Suppose $n^2, n \in \mathbb{Z}$, is our perfect square. By the division algorithm, $n = 2k$ or $n = 2k + 1, k \in \mathbb{Z}$.

(1) $n = 2k$ (even):

Then $n^2 = 4k^2$ is divisible by 4.

(2) $n = 2k + 1$ (odd):

$$\begin{aligned} n^2 &= 4k^2 + 4k + 1 \\ &= 4k\left(k + 1\right) + 1 \\ &\implies \text{remainder} = 1 \end{aligned}$$

Problem 12

When an odd perfect square is divided by 8, the remainder is always 1.

Problem 13

Show that no number in the (infinite) sequence

$$11, 111, 1111, 11111, \cdots$$

is a perfect square.

Proof. All numbers in the sequence have a remainder of 3 when divided by 4.

$$11, 1111 = 100 + 11, 1111 = 100 * 11 + 11, \cdots$$

However, the possible remainders of a perfect square divided by 4 are only 0 and 1. □

Theorem 4.2.1: Fermat

If p is an odd prime, then it can be written as a sum of two perfect squares *if and only if* it has remainder 1 when divided by 4.

Full proof will come much later, but we will show the easy part:

Proposition 4.2.2

If we have an *odd* number, that is a sum of two perfect squares, then it must have a remainder of 1 when divide by 4.

Proof. Suppose $n \in \mathbb{Z}$ is odd and $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.
a^2, b^2 are perfect squares, and so only possible remainders when divided by 4 are 0 and 1.
$\implies$ only possible remainder of n when divided by 4 are $0 + 0, 0 + 1, 1 + 0,$ and, $1 + 1$, in other words, $0, 1, 2$.
Since n is odd, 0 and 2 are not possible.
The conclusion follows. □

4.3 Divisibility

Definition 4.3.1: $a \mid b$

Suppose $a, b \in \mathbb{Z}$. We say that **a divides b**, and write $a \mid b$, if there is an integer c such that $b = ac$.

Example 4.3.2.

$$1 \mid n, n = 1 \cdot n$$

$$n \mid n, n = n \cdot 1$$

$$3 \mid 6, 10 \mid 20$$

$$3 \nmid 2$$

$$3 \nmid 5$$

Definition 4.3.3: Greatest Common Divisor (*gcd*)

Suppose $a, b \in \mathbb{Z}$. Then a positive integer d is called the *greatest common divisor* (gcd) of a and b if

(1) $d \mid a$ and $d \mid b$

(2) $c \in \mathbb{N}$ such that $c \mid a$ and $c \mid b \implies c \leqslant d$

Example 4.3.4.

(1) $\gcd(4, 6) = 2$

4 has divisors $1, 2, 4$.

6 has divisors $1, 2, 3, 6$

(2) $\gcd(-5, 5) = 5$

Positive division of $-5 : 1, 5$

$5 : 1, 5$

Problem 14

$\gcd(2016! + 1, 2017! + 1) = ?$

We will use the following fact:

$$(d \mid a, \quad d \mid b) \Leftrightarrow (d \mid a, \quad d \mid b - a)$$

Solution

$$\begin{aligned}
\gcd(2016!+1, 2017!+1) &= \gcd(2016!+1, (2017!+1) - 2017(2016!+1)) && \text{Applying the fact given above} \\
&= \gcd(2016!+1, (2017!+1) - (2017!) - 2017) \\
&= \gcd(2016!+1, -2016) \\
&= \gcd((2016!+1) - (2015!)(2016), -2016) \\
&= \gcd(1, -2016) \\
&= 1
\end{aligned}$$

Problem 15: Exercise

If F_n are the Fibonacci numbers, then $\gcd(F_n, F_{n+1}) = 1$

$\gcd(F_m, F_n) = F_{\gcd(m,n)}$

Proposition 4.3.5

Suppose $k, a, b \in \mathbb{Z}$. Then for $d \in \mathbb{N}$,

$$(d \mid a, d \mid b) \Leftrightarrow (d \mid a, d \mid b - ka)$$

$$\implies \{d \in \mathbb{N} : d \mid a, d \mid b\} = \{d \in \mathbb{N} : d \mid a, d \mid b - ka\}$$

$$\implies \max\{d \in \mathbb{N} : d \mid a, d \mid b\} = \max\{d \in \mathbb{N} : d \mid a, d \mid b - ka\}$$

$$\gcd(a, b) = \gcd(a, b - ka)$$

Recall that the Fibonacci sequence is recursively defined as $F_0 = 1, F_1 = 1$, and

$$F_{n+1} = F_n + F_{n-1} \quad \text{for } n \geqslant 1$$

We have

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

Problem 16

Show that for every n,

$$\gcd(F_n, F_{n+1}) = 1$$

Proof. We use induction on n.

Base case: For $n = 0$, we have

$$\gcd(F_0, F_1) = \gcd(1, 1) = 1$$

Induction Hypothesis: Assume the statement is true for $n = k$.

Induction Step: We show that this implies the validity for $n = k + 1$

$$\begin{aligned}\gcd(F_{k+1}, F_{k+2}) &= \gcd(F_{k_1}, F_{k+1} + F_k) \\ &= \gcd(F_{k+1}, (F_{k+1} + F_k) - F_{k+1}) \qquad \text{Using } \gcd(a,b) = \gcd(a, b-a) \\ &= \gcd(F_{k+1}, F_k)\end{aligned}$$

By the inductive assumption, this latter quantity is 1.
The conclusion follows induction. □

4.4 Basic Properties of Divisibility

Theorem 4.4.1

(1)
$$n \mid n, 1 \mid n, n \mid 0$$

(2)
$$a \mid b, b \mid c \implies a \mid c$$

(3)
$$a \mid b, b \mid a \implies a \pm b$$

(4)
$$a \mid b, b \neq 0 \implies |a| \leqslant |b|$$

(5)
$$d \mid a, d \mid b \implies \forall x, y \in \mathbb{Z}, \quad d \mid ax + by$$

Proof. (1) Clear

(2) $a \mid b \implies$ There is $r \in \mathbb{Z}$ such that $b = ar$.

$b \mid c \implies$ There is $s \in \mathbb{Z}$ such that $c = sb$

$$\implies c = sb = s(ar) = (rs)\, a$$

$$\implies a \mid c$$

(3) If one of a, b is 0, the other must also be 0. $0 \mid 0 \Leftrightarrow$ There is $n \in \mathbb{Z}$ such that $0 = n \cdot 0$

Then the conclusion is clear.

Otherwise,

$$\begin{aligned} a \mid b &\implies b = ra \text{ for some } r \in \mathbb{Z} \\ b \mid a &\implies a = sb \text{ for some } s \in \mathbb{Z} \\ &\implies a = rsa \\ &\implies rs = 1 \\ &\implies r = \pm 1 \end{aligned}$$

(4) $a \mid b, b \neq 0$.

There is $r \in \mathbb{Z}$ such that

$$\begin{aligned} & b = ra \\ \implies & |b| = |r||a| \\ \implies & |b| = |r||a| \geqslant a \end{aligned}$$

(5) If $d \mid a$, then $a = dr, r \in \mathbb{Z}$

If $d \mid b$, then $b = ds, s \in \mathbb{Z}$

If $x, y \in \mathbb{Z}$, then

$$\begin{aligned} ax + by &= drx + dsy \\ &= d(rx + sy) \\ &\implies d \mid ax + by \end{aligned}$$

□

Theorem 4.4.2: Main theorem about gcds: Bézout's Theorem

Suppose $a, b \in \mathbb{Z}$, at least one of which is nonzero.

Then there are integers $m, n \in \mathbb{Z}$, such that

$$\gcd(a, b) = am + bn$$

Example 4.4.3.

$$1 = \gcd(5, 2) = 5 \cdot (1) + 2 \cdot (-2)$$

Proof. We use the well-ordering principle. Consider the set

$$S := \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}.$$

Assume without loss of generality that $a \neq 0$.

If $a > 0$, then $a = a \cdot 1 + b \cdot 0 \in S$.

If $a < 0$, then $|a| = a \cdot (-1) + b \cdot 0 \in S$

Therefore, $S \neq \varnothing$.

By the well-ordering principle, S has a minimal element $d > 0$.

The claim is that $d = \gcd(a, b)$.

We first show that $d \mid a, d \mid b$.

Let's show that $d \mid a$.

By the division algorithm,

$$a = dq + r, \quad \text{for some } q, r \in \mathbb{Z}, \quad 0 \leqslant r < d.$$

Since $d \in S$, there are $x, y \in \mathbb{Z}$, such that

$$d = ax + by$$

Then

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)\, q \\ &= a - axq - byq \\ &= a\,(1 - xq) - byq \end{aligned}$$

And so r is a linear combination of a and b.

If $r > 0$, then r would contradict the minimality of d.

This contradiction implies that $r = 0 \implies d \mid a$.

The exact same argument gives $d \mid b$.

Now we show that d is the *greatest* common divisor of a, b.

If $c \mid a, c \mid b \implies c \mid ax + by = d \implies |c| \leqslant |d| = d$

So $d = \gcd(a, b)$. □

Chapter 5

Week 5: GCDs; Congruence

5.1 Divisibility and gcds

Last time, we proved the Main Theorem on gcds:

Theorem 5.1.1: Main Theorem on gcds

If $a, b \in \mathbb{Z}$, at least one of which is nonzero, then there are $m, n \in \mathbb{Z}$ such that

$$\gcd(a, b) = am + bn$$

Theorem 5.1.2

Suppose $a, b \in \mathbb{Z}$, at least on of which is nonzero. Then

$$\gcd(a, b)\,\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\}$$

Note: $2\mathbb{Z} = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$

Proof. If we consider $ax + by, \quad x, y \in \mathbb{Z}$, then since $\gcd(a, b) \mid a, b, \quad \gcd(a, b) \mid ax + by$.

$$\implies ax + by \in \gcd(a, b)\mathbb{Z}$$

Conversely, if we have a multiple $n \gcd(a, b), \quad n \in \mathbb{Z}$, since

$$\gcd(a, b) = ax + by$$

for some $x, y \in \mathbb{Z}$,

$$n \gcd(a, b) = anx + bny$$

This concludes the proof. □

Corollary 5.1.3:

Suppose $a, b \in \mathbb{Z}$ as before. Then $\gcd(a,b) = 1$ if and only if there are integers $x, y \in \mathbb{Z}$ such that

$$1 = ax + by$$

Proof. If $\gcd(a,b) = 1$, then the main theorem on gcds, there are $x, y \in \mathbb{Z}$ such that

$$1 = \gcd(a,b) = ax + by$$

If $ax + by = 1$, then since $\gcd(a,b) \mid a, b$, $\quad \gcd(a,b) \mid ax + by = 1 \implies \gcd(a,b) = 1$ □

Proposition 5.1.4

Suppose $a \mid bc$ and $\gcd(a,b) = 1$. Then $a \mid c$.

Example 5.1.5.

$$4 \mid 3 \cdot 4$$

Proof. Since $\gcd(a,b) = 1$, there are integers $x, y \in \mathbb{Z}$ such that

$$ax + by = 1. \quad (*)$$

Multiply both sides of $(*)$ by c to get

$$acx + bcy = c$$

Note that $a \mid ac$ and we are given $a \mid bc$. Therefore,

$$a \mid (ac)\, x + (bc)\, y = c$$

□

Problem 17: Homework Problem

If p is a prime and $1 \leqslant k \leqslant p-1$, then $p \mid \binom{p}{k}$.

Solution

$$\mathbb{Z} \ni \binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$
$$\implies k! \mid p(p-1)\cdots(p-k+1)$$

Since $\gcd(k!, p) = 1$, $k! \mid (p-1)(p-2)\cdots(p-k+1)$

Proposition 5.1.6

Suppose $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. If $a \mid c$, $b \mid c$, then

$$ab \mid c.$$

Example 5.1.7.

$$2 \mid n$$
$$3 \mid n$$
$$\implies 6 = 2 \cdot 3 \mid n$$

Proof. Since $\gcd(a, b) = 1$, we know by the main theorem on gcds, that there are $x, y \in \mathbb{Z}$, such that

$$ax + by = 1.$$

Multiply by c to get

$$acx + bcy = c$$

Since $b \mid c$, $ab \mid ac$.

$$\left(\frac{c}{b} \in \mathbb{Z} \implies \frac{ac}{ab} = \frac{c}{b} \in \mathbb{Z}\right)$$

By the same argument, $a \mid c \implies ab \mid bc$.

We conclude that

$$ab \mid acx + bcy = c$$

□

Problem 18

Show that

$$21x^2 - 7y^2 = 9$$

has no integer solutions.

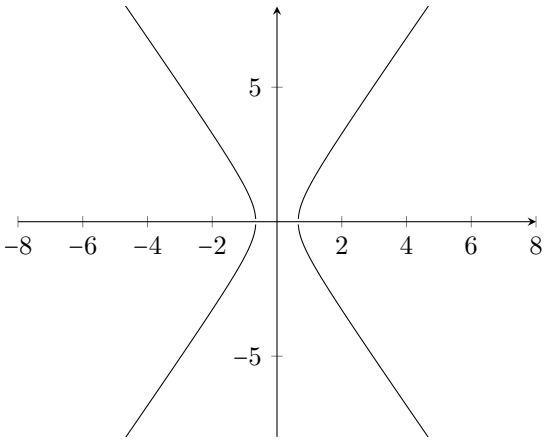

Figure 5.1: $21x^2 - 7y^2 = 9$

Solution

Since $3 \mid 9$ and $3 \mid 21x^2$, $3 \mid 7y^2$. Since $\gcd(3,7) = 1$,

$$\begin{aligned} 3 \mid y^2 = y \cdot y &\implies 3 \mid y \\ &\implies y = 3y_1, \quad \text{for some } y_1 \in \mathbb{Z} \end{aligned}$$

Therefore,

$$\begin{aligned} & 21x^2 - 7(3y_1)^2 = 9 \\ \Leftrightarrow & 21x^2 - 7 \cdot 3 \cdot 3y_1^2 = 9 \\ \Leftrightarrow & 7x^2 - 21y_1^2 = 3 \end{aligned}$$

Since $3 \mid 3$ and $3 \mid 21y^2$, we must have $3 \mid 7x^2$. Again , this implies that $3 \mid x \implies x = 3x_1,$ for some $x_1 \in \mathbb{Z}$

$$\begin{aligned} & 7(3x_1)^2 - 21y_1^2 = 3 \\ \Leftrightarrow & 21x_1^2 - 7y_1^2 = 1 \\ \Leftrightarrow & 21x_1^2 - 6y_1^2 - y_1^2 = 1 \\ \Leftrightarrow & \underbrace{\left(21x_1^2 - 6y_1^2 - 3\right)}_{\text{divisible by 3}} + 2 = y_1^2 \end{aligned}$$

This implies that y_1^2 has remainder 2 when divided by 3.

However, no such perfect square exists.

Problem 19

Show that

$$x^2 + y^2 + z^2 = 2xyz$$

has no integer solutions except for $x = y = z = 0$.

Solution: Sketch

Let $k \geqslant 0$ one the largest power of 2 such that $2^k \mid x, y, z$. Write

$$x = 2^k x_1, y = 2^k y_1, z = 2^k z_1$$

Then $x_1^2 + y_1^2 + z_1^2 = 2^{k+1} x_1 y_1 z_1$.
You can conclude that exactly one of x_1, y_1, z_1 is even, say x_1.
This implies that

$$\begin{aligned} & y_1^2 + z_1^2 = 2^{k+1} x_1 y_1 z_1 - x_1^2 \qquad \text{Note that } 2 \mid x_1 \\ \implies & 4 \mid y_1^2 + z_1^2 \end{aligned}$$

Thus, there is a contradiction that $y_1\ z_1$ are odd, thus $y_1^2 + z_1^2 \equiv 1 + 1 \equiv 2 \mod 4$.

5.2 Gcds and Congruences

Definition 5.2.1: Congruence

We say that $a, b \in \mathbb{Z}$ are congruent modulo (or mod) $n \in \mathbb{N}$, and write $a \equiv b \pmod{n}$, if $n \mid a - b$.

Example 5.2.2.

$$\begin{aligned} -1 &\equiv 2 \pmod 3 \\ 7 &\equiv 3 \pmod 4 \\ 3 &\equiv 1 \pmod 2 \\ 11 &\equiv 2 \pmod 9 \end{aligned}$$

If a is odd, then $a^2 \equiv 1 \pmod 8$.
If $a \in \mathbb{Z}$, then $a^2 \equiv 0$ or $1 \pmod 4$.
If $a \in \mathbb{Z}$, then $a^2 \equiv 0$ or $1 \pmod 3$.

Problem 20

Are there integer solutions to $21x^2 - 7y^2 = 9$

Solution

See the solution back to Problem 18.
The point of the solution was that, in the notation of the solution to problem 18, we ended up with $y_1^2 \equiv -1 = 2 \bmod 3$, which is impossible.

Theorem 5.2.3

(1) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a + c \equiv b + d \pmod n$.

(2) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$.

Proof. Since $a \equiv b \pmod n$, $n \mid a - b \implies$ there exists $r \in \mathbb{Z}$ such that $a - b = nr \implies a = b + nr$
Similarly, there is $s \in \mathbb{Z}$ such that $c = d + ns$.
Therefore,

$$\begin{aligned} a + c &= (b + nr) + (d + ns) \\ &= (b + d) + n(r + s) \\ &\implies n \mid (a + c) - (b + d) \\ &\Leftrightarrow a + c \equiv b + d \pmod n \end{aligned}$$

This concludes the proof of (1).

$$\begin{aligned} ac &= (b + nr)(d + ns) \\ &= bd + nbs + ndr + n^2 rs \\ &= bd + n(bs + dr + nrs) \\ &\implies n \mid ac - bd \\ &\Leftrightarrow ac \equiv bd \pmod n \end{aligned}$$

□

Corollary 5.2.4

Suppose $P \in \mathbb{Z}[X]$ $(= \{a_0 + a_1 X + \cdots + a_k X^k \mid k \geqslant 0, k \in \mathbb{Z}, a_i \in \mathbb{Z} \text{ for every } i\}$ = polynomials with $\mathbb{Z}$ coeff .)
Then $a \equiv b \pmod n \implies P(a) \equiv P(b) \pmod n$.

Proof. Suppose

$$P(X) = a_0 + a_1 X + \cdots + a_k X^k, \quad \text{with } a_i \in \mathbb{Z}$$

Then, $a \equiv b \pmod n \implies a^j \equiv b^j \pmod n$ for any $j \geqslant 0$.
Thus , for every $j \geqslant 0, a_j \cdot a^j \equiv a_j \cdot b^j \pmod n \implies P(a) \equiv P(b) \pmod n$. □

Proposition 5.2.5

If $a \in \mathbb{Z}$, then $a^2 \equiv 0$ or $1 \pmod 3$.

Proof. by the division algorithm,

$$a \equiv 0, 1, 2 \pmod 3$$
$$\implies a^2 \equiv 0^2, 1^2, 2^2 \pmod 3$$

□

Proposition 5.2.6

If $a \in \mathbb{Z}$, then $a^2 \equiv 0$ or $1 \pmod 4$.

Proof. By the division algorithm

$$a \equiv 0, 1, 2, 3 \pmod 4$$

Therefore,

$$a^2 \equiv 0^2, 1^2, 2^2, 3^2 \pmod 4$$
$$\equiv 0, 1, \pmod 4$$

□

Proposition 5.2.7

If $a \in \mathbb{Z}$ is odd, then $a^2 \equiv 1 \pmod 8$.

Proof. Since $a \in \mathbb{Z}$ is odd, the division algorithm implies that

$$a \equiv 1, 3, 5, 7 \pmod 8$$

Then,

$$a^2 \equiv 1^2, 3^2, 5^2, 7^2 \pmod 8$$
$$\equiv 1 \pmod 8$$

□

Problem 21

What are all pairs of prime numbers (p, q) such that

$$p = \frac{a^3 + a}{2}, q = \frac{a^3 - a}{2} \text{ for some } a \in \mathbb{Z}$$

Solution

If it is easy to see that this is equivalent to finding pairs of prime numbers $(p-q)^3 = p+q$.

$$\begin{aligned}(p-q)^3 &= ((p+q)-2q)^3 \\ &\equiv (0-2q)^3 \pmod{p+q} \\ &\equiv -8q^3 \pmod{p+q}\end{aligned}$$

Because $(p-q)^3 = p+q$, thus $p+q \equiv 0 \pmod{p+q} \implies p+q \mid 8q^3$.
And we know

$$\begin{aligned}p+q &= (p-q)+2q \\ &\equiv 2q \pmod{p-q}\end{aligned}$$

and because $p+q = (p-q)^3 \equiv 0 \pmod{p-q}$, thus $p-q \mid 2q$
$p \neq q$, and p, q are primes $\implies \gcd(p,q) = 1$.
Then,

$$\begin{aligned}\gcd(p-q,q) &= \gcd((p-q)+q,q) \\ &= \gcd(p,q) \\ &= 1\end{aligned}$$

Using $(a \mid bc, \gcd(a,b) = 1 \implies a \mid c)$, we obtain from $p-q \mid 2q$ that $p-q \mid 2$.
By a similar argument, (It suffies to show $\gcd(p+q,q) = 1$.)

$$\gcd\left(p+q, q^3\right) = 1.$$

Combining with $p+q \mid 8q^3$, we obtain $p+q \mid 8$.
From $p-q \mid 2$ and $p+q \mid 8$, we obtain that $(p,q) = (5,3)$.

Proposition 5.2.8

$$\gcd(a,b) = d \implies \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Proof. There are integers $x, y \in \mathbb{Z}$ such that

$$\begin{aligned}&ax + by = d \\ \implies &\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1 \\ \implies &\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1\end{aligned}$$

□

5.3 Gcds of more than two variables

Definition 5.3.1: Gcd of more than two variables

Suppose $a_1, ..., a_n$ are integers, at lead one of which is nonzero. Then the gcd of $a_1, ..., a_n$ written $\gcd(a_1, ..., a_n)$ is the largest natural number d, such that.

(1) $d \mid a_1, ..., d \mid a_n$

(2) if $c \mid a, ..., c \mid a_n$, then $c \leqslant d$

Problem 22

$$\gcd\left(2002+2, 2022^2+2, 2002^3+2, \cdots\right) = ?$$

Solution

Let $d = \gcd\left(2002+2, 2002^2+2, 2002^3+2, \cdots\right)$. Then

$$d \mid 2002+2, 2002^2+2 \implies d \mid \gcd\left(2002+2, 2002^2+2\right)$$

Note that

$$\begin{aligned} 2002^2+2 &= 2002(2000+2)+2 \\ &= 2000(2002+2)+6 \end{aligned}$$

This implies that

$$\begin{aligned} \gcd\left(2002+2, 2002^2+2\right) &= \gcd(2002+2, 6) \\ &= \gcd(2004, 6) \\ &= 6 \end{aligned}$$

Therefore $d \mid 6$. If we show that $6 \mid 2002^k + 2$ for every $k \geqslant 1$ then we would be done.
The claim is that $3 \mid 2002^k + 2$

$$\begin{aligned} 2002^k + 2 &\equiv 1^k + 2 \\ &= 1 + 2 \\ &= 3 \\ &\equiv 0 \pmod 3 \end{aligned}$$

We also know that $2002 + 2 \equiv 0^k + 0 \equiv 0 \pmod 2$.
We conclude that $6 \mid 2022^k + 2$ for every $k \geqslant 1$.

Proposition 5.3.2

A natural number is divisible by 3 (or 9) if and only if its sum of digits is divisible by 3.

Proof. Suppose n is a natural number with decimal expression

$$n = (a_0, \cdots, a_d)_{10} = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_d \cdot 10^d, \text{where } 0 \leqslant a_0, \cdots, a_d \leqslant 9$$

$$\begin{aligned} n &= a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_d \cdot 10^d \\ &\equiv a_0 + a_1 \cdot 1 + a_2 \cdot 1^2 + \cdots + a_d \cdot 1^d \pmod 9 \\ &= a_0 + a_1 + \cdots + a_d \pmod 9 \end{aligned}$$

□

Chapter 6

Week 6: Least Common Multiple (lcm), Euclidean Algorithm, Unique Prime Factorization

6.1 Least Common Multiple (lcm)

Definition 6.1.1: Least Common Multiple (lcm)

Suppose $a, b \in \mathbb{Z}$. Then the least common multiple of a and b, written $\text{lcm}(a, b)$, i s a positive integer such that

(1) $a \mid d$ and $b \mid d$

(2) if $a \mid c$ and $b \mid c$ where $c \neq 0$, then $c \geqslant d$

Example 6.1.2.

$$\text{lcm}(2, 3) = 6$$
$$\text{lcm}(4, 6) = 12$$

Theorem 6.1.3

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab$$

In other words,

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

Example 6.1.4.

$$\gcd(a,b) = 1 \Leftrightarrow \text{lcm}(a,b) = ab$$

$$\text{lcm}(4,6) = \frac{4 \cdot 6}{\gcd(4,6)} = \frac{4 \cdot 6}{2} = 12$$

6.2 cm and gcd, Euclidean algorithm

Theorem 6.2.1: lcm and gcd

For any $a, b \in \mathbb{N}$,

$$\text{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

Proof. Let $d = \gcd(a,b)$, and let

$$m = \frac{ab}{d}$$

Note that

$$m = a(\frac{b}{d}) \quad \text{and} \quad d \mid b$$

Therefore, $a \mid m$.

Similarly, $b \mid m$.

Therefore, m is a common multiple of both a and b.

We now show that m is the least common multiple.

Suppose c is a nonzero common multiple of a and b.

Consider

$$\begin{aligned} \frac{c}{m} &= \frac{c}{(\frac{ab}{d})} \\ &= \frac{cd}{ab}. \end{aligned}$$

By Bézout's theorem, there are integers x, y s.t.

$$d = ax + by.$$

(Note: Bézout's theorem was an existence result, not a constructive one.)

Consequently,

$$\begin{aligned} \frac{c}{m} &= \frac{c(ax+by)}{ab} \\ &= \frac{c}{b}x + \frac{c}{a}y \end{aligned}$$

c is a common multiple of a and b, i.e. $a, b \mid c \implies \frac{c}{b}x + \frac{c}{a}y \in \mathbb{Z}$

We conclude that $m \mid c \overset{c \neq 0}{\implies} m \leq c$. Therefore,

$$m = \text{lcm}(a,b).$$

The conclusion follows. □

Corollary 6.2.2

Suppose $a, b \in \mathbb{N}$. Then

$$\gcd(a,b) = 1 \Leftrightarrow \operatorname{lcm}(a,b) = ab$$

Example 6.2.3.

$$\operatorname{lcm}(4,5) = 4 \cdot 5 = 20$$

$$\operatorname{lcm}(6,4) = \frac{4 \cdot 6}{\gcd(4,6)} = \frac{4 \cdot 6}{2} = 12.$$

6.3 Euclidean algorithm

Theorem 6.3.1: Euclidean algorithm

The basis of the Euclidean algorithm is the division algorithm.

Theorem 6.3.2: Division algorithm.

Suppose $a, b \in \mathbb{N}$. Then there are unique integers q and r s.t.

$$a = bq + r$$

and

$$0 \leq r < b.$$

Example 6.3.3. If $b = 4$, then any $a \in \mathbb{N}$ is uniquely written as

$$a = 4q + r, 0 \leq r < 4$$

Suppose $a, b \in \mathbb{N}$. Then if

$$a = bq_1 + r_1, 0 \leq r_1 < b,$$

then

$$\begin{aligned} \gcd(a,b) &= \gcd(bq_1 + r_1, b) \\ &= \gcd((bq_1 + r_1) - bq_1, b) \\ &= \gcd(b, r_1) \end{aligned}$$

Now repeating the process, as follows:

$$\begin{aligned} b &= q_1 r_1 + r_2, && 0 \le r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3, && 0 \le r_3 < r_2 \\ &\vdots \\ r_{n-1} &= q_n r_n + r_{n+1}, && 0 \le r_{n+1} < r_n \\ r_n &= q_{n+1} r_{n+1} + 0 \end{aligned}$$

Therefore,

$$\begin{aligned} \gcd(a,b) &= \gcd(b, r_1) \\ &= \gcd(r_1, r_2) \\ &\vdots \\ &= \gcd(r_{n+1}, 0) \\ &= r_{n+1} \end{aligned}$$

Note that for any $n \in \mathbb{N}$,

$$\gcd(n, 0) = n.$$

Example 6.3.4: $\gcd(20, 15) = ?$. Using the Euclidean algorithm, we write

$$\begin{aligned} 20 &= 1 \cdot 15 + 5 \\ 15 &= 3 \cdot 5 + 0 \end{aligned}$$

Thus,

$$\gcd(20, 15) = 5.$$

Example 6.3.5: (from textbook).

$$\gcd(12378, 3054) = ?$$

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

Therefore,

$$\gcd(12378, 3054) = 6.$$

If we want to find x, y, s.t.

$$12378x + 3054y = 6.$$

We do the following process:

$$\begin{aligned}
6 &= 24 - 1 \cdot 18 \\
&= 24 - 1 \cdot (138 - 5 \cdot 24) \\
&= 6 \cdot 24 - 1 \cdot 138 \\
&= 6 \cdot (162 - 1 \cdot 138) - 1 \cdot 138 \\
&= 6 \cdot 162 - 7 \cdot 138 \\
&= 6 \cdot 162 - 7 \cdot (3054 - 18 \cdot 162) \\
&= (6 + 7 \cdot 18) - 7 \cdot 3054 \\
&= 132 \cdot 162 - 7 \cdot 3054 \\
&= 132 \cdot (12378 - 4 \cdot 3054) - 7 \cdot 3054 \\
&= 132 \cdot 12378 - (132 \cdot 4 + 7) \cdot 3054 \\
&= 132 \cdot 12378 - 535 \cdot 3054
\end{aligned}$$

Therefore, we can take

$$(x, y) = (132, -535)$$

to get

$$12378x + 2054y = 6$$

Since $\gcd = 6$, we obtain

$$\operatorname{lcm}(12378, 3054) = \frac{12378 \cdot 3054}{6}.$$

Property 6.3.6

For gcd, we know the property about divisibility that

$$d \mid a, d \mid b \implies d \mid a + kb, b \implies \gcd(a, b) = \gcd(a + kb, b)$$

For lcm, however, $\operatorname{lcm}(a, b) \neq \operatorname{lcm}(a, a + kb)$, because such property fails:

$$a \mid m, b \mid m \not\implies a + kb \mid m.$$

Instead, we use

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

Example 6.3.7. We have $\operatorname{lcm}(6, 4) = 12$, but $\operatorname{lcm}(6 - 4, 4) = \operatorname{lcm}(2, 4) = 4 \neq 12$.

Proposition 6.3.8

Suppose $\gcd(a,b) = 1$. Then

$$\gcd(a, b^3) = 1$$

Proof. By Bézout's theorem,

$$1 = ax + by \text{ for some } x, y \in \mathbb{Z}.$$

$$\begin{aligned} 1 = 1^3 &= (ax+by)^3 \\ &\overset{NBT}{=} a^3x^3 + 3a^2x^2by + 3axb^2y^2 + b^3y^3 \\ &= a(a^2x^3 + 3ax^2by + 3xb^2y^2) + b^3y^3 \\ \implies &\gcd(a, b^3) = 1 \end{aligned}$$

Note: This is using the corollary 5.1. Suppose $a, b \in \mathbb{Z}$ as before. Then $\gcd(a,b) = 1$ if and only if there are integers $x, y \in \mathbb{Z}$ such that

$$1 = ax + by$$

□

Proposition 6.3.9

If $\gcd(a,b) = 1$, then $\gcd(a^2 + b^2, b^3) = 1$.

Proof. By the previous problem, it suffices to show that $\gcd(a^2 + b^2, b) = 1$. However, $\gcd(a^2 + b^2, b) = \gcd((a^2 + b^2) - b \cdot b, b)$

A second application of the previous problem gives

$$\gcd(a^2, b) = 1 \text{ since } \gcd(a,b) = 1$$

□

6.4 General Solution of $\gcd(a,b) = ax + by$

How do we find integer solutions to

$$\gcd(a,b) = ax + by?$$

The Euclidean algorithm only gave one solution.

$ax + by = \gcd(a,b)$ is a line with rational slope. Since we also have at leas one solution, we expect infinitely many many integer solutions.

Theorem 6.4.1

Suppose a and b are as before and $c \in \mathbb{Z}$. Then $ax + by = c$ has an integer solution $\Leftrightarrow d = \gcd(a,b) \mid c$. If $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ is a solution, then *all* solutions of $ax + by = c$ are given by

$$\begin{aligned} x &= x_0 - (\tfrac{b}{d})t \\ y &= y_0 + (\tfrac{a}{d})t \end{aligned}, t \in \mathbb{Z}$$

Example 6.4.2. Last class, we computed

$$\gcd(12378, 3054)$$

and found

$$(x_0, y_0) = (132, -535)$$

as a solution to

$$12378x + 3054y = 6$$

By this theorem, all solutions are

$$\begin{aligned} x &= 132 - (\frac{3054}{6})t \\ y &= -535 + \frac{12378}{6}t \end{aligned}$$

Proof. If $ax + by = c$ has an integer solution, then $d \mid a$, $d \mid b \implies d \mid ax + by = c$.
On the other hand, suppose $d \mid c$. Then $c = dk$ for some $k \in \mathbb{Z}$.
By Bézout's theorem, there are integers x', y' s.t.

$$ax' + by' = d.$$

Multiplying both sides by k, we obtain

$$a(kx') + b(ky') = dk = c$$

Suppose $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a solution. Then

$$ax + by = c \tag{1}$$

We also have

$$ax_0 + by_0 = c \tag{2}$$

$(1) - (2)$ given

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= c - c = 0 \\ \implies a(x - x_0) &= b(y_0 - y) \end{aligned}$$

Divided by d to obtain

$$(\frac{a}{d})(x - x_0) = (\frac{b}{d})(y_0 - y) \tag{3}$$

$$\gcd(a, b) = d \implies \gcd(\frac{a}{d}, \frac{b}{d}) = 1$$

From (3), we have

$$\frac{a}{d} \Big| (\frac{b}{d})(y_0 - y)$$

(In general, if $s \mid uv$, $\gcd(s,u) = 1 \implies s \mid v$)

Therefore,

$$\frac{a}{d} \mid y_0 - y$$

$\implies$ there is an integer t_1, s.t.

$$\begin{aligned} y_0 - y &= -\frac{a}{d}t_1 \\ \implies y &= y_0 + \frac{a}{d}t_1 \end{aligned}$$

Similarly, there is an integer t_2, s.t.

$$\begin{aligned} \frac{b}{d} &\mid x - x_0 \\ \implies x - x_0 &= -\frac{b}{d}t_2 \\ \implies x &= x_0 - \frac{b}{d}t_2 \end{aligned}$$

We know that

$$\begin{cases} y_0 - y = -\frac{a}{d}t_1 \\ x - x_0 = -\frac{b}{d}t_2 \\ (\frac{a}{d})(x - x_0) = (\frac{b}{d})(y_0 - y) \end{cases}$$

From this, we obtain that $t_1 = t_2$. So all solutions are of the stated form.

Note furthermore that if

$$\begin{aligned} x &= x_0 - \frac{b}{d}t \\ y &= y_0 + \frac{a}{d}t, \end{aligned}$$

then

$$\begin{aligned} ax + by &= a(x_0 - \frac{b}{d}t) + b(y_0 + \frac{a}{d}t) \\ &= ax_0 + by_0 - \frac{ab}{d}t + \frac{ab}{d}t \\ &= c \end{aligned}$$

□

6.5 Unique Factorization

Definition 6.5.1: Prime Numbers

A natural number $p \geq 2$ is said to be prime if its *only* divisors are 1 and p.

Example 6.5.2.

$$5, 7, 11, 13, 17, 19$$

are prime numbers.

Definition 6.5.3: Composite

If $n \geq 2$ is an integer, it is called **composite** if there are integers $a, b \geq 2$ s.t.

$$n = a \cdot b.$$

Example 6.5.4. $6 = 2 \cdot 3$, $10 = 2 \cdot 5$, $12 = 2^2 \cdot 3$

Theorem 6.5.5: Unique prime factorization

Every integer $n \geq 2$ is a product of prime numbers

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, (p_1, \cdots, p_k \text{ primes})$$

and this decomposition is unique up to rearranging the prime numbers.

Proof. We prove existence using strong induction on $n \geq 2$. Clearly, $n = 2$ is a prime number and so this settles the base case. Now suppose the existence part if valid for every $2 \leq n \leq k$.

Consider $n = k + 1$.

We are done if $k + 1$ is a prime. Otherwise, $k + 1 = a \cdot b$ for some $a, b \geq 2$.

$$\implies a = \frac{k+1}{b} \leq \frac{k+1}{2} \leq k$$

$$b \leq k.$$

By the inductive assumption, both a and b have a prime decomposition, and so does $k+1 = a \cdot b$. Existence follows from strong induction.

For uniqueness, suppose

$$\begin{aligned} n &= p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \geq 0 \\ &= p_1^{\beta_1} \cdots p_k^{\beta_k}, \beta_i \geq 0 \end{aligned}$$

Suppose $\alpha_1 \geq 1$, and so

$$p_1^{\alpha_1} \mid n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

(Recall that if $a \mid bc$ and $\gcd(a, b) = 1 \implies a \mid c$.)

We know that $\gcd(p_1^{\alpha_1}, p_2) = \gcd(p_1^{\alpha_1}, p_3) = \cdots = \gcd(p_1^{\alpha_1}, p_k) = 1$

Therefore, we obtain that

$$p_1^{\alpha_1} \mid p_1^{\beta_1} p_2^{\max\{\beta_2 - 1, 0\}} \cdots p_k^{\max\{\beta_k - 1, 0\}}.$$

Repeating the process, we many eliminate all $p_2, \cdots, p_k$.

Consequently,

$$p_1^{\alpha_1} \mid p_1^{\beta_1}$$

$$\implies \alpha_1 \leq \beta_1.$$

Similarly, $\beta_1 \le \alpha_1$.

Therefore, $\alpha_1 = \beta_1$. We can similarly show that $\alpha_2 = \beta_2, \cdots, \alpha_k = \beta_k$.

This concludes the proof of uniqueness. □

Theorem 6.5.6: How is g.c.d related to prime factorizations

Suppose

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, (\alpha_i \ge 0)$$
$$b = p_1^{\beta_1} \cdots p_k^{\beta_k}, (\beta_i \ge 0)$$

Then

$$\gcd(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$$

Proof. Proof sketch:

Suppose $d \mid a, b$.

Then

$$d = p_1^{\gamma_1} \cdots p_k^{\gamma_k} \Big| p_1^{\alpha_1} \cdots p_k^{\alpha_k}, p_1^{\beta_1} \cdots p_k^{\beta_k}$$
$$\implies \text{For every } i, \gamma_i \le \min\{\alpha_i, \beta_i\}.$$

Therefore,

$$\gcd(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}.$$

□

Example 6.5.7.

$$\gcd(12,15) = \gcd(2^2 \cdot 3, 3 \cdot 5) = 2^{\min\{0,2\}} \cdot 3^{\min\{1,1\}} \cdot 5^{\min\{0,1\}} = 3$$

Proof. Complete proof:

Basic observation: If $d \mid n$, then $n = dr$ for some $r \in \mathbb{Z}$.

By unique prime factorization, any prime appearing in d must also appear in n.

Furthermore, the largest power of any such prime must be at most the power of this prime appearing in n.

Now suppose that $d \mid a$ and $d \mid b$, $d, a, b \in \mathbb{N}$.

Then writing

$$\begin{matrix} a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ b = p_1^{\beta_1} \cdots p_k^{\beta_k} \end{matrix}, p_i \text{ distinct prime numbers,}$$

then

$$d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$$

where $\gamma_i \le \alpha_i, \beta_i$ and $\alpha_i, \beta_i \ge 0$.

Thus for every i,

$$\gamma_i \le \min\{\alpha_i, \beta_i\}.$$

From this, we obtain that

$$\gcd(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$$

By the exact same argument, if

$$\begin{aligned} a_1 &= p_1^{\alpha_{1,1}} \cdots p_k^{\alpha_{1,k}} \\ &\vdots \qquad\qquad , \alpha_{i,j} \geq 0, \text{ then} \\ a_n &= p_1^{\alpha_{n,1}} \cdots p_k^{\alpha_{n,k}} \end{aligned}$$

$$\gcd(a_1, \cdots, a_n) = p_1^{\min\{\alpha_{1,1},\alpha_{2,1},\cdots,\alpha_{n,1}\}} \cdots p_k^{\min\{\alpha_{1,k},\alpha_{2,k},\cdots,\alpha_{n,k}\}}$$

Warning. $\gcd(a,b,c) = 1 \implies \gcd(a,b) = 1$

Example 6.5.8. $\gcd(2\cdot 3, 3\cdot 5, 5\cdot 2) = 1$. but $\gcd(2\cdot 3, 3\cdot 5) = 3 \neq 1$.

□

Theorem 6.5.9: How l.c.m is related to prime factorizations

From lcm, note the following.

If $a \mid m$ and $b \mid m$, where

$$\begin{aligned} a &= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ b &= p_1^{\beta_1} \cdots p_k^{\beta_k} \\ m &= p_1^{\gamma_1} \cdots p_k^{\gamma_k}, \end{aligned}$$

then $\alpha_i, \beta_i \leq \gamma_i$, i.e. $\max\{\alpha_i, \beta_i\} \leq \gamma_i$ for every i.

From this, we obtain that

$$\operatorname{lcm}(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}.$$

Example 6.5.10.

$$\begin{aligned} \operatorname{lcm}(12,15) &= \operatorname{lcm}(2^2 \cdot 3, 3 \cdot 5) \\ &= 2^{\max\{2,0\}} \cdot 3^{\max\{1,1\}} \cdot 5^{\max\{0,1\}} \\ &= 2^2 \cdot 3 \cdot 5 \\ &= 60 \end{aligned}$$

These verify $60 = \operatorname{lcm}(12,15) = \frac{12\cdot 15}{\gcd(12,15)} = \frac{12\cdot 15}{3}$.

Chapter 7

Week 7: P-adic Valuations, (Ir)rationality, Counting Primes

7.1 P-adic Valuations

Definition 7.1.1: P-adic Valuations

For a natural number n,

$$v_p(n) = \text{largest power of prime } p \text{ dividing } n.$$

Example 7.1.2.

$$v_2(12) = v_2(2^2 \cdot 3) = 2$$

$$v_2(5) = 0$$

$$v_5(5^2) = 2$$

In general, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $v_{p_i}(n) = \alpha_i$.

Proposition 7.1.3: Generalization of Unique Factorization to Rational Numbers

We can generalize unique factorization to rational numbers by the following:
Give a rational number x, write it in reduced form and then write

$$x = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \in \mathbb{Z}.$$

Example 7.1.4.

$$\frac{15}{20} = \frac{3}{4} = \frac{3}{2^2} = 2^{-2} \cdot 3$$

$$\frac{15}{20} = \frac{3 \cdot 5}{2^2 \cdot 5} = (3 \cdot 5) \cdot 2^{-2} \cdot 5^{-1} = 2^{-2} \cdot 3$$

Definition 7.1.5

Given a prime number p, the p-adic valuation is the function

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

given by sending a rational number x to the power of p appearing in x.
Note: v_0 of any number is ∞.

Property 7.1.6: Properties of p-adic valuations

(a)

$$v_p(ab) = v_p(a) + v_p(b)$$

(b)

$$d \mid n \Leftrightarrow \text{ for every prime } p, v_p(d) \leq v_p(n)$$

(c)

$$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$$

Proof. Proof of (c).
If

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

and

$$b = p_1^{\beta_1} \cdots p_k^{\beta_k},$$

assume $\alpha_1 \leq \beta_1$, then

$$a + b = p_1^{\alpha_1}\left(p_2^{\alpha_2} \cdots p_k^{\alpha_k} + p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \cdots p_k^{\beta_k}\right)$$
$$\implies v_{p_1}(a+b) \geq \alpha_1 = \min\{\alpha_1, \beta_1\} = \min\{v_{p_1}(a), v_{p_1}(b)\}.$$

□

Example 7.1.7.

$$\begin{aligned} & v_2(12+10) \\ =& v_2(2^2 \cdot 3 + 2 \cdot 5) \\ =& v_2(2(2 \cdot 3 + 5)) \\ \geq& 1 = \min\{v_2(12), v_2(10).\} \end{aligned}$$

Example 7.1.8.

$$v_2(2+6) = v_2(8) = 3$$

$$v_2(2) = 1$$

$$v_2(6) = 1$$

$$\min\{v_2(2), v_2(6)\} = 1$$

Problem 23

Let $a, b, c, \in \mathbb{N}$. Then that

$$\text{lcm}(a,b,c)^2 \big| \text{lcm}(a,b) \cdot \text{lcm}(b,c) \cdot \text{lcm}(c,a) \text{ for any } a, b, c \in \mathbb{N}.$$

Proof. It suffices to show that for any prime p,

$$v_p(\text{lcm}(a,b,c)^2) \leq v_p\big(\text{lcm}(a,b) \cdot \text{lcm}(b,c) \cdot \text{lcm}(c,a)\big).$$

Note that

$$\begin{aligned} v_p(\text{lcm}(a,b,c)^2) &= v_p(\text{lcm}(a,b,c) \cdot \text{lcm}(a,b,c)) \\ &= 2v_p(\text{lcm}(a,b,c)) \\ &= 2\max\{v_p(a), v_p(b), v_p(c)\} \end{aligned}$$

On the other hand,

$$\begin{aligned} v_p\big(\text{lcm}(a,b) \cdot \text{lcm}(b,c) \cdot \text{lcm}(c,a)\big) &= v_p(\text{lcm}(a,b)) + v_p(\text{lcm}(b,c)) + v_p(\text{lcm}(c,a)) \\ &= \max\{v_p(a), v_p(b)\} + \max\{v_p(b), v_p(c)\} + \max\{v_p(c), v_p(a)\}. \end{aligned}$$

Lemma 7.1.8.1

If $x, y, z \geq 0$, then

$$2\max\{x,y,z\} \leq \max\{x,y\} + \max\{y,z\} + \max\{z,x\}$$

Proof. If you permute x, y, z, the inequality does not change.

Therefore, we may assume without loss of generality that

$$x \geq y \geq z.$$

Then the inequality becomes

$$\begin{aligned} 2x &\leq x + y + x \\ &= 2x + y \\ \Leftrightarrow y &\geq 0, \end{aligned}$$

which is true. □

Apply this lemma to

$$x = v_p(a), y = v_p(b), z = v_p(c)$$

completes the proof. □

Problem 24

If $a, b \in \mathbb{N}$ s.t.

$$a \mid b^2, b^3 \mid a^4, a^5 \mid b^6, \cdots$$

then

$$a = b.$$

Proof. We show that for any prime p,

$$v_p(a) = v_p(b).$$

Note that we have

$$a^{4n+1} \mid b^{4n+2} \text{ and } b^{4n+3} \mid a^{4n+4}$$

for every n.

$$\begin{aligned} v_p(a^{4n+1}) &\le v_p(b^{4n+2}) \\ (4n+1)v_p(a) &\le (4n+2)v_p(b) \\ \implies v_p(a) &\le \frac{4n+2}{4n+1} v_p(b) \qquad \text{for every } n \in \mathbb{N} \\ \implies v_p(a) &\le \left(\lim_{n\to\infty} \frac{4n+2}{4n+1} \right) v_p(b) = v_p(b). \end{aligned}$$

We can use the second divisibility to similarly obtain that $v_p(b) \le v_p(a)$, thus we have that for every prime p,

$$v_p(a) = v_p(b).$$

Therefore, $a = b$ is derived from unique prime factorization. □

7.2 (Ir)rationality

Definition 7.2.1: Rational Numbers

A *rational number* is any element of the set

$$\mathbb{Q} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

Theorem 7.2.2

$\sqrt{2}$ is irrational.

Proof. Assume to the contrary that $\sqrt{2}$ is rational, that is, there are $a, b \in \mathbb{Z}$ s.t.

$$\sqrt{2} = \frac{a}{b}.$$

This implies that

$$2b^2 = a^2$$

Then

$$\begin{aligned} v_2(2b^2) &= v_2(a^2) \\ v_2(2) + 2v_2(b) &= 2v_2(a) \\ 1 + 2v_2(b) &= 2v_2(a) \end{aligned}$$

The left hand side is odd while the right hand side is even.

Therefore, $\sqrt{2}$ is irrational. □

Problem 25

Show that $\sqrt{2} + \sqrt{3}$ is irrational.

Solution

Assume to the contrary that

$$\sqrt{2} + \sqrt{3} = \frac{a}{b}, \quad a, b \in \mathbb{Z}$$

Then

$$\begin{aligned} \sqrt{3} &= \frac{a}{b} - \sqrt{2} \\ 3 &= \frac{a^2}{b^2} - \frac{2a}{b}\sqrt{2} + 2 \\ \sqrt{2} &= \frac{b}{2a}(3 - 2 - \frac{a^2}{b^2}) \end{aligned}$$

Therefore, if $\sqrt{2} + \sqrt{3}$ is rational, then $\sqrt{2}$ would also be rational. This is a contradiction.

Definition 7.2.3: Recollection on $\log x$

$$\log x := \int_1^x \frac{1}{t}\,\mathrm{d}t, \quad x \geqslant 1$$

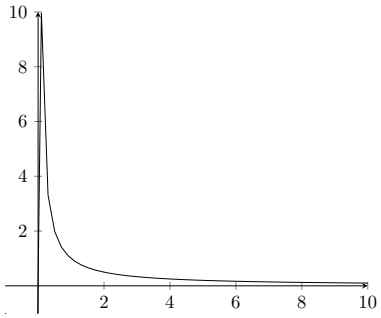

Figure 7.1: $f(t) = \frac{1}{t}$

Definition 7.2.4: Recollection on e

$e > 0$ is the real number s.t.

$$\log e = 1, \qquad \text{i.e.} \int_1^e \frac{1}{t}\,\mathrm{d}t = 1$$

It be shown that

$$\log(e^x) = x, \text{ for any } x \in \mathbb{R}$$

Let $y = e^x$. Take log of both sides to get

$$\log y = \log(e^x) = x.$$

Differentiating, we get

$$\frac{y'}{y} = 1 \implies y' = y.$$

Then we can write the Taylor expansion of $f(x) = e^x$ centered at 0.

$$\begin{aligned} e^x &= \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n \\ &= \sum_{n=0}^{\infty} \frac{x^n}{n!} \end{aligned}$$

For $x = 1$

$$\begin{aligned} e &= \sum_{n=0}^{\infty} \frac{1}{n!} \\ &= 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots \end{aligned}$$

You can estimate that $2 < e < 3$.

Theorem 7.2.5

e is irrational.

Proof. (Fourier).

Assume to the contrary that

$$e = \frac{a}{b}, \qquad a, b \in \mathbb{N}.$$

From $2 < e < 3$, we know that $e \notin \mathbb{Z}$ and so $b \geq 2$.

Consider the number

$$S = b!\left(e - \sum_{n=0}^{b} \frac{1}{n!}\right)$$

S is an integer as

$$\begin{aligned} S &= b!\left(\frac{a}{b} - \sum_{n=0}^{b} \frac{1}{n!}\right) \\ &= (b-1)!a - \sum_{n=0}^{b} \frac{b!}{n!} \end{aligned}$$

On the other hand, we could show that $0 < S < 1$.

Indeed, $S > 0$ because

$$\begin{aligned} S &= b!\left(\sum_{n=0}^{\infty}\frac{1}{n!} - \sum_{n=0}^{b}\frac{1}{n!}\right) \\ &= b!\sum_{n=b+1}^{\infty}\frac{1}{n!} > 0 \end{aligned}$$

We also have $S < 1$ since

$$\begin{aligned} S &= b!\sum_{n=b+1}^{\infty}\frac{1}{n!} \\ &= b!\left(\frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \cdots\right) \\ &= \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \cdots \\ &< \frac{1}{b+1} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + \cdots \\ &= \frac{1}{b+1}\left(\frac{1}{1-\frac{1}{b+1}}\right) \\ &= \frac{1}{b} \le \frac{1}{2} < 1 \end{aligned}$$

Since there are no integers S such that $0 < S < 1$, we reach a contradiction.

The conclusion follows the contradiction. □

Problem 26: Open Problem

Is the Euler constant $\gamma := \lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right)$ irrational? This problem has been open for a very long time. It is a constant that appears in various places in mathematics.

Theorem 7.2.6

π is irrational.

Proof. (Hermite, variation due to N. Bourbaki)

Assume to the contrary that

$$\pi = \frac{a}{b}, a, b \in \mathbb{N}.$$

Consider

$$T(n) := b^n \int_0^{\pi} \frac{x^n (\pi - x)^n}{n!} \sin x \, \mathrm{d}x$$

First, note that $x(\pi - x)$ is positive on $(0, \pi)$ and 0 only at the boundaries.

Similarly for $\sin x$.

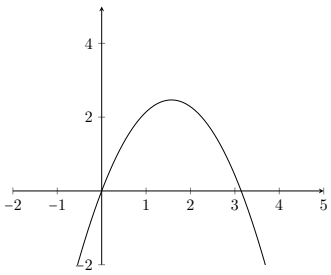

Figure 7.2: $y = x(\pi - x)$

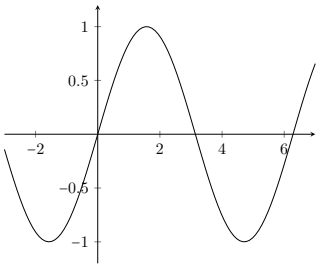

Figure 7.3: $y = \sin x$

Therefore, we always have

$$T(n) > 0.$$

Now let us show that for n sufficiently large,

$$T(n) < 1.$$

In order to show this, note that

$$x(\pi - x) \leq (\frac{\pi}{2})^2 \text{ for } 0 \leq x \leq \pi.$$

Therefore,

$$\begin{aligned} T(n) &= b^n \int_0^\pi \frac{x^n(\pi - x)^n}{n!} \sin x \, \mathrm{d}x \\ &\leq \frac{b^n}{n!} \int_0^\pi \left(\frac{\pi}{2}\right)^{2n} \mathrm{d}x \\ &= \frac{b^n \pi (\frac{\pi}{2})^{2n}}{n!} \\ &= \frac{\pi (\frac{b\pi^2}{4})^n}{n!} \overset{n\to\infty}{\to} 0 \end{aligned}$$

The terms are those of the convergent series expansion of $\pi e^{b\pi^2/4}$ from which the convergence to 0 follows. Choose such an n large enough to have

$$0 < T(n) < 1.$$

$$T(n) = \int_0^\pi \frac{b^n x^n (\pi - x)^n}{n!} \sin x \, \mathrm{d}x$$

In order to reach a contradiction, we show that $T(n)$ is an integer. For convenience, let

$$\begin{aligned} f(x) &:= \frac{b^n x^n (\pi - x)^n}{n!} \\ &= \frac{x^n (b\pi - bx)^n}{n!} \\ &= \frac{x^n (a - bx)^n}{n!} \end{aligned}$$

$f(x)$ is a polynomial of degree $2n$.
Apply IBP with $u = f(x)$, $\mathrm{d}v = \sin x \mathrm{d}x$ to obtain

$$T(n) = [-f(x)\cos x]_0^\pi + \int_0^\pi f'(x)\cos x dx.$$

The first term is an integer. In fact, it vanishes. By repeatedly applying integration by parts $2n+1$ times ($2n+1$ times because f is a polynomial of degree $2n$, and so after differentiating $2n+1$ time it becomes 0), we can then show that $T(n) \in \mathbb{Z}$. In the differentiations of f, terms containing $x(a-bx)$ as a factor vanish when evaluated at 0 or π. Otherwise, we have differentiated one of x^n or $(a-bx)^n$ at least n times, thus cancelling the $n!$ in the denominator. These terms will also be integers when evaluated at 0 or π.
Since we cannot have an integer $T(n)$ such that $0 < T(n) < 1$, π must be irrational. □

7.3 Counting Primes

Theorem 7.3.1: The Infinitude of Primes (Euclid)

There are infinitely many primes.

Proof. Assume to the contrary that there are only finitely many primes $p_1, \cdots, p_k$.
Consider

$$N := p_1, \cdots, p_k + 1.$$

$N > 1$, and so there is a prime number p such that $p \mid N$.
Then $p \notin \{p_1, \cdots, p_k\}$.
Indeed,

$$\begin{aligned} & p_i \mid p_1 \cdots p_k + 1 \\ \implies & p_i \mid 1, \end{aligned}$$

a contradiction.
Therefore, $p_1, \cdots, p_k$ cannot be all the prime numbers. This contradiction implies that we must have infinitely many primes. □

Corollary 7.3.2

Order the primes $p_1 = 2 < p_2 = 3 < p_3 < \cdots$. Then

$$p_{k+1} \le p_1 \cdots p_k + 1.$$

Proof. By the proof of the previous theorem, there is a prime p such that

$$p \mid p_1 \cdots p_k + 1,$$

and so $p \leq p_1 \cdots p_k + 1$. Since p cannot be one of the p_i, we must have $p \geq p_{k+1}$. The conclusion follows. □

Definition 7.3.3: Counting of Prime Numbers

Let

$$\pi(x) := \#\{p \text{ prime} \leq x\}.$$

This function counts the number of primes that are at most x.

Problem 27

How does $\pi(x)$ grow as $x \to +\infty$?

Theorem 7.3.4: Prime Number Theorem(PNT)

$$\pi(x) \sim \frac{x}{\log x} \qquad \text{as } x \to +\infty$$

i.e.

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

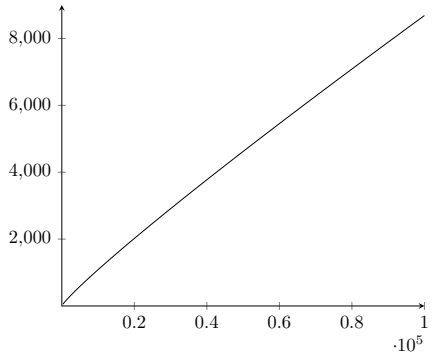

Figure 7.4: $\pi(x) \sim \frac{x}{\log x}$

The proof of this theorem is long and requires a serious understanding of complex analysis which is beyond the scope of this course. However, what can we say by elementary means?

Proposition 7.3.5

$$p_k < 2^{2^k}$$

Proof. We use strong induction on k.

$$p_1 = 2 < 2^{2^1}$$
$$p_2 = 3 < 2^{2^2}$$

Assume it is true for $1 \le k \le n$.
Using

$$p_{n+1} \le p_1 \cdots p_n + 1$$

and the inductive assumption, we have

$$\begin{aligned} p_{n+1} &< 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^n} + 1 \\ &= 2^{2+2^2+\cdots+2^n} + 1 \\ &= 2^{2^{n+1}-2} + 1 \\ &< 2^{2^{n+1}} \end{aligned}$$

The conclusion follows from strong induction. □

Theorem 7.3.6

$$\pi(x) \ge \log(\log x).$$

Proof. Given $x \ge 3$, choose $n \in \mathbb{N}$ s.t.

$$e^{e^{n-1}} \le x < e^{e^n}$$

From the previous proposition,

$$\pi(2^{2^n}) \ge n, \tag{0}$$

Then from $x \le e^{e^n}$ we obtain that

$$n \ge \log(\log x).$$

On the other hand,

$$\pi(x) \ge \pi(e^{e^{n-1}}), \tag{1}$$

and if $n > 3$, then

$$\begin{aligned} & e^{n-1} \ge 2^n \qquad (2) \\ \Leftrightarrow & \left(\frac{e}{2}\right)^n \ge e \qquad \text{for } n > 2 \end{aligned}$$

Therefore, from (0), (1) and (2), we obtain for $n > 2$

$$\begin{aligned} \pi(x) &\ge \pi(e^{2^n}) \\ &\ge \pi(2^{2^n}) \\ &\ge n \\ &\ge \log(\log x). \end{aligned}$$

If we have $n \leq 3$, then for $x \geq 5$,

$$\pi(x) \geqslant \pi(5) = 3 \geqslant n.$$

The above works for such x even if $n \leq 3$. We can manually check that the proposition also holds for $x < 5$.

The conclusion follows. □

Theorem 7.3.7

$$\sum_{p \text{ prime} \leq n} \frac{1}{p} > \log(\log n) - \frac{1}{2}$$

Corollary 7.3.8

$$\pi(n) \geq 2\log(\log n) - 1$$

Proof. Proof of corollary assuming previous theorem.

$$\sum_{p \text{ prime} \leq n} \frac{1}{2} > \sum_{p \text{ prime} \leq n} \frac{1}{p} \geq \log(\log n) - \frac{1}{2}.$$

And we have

$$\sum_{p \text{ prime} \leq n} \frac{1}{2} = \frac{\pi(n)}{2}$$

This implies

$$\pi(n) \geq 2\log(\log n) - 1.$$

□

Definition 7.3.9: ∏

The analogue of $\sum$ for summation is $\prod$ for products.

$$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n$$

Proof of theorem. Consider

$$\begin{aligned} &\prod_{p \text{ prime}, p \leq n} \left(\frac{1}{1 - \frac{1}{p}} \right) \\ &= \prod_{p \text{ prime}, p \leq n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) \\ &\geq \sum_{k=1}^{n} \frac{1}{k} \end{aligned}$$

Why? Every $1 \leq k \leq n$ has a prime factorization

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_e^{\alpha_e}$$

s.t. $p_i \leq k \leq n$ for all i.

Since $k \le n$, $p_i \le n$. Therefore,

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \cdots\right) \cdots \left(1 + \frac{1}{p_e} + \frac{1}{p_e^2} + \frac{1}{p_e^3} + \cdots\right), \tag{3}$$

is a factor of

$$\prod_{p \text{ prime},\, p \le n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right), \tag{4}$$

Note that $\frac{1}{k} = \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_e^{\alpha_e}}$ appears as a term in the expansion of (3), and therefore also in the expansion of (4). As a result,

$$\prod_{p \text{ prime},\, p \le n} \left(\frac{1}{1 - \frac{1}{p}}\right) \ge \sum_{k=1}^{n} \frac{1}{k}.$$

In the following, p is always implicitly a prime number.

We have this chain of (in)equalities:

$$\begin{aligned} -\sum_{p \le n} \log(1 - \frac{1}{p}) &= \log \prod_{p \le n} (1 - \frac{1}{p})^{-1} \\ &\ge \log(\sum_{k=1}^{n} \frac{1}{k}) \\ &\ge \log\left(\int_1^n \frac{1}{t}\, \mathrm{d}t\right) \\ &= \log(\log n) \end{aligned}$$

On the other hand, it can be shown that

$$\sum_{p \le n} \frac{1}{p} + \frac{1}{2} \ge -\sum_{p \le n} \log(1 - \frac{1}{p}), \tag{5}$$

Indeed, recall the Taylor expansion

$$-\log(1 - x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$$

Using this, we obtain

$$-\sum_{p \le n} \log(1 - \frac{1}{p}) = \sum_{p \le n} \sum_{k=1}^{\infty} \frac{1}{kp^k}$$

Note that

$$\sum_{p \le n} \sum_{k=1}^{\infty} \frac{1}{kp^k} = \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \sum_{k=2}^{\infty} \frac{1}{kp^k}$$

I will show that

$$\sum_{p \le n} \sum_{k=2}^{\infty} \frac{1}{kp^k} < \frac{1}{2}$$

We have the inequalities

$$\begin{aligned}
\sum_{p\le n}\sum_{k=2}^{\infty}\frac{1}{kp^k} &< \sum_{p\le n}\frac{1}{2p^2}\sum_{k=0}^{\infty}\frac{1}{p^k}\\
&= \frac{1}{2}\sum_{p\le n}\frac{1}{p^2}\left(\frac{1}{1-\frac{1}{p}}\right)\\
&= \frac{1}{2}\sum_{p\le n}\frac{1}{p(p-1)}\\
&< \frac{1}{2}\sum_{k=2}^{n}\frac{1}{k(k-1)}\\
&= \frac{1}{2}\sum_{k=2}^{n}\left(\frac{1}{k-1}-\frac{1}{k}\right)\\
&= \frac{1}{2}\left(1-\frac{1}{2}+\frac{1}{2}-\frac{1}{3}+\cdots-\frac{1}{n-1}+\frac{1}{n-1}-\frac{1}{n}\right)=\frac{1}{2}\left(1-\frac{1}{n}\right)\\
&< \frac{1}{2}.
\end{aligned}$$

This settles inequality (5).

Hence, we have

$$\sum_{p \text{ prime}\le n}\frac{1}{p}+\frac{1}{2} > \log(\log n)$$

as required (move the $\frac{1}{2}$ to the other side). □

Recall that for any $\epsilon > 0$,

$$\lim_{x\to\infty}\frac{\log x}{x^\epsilon} = 0$$

In particular, for x sufficiently large, depending on ϵ,

$$\frac{\log x}{x^\epsilon} < 1 \iff \log x < x^\epsilon$$

Take $\epsilon = \frac{1}{2}$. Then for x sufficiently large,

$$\frac{x}{\log x} \ge \frac{x}{x^{\frac{1}{2}}} = \sqrt{x}.$$

$$\begin{aligned}
\log(\log x) &\le \frac{1}{2}\log x\\
&\le \frac{1}{2}x^{\frac{1}{3}} \qquad \text{for } x \text{ sufficiently large}
\end{aligned}$$

Theorem 7.3.10

$$\sum_{p \text{ prime}\leqslant n}\frac{1}{p} > \log\left(\log\left(n\right)\right) - \frac{1}{2}$$

Corollary 7.3.11

$$\begin{aligned}\frac{\pi(n)}{2} &= \sum_{p \text{ prime} \leqslant n} \frac{1}{2} \\ &\geqslant \sum_{p \text{ prime} \leqslant n} \frac{1}{p} \\ &> \log(\log(n)) - \frac{1}{2} \\ &\implies \pi(n) > 2\log(\log(n)) - 1\end{aligned}$$

Problem 28

Therefore, $\log(\log(x))$ is much smaller than $\frac{x}{\log x}$. This implies that our lower bound $\pi(x) \geq \log\log(x)$ is not too good. Can we do better?

Solution

Let $x \in \mathbb{N}$, and let $m := \pi(x)$. Write $\{p \text{ prime} \leq x\} = \{p_1, \cdots, p_m\}$.
x natural number n such that $1 \leq n \leq x$ have all their prime divisors among $\{p_1, \cdots, p_m\}$.
Given $1 \leqslant n \leqslant x$, $n = r^2 \cdot s$, where $r \in \mathbb{N}$, s is a product of distinct prime numbers.

Example 7.3.12.

$$\begin{aligned}n &= 2^3 \cdot 3^4 \cdot 7 \\ &= (2^2 \cdot 3^4) \cdot 2 \cdot 7 \\ &= (2 \cdot 3^2)^2 \cdot 2 \cdot 7\end{aligned}$$

$$n = 11^3 = 11^2 \cdot 11$$

Since $1 \leq n \leq x$, s is a product of distinct primes chosen from

$$\{p_1, \cdots, p_m\}$$

So there are $2^m = 2^{\pi(x)}$ choices for s.
On the other hand,

$$\begin{aligned}r^2 \leq r^2 s = n \leq x \\ \implies r \leq \sqrt{x}.\end{aligned}$$

Putting all this together, we obtain that

$$x \leq \sqrt{x} \cdot 2^{\pi(x)}$$

Consequently,

$$\sqrt{x} \leq 2^{\pi(x)}$$

Taking log, we have

$$\frac{1}{2}\log x \le \pi(x)\log 2$$
$$\implies \pi(x) \ge \frac{\log x}{2\log 2}$$

This lower bound is better than the lower bound $\log(\log(x))$.

Problem 29

By the prime number theorem, for sufficiently large x,

$$0.99 < \frac{\pi(x)}{\frac{x}{\log x}} < 1.01$$
$$\implies \frac{0.99x}{\log x} < \pi(x) < \frac{1.01x}{\log x} \qquad \text{for } x \text{ sufficiently large.}$$

Can we prove that for say $x \ge 6$ that there is a constant $c > 0$ s.t. $\pi(x) \ge \frac{cx}{\log x}$?

Solution

Consider the function

$$\boxed{\psi(n) = \sum_{\substack{\alpha\in\mathbb{N} \\ p \text{ prime} \\ p^\alpha \le n}} \log p.}$$

e.g.

$$\psi(8) = \log 2 + \log 2 + \log 2 + \log 3 + \log 5 + \log 7$$
$$= \log(2^3 \cdot 3 \cdot 5 \cdot 7)$$

Exercise.

$$\psi(n) = \log \operatorname{lcm}(1, 2, 3, \cdots, n)$$

i.e.

$$e^{\psi(n)} = \operatorname{lcm}(1, 2, 3, \cdots, n).$$

Consider now the integral

$$\begin{aligned}
&\int_0^1 x^n(1-x)^n\,dx \\
\overset{BT}{=}&\int_0^1 x^n \sum_{k=0}^{n}\binom{n}{k}(-x)^k\,\mathrm{d}x \\
=&\sum_{k=0}^{n}(-1)^k\binom{n}{k}\int_0^1 x^{n+k}\,\mathrm{d}x \\
=&\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{x^{n+k+1}}{n+k+1}\Big|_0^1 \\
=&\sum_{k=0}^{n}(-1)^k\binom{n}{k}\cdot\frac{1}{n+k+1} \\
\Longrightarrow& e^{\psi(2n+1)}\int_0^1 x^n(1-x)^n\,\mathrm{d}x \\
=&\mathrm{lcm}(1,2,\cdots,2n+1)\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{1}{n+k+1} \\
=&\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{\mathrm{lcm}(1,2,\cdots,2n+1)}{n+k+1}
\end{aligned}$$

is an integer. It is also positive! Therefore, it is a natural number, and so

$$e^{\psi(2n+1)}\int_0^1 x^n(1-x)^n dx \geq 1.$$

On the other hand,

$$\begin{aligned}
&x(1-x)\leq\frac{1}{4} \\
\Longrightarrow\ &x^n(1-x)^n\leq(\frac{1}{4})^n
\end{aligned}$$

Therefore,

$$1\leq e^{\psi(2n+1)}\int_0^1 x^n(1-x)^n dx\leq\frac{e^{\psi(2n+1)}}{4^n}$$

and so,

$$\psi(2n+1)\geq 2n\log 2$$

Suppose $n\in\mathbb{N}$. Then choose $n\in\mathbb{N}$ s.t.

$$2n-1\leq x<2n+1$$

Then we have

$$\begin{aligned}
\psi(x)&\geq\psi(2n-1)\\
&\geq 2(n-1)\log 2\\
&=(2n-2)\log 2\\
&\geq(x-3)\log 2\\
&\geq\frac{x}{2}\log 2
\end{aligned}$$

where the last inequality follows from the fact that $x\geq 6$ implies that $x-3\geq\frac{x}{2}$.

If $p^\alpha \le x$, then $\alpha \log p \le \log x \implies \alpha \le \frac{\log x}{\log p}$. Therefore, for each prime $p \le x$, $\log p$ may appear at most $\frac{\log x}{\log p}$ times. Consequently, we have

$$\psi(x) = \sum_{\substack{\alpha \in \mathbb{N} \\ p \text{ prime} \\ p^\alpha \le x}} \log p \le \sum_{\substack{p \text{ prime} \\ p \le x}} \frac{\log x}{\log p} \cdot \log p = \pi(x) \log x.$$

From the inequality $\psi(x) \ge \frac{x}{2} \log 2$ above and $\psi(x) \le \pi(x) \log x$, we obtain

$$\pi(x) \ge \frac{x \log 2}{2 \log x}$$

for each $x \ge 6$. We have proved the following theorem.

Theorem 7.3.13

For $x \ge 6$, we have

$$\pi(x) \ge \frac{x \log 2}{2 \log x}$$

By the Prime Number Theorem,

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

In particular, for large enough x, we have

$$0.99 < \frac{\pi(x)}{\frac{x}{\log x}}$$
$$\implies \pi(x) > 0.99 \frac{x}{\log x} \quad \text{for } x \text{ large enough}$$

Remark. We know that

$$\prod_{i=1}^{n} a_i := a_1 a_2 \cdots a_n.$$

We have a obervation:

$$\prod_{p \text{ prime}, n < p \le 2n} \left| \binom{2n}{n} \right.$$

Notw that

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

Any prime p such that $n < p \leqslant 2n$ does not divide the denominator while it divides the numerator.
Using the general fact that

$$\gcd(a, b) = 1, \qquad a \mid c, \quad b \mid c$$
$$\implies ab \mid c$$

We obtain

$$\prod_{n < p \leqslant 2n} p \left| \binom{2n}{n} \right.$$

This implies that

$$\prod_{n<p\leqslant 2n} p \leqslant \binom{2n}{n} \tag{1}$$

This is using general fact that $a, b \in \mathbb{N}$, $a|b$, $b \neq 0 \implies a \leqslant b$.

Using

$$\binom{2n}{n} \leqslant \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{2n} = (1+1)^{2n}$$

We have

$$\binom{2n}{n} \leqslant 2^{2n} \tag{2}$$

Combininng (1) and (2), we obtian

$$\prod_{n<p\leqslant 2n} p \leqslant p^{2n}$$

Taking logs, we have

$$\sum_{n<p\leqslant 2n} \log p \leqslant \log 2^{2n} = 2n \log 2 \tag{3}$$

Let's introduce the function

$$\theta(x) := \sum_{p\leqslant x} \log p$$

(3) may be written as

$$\sum_{p\leqslant 2n} \log p - \sum_{p\leqslant n} \log p \leqslant 2n \log 2$$

$$\implies \theta(2n) - \theta(n) \leqslant 2n \log 2 \tag{4}$$

Lemma 7.3.13.1

For every $r \in \mathbb{N}$,

$$\theta(2^r) \leqslant 2^{r+1} \log 2$$

Proof. We induct on r. If $r = 1$, then

$$\theta(2) = \log 2$$

while the RHS is $2^2 \log 2$

If we have

$$\theta\left(2^k\right) \leqslant 2^{k+1} \log 2, \tag{5}$$

then from (4) with $n = 2^k$

$$\begin{aligned} \theta\left(2^{k+1}\right) &\leqslant \theta\left(2^k\right) + 2 \cdot 2^k \log 2 \qquad \text{Applying } (5) \\ &\leqslant 2^{k+1} \log 2 + 2^{k+1} \log 2 \\ &= 2^{(k+1)+1} \log 2 \end{aligned}$$

□

Given $x \geqslant 2$, choose $r \in \mathbb{N}$ such that

$$2^r \leqslant x < 2^{r+1}$$

From this, we obtian

$$\begin{aligned}\theta(x) &\leqslant \theta\left(2^{r+1}\right) \leqslant 2^{r+2}\log 2\\ &= 4(\log 2)\cdot 2^n\\ &\leqslant 4x\log 2\end{aligned}$$

In particular,

$$\sum_{\sqrt{x}<p\leqslant x}\log p \leqslant \sum_{p\leqslant x}\log p = \theta(x) \leqslant 4x\log 2 \tag{6}$$

The LHS of (6) is at least

$$\begin{aligned}\sum_{\sqrt{x}<p\leqslant x}\log\sqrt{x} &= \left(\log\sqrt{x}\right)\left(\pi(x)-\pi\left(\sqrt{x}\right)\right) \qquad (7)\\ &= \frac{1}{2}(\log x)\left(\pi(x)-\pi\left(\sqrt{x}\right)\right)\end{aligned}$$

(6) combined with (7) implies that

$$\begin{aligned}\frac{1}{2}(\log x)\left(\pi(x)-\pi\left(\sqrt{x}\right)\right) &\leqslant 4x\log 2\\ \pi(x)-\pi\left(\sqrt{x}\right) &\leqslant \frac{8x\log 2}{\log x}\\ \pi(x) &\leqslant \frac{8x\log 2}{\log x}+\pi\left(\sqrt{x}\right)\\ &\leqslant \frac{8x\log 2}{\log x}+\sqrt{x}\end{aligned}$$

When is

$$\sqrt{x} \leqslant \frac{x\log 2}{\log x}?$$

If this is to be true, we must have

$$\frac{\log x}{\log 2} \leqslant \sqrt{x}$$

i.e.

$$\sqrt{x}\log 2 - \log x \geqslant 0$$

Let

$$f(x) \coloneqq \sqrt{x}\log 2 - \log x$$

For whcih x is

$$f'(x) \geqslant 0?$$

$$f'(x) = \frac{\log 2}{2\sqrt{x}} - \frac{1}{x}$$

$$\begin{aligned}f'(x)\geqslant 0 &\Leftrightarrow \frac{\log 2}{2\sqrt{x}} \geqslant \frac{1}{x}\\ &\Leftrightarrow \sqrt{x} \geqslant \frac{2}{\log 2}\\ &\Leftrightarrow x \geqslant \left(\frac{2}{\log 2}\right)^2 \qquad \text{For } x \geqslant 8.32\ldots\end{aligned}$$

Therefore

$$\sqrt{x} \leqslant \frac{x \log 2}{\log x}, \qquad \text{for } x \geqslant 10$$

We conclude that

$$\pi(x) \leqslant \frac{8x \log 2}{\log x} + \sqrt{x} \leqslant \frac{9x \log 2}{\log x} \qquad \text{for } x \geqslant 10$$

Also, we can manually check that the final inequality on x between 2 and 10 for

$$\pi(x) \leqslant \frac{9x \log 2}{\log x}$$

Thus it is valid for $2 \leqslant x \leqslant 10$, and is valid for $x \geqslant 2$, .

Chapter 8

Week 8: Fermat's Little Theorem

8.1 Fermat's Little Theorem

Theorem 8.1.1: Fermat's Little Theorem

If p is a prime number and $n \in \mathbb{N}$ such that $p \nmid n$ (i.e. $\gcd(p, n) = 1$), then

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

i.e.

$$p \mid n^{p-1} - 1$$

Example 8.1.2. Let $p = 5$ and $n = 3$. Then

$$3^{5-1} \equiv 1 \pmod{5}$$

Problem 30: Some application

What are the last digit of 3^{1001}?

Solution

We want to find $3^{1001} \pmod{10}$.

$$\begin{aligned} 3^{1001} &\equiv 1^{1001} \pmod{2} \\ &= 1 \pmod{2} \end{aligned}$$

Also

$$\begin{aligned} 3^{1001} &= 3^{1000} \cdot 3 \\ &= \left(3^4\right)^{250} \cdot 3 \\ &\equiv 1^{250} \cdot 3 \pmod 5 \\ &\equiv 3 \pmod 5 \end{aligned}$$

Consider the remainders of 3^{1001} divided by 10 is one of the numbers from

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

$$r \equiv 3^{1001} \pmod{10}$$

$$\implies \begin{cases} r \equiv 3^{1001} \pmod 5 \\ r \equiv 3^{1001} \pmod 2 \end{cases}$$

The only possible number among $0, 1, \cdots, 9$ with

$$\begin{cases} r \equiv 3 \pmod 5 \\ r \equiv 1 \pmod 2 \end{cases}$$

is 3.

Problem 31

What is the last digit of 2^{1002}?

Solution

We want to find

$$2^{1002} \mod 10$$

By Fermat's Little Theorem,

$$2^4 \equiv 1 \pmod 5$$

Therefore,

$$2^{1002} \equiv \left(2^4\right)^{250} \cdot 2^2 \equiv 1^{250} \cdot 2^2 \equiv 4 \pmod 5$$

We also have that

$$2^{1002} \equiv 0 \pmod 2$$

You can easily check that then

$$2^{1002} \equiv 4 \pmod{10}$$

We want to be able to find, for e.g.,

$$2^{1002} \mod 51.$$

Lemma 8.1.2.1

Suppose $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Then

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

has a solution, if and only if

$$d := \gcd(a, n) \mid b \tag{1}$$

In fact, modulo n, there are exactly d solutions.

Proof. Finding x such that

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

is equivalent to solving the equation

$$\begin{aligned} & ax - b = ny, \qquad y \in \mathbb{Z} \\ \implies & ax - ny = b \end{aligned} \tag{2}$$

This has integer solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ if and only if

$$d := \gcd(a, n) \mid b$$

(Essentially, Bezout's Theorem).

Recall that if (x_0, y_0) is a solution of (2), then *all* integer solutions are of the form

$$\begin{cases} x = x_0 + \frac{n}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases}, t \in \mathbb{Z}$$

Let t range from 0 to $d - 1$.

We then have solutions

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \cdots, x_0 + \frac{(d-1)\,n}{d}$$

to (1).

Why are they distinct modulo n?

Assume to the contrary that

$$n \left| \left(x_0 + \frac{in}{d}\right) - \left(x_0 + \frac{jn}{d}\right), \right.$$

where $0 \leqslant i, j \leqslant d - 1$, and $i \neq j$.

Then

$$n \left| (i - j)\,\frac{n}{d}. \right.$$

However, note that

$$\left| (i - j)\,\frac{n}{d} \right| \leqslant \frac{d-1}{d} \cdot n < n$$

n cannot divide a natural number less than n. This contradiction implies that they must all be distinct modulo n.

If

$$x_0 + \frac{n}{d}t$$

is a solution, then we can use the division algorithm to write

$$t = qd + r, 0 \leqslant r \leqslant d - 1,$$

from which it follows that

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + \frac{nr}{d} + nq.$$

As $x_0 + \frac{nr}{d}$ is one of the d distiniguished elements above, and $x_0 + \frac{n}{d}t \equiv x_0 + \frac{nr}{d} \bmod n$, we have that modulo n all solutions are congruent to one of the d elements.

This concludes the proof. □

Corollary 8.1.3:

Suppose $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Then

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if

$$\gcd(a, n) = 1.$$

In fact, if $\gcd(a, n) = 1$, there is exactly one solution modulo n.

Chapter 9

Week 9: Chinese Remainder Theorem; Euler's Totient Function; Euler's Thoerem

9.1 Chinese Remainder Theorem

Theorem 9.1.1: Chinese Remainder Theorem

Suppose $n_1, n_2, \cdots, n_k$ are natural numbers such that for every $i \neq j$, $\gcd(n_i, n_j) = 1$. Also, let $a_1, \cdots, a_k \in \mathbb{Z}$. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution x modulo $n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

Proof. Why must a solution exist?

Let

$$\begin{aligned} N_1 &= \frac{n_1 \cdot \cdots \cdot n_k}{n_1} \\ &\vdots \\ N_k &= \frac{n_1 \cdot \cdots \cdot n_k}{n_k} \end{aligned}$$

Note that

$$\gcd(N_1, n_1) = \cdots = \gcd(N_k, n_k) = 1$$

By the corollary 8.1.3, there are

$$x_1, \ldots, x_k \in \mathbb{Z}$$

such that

$$N_1 x_1 \equiv 1 \pmod{n}, \cdots, N_k x_k \equiv 1 \pmod{n_k}$$

Then let

$$\boxed{x = a_1 N_1 x_1 + \cdots + a_k N_k x_k.}$$

Note that $n_1 | N_2, \cdots, N_k$. Therefore,

$$\begin{aligned} x &\equiv a_1 N_1 x_1 + \underbrace{0, \cdots, 0}_{k-1} \\ &\equiv a_1 \cdot 1 \\ &\equiv a_1 \bmod n_1. \end{aligned}$$

Similarly, x satisfies the other congruence conditions modulo $n_2, \cdots, n_k$.

To show uniqueness of the solution modulo $n_1 \cdot \cdots \cdot n_k$, suppose x' and x'' are two solutions. Then

$$\begin{aligned} x' \equiv a_1 \equiv x'' \pmod{n_1} \\ \vdots \\ x' \equiv a_k \equiv x'' \pmod{n_k} \end{aligned}$$

Therefore

$$\begin{aligned} n_1 \mid x' - x'' \\ \vdots \\ n_k \mid x' - x'' \end{aligned}$$

Since for every $i \neq j$, $\gcd(n_i, n_j) = 1$,

$$n_1 \cdot \cdots \cdot n_k \mid x' - x''$$

i.e

$$x' \equiv x'' \pmod{n_1 \cdot \cdots n_k}.$$

This means that x' and x'' are, in fact, the same modulo $n_1 \cdots n_k$, as required. □

Problem 32

Find all solutions to the system

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

Solution

Let $N_1 = 3 \cdot 5$, $N_2 = 2 \cdot 5$, $N_3 = 2 \cdot 3$.
Then we first find x_1 such that

$$N_1 x_1 \equiv 15x_1 \equiv 1 \pmod 2$$

Note that

$$15x_1 \equiv x_1 \pmod 2$$

So $x_1 = 1$ is a solution.
We also want x_2 such that

$$N_2 x_2 = 10x_2 \equiv 1 \pmod 3$$

Again,

$$1 \equiv 10x \equiv x_2 \pmod 3$$

and so we can take $x_2 = 1$.
Finally, we want x_3 such that

$$N_3 x_3 = 6x_3 \equiv 1 \pmod 5$$
$$\implies x_3 \equiv 1 \pmod 5.$$

Therefore, we can take $x_3 = 1$.
Then

$$\begin{aligned} x &= a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \\ &= 1 \cdot 3 \cdot 5 \cdot 1 + 2 \cdot 2 \cdot 5 \cdot 1 + 3 \cdot 2 \cdot 3 \cdot 1 \\ &= 15 + 20 + 18 \\ &= 53 \end{aligned}$$

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

Therefore, $x \in \mathbb{Z}$, such that

$$x \equiv 53 \equiv 23 \pmod{30}$$

are all the solutions.

Problem 33

There are 17 thieves who rob a bank. They try to divide the $ equally amongst themselves, but $3 remain. Along the way, one of them dies. When they return return to their hiding place, they try again, but $10 remain. One of them kills another out of greed. They try again, and they manage to divide the money equally this time. What is the minim amount of $ they stole?

Solution: Using CRT

Let d be the number of dollars stolen. Then

$$\begin{cases} d \equiv 3 \pmod{17} \\ d \equiv 10 \pmod{16} \\ d \equiv 0 \pmod{15} \end{cases}$$

In this case, we have

$$N_1 = 16 \cdot 15$$
$$N_2 = 17 \cdot 15$$
$$N_3 = 17 \cdot 16$$

We want to find $x_1, x_2, x_3 \in \mathbb{N}$ such that

$$16 \cdot 15x_1 = N_1x_1 \equiv 1 \pmod{17}$$
$$17 \cdot 15x_2 = N_2x_2 \equiv 1 \pmod{16}$$
$$17 \cdot 16x_3 = N_3x_3 \equiv 1 \pmod{15}$$

$$\begin{aligned} & 1 \equiv 16 \cdot 15x_1 \equiv (-1) \cdot (-2)\, x_1 \pmod{17} \\ \Leftrightarrow \quad & 2x \equiv 1 \pmod{17} \\ \Longrightarrow \quad & x_1 \equiv 18x_1 = 9 \cdot 2x_1 \equiv 9 \pmod{17} \end{aligned}$$

Take $x_1 = 9$.

$$\begin{aligned} & 1 \equiv 17 \cdot 15x_2 \equiv 1 \cdot (-1)\, x_2 \pmod{16} \\ \Leftrightarrow \quad & -x_2 \equiv 1 \pmod{16} \\ \Leftrightarrow \quad & x_2 \equiv -1 \equiv 15 \pmod{16} \end{aligned}$$

Take $x_2 = 15$.

$$\begin{aligned} 1 \equiv 17 \cdot 16x_3 \equiv 2 \cdot 1x_3 \equiv 2x_3 \pmod{15} & \\ 16x_3 \equiv 8 \pmod{15} & \quad \text{Multiply both side by } 8 \\ x_3 \equiv 8 \pmod{15} & \end{aligned}$$

Take $x_3 = 8$.

Then all solutions are congruent to

$$\begin{aligned} x &= a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 \\ &= 3 \cdot 16 \cdot 15 \cdot 9 + 10 \cdot 17 \cdot 15 \cdot 15 + \underbrace{0}_{=a_3} \cdots \pmod{17 \cdot 16 \cdot 15} \end{aligned}$$

Equivalently

$$d \equiv 3930 \pmod{4080}$$

The smallest such $d \in \mathbb{N}$ is 3930.

Solution: Not Using CRT

$$\begin{cases} d \equiv 3 \pmod{17} \\ d \equiv 10 \pmod{16} \\ d \equiv 0 \pmod{15} \end{cases}$$

From the last equation,

$$d = 15x \qquad \text{for some } x \in \mathbb{Z}$$

From the second equation,

$$\begin{aligned} 15x = d &\equiv 10 \pmod{16} \\ -x &\equiv 10 \pmod{16} \\ x &\equiv -10 \equiv 6 \pmod{16} \end{aligned}$$

This implies that

$$\begin{aligned} x &= 16y + 6 \qquad \text{with } y \in \mathbb{Z} \\ \implies d = 15x &= 15\,(16y + 6) \\ &= 15 \cdot 16y + 90 \end{aligned}$$

From the first equation,

$$15 \cdot 16y + 90 = d \equiv 3 \pmod{16}$$

Therefore,

$$\begin{aligned} 15 \cdot 16y &\equiv 3 - 90 \pmod{17} \\ \implies 2y &\equiv -87 \pmod{17} \\ &\equiv -2 \pmod{17} \\ \implies y &\equiv -1 \equiv 16 \pmod{17} \\ \implies y &= 17z + 16 \qquad \text{with } z \in \mathbb{Z} \end{aligned}$$

Then

$$\begin{aligned} d &= 15 \cdot 16y + 90 \\ &= 15 \cdot 16 \left(17z + 16\right) + 90 \\ &= 15 \cdot 16 \cdot 17z + \left(16^2 \cdot 15 + 90\right) \\ &= 4080z + 3930 \qquad z \in \mathbb{Z} \end{aligned}$$

The smallest such $d \in \mathbb{N}$ is 3980.

Recall the following proposition:

Proposition 9.1.2

If $a \in \mathbb{Z}$, $n \in \mathbb{Z}$, then

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $\gcd(a, n) = 1$.
In fact, if $\gcd(a, n) = 1$, it has a *unique* solution modulo n.

Moral of this proposition is that you can "**invert**" a modulo n (which is $a^{-1} \mod n$) if and only if $\gcd(a, n) = 1$.

Example 9.1.3.

$$5x \equiv 1 \pmod{3}$$

If $x \equiv 2 \pmod{3}$, then

$$5x \equiv 5 \cdot 2 = 10 \equiv 1 \pmod{3}$$

In inverse, when $\gcd(a, n) = 1$, we can speak of $x \equiv a^{-1} \mod n$.
In the above situation, $5^{-1} \equiv 2 \pmod{3}$.

Example 9.1.4.

$$7x \equiv 1 \pmod{9}$$

If $x \equiv 4 \pmod{9}$, then

$$7x \equiv 7 \cdot 4 = 28 \equiv 1 \pmod{9}$$

Therefore,

$$7^{-1} \equiv 4 \pmod{9}$$

If you want to use Euclidean algorithm, then solving $7x \equiv 1 \pmod{9}$ is more or less the same if as solving

$$\begin{aligned} 7x - 1 &= 9y \\ 7x - 9y &= 1 \end{aligned}$$

9.2 New proof of Fermat's Little Theorem

Consider a prime p and the numbers

$$1, 2, 3, \cdots, p-1$$

If you take $x \in \mathbb{Z}$ such that $p \nmid x$, then

$$x = pq + r \qquad 0 < r \leqslant p-1$$

In order to prove that if $p \nmid a$ then

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

what we can do is consider

$$a, 2a, 3a, \cdots, (p-1)\,a \mod p$$

Proposition 9.2.1

$a, 2a, 3a, \cdots, (p-1)\,a$ reduced modulo p is exactly the set $1, 2, 3, \cdots, p-1$ again.

Proof. It suffices to show that none of $a, 2a, 3a, \cdots, (p-1)\,a$ is divisible by p, and that they are distinct modulo p.
None of them is divisible by p because $p \nmid a$ and $p \nmid i$ for any $1 \leqslant i \leqslant p-1$.
They are also all distinct modulo p.
Otherwise, we can find $1 \leqslant i, j \leqslant p-1$ such that $i \neq j$ and

$$ai \equiv aj \pmod{p} \tag{1}$$

However, $\gcd(a, p) = 1$, so there exists $a^{-1} \pmod{p}$, and so

$$\begin{aligned} i &\equiv 1 \cdot i \\ &\equiv \left(a^{-1}a\right) \cdot i \\ &\equiv a^{-1}(a \cdot i) \\ &\equiv a^{-1}(a \cdot j) \\ &\equiv 1 \cdot j \\ &\equiv j \pmod{p} \end{aligned}$$

Since $\gcd(a, p) = 1$, there is an x such that

$$ax \equiv 1 \pmod{p} \qquad \text{Applying 8.1}$$

Multiplying both sides of (1) by x.
(1) is equivalent to

$$p \mid ai - aj = a(i-j)$$

$$p \nmid a \implies p \mid i - j$$

Since $i \equiv j \pmod{p}$ and $i \leqslant i, j \leqslant p-1$,

$$i = j$$

□

Now since $a, 2a, \cdots, (p-1)\,a$ are exactly $1, 2, 3, \cdots, p-1 \pmod p$.
We have

$$\begin{aligned} & a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)\,a) \\ \equiv & 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod p \end{aligned}$$

i.e.

$$\begin{aligned} & a^{p-1}\,(p-1)! \\ \equiv & (p-1)! \pmod p \end{aligned}$$

Since p is a prime, $p \nmid (p-1)!$. Therefore, $(p-1)!$ is invariable modulo p.
This implies

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

as required.

9.3 Euler Totient Function and Euer's Theorem

Definition 9.3.1

The Euler's *totient* function φ is given by

$$\varphi(n) := \#\{a \in \mathbb{N} \mid 1 \leqslant a \leqslant n \text{ such that } \gcd(a, n) = 1\}$$

Example 9.3.2.

$$\begin{aligned} \varphi(3) &= \#\{1 \leqslant a \leqslant 3 \text{ such that } \gcd(a, 3) = 1\} \\ &= \#\{1, 2\} \\ &= 2 \end{aligned}$$

More generally, if p is a prime number, then

$$\begin{aligned} \varphi(p) &= \#\{a \in \mathbb{N} \mid 1 \leqslant a \leqslant p \quad \gcd(a, p) = 1\} \\ &= \#\{1, 2, \cdots, p-1\} \\ &= p-1 \end{aligned}$$

Example 9.3.3.

$$\begin{aligned} \varphi(4) &= \#\{1 \leqslant a \leqslant 4 : \gcd(a, 4) = 1\} \\ &= \#\{1, 3\} \\ &= 2 \end{aligned}$$

Euler generalized Fermat's Little Theorem as follows:

Theorem 9.3.4: Euler's Theorem

If $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $\gcd(a,n) = 1$, then

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

If $n = p$ is a prime number then if $\gcd(a,p) = 1$,

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

But note that

$$\begin{aligned}\varphi(p) &= \#\{1 \leqslant a \leqslant p : \quad \gcd(a,p) = 1\} \\ &= \{1, 2, \cdots, p-1\} \\ &= p - 1\end{aligned}$$

Proof of Euler's Theorem. Consider

$$\left\{a_1, \cdots, a_{\varphi(n)}\right\} = \{a \in \mathbb{N} : 1 \leqslant a \leqslant n, \gcd(a,n) = 1\}$$

Then if $\gcd(a,n) = 1$, we have by a similar argument as in the proof of Fermat's Little Theorem that modulo n

$$aa_1, aa_2, \cdots, aa_{\varphi(n)}$$

is the same as

$$a_1, a_2, \cdots, a_{\varphi(n)}$$

$$\gcd\left(n, a_1, \cdots, a_{\varphi(n)}\right) = 1$$

and so

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

□

How to compute $\varphi(n)$ in general?

Proposition 9.3.5: Computation of $\varphi(n)$ in general

Consider

$$\frac{\varphi(n)}{n} = \mathbb{P}[1 \leqslant a \leqslant n \mid \gcd(a,n) = 1]$$

Let $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$ be the prime factor of n.

Then the probability that $1 \leqslant a \leqslant n$ and $p_i \nmid a$ is $1 - \frac{1}{p_i}$. This is true for each p_i.

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

Example 9.3.6.

$$\begin{aligned}\varphi\left(3^3\right) &= 3^3\left(1-\frac{1}{3}\right)\\ &= 3^2(3-1)\\ &= 18\end{aligned}$$

Example 9.3.7. If p is a prime, then

$$\begin{aligned}\varphi\left(p^k\right) &= p^k\left(1-\frac{1}{p}\right)\\ &= p^{k-1}(p-1)\end{aligned}$$

For instance,

$$\begin{aligned}\varphi\left(2^4\right) &= 2^3(2-1)\\ &= 8\\ \implies 3^8 &\equiv 1 \pmod{16}\end{aligned}$$

Proof of the proposition. An argument is probabilistic. Note that

$$\frac{\varphi(n)}{n} = \mathbb{P}\left[1 \leqslant a \leqslant n \mid \gcd(a,n) = 1\right]$$

A number is $1 \leqslant a \leqslant n$ is relatively prime to $n \Leftrightarrow p_1 \nmid a, p_2 \nmid a, \cdots, p_k \nmid a$.

The probability that $p_i \nmid a$ is 1 minus the probability that $p_i \mid a$, i.e.

$$\begin{aligned}1-\frac{\frac{n}{p_i}}{n} &= 1-\frac{1}{p_i}\\ \frac{\varphi(n)}{n} &= \left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ \varphi(n) &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\end{aligned}$$

as required. □

Problem 34

$$2^{1003} \pmod{45}?$$

Solution

$$\gcd(2, 45) = 1$$

By Euler's theorem,

$$2^{\varphi(45)} \equiv 1 \pmod{45}$$

$$\begin{aligned}\varphi(45) &= \varphi\left(3^2 \cdot 5\right) \\ &= 3^2 \cdot 5\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= 3^2 \cdot 5\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) \\ &= 3 \cdot 2 \cdot 4 \\ &= 24\end{aligned}$$

ans so

$$2^{24} \equiv 1 \pmod{45}$$

How can we write

$$\begin{aligned}1003 &= 24q + r, \qquad 0 \leqslant r \leqslant 23 \\ &= 24 \cdot 41 + 19\end{aligned}$$

So

$$\begin{aligned}2^{1003} &= 2^{24 \cdot 41 + 19} \\ &= \left(2^{24}\right)^{41} \cdot 2^{19} \pmod{45} \\ &\equiv 2^{19} \pmod{45}\end{aligned}$$

So now we have a sub problem, find

$$2^{19} \pmod{45}$$

Then let's find

$$2^{19} \pmod{3^2}$$

and

$$2^{19} \pmod{5}$$

By Euler's theorem

$$2^{\varphi(3^2)} \equiv 1 \pmod{3^2} \qquad \text{By Euler's theorem}$$

$$\begin{aligned}\varphi\left(3^2\right) &= 3^2\left(1 - \frac{1}{3}\right) \\ &= 9 \cdot \frac{2}{3} \\ &= 6\end{aligned}$$

Thus,

$$\begin{aligned} 2^{19} &= 2^{6\cdot 3+1} \\ &\equiv 2^1 \pmod 9 \\ &\equiv 2 \pmod 9 \end{aligned}$$

By FLT,

$$2^4 \equiv 1 \pmod 5$$

$19 = 4 \cdot 4 + 3$, and

$$\begin{aligned} 2^{19} &= 2^{4\cdot 4+3} \\ &= \left(2^4\right)^4 \cdot 2^3 \\ &\equiv 2^3 \\ &\equiv 3 \pmod 5 \end{aligned}$$

Now we have the system

$$\begin{cases} 2^{1003} \equiv 2^{19} \equiv 2 \pmod 9 \\ 2^{1003} \equiv 2^{19} \equiv 3 \pmod 5 \end{cases}$$

By the CRT, there is a unique solution modulo 45 to

$$\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 3 \pmod 5 \end{cases}$$

Let $N_1 = 5$, $N_2 = 9$.
Then we want to find x_1 and x_2 such that

$$5x_1 \equiv N_1 x_1 \equiv 1 \pmod 9 \tag{1}$$

$$9x_2 \equiv N_2 x_2 \equiv 1 \pmod 5 \tag{2}$$

Multiply (1) by 2 to get

$$x_1 \equiv 10x_1 \equiv 2 \pmod 9$$

Take $x_1 = 2$.
Note that $9 \equiv -1 \pmod 5$ and so (2) is equivalent to

$$\begin{aligned} -x_2 \equiv 9x_2 &\equiv 1 \pmod 5 \\ \implies x_2 &\equiv -1 \equiv 4 \pmod 5 \end{aligned}$$

Take $x_2 = 4$.

By the CRT,

$$\begin{aligned} x &= a_1 N_1 x_1 + a_2 N_2 x_2 \\ &= 2 \cdot 5 \cdot 2 + 3 \cdot 9 \cdot 4 \\ &= 20 + 108 \\ &= 128 \\ &\equiv 38 \pmod{45} \end{aligned}$$

is the unique solution modulo 45.

Chapter 10

Week 10: Wilson Theorem; Reformulation of Fermat's Little Theorem; P-adic Valuations of $n!$

10.1 Wilson Theorem

Theorem 10.1.1: Wilson Theorem

If p is a prime number, then

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

Example 10.1.2.

(1) If $p = 3$, then we have

$$(3-1)! = 2! = 2 \equiv -1 \pmod{3}$$

(2) If $p = 5$, then we have

$$(5-1)! = 4! = 24 \equiv -1 \pmod{5}$$

Recall the following:
If $\gcd(a, p) = 1$, then

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

has a unique solution modulo p.

Proof. Write

$$(p-1)! = 1 \cdot 2 \cdot \cdots (p-1)$$

Whenever $x \in \{1, 2, \cdots, p-1\}$ and $x^2 \not\equiv 1 \pmod{p}$, you can find a $y \in \{1, 2, \cdots, p-1\}$ such that $y \neq x$ and $xy \equiv 1 \pmod{p}$.
Which ones *cannot* be paired with *another* number?

Exactly those x such that

$$x^2 \equiv 1 \pmod{p}$$

Equivalently, when

$$p \mid x^2 - 1 = (x-1)(x+1)$$

i.e.

$$p \mid x-1 \text{ or } p \mid x+1$$

i.e.

$$x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \equiv p-1 \pmod{p}$$

Therefore,

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

□

Note that when $p = 2$, we have

$$(2-1)! = 1 \equiv -1 \pmod{2}$$

Theorem 10.1.3

Suppose p is an odd prime number. Then

$$x^2 \equiv -1 \pmod{p}$$

has a solution if and only if

$$p \equiv 1 \pmod{4}$$

Example 10.1.4.

(1) If $p = 5$, the theorem claims that

$$x^2 \equiv -1 \pmod{5}$$

$x = 2$ is a solution since

$$2^2 = 4 \equiv -1 \pmod{5}$$

(2) For $p = 13$, we have $x = 5$ as a solution to

$$x^2 \equiv -1 \pmod{13}$$

Indeed,

$$5^2 = 25 \equiv -1 \pmod{13}$$

One direction: If p is an *odd* prime number that

$$p \equiv 1 \pmod{4}$$

Then

$$x^2 \equiv -1 \pmod{p}$$

has a solution.

> *Proof of one direction.* By Wilson's theorem, we know that
>
> $$(p-1)! \equiv -1 \pmod{p}$$
>
> Note that
>
> $$(p-1)! = 1 \cdot 2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdot \cdots \cdot (p-1)$$
>
> And
>
> $$\begin{aligned} \frac{p+1}{2} &= p - \frac{p-1}{2} \equiv -\left(\frac{p-1}{2}\right) \pmod{p} \\ \frac{p+3}{2} &= p - \frac{p-3}{2} \equiv -\left(\frac{p-3}{2}\right) \pmod{p} \\ &\vdots \\ p-1 &= p-1 \equiv -1 \pmod{p} \end{aligned}$$
>
> Consequently,
>
> $$\begin{aligned} (p-1)! &\equiv 1 \cdot 2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right) \cdot (-1) \cdot (-2) \cdot \cdots \cdot \left(-\left(\frac{p-1}{2}\right)\right) \\ &\equiv (-1)^{\frac{p-1}{2}} \left[1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right]^2 \pmod{p} \end{aligned}$$
>
> Since $p \equiv 1 \pmod{4}$, $\frac{p-1}{2}$ is even!
> We have deduced that when $p \equiv 1 \pmod{4}$,
>
> $$(p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$
>
> By Wilson's theorem, this is $\equiv -1 \pmod{p}$. Thus, $x = \left[\left(\frac{p-1}{2}\right)!\right]^2$ is a solution.
> One direction of the theorem is proved. □

When $p = 5$, the proof boils down to the following computation:

$$\begin{aligned} -1 &\equiv (5-1)! \\ &= 1 \cdot 2 \cdot 3 \cdot 4 \pmod{5} \\ &= (1 \cdot 2)(5-2)(5-1) \\ &\equiv (1 \cdot 2)(-2)(-1) \\ &\equiv (-1)^2 (2!)^2 \\ &= 2^2 \pmod{5} \end{aligned}$$

The other direction: if p is an *odd* prime number and

$$x^2 \equiv -1 \pmod{p}$$

has a solution, then

$$p \equiv 1 \pmod 4$$

Definition 10.1.5: Order of a modulo

Suppose $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $\gcd(a,n) = 1$. Then the *order* of a modulo n, denoted by $\operatorname{ord}(n)$, is the smallest $k \in \mathbb{N}$ such that

$$a^k \equiv 1 \pmod n$$

Warning: Fermat's Little Theorem and Euler's theorem do *not necessarily* provide the smallest power k for which $a^k \equiv 1 \pmod n$.

Example 10.1.6. Take $n = p = 7$ and $a = 2$.
Fermat's Little Theorem say that $2^{7-1} \equiv 1 \pmod 7$.
However, we have

$$2^3 = 8 \equiv 1 \pmod 7$$

Theorem 10.1.7

Suppose $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $\gcd(a,n) = 1$. Then let $\operatorname{ord}_n(a)$ be the order of a modulo n. $\left(\operatorname{ord}_n(a) \in \mathbb{N}$ such that $a^{ord_n(a)} \equiv 1 \pmod n.\right)$
If $a^m \equiv 1 \pmod n$, then

$$\operatorname{ord}(a) \mid m$$

Proof. Assume to the contrary that

$$\operatorname{ord}_n(a) \nmid m.$$

This assumption, combined with the division algorithm, implies that

$$m = \operatorname{ord}_n(a)\, q + r, \qquad q, r \in \mathbb{N}, \quad 0 < r < \operatorname{ord}_a(n)$$

We then have

$$\begin{aligned} 1 &\equiv a^m \\ &\equiv a^{\operatorname{ord}_n(a)q+r} \pmod n \\ &= \left(a^{\operatorname{ord}_n(a)}\right)^q \cdot a^r \pmod n \\ &\equiv 1^q \cdot a^r \\ &= a^r \pmod n \end{aligned}$$

Since $0 < r < \operatorname{ord}_a(n)$, this contradicts the minimality of $\operatorname{ord}_n(a)$.
The collusion follows. □

Back to the proof of the other direction.

Proof of the other direction. To prove the other direction, note that

$$x^2 \equiv -1 \pmod{p} \implies x^4 \equiv 1 \pmod{p}.$$

Therefore,

$$\operatorname{ord}_p(x) \mid 4$$

Consequently, it is 1, 2, or 4. It is not 1 or 2 as

$$x^2 \equiv -1 \not\equiv 1 \pmod{p} \qquad p \text{ is odd}$$

The order of x is, therefore, 4.
On the other hand, note that

$$x^2 \equiv -1 \pmod{p} \implies \gcd(x, p) = 1$$

Indeed, if $p \mid x$, then from $p \mid x^2 + 1$, we would botian $p \mid 1$, a contradiction.
By Fermat's Little Theorem, we have

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

By the previous theorem, we must have

$$\operatorname{ord}_p(x) \mid p-1 \implies 4 \mid p-1,$$

that is, $p \equiv 1 \bmod 4$, as required. □

10.2 Reformulation of Fermat's Little Theorem

Suppose p is a prime number.
Consider the sets

$$\begin{aligned}
\overline{0} &= p\mathbb{Z} &&= \{\cdots, -2p, -p, 0, p, 2p, \cdots\} \\
\overline{1} &= 1 + p\mathbb{Z} &&= \{\cdots, 1-2p, 1-p, 1, 1+p, 1+2p, \cdots\} \\
&\vdots &&\vdots \\
\overline{p-1} &= (p-1) + p\mathbb{Z}
\end{aligned}$$

Recall the following:

$$\begin{cases} a \equiv b \pmod{p} \\ c \equiv d \pmod{p} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{p} \\ ac \equiv bd \pmod{p} \end{cases}$$

$$\begin{cases} \overline{a} \equiv \overline{b} \pmod{p} \\ \overline{c} \equiv \overline{d} \pmod{p} \end{cases} \implies \begin{cases} \overline{a+c} \equiv \overline{b+d} \pmod{p} \\ \overline{ac} \equiv \overline{bd} \pmod{p} \end{cases}$$

From $\overline{0}, \overline{1}, \cdots, \overline{p-1}$, let's keep only those elements $\overline{a}$ such that there is an $\overline{x}$ satisfying

$$\overline{ax} = \overline{a} \cdot \overline{x} = \overline{1} \Leftrightarrow ax \equiv 1 \pmod{p}$$

Note that for any $\overline{a} \in \left\{\overline{0}, \overline{1}, \cdots, \overline{p-1}\right\}$

$$\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$$

The "invertible" $\overline{a}$ are precisely these a such that $\gcd(a,p)=1$.

Therefore, every element of

$$\left\{\overline{1},\overline{2},\cdots,\overline{p-1}\right\}$$

has an inverse.

We also have that

$$\left(\overline{a}\cdot\overline{b}\right)\overline{c}=\overline{abc}=\overline{a}\cdot\left(\overline{b}\cdot\overline{c}\right)$$

(associativity).

Definition 10.2.1: Group

A **group** $(G,*)$ is a set G with a binary operation

$$*: G\times G\to G$$

satisfying

(1) there is a distinguished element $1\in G$ such that for every $g\in G$, $1*g=g*1=g$.

(2) $*$ is associative:

$$a*(b*c)=(a*b)*c$$

for every $a,b,c\in G$.

(3) for every $g\in G$ there is an $x\in G$ such that

$$g*x=x*g=1$$

Example 10.2.2.

$$(\mathbb{Z}/p\mathbb{Z})^{\times}=\left\{\overline{1},\overline{2},\cdots,\overline{p-1}\right\}$$

under multiplication (modulo p).

Theorem 10.2.3: Lagrange

If G is a finite group with $|G|$ elements, then for every $g\in G$,

$$g^{|G|}=1.$$

Example 10.2.4. In $(\mathbb{Z}/p\mathbb{Z})^{\times}$,

$$\overline{a}^{p-1}=\overline{1}$$

i.e. $a^{p-1}\equiv 1 \pmod{p}$ for every a such that $\gcd(a,p)=1$.

10.3 P-adic Valuations of $n!$

Problem 35

For prime p, what is $v_p(n!)$?

Note that

$$n! = 1 \cdot 2 \cdot \cdots \cdot n$$

How many of $1, 2, 3, \cdots, n$ are divisible by p but not p^2?

To solve this, we have the notation:

Definition 10.3.1: Floor Function

Given $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the largest integer $\leqslant x$.

Example 10.3.2.

$$\lfloor 2.75 \rfloor = 2$$
$$\lfloor -1.25 \rfloor = -2$$

Lemma 10.3.2.1

The number of integers $1 \leqslant a \leqslant n$ such $p \mid a$ is $\left\lfloor \frac{n}{p} \right\rfloor$.

Proof.

$$p \mid a \Leftrightarrow \exists k \in \mathbb{Z} : a = pk$$

We want this multiple to satisfy

$$1 \leqslant a = pk \leqslant n.$$

Equivalently, we want

$$1 \leqslant k \leqslant \left\lfloor \frac{n}{p} \right\rfloor$$

So we have $\left\lfloor \frac{n}{p} \right\rfloor$ choices for such k.
The conclusion follows. □

Example 10.3.3.

$$1, 2, 3, 4, 5, 6, 7, 8$$

How many are multiples of 3?

Answer:

$$\left\lfloor \frac{8}{3} \right\rfloor = 2$$

Among $1, 2, 3, \cdots, n$, exactly

$$\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor.$$

have p-adic valuation 1.

How many of $a \in \{1, 2, \cdots, n\}$ satisfy

$$v_p(a) = 2?$$

The answer is

$$\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor$$

Continuing in this way, the number of $a \in \{1, \cdots, n\}$ such that $v_p(a) = k$ is

$$\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$$

So

$$\begin{aligned} v_p(n!) &= \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) + 2\left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + 3\left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor\right) + \cdots \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \end{aligned}$$

Proposition 10.3.4

p prime,

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Example 10.3.5.

$$\begin{aligned} v_2(5!) &= \left\lfloor \frac{5}{2} \right\rfloor + \left\lfloor \frac{5}{2^2} \right\rfloor + \left\lfloor \frac{5}{2^3} \right\rfloor + \cdots \\ &= 2 + 1 \\ &= 3 \end{aligned}$$

In fact,

$$5! = 120 = 2 \cdot 3 \cdot 5$$

Another way of computing $v_p(n!)$ is as follows.

Write

$$n = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p + a_0,$$

where $0 \leqslant a_i \leqslant p - 1$. (base p expansion of n)

The proposition may then be reformulated as

$$\begin{aligned} v_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \\ &= \frac{n - s_p(n)}{p-1} \\ &= \frac{n - (a_0 + a_1 + \cdots + a_k)}{p-1}. \end{aligned}$$

By definition, $s_p(n) = a_0 + \cdots + a_k$ is the sum of the digits of n in its base p expansion.

Note that

$$\begin{aligned} \left\lfloor \frac{n}{p} \right\rfloor &= \left\lfloor \frac{a_k p^k + \cdots + a_1 p + a_0}{p} \right\rfloor \\ &= \left\lfloor a_k p^{k-1} + a_{k-1} p^{k-2} + \cdots + \frac{a_0}{p} \right\rfloor \\ &= a_k p^{k-1} + \cdots + a_2 + \underbrace{\left\lfloor \frac{a_0}{p} \right\rfloor}_{=0} \end{aligned}$$

$$\begin{aligned} \left\lfloor \frac{n}{p^2} \right\rfloor &= \left\lfloor \frac{a_k p^k + \cdots + a_1 p + a_0}{p^2} \right\rfloor \\ &= \left\lfloor a_k p^{k-2} + a_{k-1} p^{k-3} + \cdots + \frac{a_1 p + a_0}{p^2} \right\rfloor \\ &= a_k p^{k-2} + \cdots + a_2 + \underbrace{\left\lfloor \frac{a_1 p + a_0}{p^2} \right\rfloor}_{=0} \qquad \text{Since } a_1 p + a_0 \leqslant (p-1)\,p + (p-1) < p^2 \end{aligned}$$

Continuing in this fashion, we end with

$$\left\lfloor \frac{n}{p^k} \right\rfloor = a_k$$

Note that $\lfloor n p^{k+1} \rfloor = 0$ and also for higher powers of p. Summing these, we obtain using geometric sums of the form

$$1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p-1}$$

that

$$\begin{aligned} v_p(n!) &= a_k(1 + p + \cdots + p^{k-1}) + a_{k-1}(1 + p + \cdots + p^{k-2}) + \cdots + a_k \\ &= a_k\left(\frac{p^k - 1}{p-1}\right) + a_{k-1}\left(\frac{p^{k-1} - 1}{p-1}\right) + \cdots + a_1\left(\frac{p-1}{p-1}\right) \\ &= \frac{(a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p) - (a_k + a_{k-1} + \cdots + a_1)}{p-1} \\ &= \frac{(a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p + a_0) - (a_k + a_{k-1} + \cdots + a_1 + a_0)}{p-1} \\ &= \frac{n - s_p(n)}{p-1} \end{aligned}$$

Example 10.3.6.

$$\begin{aligned} v_2(5!) &= \frac{5 - s_2(5)}{2-1} \\ &= \frac{5-2}{2-1} \\ &= 3 \end{aligned}$$

Problem 36

$n \in \mathbb{N}$. Then

$$n! \Bigg| \underbrace{\prod_{k=0}^{n-1} \left(2^n - 2^k\right)}_{=(2^n-2^0)(2^n-2^1)\cdots(2^n-2^{n-1})}$$

(Generalized Factorials Bhargava (fields medal in 2014))

Proof. Recall that

$$a \mid b \Leftrightarrow \text{ for every prime } p, v_p(a) \leqslant v_p(b)$$

Therefore, it suffices to show that for every prime p,

$$v_p(n!)\, v_p\left(\prod_{k=0}^{n-1} \left(2^n - 2^k\right)\right)$$

For $p = 2$, we have

$$\begin{aligned} v_2\left(\prod_{k=0}^{n-1} \left(2^n - 2^k\right)\right) &\geqslant v_2\left(2^n - 2^{n-1}\right) \\ &= v_2\left(2^{n-1}\right) \\ &= n-1 \end{aligned}$$

On the other hand

$$\begin{aligned} v_2(n!) &= \frac{n - s_2(n)}{2-1} \\ &\leqslant \frac{n-1}{2-1} \\ &= n-1 \end{aligned}$$

Now suppose p is an odd prime.

Since p is odd, $\gcd(2, p) = 1$.

By Fermat's Little Theorem, (if $1 \leqslant k(p-1) \leqslant n$)

$$2^{p-1} \equiv 1 \pmod{p} \implies 2^{j(p-1)} \equiv 1 \pmod{p} \quad \text{for any } j \in \mathbb{N}$$

First note that

$$\begin{aligned} v_p(n!) &= \frac{n - s_p(n)}{p-1} \\ &\leqslant \left\lfloor \frac{n-1}{p-1} \right\rfloor \end{aligned}$$

On the other hand, $2^{j(p-1)} \equiv 1 \pmod{p}$

$$\implies p \mid 2^{j(p-1)} - 1$$

Also, for p odd,

$$\begin{aligned}
&v_p\left(\prod_{k=0}^{n-1}\left(2^n - 2^k\right)\right) \\
=&v_p\left(2^0 \cdot 2^1 \cdot \cdots \cdot \prod_{k=0}^{n-1}\left(2^{n-k} - 1\right)\right) \\
=&\underbrace{v_p\left(2^{\frac{n(n-1)}{2}}\right)}_{=0} + \prod_{k=1}^{n} v_p\left(2^k - 1\right)
\end{aligned}$$

At least how many of $2^k - 1$ are divisible by p?

By Fermat's Little Theorem, at least those $k = j(p-1)$ s.t. $1 \leqslant k = j\,(p-1) \leqslant n$.

The number of such j is at least $\left\lfloor \frac{n}{n-1} \right\rfloor$, so at least this many of $2^k - 1$ have p-adic valuation at least 1. Therefore, from the above computations and this fact, we have

$$\begin{aligned}
&v_p\left(\prod_{k=0}^{n-1}(2^n - 2^k)\right) \\
\geqslant &\sum_{k=1}^{n} v_p(2^k - 1) \\
\geqslant &\sum_{j:1\leq j(p-1)\leq n}^{n} v_p(2^k - 1) \\
\geqslant &\sum_{j\in\mathbb{N}:1\leqslant j(p-1)\leqslant n}^{n} 1 \\
\geqslant &\left\lfloor \frac{n}{p-1} \right\rfloor \\
\geqslant &\left\lfloor \frac{n-1}{p-1} \right\rfloor \\
\geqslant &v_p\left(n!\right)
\end{aligned}$$

We have deduced that for every odd prime p as well that $v_p(n!) \leqslant v_p\left(\prod_{k=0}^{n-1}(2^n - 2^k)\right)$. We also have it for $p = 2$ above. We conclude the solution to the problem. □

Remark. This divisibility result fits within the much larger framework of generalized factorials whose foundations were laid out in the undergraduate Harvard thesis of the recent fields medalist (equivalent of the Nobel prize in mathematics) Manjul Bhargava (professor at Princeton). Of course, his fields medal was not awarded for this work!

Chapter 11

Week 11: Group Theory

11.1 A Taste of Group Theorem

Recall the following definition

Definition 11.1.1: Group

A **group** $(G, *)$ is a set G equipped with a binary operation

$$* : G \times G \to G$$

such that

(1) There is an element $e \in G$ such that for every $x \in G$

$$x * e = e * x = x$$

(2) **Associativity**: for any three elements $x, y, z \in G$

$$(x * y) * z = x * (y * z)$$

(3) For any $x \in G$, there is a $y \in G$ such that

$$x * y = y * x = e$$

Example 11.1.2.

$$G = \mathbb{R}^\times := \mathbb{R}\backslash\{0\}$$

$$* = \text{multiplication}$$

$$e = 1 \quad (\text{for any } x \in \mathbb{R}\backslash\{0\},\ x \cdot 1 = 1 \cdot x = x)$$

It is associative, for any $x \in \mathbb{R}\backslash\{0\}$,

$$x \cdot \left(\frac{1}{x}\right) = \left(\frac{1}{x}\right) \cdot x = 1$$

Example 11.1.3.

$$G = \mathbb{Z}$$

$$* = +$$

$$e = 0 \quad \text{(for any } x \in \mathbb{Z},\ x + 0 = 0 + x = x\text{)}$$

It is clearly associative, and for any $x \in \mathbb{Z}$,

$$x + (-x) = (-x) + x = 0$$

Example 11.1.4.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\} \begin{cases} \overline{0} = \overline{n} \\ \overline{-1} = \overline{n-1} \end{cases}$$

$* = +$ modulo n.

For instance

$$\overline{1} + \overline{2} = \overline{1+2} = \overline{3}$$

$$\overline{n-1} + \overline{1} = \overline{n} = \overline{0}$$

$+$ modulo n is associative:

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

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

Furthermore, for any $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, we have additive inverses:

$$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}$$

$$\overline{-a} + \overline{a} = \overline{(-a) + a} = \overline{0}$$

Example 11.1.5.

$$(\mathbb{Z}/p\mathbb{Z})^{\times} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\} \qquad p \text{ prime}$$

$$* = \text{multiplication modulo } p$$

It is associative:

$$\overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right) = \overline{a} \cdot \left(\overline{bc}\right) = \overline{a \cdot (bc)} = \overline{abc}$$

If $\gcd(a,p) = \gcd(b,p) = 1$. Then

$$\gcd(ab,p) = 1$$

$$\overline{ab} = \overline{r} \in (\mathbb{Z}/p\mathbb{Z})^\times \quad , \quad ab = pq + r \qquad q,r \in \mathbb{Z}, 0 < r < p$$

Also note that for any $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$,

$$\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a} = \overline{a} \cdot \overline{1}$$

For any $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, there is a $\overline{b} \in (\mathbb{Z}/p\mathbb{Z})$ such that

$$\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1}$$

Why?

$$\overline{a} \cdot \overline{b} = \overline{1} \quad \Leftrightarrow \quad ab \equiv 1. \pmod{p}$$

This has a solution in b because $\gcd(a,p) = 1$. All of this means that $\left((\mathbb{Z}/p\mathbb{Z})^\times, \cdot\right)$ is a group.
Note that

$$|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$$

Example 11.1.6.

$$\{1 \leqslant a \leqslant n : \gcd(a,n) = 1\} = \left\{a_1, \cdots a_{\varphi(n)}\right\}$$

Then let

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{\overline{a_1}, \cdots \overline{a_{\varphi(n)}}\right\}$$

$$* = \text{ multiplication modulo } n$$

Note that we always have $\overline{1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ since $\gcd(1,n) = 1$. This is the unit $e = \overline{1}$.
$*$ is clearly associative as in the previous example where n is a prime.
By the exact same argument, every $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ has an inverse $\pmod{n}$.
Note that

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n).$$

Theorem 11.1.7: Lagrange

If G is a finite group, then for every $x \in G$ of size $|G|$

$$\underbrace{\underbrace{x}^{|G|}}_{\underbrace{x * x * \cdots * x}_{|G| \text{ times}}} = e$$

Example 11.1.8.

(1) In $(\mathbb{Z}/p\mathbb{Z})^\times$, Lagrange's theorem says that for any $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$,

$$\overline{a}^{\overline{p-1}} = \overline{1}$$

i.e. for any $a \in \mathbb{Z}$ such that $\gcd(a,p) = 1$

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

i.e. Fermat's Little Theorem.

(2) In $(\mathbb{Z}/n\mathbb{Z})^\times$, it says that for any $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\overline{a}^{\varphi(n)} = \overline{1},$$

i.e. Euler's theorem.

Example 11.1.9.

$$GL_2(\mathbb{R}) := \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R} \text{ such that } \det(A) = ad - bc \neq 0 \right\}$$

$* =$ matrix multiplication

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

Note that matrix $GL_2(\mathbb{R})$ is closed under matrix multiplication because $\det(AB) = \det(A)\det(B)$. This implies that if $\det(A) \neq 0 \neq \det(B)$, then $\det(AB) \neq 0$, and so $AB \in GL_2(\mathbb{R})$.
As you know from linear algebra, matrix multiplication is associative.
Since $\det(A) \neq 0$ for any $A \in GL_2(\mathbb{R})$, there is an inverse $A^{-1} \in GL_2(\mathbb{R})$.
$GL_2(\mathbb{R})$ is a group, but it is not true in general that

$$AB = BA$$

For example:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

11.2 Applications of Group Theory to Combinations

Problem 37

Consider an 8×8 board filled by checkers as follows

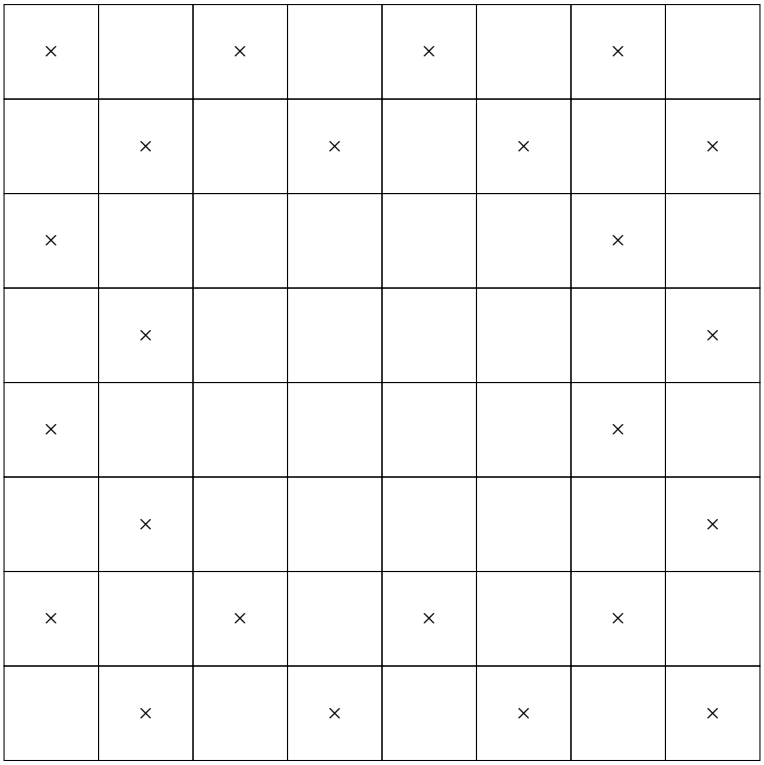

Figure 11.1: 8×8 board filled by checkers

The rule is that you can jump diagonally over a piece in an adjacent square into an empty square, and then remove the piece over which you have jumped.

Is it possible to find a sequence of moves and end up with exactly 1 piece on the board at the end?

Solution

Answer: It is impossible.

Consider the symmetries of a rectangle that is not a square. a represents flipping along the verticle line, b represents flipping along the horizontal line, c represents rotation by $180°$, while e represents doing nothing.

$$G := \{a, b, c, e\} \qquad \text{(Klein 4-group)}$$

is closed under composition of the moves. It is clear that e is the identity, it is associative. Also, each element is its own inverse.

This forms a group with the properties

$$a^2 = b^2 = c^2 = e$$

$$ab = c, \quad bc = a, \quad ca = b$$

that you can see geometrically. Note that $ab = ba$, $bc = cb$, $ca = ac$ (it is an abelian group, i.e. for any $x, y \in G$, $xy = yx$).

You can also identify G with

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (1,0), (0,1), (1,1)\}$$

where the composition law is component-wise addition modulo 2. You can view e as $(0,0)$, a as $(1,0)$, b as $(0,1)$, and c as $(1,1)$.

b		a		c		b	
	c		b		a		c
b		a		c		b	
	c		b		a		c
b		a		c		b	
	c		b		a		c
b		a		c		b	
	c		b		a		c

Figure 11.2: Coloring

Color the squares of the board using the elements of G as above.

The crucial observation is that we can define a quantity that does not change under the admissible moves. Let I be the product of all elements of G in the squares with a checker piece. When a move is made, for example with a piece on a square labeled as a over a piece labeled as b, the two pieces are removed and a piece is placed on a square with label c. Since $ab = c$, the quantity I does not change under such a move. Similarly, I does not change under the other jumps.

Initially, the product of the elements in squares with a checker piece is $I = b^4c^4a^2b^2c^2a^2b^4c^4 = e$. A board with exactly one checker on it has I equal to either a, b, or c. Since I does not change under our possible moves, we cannot get from our initial state to a state with exactly one checker piece.

Therefore, it is impossible to end up with exactly one checker piece.

Remark. The idea of invariants is pervasive in mathematics. It is another proof idea. Usually, when one wants to prove the impossibility of a phenomenon, or that two geometric objects are fundamentally different, one associates an object that does not change under the possible allowed moves. If the two geometric objects or states or...have different gadgets associated to them, then it is impossible to go from the first state to the final state using only the allowed sequence of operations.

An idea underlying invariants is that, typically, we are dealing with very complicated objects. Therefore, we try to extract something more tractable from the objects. Our brains do this all the time. If we want to prove that person X is not person Y, we may look at their eye colors or hair colors. If they have different eye colors, they are different people (assuming eye color does not change or that it is measured at the exact same time). However, different people often have the same eye colors, and so we look for different physical features. Sometimes, people are identical twins, making distinctions more difficult. Therefore, we look for psychological differences. If that fails, we look at gene expression and epigenetic information (identical twins have the same DNA, from my understanding). The analogue of this search for finer and finer invariants also happens in mathematics. Sometimes, this becomes extremely difficult, as the finer the invariants becomes, the more difficult it is to compute them. The construction of invariants is an art.

In mathematics, the invariants could be as simple as in the above problem, some other algebraic gadget, counts of solutions to equations (for example, coming from physics), or some other object. There is a wealth of mathematics dedicated to interesting invariants in various settings.

11.3 Special Functions in Group Theory

Problem 38

Suppose we have a 4×11 rectangle.

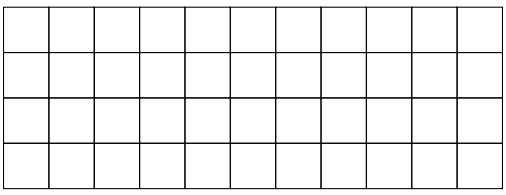

Figure 11.3: 4×11 rectangle

Is it possible to tile the 4×11 rectangle using the following L-shaped pieces?

Figure 11.4: L shape piece

Definition 11.3.1: $\tau(n)$

Suppose $n \in \mathbb{N}$. Then

$$\tau(n) := \sum_{d|n, d\in\mathbb{N}} 1 = \text{number of positive divisors of } n$$

Proposition 11.3.2: Computation of $\tau(n)$

Let $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$, p_i distinct primes, $\alpha_i \geqslant 1$ integers.

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$$

Example 11.3.3.

$$\tau(10) = \tau(2 \cdot 5)$$

I can have 0 or 1 number of 2's in the divisor.
I can have 0 or 1 number of 5's in the divisor.

$$\tau(10) = 2 \cdot 2 = 4$$

In fact, we have $1, 2, 5, 10$.

Proof of proposition. If $d \mid n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, $\beta_i \geq 0$, where

$$0 \leq \beta i \leq \alpha_i$$

There are $\alpha_i + 1$ probabilities for β_i.
Therefore,

$$\tau(n) = (\alpha_1 + 1)\cdots(\alpha_k + 1).$$

□

Example 11.3.4.

$$\begin{aligned}\tau(200) &= \tau(2^3 \cdot 5^2)\\ &= (3+1)(2+1)\\ &= 12.\end{aligned}$$

Note that

$$\tau(2^3)\tau(5^2) = (3+1)(2+1) = 12$$

Proposition 11.3.5

If $m, n \in \mathbb{N}$ s.t. $\gcd(m,n) = 1$, then

$$\tau(mn) = \tau(m)\tau(n)$$

Warning: Not true in general if m, n are not relatively prime.

Example 11.3.6.

$$\tau(2^3) = 4$$

$$\tau(2)\tau(2^2) = (1+1)(2+1) = 6 \neq 4$$

Proof of proposition. Write

$$\begin{aligned}m &= p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \geq 1\\ n &= q_1^{\beta_1} \cdots q_l^{\beta_l}, \beta_j \geq 1.\end{aligned}$$

Since $\gcd(m,n) = 1$,

$$\{p_1, \cdots, p_k\} \cap \{q_1, \cdots, q_l\} = \varnothing$$

Thus,

$$\begin{aligned}\tau(mn) &= \tau\left(p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdots q_e^{\beta_e}\right)\\ &= \underbrace{(\alpha_1+1)\cdots(\alpha_k+1)}_{\tau(m)}\underbrace{(\beta_1+1)\cdots(\beta_e+1)}_{\tau(n)}\\ &= \tau(m)\,\tau(n)\end{aligned}$$

□

Definition 11.3.7: $\sigma(n)$

For $n \in \mathbb{N}$,

$$\sigma(n) = \sum_{d \mid n, d \in \mathbb{N}} d$$

is the sum of the positive divisors of n.

Question: How to compute this (if we know the prime fact. of n?)

Proposition 11.3.8: Computation of $\sigma(n)$

If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \geq 1, p_i$ distinct primes, then

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right) \cdot \left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right)$$

Example 11.3.9.

$$\begin{aligned}
\sigma(20) &= \sigma(2^2 \cdot 5) \\
&= (1+2+2^2)(1+5) \\
&= \sum_{\substack{0\leq\alpha\leq 2 \\ 0\leq\beta\leq 1}} 2^\alpha 5^\beta \\
&= \left(\sum_{0\leq\alpha\leq 2} 2^\alpha\right)\left(\sum_{0\leq\beta\leq 1} 5^\beta\right) \\
&= (1+2+2^2)(1+5)
\end{aligned}$$

Proof of proposition.

$$\begin{aligned}
\sigma(n) &= (1+p_1+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2}) \cdots (1+p_k+\cdots+p_k^{\alpha_k}) \\
&= \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right) \cdot \left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right).
\end{aligned}$$

□

Example 11.3.10.

$$\begin{aligned}
\sigma(20) &= \sigma(2^2 \cdot 5^1) \\
&= \left(\frac{2^3-1}{2-1}\right)\left(\frac{5^2-1}{5-1}\right) \\
&= 7 \cdot \left(\frac{24}{4}\right) \\
&= 7 \cdot 6 \\
&= 42.
\end{aligned}$$

Lemma 11.3.10.1

For $r \neq 1$,

$$a + ar + ar^2 + \cdot s + ar^k = \frac{a(r^{k+1}-1)-1}{r-1}.$$

Proof. Let $S = a + ar + ar^2 + \cdots + ar^k$.

Then $rS = ar + ar^2 + \cdots ar^k + ar^{k+1}$.

$$rS - S = ar^{k+1} - a$$
$$(r-1)S = a(r^{k+1} - 1)$$
$$\xRightarrow{r\neq 1} \quad S = \frac{a(r^{k+1}-1}{r-1}.$$

□

Proposition 11.3.11

If $m, n \in \mathbb{N}$ s.t. $\gcd(m,n) = 1$, then

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Proof. Suppose

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$
$$n = q_1^{\beta_1} \cdots q_l^{\beta_l},$$

where $\alpha_i \geq 1, \beta_i \geq 1, p_i, q_j$ distinct primes.
Since $\gcd(m,n) = 1$,

$$\{p_1, \cdots, p_k\} \cap \{q_1, \cdots, q_l\} = \varnothing$$

By the previous prop,

$$\begin{aligned}\sigma(mn) &= \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}) \\ &= \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right)\left(\frac{q_1^{\beta_1+1}-1}{q_1-1}\right) \cdots \left(\frac{q_l^{\beta_k+1}-1}{q_l-1}\right) \\ &= \sigma(m)\sigma(n).\end{aligned}$$

□

Again, note that the proposition is false if m and n are not necessarily relatively prime. For example, $\sigma(2^2) = 7$ while $\sigma(2) = 3$. Therefore, $\sigma(2^2) \neq \sigma(2)\sigma(2)$.

Lemma 11.3.11.1: Gauss' Lemma

For $n \in \mathbb{N}$,

$$n = \sum_{d|n} \varphi(d).$$

Proof. Consider the numbers

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots, \frac{n}{n}$$

This consists of n number.
Reduce each of the number to lowest fractions. Then for each d, we have the $\varphi(d)$ numbers of the form $\frac{i}{d}$, where $\gcd(i,d) = 1$.

For each $d \mid n$, we have $\varphi(d)$ such numbers in

$$\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}.$$

Therefore,

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

□

Example 11.3.12. Let $n = 6$,

$$\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6}.$$

In reduced form, this collection of 6 numbers is

$$\frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}, \frac{1}{1}.$$

If $1 \mid 6$, we have $1 = \varphi(1)$ numbers.

If $2 \mid 6$, we have $1 = \varphi(2)$ numbers.

For $3 \mid 6$, we have the numbers $\frac{1}{3}$ and $\frac{2}{3}$, so we have $2 = \varphi(3)$ numbers.

For $6 \mid 6$, we have the numbers $\frac{1}{6}$ and $\frac{5}{6}$, so we have $2 = \varphi(6)$ numbers.

From this, we obtain

$$\begin{aligned} 6 &= 1 + 1 + 2 + 2 \\ &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) \\ &= \sum_{d|6} \varphi(d) \end{aligned}$$

Problem 39

Find a formula for

$$\sum_{\substack{1 \le a \le n \\ \gcd(a,n)=1}} a,$$

when $n > 1$.

Solution

The claim is that

$$\sum_{\substack{1 \le a \le n \\ \gcd(a,n)=1}} a = \frac{n\varphi(n)}{2}.$$

Proof. If $n = 2$, then

$$\sum_{\substack{1 \le a \le 2 \\ \gcd(a,2)=1}} a = 1 = \frac{2\varphi(2)}{2}$$

Order the numbers $1 \le a \le n$ s.t. $\gcd(a, n) = 1$ as follows:

$$a_1 < \cdots < a_{\varphi(n)}.$$

If $\gcd(a,n)=1$, then $\gcd(n-a,n)=1$.

If you take a_1, then $n-a_1=a_{\varphi(n)}$.

Similarly,

$$(*)\begin{cases} a_2+a_{\varphi(n)-1}=n \\ \quad\vdots \\ a_{\varphi(n)}+a_1=n. \end{cases}$$

You should note that we never have $a_i=n-a_i$ if $n\geq 3$, but this does not matter that much.
(Why? Otherwise, $2a_i=n \overset{\gcd(a_i,n)=1}{\Longrightarrow} a_i=1 \implies n=2$.)

Summing $(*)$, we obtain

$$2\sum_{\substack{1\leq a\leq n\\ \gcd(a,n)=1}} a=n\varphi(n)$$

$$\implies \sum_{\substack{1\leq a\leq n\\ \gcd(a,n)=1}} a=\frac{n\varphi(n)}{2}$$

□

Definition 11.3.13: Arithmetic Function

An *arithmetic* function is any function

$$f:\mathbb{N}\to\mathbb{R} \text{ (or } \mathbb{C}).$$

Definition 11.3.14: Multiplicative Function

A *multiplicative* function is an arithmetic function $f:\mathbb{N}\to\mathbb{C}$ s.t. for any $m,n\in\mathbb{N}$ satisfying $\gcd(m,n)=1$,

$$f(mn)=f(m)f(n).$$

Example 11.3.15: Examples of multiplicative function.

- φ Euler's totient function
- τ number of divisors
- σ sum of divisors
- id: $\mathbb{N}\to\mathbb{N}\subset\mathbb{C}$, $n\mapsto n$, $id(mn)=id(m)id(n)$

Note that

$$\tau(n)=\sum_{d|n}1$$

and

$$\sigma(n)=\sum_{d|n}d.$$

Proposition 11.3.16

If $f : \mathbb{N} \to \mathbb{C}$ is multiplicative, then

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

is also multiplicative.

Proof. Suppose $m, n \in \mathbb{N}$ s.t. $\gcd(m,n) = 1$. We want to show that

$$g(mn) = g(m)g(n).$$

By definition,

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

Since $\gcd(m,n) = 1, d = \gcd(m,d)\gcd(n,d)$.
From this, it can be seen that

$$\sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2). \tag{1}$$

Since $\gcd(m,n) = 1$, and $d_1 \mid m, d_2 \mid n$,

$$\gcd(d_1, d_2) = 1.$$

Since f is multiplicative,

$$f(d_1 d_2) = f(d_1)f(d_2).$$

Therefore from (1),

$$\begin{aligned} g(mn) &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2) \\ &= \sum_{d_1|m} \left(f(d_1) \sum_{d_2|n} f(d_2) \right) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) \\ &= g(m)g(n) \end{aligned}$$

□

Recall that

$$\begin{aligned} &\int_{\mathbb{R}} \int_{\mathbb{R}} f(x)g(y)\,dx\,dy \\ &= \int_{\mathbb{R}} g(y) \left(\int_{\mathbb{R}} f(x)\,dx \right) dy \\ &= \left(\int_{\mathbb{R}} g(y)\,dy \right) \left(\int_{\mathbb{R}} f(x)\,dx \right). \end{aligned}$$

Also

$$\begin{aligned}\sum_{j=1}^{N} a_j I &= a_1 I + a_2 I + \cdots + a_N I \\ &= (a_1 + \cdots + a_N) I \\ &= I \sum_{j=1}^{N} a_j .\end{aligned}$$

Suppose that we have an arithmetic function $f : \mathbb{N} \to \mathbb{C}$.

Then define the function

$$g(n) \coloneqq \sum_{d|n} f(d).$$

g has a lot information about f.

Question. Can we recover f knowing $g(n)$ for all $n \in \mathbb{N}$?

Answer. Yes! Möbius Inversion Formula.

Chapter 12

Week 12: Mobius Inversion

12.1 Mobius Inversion

Recall from last class that given an *arithmetic* function

$$f : \mathbb{N} \to \mathbb{C}$$

I defined $g : \mathbb{N} \to \mathbb{C}$ given by

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

Question: g contains a lot of information of f. Can e recover f given g?

$$g(1) = \sum_{d|1} f(d) = f(1)$$

$$g(2) = \sum_{d|2} f(d) = f(1) + f(2) = g(1) + f(2) \implies f(2) = g(2) - g(1)$$

$$g(3) = \sum_{d|3} f(d) = f(1) + f(3) = g(1) + f(3) \implies f(3) = g(3) - g(1)$$

$$g(4) = \sum_{d|4} f(d) = f(1) + f(2) + f(4) = g(1) + (g(2) - g(1)) + f(4) \implies f(4) = g(4) - g(2)$$

Can we recover $f(n)$ for every $n \in \mathbb{N}$ if we know $g(n)$ for every $n \in \mathbb{N}$?

Answer: Yes!

Definition 12.1.1: Mobius Function

The **Mobius Function** $\mu : \mathbb{N} \to \mathbb{R}$ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 \cdots p_r, \quad p_i \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Proposition 12.1.2

μ is a *multiplicative* function, i.e. if $m, n \in \mathbb{N}$ such that $\gcd(m.n) = 1$, then

$$\mu(mn) = \mu(m)\,\mu(n)$$

Proof. Clearly, if m or $n = 1$, then this follows from $\mu(1) = 1$.
If there is a prime p such that $p^2 \mid m$ or $p^2 \mid n$, then $\mu(m) = 0$ or $\mu(n) = 0$, respectively. Further more, $p^2 \mid mn \implies \mu(mn) = 0$ as well.
It remains to consider the case where

$$m = p_1 \cdots p_r, \quad n = q_1, \cdots q_e, \qquad p_i \text{ distinct}, q_j \text{ distinct}$$

Since $\gcd(m, n) = 1$,

$$\{p_1, \cdots, p_r\} \cap \{q_1, \cdots, q_e\} = \varnothing$$

Therefore,

$$\begin{aligned}
\mu(mn) = \mu(p_1 \cdots p_r q_q \cdots q_e) &= (-1)^{r+e} \\
&= (-1)^r (-1)^e \\
&= \mu(p_1 \cdots p_r)\,\mu(q_1 \cdots q_e) \\
&= \mu(m)\,\mu(n)
\end{aligned}$$

□

Proposition 12.1.3

For every $n \in \mathbb{N}$,

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$
$$:= e(n)$$

Proof. Recall from last class that since μ is multiplicative, so is

$$e(n) := \sum_{d \mid n} \mu(d)$$

Therefore, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $\alpha_i \geqslant 1$, p_i distinct primes, then

$$e(n) = e\left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) = e\left(p_1^{\alpha_1}\right) e\left(p_2^{\alpha_2}\right) \cdots e\left(p_k^{\alpha_k}\right)$$

If $n = 1$, then

$$e(1) = \sum_{d \mid 1} \mu(d) = \mu(1) = 1$$

It suffices to show that if $n = p^\alpha$, $\alpha \geqslant 1$, p prime, then

$$e(p^\alpha) = 0$$

Computing this, we have

$$\begin{aligned} e(p^\alpha) &= \sum_{d|p^\alpha} \mu(d) \\ &= \mu(1) + \mu(p) + \underbrace{\mu(p^2) + \cdots + \mu(p^\alpha)}_{=0} \\ &= 1 + (-1) \\ &= 0 \end{aligned}$$

□

Definition 12.1.4: $e(n)$ and $I(n)$

For $n \in \mathbb{N}$,

- $$e(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$
- $$I(n) = 1$$

Theorem 12.1.5: Mobius Inversion Formula

If $f : \mathbb{N} \to \mathbb{C}$ and for every $n \in \mathbb{N}$

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

then

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

The converse is also true: if f is given as above in terms of g, then g satisfies the above formula in terms of f.

Note that

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Indeed, d ranges over all divisors of n if and only if n/d ranges over all divisors of n (as d ranges over all divisors of n).

Definition 12.1.6: Dirichlet Convolution

Given, $f, g : \mathbb{N} \to \mathbb{C}$,

$$\begin{aligned}(f * g)(n) &:= \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) \\ &= \sum_{\substack{d_1 d_2 = n \\ d_1, d_2 \in \mathbb{N}}} f(d_1)\, g(d_2) \\ &= (g * f)(n)\end{aligned}$$

In the language of Dirichlet convolutions,

$$\sum_{d|n} f(d) = \sum_{d|n} f(d)\, I\left(\frac{n}{d}\right) = f * I$$

The statement that

$$\sum_{d|n} \mu(d) = e(n)$$

is equivalent to $\mu * I = e$.

Mobius Inversion is equivalent to $g = f * I \iff f = \mu * g$.

Proposition 12.1.7

Given $f, g : \mathbb{N} \to \mathbb{C}$,

(1)

$$f * g = g * f$$

(2)

$$(f * g) * h = f * (g * h) \qquad \text{Associativity}$$

(3)

$$f * e = f$$

Proof. (1) is clear.

For (2), note that

$$\begin{aligned}((f * g) * h)(n) &= \sum_{\substack{d_1 d_2 = n \\ d_1 d_2 \in \mathbb{N}}} (f * g)(d_1) h(d_2) \\ &= \sum_{\substack{uvd_2 = n \\ u, v, d_2 \in \mathbb{N}}} f(u) g(v) h(d_2)\end{aligned}$$

You can similarly show that

$$(f * (g * h))(n) = \sum_{\substack{u, v, d_2 \in \mathbb{N} \\ uvd_2 = n}} f(u) g(v) h(d_2)$$

For (3), note that

$$(f * e)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) e(d) = f(n)$$

□

Proof of Möbius Inversion using this formalism.

$$g(n) := \sum_{d|n} f(d) = (f * I)(n) \iff g = I * f$$

We also know that $\mu * I = e$. Therefore, using the previous proposition,

$$\mu * g = \mu * (I * f) = (\mu * I) * f = e * f = f,$$

that is,

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

Conversely, if this is satisfied, $f = \mu * g$, and so convolving with I on both sides gives

$$I * f = I * (\mu * g) = (I * \mu) * g = e * g = g,$$

that is,

$$g(n) := \sum_{d|n} f(d).$$

□

Remark. If $\mathcal{A}^* := \{f : \mathbb{N} \to \mathbb{C} \mid f(1) \neq 0\}$, Then $(\mathcal{A}^*, *)$ is a group.

Problem 40

Show that for every $n \in \mathbb{N}$,

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d).$$

Solution

By definition,

$$\tau(n) = \sum_{d|n} 1.$$

By Möbius inversion,

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d)$$

Problem 41

Show that

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Solution

Recall from Gauss' Lemma that

$$n = \sum_{d|n} \varphi(d).$$

Applying Möbius inversion, we obtain

$$\begin{aligned}\varphi(n) &= \sum_{d|n} \mu(d)\frac{n}{d} \\ &= n\sum_{d|n}\frac{\mu(d)}{d},\end{aligned}$$

as required.

One could use this to show that

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

if $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}, \alpha_i \geq 1, p_i$ distinct. This would give a non-probabilistic proof of this formula that we saw earlier in the course.

Problem 42

$$n = \sum_{d|n} \mu\left(\frac{n}{d}\right)\sigma(d).$$

$$\sigma(n) = \sum_{d|n} d.$$

Recall that Gauss' Lemma states that for every $n \in \mathbb{N}$,

$$id(n) = n = \sum_{d|n}\varphi(d).$$

By Möbius inversion,

$$\begin{aligned}\varphi(n) &= \sum_{d|n} idc\left(\frac{n}{d}\right)\mu(d) \\ &= \sum_{d|n}\frac{n}{d}\mu(d) \\ &= n\sum_{d|n}\frac{\mu(d)}{d}\end{aligned}$$

$\frac{\mu(d)}{d}$ is a multiplicative function, and so

$$\varphi(n) = n\sum_{d|n}\frac{\mu(d)}{d}$$

is a multiplicative function. This is a new proof that φ is multiplicative.

I want to give a new proof that if $n < p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, $\alpha_i \geq 1$, p_i distinct primes, then

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

The idea of the proof is the same idea I used to show that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}.$$

Since φ is multiplicative,

$$\varphi(p_1^{\alpha_1} \cdots \varphi_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$$

For each prime p and $\alpha \geq 1$ to

$$\begin{aligned} \varphi(p^\alpha) &= p^\alpha \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p} + \underbrace{\frac{\mu(p^2)}{p^2} + \cdots + \frac{\mu(p^\alpha)}{p^\alpha}}_{=0 \text{ by def. of } \mu} \right) \\ &= p^\alpha \left(1 - \frac{1}{p}\right) \end{aligned}$$

Therefore,

$$\begin{aligned} \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) \\ &= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Problem 43

Suppose $f : \mathbb{N} \to \mathbb{C}$ (or $\mathbb{R}$) s.t. for every $n \in \mathbb{N}$, $f(n) \neq 0$ and is multiplicative. Then find a formula for

$$g(n) := \sum_{d|n} \frac{\mu(d)}{f(d)}$$

Solution

Since φ is multiplicative,

$$\varphi(p_1^{\alpha_1} \cdots \varphi_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$$

For each prime p and $\alpha \geq 1$ to

$$\begin{aligned} \varphi(p^\alpha) &= p^\alpha \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p} + \underbrace{\frac{\mu(p^2)}{p^2} + \cdots + \frac{\mu(p^\alpha)}{p^\alpha}}_{=0 \text{ by def. of } \mu} \right) \\ &= p^\alpha \left(1 - \frac{1}{p}\right) \end{aligned}$$

Therefore,

$$\begin{aligned}\varphi(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) &= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)\\ &= p_1^{\alpha_1}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

Problem. Suppose $f:\mathbb{N}\to\mathbb{C}$ (or $\mathbb{R}$) s.t. for every $n\in\mathbb{N}$, $f(n)\neq 0$ and is multiplicative. Then find a formula for

$$g(n) := \sum_{d|n}\frac{\mu(d)}{f(d)}$$

Since μ, f are multiplicative, so is $\frac{\mu}{f}$ (note that f never vanishes).
If $n=1$, then we have

$$g(1) = \sum_{d|1}\frac{\mu(d)}{f(d)} = \frac{\mu(1)}{f(1)} = \frac{1}{f(1)}.$$

For $n\geq 2$, write

$$n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}, \alpha_i\geq 1, p_i \textit{ distinct primes}.$$

Then

$$\begin{aligned}g(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) &= g(p_1^{\alpha_1})\cdots g(p_k^{\alpha_k})\\ &= \left(\sum_{d|p_1^{\alpha_1}}\frac{\mu(d)}{f(d)}\right)\cdots\left(\sum_{d|p_k^{\alpha_k}}\frac{\mu(d)}{f(d)}\right)\\ &= \left(\frac{\mu(1)}{f(1)}+\frac{\mu(p_1)}{f(p_1)}+\underbrace{\frac{\mu(p_1^2)}{f(p_1^2)}+\cdots+\frac{\mu(p_1^{\alpha_1})}{f(p_1^{\alpha_1})}}_{=0}\right)\\ &\quad\cdots\left(\frac{\mu(1)}{f(1)}+\frac{\mu(p_k)}{f(p_k)}+\underbrace{\frac{\mu(p_k^2)}{f(p_k^2)}+\cdots+\frac{\mu(p_k^{\alpha_k})}{f(p_k^{\alpha_k})}}_{=0}\right)\\ &= \left(\frac{1}{f(1)}-\frac{1}{f(p_1)}\right)\cdots\left(\frac{1}{f(1)}-\frac{1}{f(p_k)}\right)\end{aligned}$$

Note that if you expand

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= n\left(1-\left(\frac{1}{p_1}+\cdots+\frac{1}{p_k}\right)+\sum_{i_1\neq i_2}\frac{1}{p_{i_1}p_{i_2}}-\sum_{i_1,i_2,i_3\text{ distinct}}\frac{1}{p_{i_1}p_{i_2}p_{i_3}}\right)\end{aligned}$$

This could be interpreted using the principle of inclusion-exclusion. In fact, Mobius inversion may be put within a general framework that specialize to both Mobius inversion and the principle of inclusion-exclusion.

12.2 Multiplicative version of Möbius inversion

Theorem 12.2.1

Suppose $f : \mathbb{N} \to \mathbb{N}$ and let

$$g(n) = \prod_{d|n} f(d)$$

Then

$$f(n) = \prod_{d|n} g(d)^{\mu(\frac{n}{d})}$$

Proof. Take logarithms to reduce to

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

$$\begin{aligned} \xrightarrow{\text{Möbius inversion}} \log f(n) &= \sum_{d|n} \mu(\frac{n}{d}) \log g(d) \\ &= \sum_{d|n} \log g(d)^{\mu(\frac{n}{d})} \\ &= \log \prod_{d|n} g(d)^{\mu(\frac{n}{d})} \\ \xrightarrow{exp.} f(n) &= \prod_{d|n} g(d)^{\mu(\frac{n}{d})}. \end{aligned}$$

□

Problem 44

Suppose $a_1, a_2, \cdots$ is a sequence of natural numbers s.t.

$$\gcd(a_m, a_n) = a_{\gcd(m,n)}.$$

Show that there is a unique seq of natural number $b_1, b_2, \cdots$ s.t. for every $n \in \mathbb{N}$,

$$a_n = \prod_{d|n} b_d.$$

Chapter 13

Week 13: Quadratic reciprocity

13.1 Quadratic reciprocity

Recall the following theorem.

Theorem 13.1.1

Suppose p is an *odd* prime. Then $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$

Question. Suppose $a \in \mathbb{Z}$ and p is a prime. When does

$$x^2 \equiv a \pmod{p}$$

have a solution?

Definition 13.1.2: Legendre Symbol

Suppose $a \in \mathbb{Z}$, p prime (almost always odd).

Then

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ has } \textit{no} \text{ solutions} \\ 1 & \text{otherwise} \end{cases}$$

Definition 13.1.3: Quadratic Residue

$a \in \mathbb{Z}$ is a **quadratic residue** mod p if

$$x^2 \equiv a \pmod{p}$$

has a solution.

Otherwise, a is a **quadratic non-residue.**

Theorem 13.1.4: Reformulation of previous theorem

If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Indeed, if $p \equiv 1 \pmod 4$, then

$$4 \mid p-1 \implies 2 \mid \frac{p-1}{2} \implies (-1)^{\frac{p-1}{2}} = 1.$$

If $p \equiv 3 \pmod 4$ then $p-1 = 4k+2$ for some $k \in \mathbb{Z} \implies \frac{p-1}{2} = 2k+1$ is odd $\implies (-1)^{\frac{p-1}{2}} = -1$.

Theorem 13.1.5

For p odd prime,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

If $p \mid a$, then by def,

$$\left(\frac{a}{p}\right) = 0.$$

Also

$$p \mid a^{\frac{p-1}{2}}.$$

If $p \nmid a$, then by Fermat's Little Theorem,

$$\begin{aligned} & a^{p-1} \equiv 1 \pmod p \\ \implies & p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \\ \implies & p \mid (a^{\frac{p-1}{2}} - 1) \text{ or } p \mid (a^{\frac{p-1}{2}} + 1) \\ \implies & a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p \end{aligned}$$

To prove the above theorem, it suffices to show that if $p \nmid a$, then

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p \iff \textit{a is a quadratic residue.}$$

Proof of ($\Leftarrow$). If $x^2 \equiv a \pmod p$ has a solution, then

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \overset{FLT}{\equiv} 1 \pmod p.$$

Note that since $p \nmid a$ and $x^2 \equiv a \bmod p$, $p \nmid x$ as well and so FLT may be applied. □

Remark on previous material:

(1) Möbius Inversion formula is a number theoretic version of the fundamental theorem of calculus.

(2) Möbius inversion was generalized beyond number theory in the 60's, Gian Carlo Rota wrote some papers on Möbius inversion on posets.

(3) Recall the prime number theorem:

$$\pi(x) \sim \frac{x}{\log x}.$$

It is known that this is *equivalent*

$$\lim_{N\to\infty} \frac{\sum_{n\le N} \mu(n)}{N} = 0.$$

(4) Riemann hypothesis (one of the most important conjectures yet to be proved) is equivalent to showing that for any $\epsilon > 0$,

$$\lim_{N\to\infty} \frac{1}{N^{\frac{1}{2}+\epsilon}} \sum_{n\le N} \mu(n)$$

is bounded.

Theorem 13.1.6: Euler's criterion

If p is an *odd* prime, then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Proposition 13.1.7

If p *odd* prime and $p \nmid a$, then

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow x^2 \equiv a \pmod{p}$$

has a solution.

Proof. I showed that if $x^2 \equiv a \pmod{p}$ has a solution, then

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

Suppose now that $x^2 \equiv a \pmod{p}$ has no solution. We must show that

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

Consider the set

$$S := \{1, 2, 3, \cdots, p-1\}$$

For each $i \in S$, find $j \in S$ such that

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

j must be unique. If you choose j, then by uniqueness again, it will be paired with i.
Since a is not a square $\bmod p$, $j \neq i$. This fives us a pairing between the numbers

$$1, 2, \cdots, p-1$$

We have a total of $\frac{p-1}{2}$ pairs such that for every pair $\{i, j\}$, $ij \equiv a \pmod{p}$.
Therefore,

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$$

By Wilson's Theorem, the left hand side is $\equiv -1 \pmod{p}$. □

Theorem 13.1.8

$a, b \in \mathbb{Z}$, p odd prime

(1)
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(2)
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

(3) The product of a nonzero (mod p) quadratic residue and a quadratic non-residue is a quadratic non-residue.

(4) The product of two quadratic non-residues is a quadratic residue.

Proof of (1). By Euler's criterion,

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} \\ &= a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p} \\ &\implies p \mid \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\end{aligned}$$

Since

$$-1 \leqslant \left(\frac{ab}{p}\right), \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \leqslant 1$$

$$\implies \left|\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right| \leqslant 2$$

p odd $\implies p \geqslant 3$

If

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \neq 0,$$

then

$$3 \leq p \leq \left|\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right| \leq 2$$

Contradiction. Therefore,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Example 13.1.9. Consider $\mod 5$.

The possible squares $\mod 5$ are

$$\left.\begin{aligned} 0^2 &\equiv 0 \pmod 5 \\ 1^2 &\equiv 1 \pmod 5 \\ 2^2 &\equiv 4 \pmod 5 \\ 3^2 &\equiv 4 \pmod 5 \\ 4^2 &\equiv 1 \pmod 5 \end{aligned}\right\} \implies \begin{array}{c} 0,1,4 \text{ are the only quadratic residues mod } 5; \\ 2,3 \text{ are the quadratic non-residues} \end{array}$$

$$\left(\frac{2\cdot 3}{5}\right) = 1.$$

$$\left(\frac{2}{3}\right), \left(\frac{3}{5}\right) = -1 \implies \left(\frac{2}{5}\right)\left(\frac{3}{5}\right) = 1.$$

$$\left(\frac{4\cdot 2}{5}\right) = \left(\frac{8}{5}\right) = \left(\frac{3}{5}\right) = -1$$

$$\left(\frac{4}{5}\right) = 1, \left(\frac{2}{5}\right) = -1.$$

Proposition 13.1.10

If $a \equiv b \pmod p$, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Example 13.1.11.

$$\left(\frac{2}{5}\right) = -1$$

and

$$2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1 \pmod 5$$

So

$$\left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} \pmod 5$$

as predicted by Euler's criterion.

Example 13.1.12.

$$\left(\frac{1002}{5}\right) = \left(\frac{2}{5}\right) = -1$$

Example 13.1.13.

$$\left(\frac{1004}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1$$

Example 13.1.14.

$$\left(\frac{57}{7}\right) = \left(\frac{1}{7}\right) = 1$$

Example 13.1.15.

$$\left(\frac{55}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{\frac{7-1}{2}} = -1$$

13.2 Quadratic Reciprocity of Gauss

If you have two odd prime p, q, quadratic reciprocity will tell us that studying

$$x^2 \equiv p \pmod{p}$$

is intimately related to studying $x^2 \equiv q \pmod{p}$

Theorem 13.2.1

If p, q are odd primes, then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$\Leftrightarrow \text{for } p, q \text{ odd primes, } \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

Example 13.2.2.

$$\begin{aligned}\left(\frac{3}{17}\right) &= (-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)\\ &= \left(\frac{17}{3}\right)\\ &= \left(\frac{2}{3}\right)\\ &= \left(\frac{-1}{3}\right)\\ &= (-1)^{\frac{3-1}{2}}\\ &= -1\end{aligned}$$

Thus 3 is not a quadratic residue of 17.

Example 13.2.3.

$$\begin{aligned}\left(\frac{2}{19}\right) &= \left(\frac{3}{19}\right)\left(\frac{5}{19}\right)\\ &= (-1)^{\frac{3-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{3}\right)(-1)^{\frac{5-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{5}\right)\\ &= -\left(\frac{19}{3}\right)\left(\frac{19}{5}\right)\\ &= -\left(\frac{1}{3}\right)\left(\frac{4}{5}\right)\\ &= -1\end{aligned}$$

Thus, 2 is not a quadratic residue of 19.

This computation demonstrates the general procedure. Of course, we could also do the computation as follows without using quadratic reciprocity:

$$\left(\frac{15}{19}\right) = \left(\frac{-4}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{4}{19}\right) = (-1)^{\frac{19-1}{2}} = -1.$$

$$\begin{aligned}\left(\frac{17}{19}\right) &= \left(\frac{-2}{19}\right) \\ &= \left(\frac{-1}{19}\right)\left(\frac{2}{19}\right) \\ &= (-1)^{\frac{19-1}{2}}\left(\frac{2}{19}\right) \\ &= -\left(\frac{2}{19}\right)\end{aligned}$$

Proposition 13.2.4

If p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(If x is odd, then $8 \mid x^2 - 1$)

Connoting with the example, we have

$$\left(\frac{17}{19}\right) = -\left(\frac{2}{19}\right) = (-1)\cdot(-1)^{\frac{19^2-1}{8}}$$

Note that

$$\begin{aligned}19^2 - 1 &= (19-1)(19+1) \\ &= 18 \cdot 20 \\ &= 2^3 \cdot 3^2 \cdot 5\end{aligned}$$

$$\frac{19^2-1}{8} = 45$$

$$(-1)\cdot(-1)^{\frac{19^2-1}{8}} = (-1)\cdot(-1) = 1$$

After potential argument:

$$\begin{aligned}\left(\frac{17}{19}\right) &= (-1)^{\frac{19-1}{2}\cdot\frac{17-1}{2}}\left(\frac{19}{17}\right) \\ &= \left(\frac{19}{17}\right) \\ &= \left(\frac{2}{17}\right)\end{aligned}$$

By applying the proposition, we obtain

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2}{8}} = (-1)^{\frac{(17-1)(17+1)}{8}} = 1.$$

We could also proceed by noting that

$$\left(\frac{2}{17}\right) = \left(\frac{-15}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{3}{17}\right)\left(\frac{5}{17}\right)$$

Problem 45

Find all odd primes p such that

$$x^2 \equiv -3 \pmod{p}$$

has a solution.

Solution

If $p = 3$, then $x^2 \equiv -3 \equiv 0 \pmod 3$ has $x = 0$ as a solution. So let's assume that $p \neq 3$. Then we want to find all odd $p \neq 3$ such that

$$\left(\frac{-3}{p}\right) = 1$$

$$\begin{aligned}
\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} \\
&= (-1)^{\frac{p-1}{2}+\frac{p-1}{2}}\left(\frac{p}{3}\right) \\
&= \left(\frac{p}{3}\right)
\end{aligned}$$

For $p \neq 3$,

$$\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 3$$

Answer: $p = 3$ or $p \equiv 1 \pmod 3$.

Proposition 13.2.5

There are infinitely many primes $p \equiv 1 \pmod 4$, i.e. $1, 5, 9, \cdots$ has infinitely many primes.

Proof. Assume to the contrary that there are finitely many such primes

$$5 = p_1, \cdots, p_k$$

Consider

$$N := (2p, \cdots, p_k)^2 + 1$$

There is a prime $p \mid N$,

$$\begin{aligned}
p \mid N &\implies (2p_1 \cdots p_k)^2 + q \equiv 0 \pmod p \\
&\implies x^2 \equiv -1 \pmod p \text{ has a solution} \\
&\implies \left(\frac{-1}{p}\right) = 1 \implies p \equiv 1 \pmod 4
\end{aligned}$$

It is also clear that

$$p \notin \{p_1, \cdots, p_k\}.$$

Contradiction. □

Theorem 13.2.6: Dirichlet

If $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that

$$\gcd(n, a) = 1,$$

then there are ∞ many primes p such that

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

In fact, asymptotically,

$$\#\{p \text{ prime s.t } p \equiv a \pmod{n}, \quad p \leqslant x\} \sim \frac{x}{\varphi(n) \log x}$$

Problem 46

Suppose p is a prime such that

$$p = x^2 + xy + y^2$$

for some $x, y \in \mathbb{Z}$.

Then $p = 3$ or $p \equiv 1 \pmod{3}$.

Solution

It is easy to see that $p = 2$ is not of this form.

On the other hand,

$$3 = 1^2 + 1 \cdot 1 + 1^2 \qquad x = 1, y = 1$$
$$\implies 3 \text{ is of this form.}$$

Let's assume that p is an odd prime $\neq 3$ and

$$p = x^2 + xy + y^2 \qquad \text{for some } x, y \in \mathbb{Z} \tag{1}$$

(1) implies that

$$\begin{aligned} 4p &= 4x^2 + 4xy + 4y^2 \\ &= \left((2x)^2 + 2 \cdot (2x)\, y + y^2\right) + 3y^2 \\ &= (2x + y)^2 + 3y^2 \\ &\implies (2x + y)^2 \equiv -3y^2 \pmod{p} \end{aligned} \tag{2}$$

If $p \mid y$, then $y \equiv 0 \pmod{p}$, and so

$$\begin{aligned}(2x)^2 &\equiv (2x+y)^2 \\ &\equiv -3y^2 \\ &\equiv 0 \pmod{p} \\ &\implies p \mid 4x^2 \\ &\implies p \mid x\end{aligned}$$

We then obtain

$$\begin{aligned}p = x^2 + xy + y^2 &\equiv 0 \pmod{p^2} \\ \implies p^2 &\mid p\end{aligned}$$

a contradiction.

There is a z such that

$$yz \equiv 1 \pmod{p}.$$

(2) implies that

$$\begin{aligned}z^2(2x+y)^2 &\equiv -3y^2z^2 \\ &\equiv -3 \pmod{p}\end{aligned}$$

Thus, y is invariable.

Therefore

$$\begin{aligned}p \nmid &\implies y \text{ is invertible mod } p \\ &\implies x^2 \equiv -3 \pmod{3} \text{ has a solution} \\ &\overset{p\neq 3}{\implies} \left(\frac{-3}{p}\right) = 1 \\ &\implies p \equiv 1 \pmod{3}\end{aligned}$$

Problem 47

Show that if $n \in \mathbb{N}$, then no prime divisor of $2^n + 1$ is $\equiv -1 \pmod{8}$.

Solution

Suppose n is even, and p is a prime such that $p \mid 2^n + 1$. Then

$$-1 \equiv \left(2^{\frac{n}{2}}\right)^2 \pmod{p}$$

$$\implies \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \implies p \equiv 1 \pmod{4}$$

In particular,

$$p \equiv -1 \pmod 8$$

Assume now that n is odd. In this case

$$\frac{n+1}{2} \in \mathbb{Z}$$

$$\begin{aligned} \implies \left(2^{\frac{n+1}{2}}\right)^2 &= 2^{n+1} \\ &= -2 \pmod p \end{aligned}$$

Therefore,

$$\left(\frac{-2}{p}\right) = 1$$

However,

$$\begin{aligned} \left(\frac{-2}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \\ &= (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}} \end{aligned}$$

If $p \equiv -1 \pmod 8$, then

$$p = 8k-1 \quad \text{for some } k \in \mathbb{Z}$$

$$\begin{aligned} \implies \frac{p^2-1}{8} &= \frac{\left((8k-1)^2-1\right)}{8} \\ &= \frac{64^2k^2-16k}{8} \quad \text{is even.} \end{aligned}$$

On the other hand,

$$\begin{aligned} \frac{p-1}{2} &= \frac{(8k-1)-1}{2} \\ &= 4k-1 \quad \text{is odd.} \end{aligned}$$

Theorem 13.2.7

If $a > 1$ is a natural number such that not a square, then

$$\left(\frac{a}{p}\right) = -1$$

for ∞ many primes p.

Problem 48

If $f \in \mathbb{Z}[X]$ of degree 2 such that for any prime p, there is $n \in \mathbb{N}$ such that $p \mid f(n)$, then all roots of of f are raiotnal.