MATH 430 Notes

Keyu He

December 2022

Abstract

This is the note I took in the USC MATH 430 2022 fall class. This note is also uploaded to USC OSAS.

1 Introduction

1.1 Aug 26, Induction, Well-Ordering Principle(WOP)

- Twin prime conjecture. Goldbach's conjecture
- Pythagorean triples and Fermat's Last Theorem
- The primes $p \equiv 1 \pmod 4$ are sums of two squares

Theorem

(a) Any right triangle with integer side lengths does not have area that is a square number

(b) It can never be twice a square number

It is equivalent to study the equations

$$y^2 = x^3 - d^2x \text{ for } x, y \in \mathbb{Q}$$

with $d = 1, 2$ respectively. (They have trivial solutions $\{(0,0), (\pm d, 0)\}$)

Equations of the form

$$y^2 = f(x)$$

where $f(x)$ is a polynomial of degree 3 are called elliptic curves.

Elliptic curve cryptography.

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.

1.1.2 Well-Ordering Principle

If S in $N = \{1, 2, 3, \ldots\}$ that is nonempty, then it has a minimal element, i.e., there is a in S s.t. $\forall b \in S$, $a \leq b$.

Prove that WOP $\implies$ Induction

Proof. Let $S = \{k \in \mathbb{N} : S_k \text{ is true}\}$. It suffices to show that $S = \mathbb{N}$. Assume the contrary that $S \neq \mathbb{N}$.
Let $T := \mathbb{N} \backslash S$, we are assuming that $T \neq \emptyset$, 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 $1 \notin T \implies m \geq 2$.
Consider $m - 1 \geq 1$. Since m is minimal, $m - 1$ is not in $T \implies m - 1$ is in $S \implies S_{m-1}$ is true.
From (b), we know then S_{m-1} is true $\implies S_m$ is true.
Therefore, S_m is true $\implies m \in S \implies m \notin T$.

But m is in T, we have a contradiction. □

Proposition 1. *$I_n := \int_0^\infty t^n e^{-t}\, dt = n!$ for $n \in \mathbb{N}$.*

Proof. We use induction. The base case is that $I_0 = 1$.
Indeed,

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

Now, it suffices, by induction, to show that if $I_k = k!$, then $I_{k+1} = (k+1)!$.
We have

$$\begin{aligned} I_{k+1} &= \int_0^\infty t^{k+1} e^{-t}\, dt \\ &\text{(integration by parts)}(u = t^{k+1}, v = -e^{-t}, du = (k+1)t^k\, dt, dv = e^{-t}\, dt) \\ &= -t^{k+1}e^{-t}\Big|_0^\infty + \int_0^\infty (k+1)t^k e^{-t}\, dt \\ &= 0 + (k+1)I_k \\ &= (k+1)k! \\ &= (k+1)! \end{aligned}$$

Hence we prove $I_n = n!$ by induction. □

1.2 Aug 29

Proposition 2. $S_n := 1^2 + 2^2 + \cdots + n^2 = \frac{n(2n+1)(n+1)}{6}$

Proof. We apply induction on n. The base case is when $n = 1$, in this case, $S_1 = 1^2 = 1$.

We now show that for any k, if

$$S_k = k(2k+1)(k+1) = 6,$$

then

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

Indeed, we have

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

□

Proposition 3. *Suppose $n \in \mathbb{N}$ and we have a $2^n \cdot 2^n$ board with a corner removed. Then we can tile it using tiles of the shape L (made up by three tiles).*

Proof. We apply induction on n. If $n = 1$, then our board is simply L. So we are done with the base case.

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

We want to show that such a tiling is possible for $2^{n+1} \cdot 2^{n+1}$ boards with a corner removed.

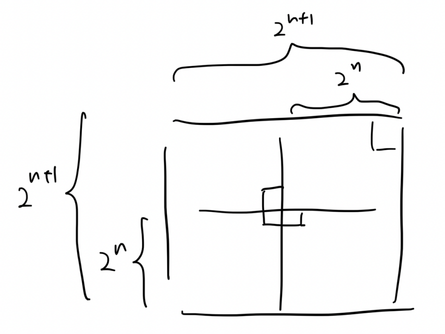


Figure 1: Way of tiling for $2^n \cdot 2^n$ board

We first separate the board into four $2^n \cdot 2^n$ boards. As figure 1 shows, we add a L tile at the middle of the boards, hence all $2^n \cdot 2^n$ boards are missing a tile. By induction hypothesis, each $2^n \cdot 2^n$ board missing a corner can be tiled by L shapes.

Therefore, the whole board can be tiled by L-shape tiles.

□

Proposition 4. $f(n) := \sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}} = 2\cos\frac{\pi}{2^{n+1}}$. *(We have n 2's)*

e.g.

$$\sqrt{2} = 2\cos\frac{\pi}{4}$$
$$\sqrt{2+\sqrt{2}} = 2\cos\frac{\pi}{8}$$
$$\sqrt{2+\sqrt{2+\sqrt{2}}} = 2\cos\frac{\pi}{16}.$$

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

$$\begin{aligned} f(k+1) &= \sqrt{2 + f(k)} \\ &= \sqrt{2 + 2\cos\frac{\pi}{2^{k+1}}} \\ &= \sqrt{2 + 2(2\cos^2\frac{\pi}{2^{k+2}} - 1)} \\ &= \sqrt{2 + 4\cos^2\frac{\pi}{2^{k+2}} - 2} \\ &= \sqrt{4\cos^2\frac{\pi}{2^{k+2}}} \\ &= 2\cos\frac{\pi}{2^{k+2}} \end{aligned}$$

□

Define the sequence

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

i.e.

$$\sqrt{2}, \sqrt{2}^{\sqrt{2}}, \sqrt{2}^{\sqrt{2}^{\sqrt{2}}}, \sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}}}}, \cdots$$

Claim 1. It is an increasing sequence (for every n, $a_n \leq a_{n+1}$).

Base case ($n = 1$): $a_1 \leq a_2$ because $\sqrt{2} \leq \sqrt{2}^{\sqrt{2}}$. Suppose now that $a_k \leq a_{k+1}$ for a given k. We want to show that this implies that

$$a_{k+1} \leq a_{k+2}.$$

However,

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

We want to show that

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

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

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

We apply induction on n.

Base case ($n = 1$): $a_1 = \sqrt{2} \leq 2$.

Suppose $a_k \leq 2$ for some k. Then $a_{k+1} = \sqrt{2}^{a_k} \leq \sqrt{2}^2 = 2$. By induction, $a_n \leq 2$ for all n.

So the sequence (a_n) converges to some $L \leq 2$.
We have

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

1.3 Aug 31

Claim: Every number in the sequence

$$1007, 10017, 100117, 1001117, \ldots$$

is divisible by 53.

Proof. Base case: $1007 = 53 \times 19 \implies a_1$ is divisible by 53.

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

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

1.3.1 Strong Induction

Suppose we have a sequence of statements

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

such that

- S_1 is true
- For every N, if S_k is true for every $k \in N$, then S_N is also true.

Then S_n is true for every n.

Proposition 5. *If α is a real number such 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

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

Now consider $n + 1$.

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

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. □

Proposition 6. *For every integer $n \geq 1$, $3^{n+1} \big| 2^{3^n} + 1$.*

Proof. For $n = 1$, we have

$$9 = 3^{1+1} \big| 2^{3^1} + 1 = 9.$$

For $n + 1$, we have

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

Also note that

$$\begin{aligned} (2^{3^n})^2 - 2^{3^n} + 1 &\equiv ((-1)^{3^n})^2 - (-1)^{3^n} + 1 \\ &\equiv (-1)^2 - (-1) + 1 \\ &= 3 \equiv 0, \end{aligned}$$

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

If $3^{n+1} \big| 2^{3^n} + 1$, then the previous imply that

$$3^{n+2} = 3^{n+1} \cdot 3 \big| 2^{3^{n+1}} + 1.$$

By induction, the conclusion follows. □

Proposition 7. *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 prove this using induction on k.

First, note that

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

The claim is equivalent to

$$105 \Big| 15k^7 + 21k^5 + 70k^3 - k =: g(k)$$

for every $k \in \mathbb{N}$.

Base case: $k = 1$: $g(1) = 15 + 21 + 70 - 1 = 105$ is divisible by 105.

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

However,

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

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

1.4 Sep 2

Usual induction.
$S_1, S_2, S_3, \ldots$ sequence of statements (a) S_1 is true (b) For any given $k \in \mathbb{N}, S_k \implies S_{k+1} \implies$ all S_n are true.

Strong induction.
$S_1, S_2, S_3, \ldots$ sequence of statements (a) S_1 is true (b) For any given $k \in \mathbb{N}, (S_1, S_2, \ldots, S_k) \implies S_{k+1} \implies$ all S_n are true.

Proposition 8. *Every natural number can be written in the form*

$$\pm 1^2 \pm 2^2 \pm \cdots \pm n^2.$$

Proof. Note that

$$\begin{aligned} 1 &= +1^2 \\ 2 &= -1^2 - 2^2 - 3^2 + 4^2 \\ 3 &= -1^2 + 2^2 \\ 4 &= +1^2 - 2^2 - 3^2 + 4^2 \end{aligned}$$

Now, in order to represent 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 the identity

$$4 = m^2 - (m+1)^2 - (m+2)^2 + (m+3)^2 \text{ for every } m$$

So

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

□

Proposition 9. *For every $N \in \mathbb{N}$, $N \geq 2$,*

$$\sqrt{2\sqrt{3\sqrt{\cdots\sqrt{N}}}} < 3.$$

Proof. Claim: For every $m \in \mathbb{N}, m \leq \mathbb{N}$,

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

This is a generalization of the problem.

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

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

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

Now assume it is true for $m = k, m \leq N$, that is,

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

We deduce it for $m = k-1$ by noting that

$$\begin{aligned} \sqrt{(k-1)\sqrt{k\sqrt{(k+1)\sqrt{\cdots\sqrt{N}}}}} &< \sqrt{(k-1)(k+1)} \\ &= \sqrt{k^2-1} \\ &< k \\ &= (k-1)+1 \end{aligned}$$

Take $m = 2$, then we prove this statement. □

1.4.1 Dyadic induction

Suppose we have sequence of statements $S_1, S_2, S_3, \cdots$.

Suppose:

(a) S_2 is true,

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

(c) Whenever S_{n+1} is true, S_n is true.

Theorem: Arithmetic mean – geometric mean inequality (AMGM)

If $x_1, \ldots, x_n \geq 0$ are real numbers, then

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}$$

Proof. Base case: For $n = 2$, this is

$$\begin{aligned}
&\frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2} \\
\iff & x_1 + x_2 \geq 2\sqrt{x_1 x_2} \\
\iff & x_1 - 2\sqrt{x_1 x_2} + x_2 \geq 0 \\
\iff & (\sqrt{x_1} - \sqrt{x_2})^2 \geq 0.
\end{aligned}$$

Suppose it is true when $n = 2^k$, we show this implies that it is true for $n = 2^{k+1}$.

Indeed,

$$\begin{aligned}
\frac{x_1 + \cdots + x_{2^{k+1}}}{2^{k+1}} &= \frac{\frac{x_1 + \cdots + x_{2^k}}{2^k} + \frac{x_{2^k+1} + \cdots + x_{2^{k+1}}}{2^k}}{2} \\
&\geq \frac{\sqrt[2^k]{x_1 \cdots x_{2^k}} + \sqrt[2^k]{x_{2^k+1} \cdots x_{2^{k+1}}}}{2} \\
&\geq \sqrt{\sqrt[2^k]{x_1 \cdots x_{2^k}} \sqrt[2^k]{x_{2^k+1} \cdots x_{2^{k+1}}}} \\
&= \sqrt[2^{k+1}]{x_1 x_2 \cdots x_{2^{k+1}}}
\end{aligned}$$

So we know by induction on the power k in $n = 2^k$ that the 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 ≥ 0, $x_1, \ldots, x_m$.

Extend this to the sequence $x_1, \ldots, x_m, \sqrt[m]{x_1 \cdots x_m}$.

We now have $m+1$ elements.

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

$$\frac{x_1 + \cdots + x_m + \sqrt[m]{x_1, \cdots, x_m}}{m+1} \geq \sqrt[m+1]{x_1 \cdots x_m \sqrt[m]{x_1, \cdots, x_m}}$$

Algebraic manipulation gives

$$\begin{aligned}
& x_1 + \cdots + x_m + \sqrt[m]{x_1 \cdots x_m} \geq (m+1) \sqrt[m]{x_1 \cdots x_m} \\
\implies & x_1 + \cdots + x_m \geq m \sqrt[m]{x_1 \cdots x_m} \\
\implies & \frac{x_1 + \cdots + x_m}{m} \geq \sqrt[m]{x_1 \cdots x_m}.
\end{aligned}$$

□

We then know that $S_{2^k} \implies S_{2^{k+1}}$ and $S_{m+1} \implies S_m$.

Therefore, S_n is true for every $n \geq 1$.

1.5 Sep 7, Binomial Coefficient, Newton's Binomial Theorem

Comment on problem 2

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

Let's find a formula for the more general summation.

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

Consider

$$\sum_{k=0}^{n} x^k = 1 + x + \cdots + x^n = \frac{x^{n+1}-1}{x-1}.$$

Differentiating both sides w.r.t. to x, we obtain

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

Multiplying by x, we obtain

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

1.5.1 Binomial Coefficient

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

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

e.g. 4 people can form $\frac{4\times 3}{2} = 6$ pairs. (Division by two because pairs were counted twice)

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

Proof. The first element may be chosen in n ways. The second element in $n-1$. $\cdots$ The k^{th} element in $n-k+1$. So the number of 'ordered' k-element subsets is

$$n(n-1)\cdots(n-k+1).$$

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

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\cdots(n-k+1)}{k!} \\ &= \frac{(n(n-1)\cdots(n-k+1))((n-k)(n-k-1)\cdots 1)}{k!((n-k)(n-k-1)\cdots 1)} \\ &= \frac{n!}{k!(n-k)!}.\end{aligned}$$

□

e.g. Suppose there are 100 employees. In how many ways can we create groups which exactly 4 members?

$$\binom{100}{4} = \frac{100!}{4!\cdot 96!} = \frac{1000\cdot 99\cdot 98\cdot 97}{24} = 3921225.$$

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

Proof.

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

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

1.5.2 Newton's Binomial Theorem

Theorem(Newton). Suppose $n \in \mathbb{N}$, a, b variables,

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

Proof. Note that

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ times}}.$$

If I choose k of the brackets and have a coming from it, the other $n-k$ brackets contribute b.

The number of ways of choosing k of the $(a+b)$ terms is $\binom{n}{k}$. So

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

□

1.5.3 Identities regarding binomial coefficients

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

   Why? Using Newton's Binomial Theorem,

   $$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n.$$

   We can also consider counting subsets of an n-element set in two ways. Take n elements and count how many ways there are to put these two elements into 2 different containers (A and B)

   a) Every element can take two states: it's either in A or in B. This gives n steps with 2 options at each step, so we get 2^n options in total.

   b) We can also think of adding up all the ways in which we can have k elements in A and $n-k$ elements in B, for $0 \leq k \leq n$. For each k, this number is: "choose k elements that will go into A". Then the other $n-k$ elements automatically go to B. So for each k this number is just $\binom{n}{k}$. Now, we add this for all k previously mentioned to get $\sum_{k=0}^{n} \binom{n}{k}$.

   And thus, $2^n = \sum_{k=0}^{n} \binom{n}{k}$.

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

3. $$\binom{n}{k} = \binom{n}{n-k} \text{ for } 0 \leq k \leq n$$

   Alg. proof.

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

Combinatorial arg. 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.

1.6 Sep 9, Binomial Coefficients Continued

More identities regarding binomial coefficients:

1. For $1 \leq k \leq n$,
$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.$$

   Proof. Here we use Combinatorial proof. The algebraic one is left for exercise.

   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 (of an n-element set) and $x \in A$.

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

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

2. Pascal's Identity

   For $1 \leq k \leq n$, we have
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

   Combinatorial argument. Take the set $\{1, 2, \cdots, n\}$ with n elements. Split the problem in two: Count subsets of size k containing 1 + Count subsets of size k not containing 1.

   # subsets of size k not containing 1 is $\binom{n-1}{k}$.

   # subsets of size k containing 1 is $\binom{n-1}{k-1}$.

   Therefore,
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Problem 1. (Vandermonde's Identity)

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

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

Corollary of this is that when $m = k = n$, we have

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

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 a different way. Take the set $\{1, 2, 3, \cdots, m, m+1, \cdots, m+n\}$.

If i of the elements of the subset are among the first m, then the rest $(k-i)$ elements have to be among $\{m+1, \cdots, m+n\}$. $\implies$ $\binom{m}{i}\binom{n}{k-i}$ ways.

Now, i could be $\{0, 1, \cdots, k\}$. So summing from $i = 0$ to $i = k$, we obtain

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

□

Sketch of the algorithmic proof.

Proof. Note that $\binom{m+n}{k}$ is the coefficient of x^k in

$$(1+x)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i.$$

On the other hand,

$$\begin{aligned}(1+x)^{m+n} &= (1+x)^m(1+x)^n \\ &= (\sum_{i=0}^{m} \binom{m}{i} x^i)(\sum_{j=0}^{n} \binom{n}{j} x^j) \\ &= \sum_{l=0}^{m+n} (\sum_{i+j=l} \binom{m}{i}\binom{n}{j}) x^l \\ &= \sum_{l=0}^{m+n} (\sum_{i=0}^{l} \binom{m}{i}\binom{n}{l-i}) x^l\end{aligned}$$

The coefficient of x^k is exactly

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

□

Problem 2.

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

Suppose we have n people. If we choose k of them in $\binom{n}{k}$ ways, the King can be chosen in k ways, and the President also in k ways. There are $k^2\binom{n}{k}$ ways of doing all this.

Since k can be any of $1, 2, \cdots, n$, we have a total of $\sum_{k=1}^{n} k^2\binom{n}{k}$ ways of doing this.

Let's count this in a different way.

Case 1: Suppose King = President.

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.

Case 2: Suppose King $\neq$ President.

In this situation, we choose the King in n ways, and the President 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.

Sum two cases up,

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

1.7 Sep 12

Last class, we had the following problem

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

Sketch of alg. proof:

Proof. The idea is similar to the calculus computation of

$$\sum_{k=1}^{n} kx^k$$

Consider

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

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

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

Set $x = 1$ to get the result

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

□

Problem Show that

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

Which is equivalent to show

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

Solution We induct on $n \geq 0$. 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

$$\begin{aligned}
f(n+1) &= \sum_{k=0}^{n+1} \binom{n+1+k}{k} \frac{1}{2^k} \\
\text{(Pascal's Identity)} &= 1 + \sum_{k=1}^{n+1} \left(\binom{n+k}{k} + \binom{n+k}{k-1} \right) \frac{1}{2^k} \\
&= 1 + \sum_{k=1}^{n+1} \binom{n+k}{k} \frac{1}{2^k} + \sum_{k=1}^{n+1} \binom{n+k}{k-1} \frac{1}{2^k} \\
&= 1 + \sum_{k=1}^{n} \binom{n+k}{k} \frac{1}{2^k} + \binom{2n+1}{n+1} \frac{1}{2^{n+1}} + \sum_{k=1}^{n+1} \binom{n+k}{k-1} \frac{1}{2^k} \\
&= f(n) + \binom{2n+1}{n+1} \frac{1}{2^{n+1}} + \sum_{k=1}^{n+1} \binom{n+k}{k-1} \frac{1}{2^k} \\
&\text{Do a change of variables. Let } i = k-1. \\
&= f(n) + \binom{2n+1}{n+1} \frac{1}{2^{n+1}} + \sum_{i=0}^{n} \binom{n+1+i}{i} \frac{1}{2^{i+1}} \\
&= f(n) + \frac{1}{2} \sum_{i=0}^{n+1} \binom{n+1+i}{i} \frac{1}{2^i} \\
&= f(n) + \frac{1}{2} f(n+1)
\end{aligned}$$

We have shown that

$$\begin{aligned}
& f(n+1) = f(n) + \frac{1}{2} f(n+1) \\
\implies & f(n+1) = 2f(n)
\end{aligned}$$

By assumption, $f(n) = 2^n$.

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

2 Number Theory

2.1 Sep 12 Continued, Division Algorithm

2.1.1 Division Algorithm

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

$$a = bq + r, 0 \leq r < b$$

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

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

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

$$S := \{a - bx | a - bx \geq 0, x \in \mathbb{Z}\}.$$

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

$$a - b(-|a|) = a + b|a| \overset{b>0}{\geq} a + |a| \geq 0$$

By the WOP, there is a $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ s.t.

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

and r is minimal.

Claim. $0 \leq r < b$.

Every element in S is ≥ 0 and

$$r \in S \implies r \geq 0.$$

Assume to the contrary that $r \geq b$. Take $x = q + 1$

$$\implies a - b(q + 1) = (a - bq) - b = r - b \geq 0$$

This means that we have found $q, r \in \mathbb{Z}$,

$$0 \leq r < b$$

s.t.

$$a = bq + r.$$

However, this would imply that $0 \leq r - b \in S$. But $r - b < r$, contradicting the minimality of r in S.

In order to show uniqueness, it suffices to show that $q_1 = q$ and $r_1 = r$. Consider

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

(1) − (2):

$$\begin{aligned}0 &= b(q-q_1)+(r-r_1)\\ \implies r_1 - r &= b(q-q_1)\\ \implies |r_1-r| &= b|q-q_1| \ (3)\end{aligned}$$

$$\begin{aligned}0 \le r_1, r < b \ &\implies |r_1 - r| < b\\ &\overset{(3)}{\implies} b|q-q_1| < b\\ &\implies 0 \le |q-q_1| < 1\end{aligned}$$

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

$$|r - r_1| = b|q-q_1| = 0$$

$$\implies r_1 = r.$$

Therefore, q and r are unique. □

2.2 Sep 14, Division Algorithm continued

Theorem 1. *Suppose $a, b \in \mathbb{Z}, b > 0$, then there are unique $q, r \in \mathbb{Z}$ s.t.*

$$a = bq + r, 0 \le r < b$$

Applications of the division algorithm

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

Solution. Suppose our perfect square is $n^2, n \in \mathbb{N}$. By the division algorithm, $n = 3k$, $3k+1$ or $3k+2$ for some $k \in \mathbb{Z}$.

Case 1: $n = 3k$.

Then

$$n^2 = 9k^2 \text{ divisible by } 3 \implies \text{remainder} = 0.$$

Case 2: $n = 3k+1$.

Then

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

Case 3: $n = 3k + 2$ Then

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

Answer. Only 0 and 1 are possible remainder.

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

Solution. $0^2 = 0, 1^1 = 1, 2^2 = 4$ remainder 0, $3^2 = 9$ remainder 1.

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

By the division algorithm, $n = 2k$ or $n = 2k + 1, k \in \mathbb{Z}$.

Case 1: $n = 2k$ (n is even).

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

Case 2: $n = 2k + 1$ (n is odd).

Then

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

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

Problem. Show that no number in the (infinite) sequence

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

is a perfect square.

Solution. All numbers in the sequence have a remainder of 3 when divided by 4. However, the possible remainder of a perfect square divided by 4 are only 0 and 1.

Theorem 2. *(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.

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

Proof. Suppose $n \in \mathbb{Z}$ is odd and $n^2 = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

a^2 and b^2 are perfect squares, and so their only possible remainders when divided by 4 are 0 or 1 $\implies$ only possible remainders of n when divided by 4 are $0+0, 0+1, 1+0$, and $1+1$. Since n is odd, 0 and 2 are not possible. □

2.2.1 Divisibility

Def. 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 $b = ac$.

Examples.

$$\begin{aligned}
&1 \mid n, n = 1 \cdot n \\
&n \mid n, n = n \cdot 1 \\
&3 \mid 6 \\
&10 \mid 20 \\
&3 \nmid 2 \\
&3 \nmid 5
\end{aligned}$$

Def. (Greatest common divisor, gcd).

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

1. $d \mid a$ and $d \mid b$.
2. $c \in \mathbb{N}$ s.t. $c \mid a$ and $c \mid b \implies c \leq d$.

Examples.

a) $\gcd(4, 6) = 2$. (4 has divisors 1, **2**, 4; 6 has divisors 1, **2**, 3, 6)

b) $\gcd(-5, 5) = 5$. (Both of them have divisors 1, **5**)

Problem.

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

We will use the following fact:

$$(d \mid a, d \mid b) \iff (d \mid a, d \mid b - ka) k \in \mathbb{Z}.$$

Solution.

$$\begin{aligned}
&\gcd(2016! + 1, 2017! + 1) \\
=&\gcd(2016! + 1, (2017! + 1) - 2017(2016! + 1)) \\
=&\gcd(2016! + 1, (2017! + 1) - 2017! - 2017) \\
=&\gcd(2016! + 1, -2016) \\
=&\gcd((2016! + 1) - 2015!2016, -2016) \\
=&\gcd(1, -2016) \\
=&1.
\end{aligned}$$

Exercise. If F_n are the Fibonacci numbers, $n \in \mathbb{N}$, then

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

And to be more generalized,

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

2.3 Sep 16, Divisibility continued

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

$$\begin{aligned}
&(d \mid a, d \mid b) \iff (d \mid a, d \mid b - ka) \\
&\implies \{d \in \mathbb{N} : d \mid a, d \mid b\} = \{d \in \mathbb{N} : d \mid a, d \mid b - ka\} \\
&\implies \max\{d \in \mathbb{N} : d \mid a, d \mid b\} = \max\{d \in \mathbb{N} : d \mid a, d \mid b - ka\} \\
&\implies \gcd(a, b) = \gcd(a, b - ka).
\end{aligned}$$

Recall that the Fibonacci sequence is recursively defined as

$$F_0 = 1, F_1 = 1, \text{ and}$$

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

Problem. Show that for every n,

$$\gcd(F_n, F_n + 1) = 1$$

Proof. We use induction on n.

For $n = 0$, we have

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

Assume the statement is true for $n = k$. We show that this implies the validity for $n = k + 1$.

$$\begin{aligned}
&\gcd(F_{k+1}, F_{k+2}) \\
=&\gcd(F_{k+1}, F_{k+2} + F_k) \\
=&\gcd(F_{k+1}, F_{k+2} + F_k - F_{k+1}) \\
=&\gcd(F_{k+1}, F_k)
\end{aligned}$$

By the inductive assumption, this latter quantity is 1.

The conclusion follows from induction. □

2.3.1 Basic properties of divisibility

Theorem 3.

$$\text{(a) } n \mid n, 1 \mid n, n \mid 0$$

$$\text{(b) } a \mid b, b \mid c \implies a \mid c$$

$$\text{(c) } a \mid b, b \mid a \implies a = \pm b$$

$$\text{(d) } a \mid b, b \neq 0 \implies |a| \leq |b|$$

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

Proof. Proof of all the properties.

(a) Clear.

(b) $a \mid b \implies$ there is $r \in \mathbb{Z}$ s.t. $b = ar$.

$b \mid c \implies$ there is $s \in \mathbb{Z}$ s.t. $c = sb$.

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

(c) If one of a, b is 0, the other must also be 0

$$0 \mid 0 \iff \text{ there is } n \in \mathbb{Z} \text{ s.t. } 0 = n \cdot 0$$

Otherwise,

$$\begin{aligned} a \mid b &\implies b = ra \text{ for some } r \in \mathbb{Z} \\ b \mid a &\implies a = sb \text{ for some } s \in \mathbb{Z} \\ &\implies a = rsa \\ &\overset{a\neq 0}{\implies} rs = 1 \\ &\implies r = \pm 1. \end{aligned}$$

Then the conclusion is clear.

(d)

$$a \mid b, b \neq 0$$

There is $r \in \mathbb{Z}$ s.t.

$$\begin{aligned} b &= ra \\ \implies |b| &= |r||a| \\ \overset{b\neq 0}{\implies}{}^{r\neq 0} |b| &= |r||a| \geq |a|. \end{aligned}$$

(e) 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

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

□

2.3.2 Main Theorem about gcd: Bézout's Theorem

Theorem 4. *Suppose $a, b \in \mathbb{Z}$, at least one of which is nonzero. Then there are integers $m, n \in \mathbb{Z}$ s.t.*

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

e.g.

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

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, $S \neq \emptyset$.

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,

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

Since $d \in S$, there are $x, y \in \mathbb{Z}$ s.t.

$$d = ax + by.$$

Then,

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

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

$$\begin{aligned} c \mid a, c \mid b &\implies c \mid ax + by = d \\ &\overset{d \neq 0}{\implies} |c| \leq |d| = d. \end{aligned}$$

So $d = \gcd(a, b)$. □

2.4 Sep 19, Divisibility and gcds

Corollary 4.1. *Suppose $a, b \in \mathbb{Z}$, at least one of which is nonzero. Then*

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

Proof. If we consider $ax + by$, $x, y \in \mathbb{Z}$, 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

$$n \gcd(a,b), n \in \mathbb{Z}$$

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

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

This concludes the proof.

Corollary 4.2. *Suppose $a, b \in \mathbb{Z}$ as before. Then $\gcd(a,b) = 1$ if and only if there are integers $x, y \in \mathbb{Z}$ s.t.*

$$1 = ax + by.$$

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

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

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

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

$$\implies \gcd(a,b) = 1$$

□

Proposition 10. *Suppose $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.*

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

$$ax + by = 1. \tag{$*$}$$

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

$$acx + bcy = c$$

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

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

□

Proposition 11. *Suppose $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$. If $a \mid c$, $b \mid c$, then*

$$ab \mid c.$$

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

$$ax+by=1.$$

Multiply by c to get

$$acx+bcy=c$$

Since $b\mid c$, $ab\mid ac$. ($\frac{c}{b}\in\mathbb{Z}\implies\frac{ac}{ab}=\frac{c}{b}\in\mathbb{Z}$) By the same argument, $a\mid c\implies ab\mid bc$. We conclude that $ab\mid acx+bcy=c$. □

Problem. Show that

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

has no integer solutions.

Proof. Since $3\mid 9$ and $3\mid 21x^2$, $3\mid 7y^2$.

Since $\gcd(3,7)=1$,

$$3\mid y^2=y\cdot y\implies 3\mid y$$

$$y=3y_1 \text{ for some } y_1\in\mathbb{Z}$$

Therefore,

$$\begin{aligned}&21x^2-7(3y_1)^2=9\\ \iff\ &21x^2-7\cdot 3\cdot 3y_1^2=9\\ \overset{\text{divide by 3}}{\iff}\ &7x^2-21y_1^2=3\end{aligned}$$

Since $3\mid 3$ and $3\mid 21y_1^2$, we must have $3\mid 7x^2$. Again, this implies that $3\mid x\implies x=3x_1$, for some $x_1\in\mathbb{Z}$.

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

This implies that y_1^2 has remainder 2 when divided by 3. However, no such perfect square exists. □

Problem. Show that

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

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

Solution Sketch. Let $k\geq 0$ be the largest power of 2 s.t. $2^k\mid x,y,z$.

Write

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

Then

$$x^2 + y^2 + z^2 = 2^{k+1} x_1 y_1 z_1.$$

You can conclude that exactly one of x_1, y_1, z_1 is even, say x_1.

But then

$$y_1^2 + z_1^2 = 2^{k+1} x_1 y_1 z_1 - x_1^2.$$

Since $2 \mid x_1$, right hand side is divisible by 4, thus

$$4 \mid y_1^2 + z_1^2.$$

On the other hand, y_1, z_1 are odd $\implies$ $y_1^2 + z_1^2$ has remainder 2 when divided by 4.

$$4 \nmid y_1^2 + z_1^2.$$

Contradiction!

Note: If $x \in \mathbb{Z}$, then the only possible remainders of x^2 when divided by 3 or 4 are 0 and 1.

2.4.1 Gcd's and Congruences

Definition: 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:

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

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

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

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

Theorem 5.

$$\left.\begin{aligned} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{aligned}\right\} \implies a + c \equiv b + d \pmod{n} \qquad (i)$$

$$\left.\begin{aligned} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{aligned}\right\} \implies ac \equiv bd \pmod{n} \qquad (ii)$$

Proof. Since $a \equiv b \pmod{n}$, $n \mid a - b \implies$ there exists $r \in \mathbb{Z}$ s.t.

$$\begin{aligned} a - b &= nr \\ \implies a &= b + nr \end{aligned}$$

Similarly, there is $s \in \mathbb{Z}$ s.t. $c = d + ns$

Therefore,

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

This completes the proof of (i). □

Proof. Proof of (ii) is shown as follows.

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

□

Corollary 5.1. *Suppose $P \in \mathbb{Z}[X](= \{a_0, +a_1x + \cdots + a_kx^k \mid k \geq 0, k \in \mathbb{Z}\})$ $=$ polynomials with $\mathbb{Z}$ coefficient*

Then $a \equiv b \pmod{n} \implies P(a) \equiv P(b) \pmod{n}$.

Proof. Suppose

$$P(x) = a_0 + a_1x + \cdots + a_kx^k, with a_i \in \mathbb{Z}.$$

Then, $a \equiv b \pmod{n} \implies a^j \equiv b^j \pmod{n}$ for any $j \geq 0$
$\implies \forall j \geq 0, a_ja^j \equiv a_jb^j \pmod{n}$
$\implies$ sum them up, $P(a) \equiv P(b) \pmod{n}$ □

Proposition 12. *If $a \in \mathbb{Z}$, then*

$$a^2 \equiv 0 \text{ or } 1 \pmod{3}.$$

Proof. By the division algorithm,

$$a \equiv 0, 1, \text{ or } 2 \pmod{3}.$$

Therefore,

$$\begin{aligned} a^2 &= 0^2, 1^2, 2^2 \pmod{3} \\ &= 0, 1 \pmod{3} \end{aligned}$$

□

Proposition 13. *If $a \in \mathbb{Z}$, then*

$$a^2 \equiv 0 \textit{ or } 1 \pmod{4}.$$

Proof. By the division algorithm,

$$a \equiv 0, 1, 2, \text{ or } 3 \pmod{4}.$$

Therefore,

$$\begin{aligned} a^2 &= 0^2, 1^2, 2^2, 3^2 \pmod{4} \\ &= 0, 1 \pmod{4} \end{aligned}$$

□

Proposition 14. *If $a \in \mathbb{Z}$ is odd, then $a^2 = 1 \pmod{8}$.*

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

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

Then,

$$\begin{aligned} a^2 &\equiv 1^2, 3^2, 5^2, 7^2 \pmod{8} \\ &\equiv 1 \pmod{8} \end{aligned}$$

□

Problem: What are all pairs of prime numbers (p, q) s.t.

$$p = \frac{a^3 + a}{2}, q = \frac{a^3 - a}{2}$$

for some $a \in \mathbb{Z}$?

Solution: It is easy to see that this is equivalent to finding pairs of prime numbers (p, q) s.t. $(p-q)^3 = p+q$.

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

Thus,

$$p-q \mid 2q.$$

We also have

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

$p \neq q$, and p, q 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,

$$\begin{aligned} &\gcd(p+q, q) = 1 \\ \implies &\gcd(p+q, q^3) = 1. \end{aligned}$$

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

Proof. There are integers $x, y \in \mathbb{Z}$ s.t.

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

□

Definition. Suppose $a_1, \cdots a_n \in \mathbb{Z}$, at least one of which is nonzero.

Then $\gcd(a_1, \cdots, a_n) = d$ is defined as the positive integer satisfying:

$$\begin{aligned}&\text{(i) } d \mid a_1, d \mid a_2, \cdots, d \mid a_n \\ &\text{(ii) } c \mid a_1, c \mid a_2, \cdots, c \mid a_n \implies c \leq d.\end{aligned}$$

Problem.

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

Solution. We will use the following lemma.

Lemma. If $c \mid a, b \implies c \mid \gcd(a, b)$

Proof. By Bézout's theorem, there are $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b) \implies c \mid ax + by = \gcd(a, b).$$

□

The answer is

$$\gcd(2022+2, 2022^2+2, 2022^3+2, \cdots) = \gcd(2002+2, 2002^2+2) = 6.$$

2.5 Sep 26, Gcds continued, lcm

2.5.1 Gcds of more than two variables

Def. Suppose $a_1, \cdots, a_n$ are integers, at least one of which is nonzero. Then the gcd of $a_1, \cdots, a_n$, written $\gcd(a_1, \cdots, a_n)$ is the largest natural number d, s.t.

1. $d \mid a_1, \cdots, a_n$.
2. if $c \mid a_1, \cdots, c \mid a_n$, then $c \leq d$.

Problem.

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

Solution. Let $d = \gcd(2022+2, 2022^2+2, 2022^3+2, \cdots)$. Then

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

Note that

$$\begin{aligned}2002^2 + 2 &= 2002(2000+2) + 2 \\ &= 2000(2002+2) + 6 \\ \implies &\gcd(2002+2, 2002^2+2) \\ &= \gcd(2002+2, 6) \ \Big(\text{for } k \in \mathbb{Z}, \gcd(a, b) = \gcd(a, b - ka)\Big) \\ &= \gcd(2004, 6) \\ &= 6\end{aligned}$$

Therefore $d \mid 6$. If we show that

$$6 \mid 2002^k + 2 \text{ for every } k \geq 1$$

then we would be done.

The claim is that $3 \mid 2002^k + 2$.

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

We also know that

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

We conclude that $6 \mid 2002^k + 2$ for every $k \geq 1$.

The answer is

$$\gcd(2022 + 2, 2022^2 + 2, 2022^3 + 2, \cdots) = 6.$$

Proposition 16. *A natural number is divisible by 3 (or 9) if and only if its sum of digits is divisible by 3 (or 9).*

Proof. Suppose n is a natural number with decimal expression

$$\begin{aligned} n &= (a_0 \cdots a_d)_{10} \\ &= a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_d \cdot 10^d, \text{ where } 0 \leq a_0, \cdots, a_d \leq 9 \\ &\equiv a_0 + a_1 \cdot 1 + a_2 \cdot 1^2 + \cdots a_d \cdot 1^d \pmod 9 \\ &= a_0 + a_1 + a_2 + \cdots + a_d \pmod 9. \end{aligned}$$

□

2.5.2 Least Common Multiple (lcm)

Def. Suppose $a, b \in \mathbf{Z}$. Then the least common multiple of a and b, written $\operatorname{lcm}(a, b)$, is a positive integer d s.t.

1. $a \mid d$ and $b \mid d$
2. if $a \mid c$ and $b \mid c$ ($c \neq 0$), the $c \geq d$

Example. $\operatorname{lcm}(2, 3) = 6$, $\operatorname{lcm}(4, 6) = 12$

Theorem 6.

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

i.e.

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

Example. $\gcd(a, b) = 1 \implies \operatorname{lcm}(a, b) = ab$.

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

2.6 Sep 28, lcm and gcd, Euclidean algorithm

2.6.1 lcm and gcd

Theorem 7. *For any $a, b \in \mathbb{N}$,*

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

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

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

Note that

$$m = a(\frac{b}{d})$$

and $d \mid b$. 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 <u>least</u> 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. $a, b \mid c \implies \frac{c}{b}x + \frac{c}{a}y\mathbb{Z}$

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

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

The conclusion follows. □

Corollary 7.1. *Suppose* $a, b \in \mathbf{N}$*. Then*

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

Example.

$$\operatorname{lcm}(4, 5) = 4 \cdot 5 = 20$$
$$\operatorname{lcm}(6, 4) = \frac{4 \cdot 6}{\gcd(4, 6)} = \frac{4 \cdot 6}{2} = 12.$$

2.6.2 Euclidean algorithm

The basis of the Euclidean algorithm is the division algorithm.

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

$$a = bq + r$$

and

$$0 \leq r < b.$$

Example. 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:

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

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

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. (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 an take

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

to get

$$12378x + 2054y = 6$$

Since gcd = 6, we obtain

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

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

For gcd,

$$d \mid a, b \implies d \mid a + kb, b.$$

For lcm,

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

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

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

Solution. By Bézout's theorem,

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

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

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

Solution. 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

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

2.7 Sep 30

2.7.1 General Solutions

How do we find integer solutions to

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

The Euclidean algorithm gave only one solution

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

is a line with rational slope. Since we also have at least one solution, we expect infinitely many integer solutions.

How do we find all solutions?

Theorem 8. *Suppose a and b are as before and $c \in \mathbb{Z}$. Then $ax + by = c$ has an integer solution $\iff$ $d = \gcd(a,b) \mid c$. If $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ is a solution, then all solutions of $ax + by = c$ are given by*

$$\begin{array}{l} x = x_0 - (\frac{b}{d})t \\ y = y_0 + (\frac{a}{d})t \end{array}, t \in \mathbb{Z}$$

Example. 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,

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

$\implies$ 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.

$$\begin{aligned}
&\frac{b}{d} \,\Big|\, x - x_0 \\
\Longrightarrow\ & x - x_0 = -\frac{b}{d}t_2 \\
\Longrightarrow\ & x = x_0 - \frac{b}{d}t_2
\end{aligned}$$

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

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

□

2.7.2 Unique Factorization.

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

e.g. 5, 7, 11, 13, 17, 19

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

$$n = a \cdot b.$$

e.g. $6 = 2 \cdot 3$, $10 = 2 \cdot 5$, $12 = 2^2 \cdot 3$

Theorem 9. *(Unique prime factorization) Every integer $n \geq 2$ is a product of prime numbers*

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

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 $a, b \geq 2$.

$$\begin{aligned} \implies a &= \frac{k+1}{b} \leq \frac{k+1}{2} \leq k \\ b &\leq k. \end{aligned}$$

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

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

(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

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

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

$$\begin{aligned} p_1^{\alpha_1} &\biggm| p_1^{\beta_1} \\ \implies \alpha_1 &\leq \beta_1. \end{aligned}$$

Similarly, $\beta_1 \leq \alpha_1$.

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. □

How is gcd related to prime factorization?

Theorem 10. *Suppose*

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

Then

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

Proof sketch. Suppose $d \mid a, b$.

Then

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

Therefore,

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

Example.

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

Problem.

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

2.8 Oct 3, p-adic valuations

2.8.1 More on gcd, lcm, and unique prime factorization

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

$$\begin{matrix} a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ b = p_1^{\beta_1} \cdots p_k^{\beta_k} \end{matrix}, p_i \text{ distinct prime numbers}, \alpha_i, \beta_i \geq 0$$

then

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

where $\gamma_i \leq \alpha_i, \beta_i$.

Thus for every i,

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

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

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

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

Warning. $\gcd(a,b,c) = 1 \not\Longrightarrow \gcd(a,b) = 1$ **Example.** $\gcd(2\cdot3, 3\cdot5, 5\cdot2) = 1$. but $\gcd(2 \cdot 3, 3 \cdot 5) = 3 \neq 1$.

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.

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

These verify $60 = \operatorname{lcm}(12,15) = \frac{12\cdot15}{\gcd(12,15)} = \frac{12\cdot15}{3}$.

2.8.2 p-adic valuations

For a natural number n,

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

Example.

$$v_2(12) = v_2(2^2 \cdot 3) = 2$$
$$v_2(5) = 0$$
$$v_5(5^2) = 2$$

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

You can generalize unique factorization to rational numbers. How? 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.

$$\frac{15}{20} = \frac{3}{4} = \frac{3}{2^2} = 2^{-2} \cdot 3$$
$$\frac{15}{20} = \frac{3 \cdot 5}{2^2 \cdot 5} = (3 \cdot 5) \cdot 2^{-2} \cdot 5^{-1} = 2^{-2} \cdot 3$$

Def. 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.

Proposition 17.

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

(b) $d \mid n \iff$ *for every prime* $p, v_p(d) \leq v_p(n)$

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

Why (c)? If $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, 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.

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

Example.

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

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

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

$$\operatorname{lcm}(a,b,c)^2 \;\Big|\; \operatorname{lcm}(a,b)\operatorname{lcm}(b,c)\operatorname{lcm}(c,a).$$

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

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

Note that

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

On the other hand,

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

Lemma. If $x, y, z \ge 0$, then

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

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

Therefore, we may assume without loss of generality that

$$x \ge y \ge z.$$

Then the inequality becomes

$$\begin{aligned}
2x &\le x + y + x\\
&= 2x + y\\
\iff y &\ge 0,
\end{aligned}$$

which is true. □

Apply this lemma to

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

completes the proof.

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

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

then

$$a = b.$$

Solution. 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.

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

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

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

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

2.9 Oct 5, (Ir)rationality

Def. A rational number is any element of the set

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

Theorem 11. $\sqrt{2}$ *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

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

The left hand side is odd while the right hand side is even. Therefore, $\sqrt{2}$ is irrational.

□

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

Solution. Assume to the contrary that

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

Then

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

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

Recollections on e

$$\log x := \int_1^x \frac{dt}{t}.$$

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

$$\log e = 1, i.e. \int_1^e \frac{dt}{t} = 1.$$

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 12. *e is irrational.*

Proof. (Fourier). Assume to the contrary that

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

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

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

We also have $S < 1$ since

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

Since there are no integers S such that $0 < S < 1$, we obtain a contradiction. Thus, e is irrational, as requires. □

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

Theorem 13. *π is irrational.*

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

Assume to the contrary that

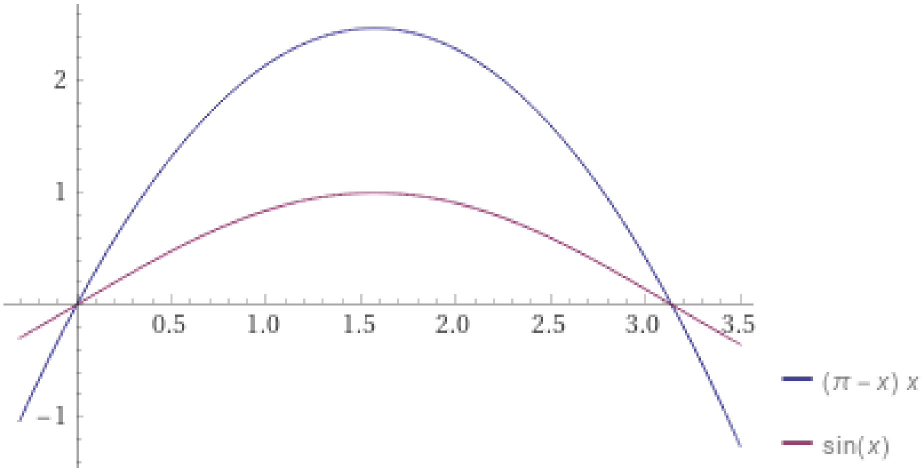
$$\pi = \frac{a}{b}, a, b \in \mathbb{N}.$$

Consider

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

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

Similarly for $\sin x$.



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,

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

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

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

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

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 $u = f(x)$, $dv = \sin x dx$ to obtain

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

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. □

2.10 Oct 7, Counting primes

2.10.1 Sketch of solution to last bonus problem

Problem. Suppose $s, t \in \mathbb{N}, s \neq t, s.t.$

$$s^2 + st + t^2 \mid st(s + t)$$

Then we want to show that $|s - t| \geq \sqrt[3]{st}$

Solution. Let $g := \gcd(s, t)$. Then $\gcd(\frac{s}{g}, \frac{t}{g}) = 1$.

Write

$$\begin{aligned} s &= gx \\ t &= gy. \end{aligned}$$

Then $\gcd(x, y) = 1$.

We have that

$$\begin{aligned}\frac{st(s+t)}{s^2+st+t^2} &= \frac{g^3xy(x+y)}{g^2(x^2+xy+y^2)}\\ &= \frac{gxy(x+y)}{x^2+xy+y^2}\end{aligned}$$

is an integer, i.e.

$$x^2 + xy + y^2 \mid gxy(x + y).$$

If we show that $\gcd(x^2 + xy + y^2, xy(x + y)) = 1$, then we will have

$$x^2 + xy + y^2|g$$

and so

$$x^2 + xy + y^2 \leq g.$$

(Using the fact that $(a \mid bc, \gcd(a, b) = 1) \implies (a \mid c)$) Let me show that

$$\gcd(x^2 + xy + y^2, x) = 1$$

and leave the other situations to you. Indeed,

$$\begin{aligned}\gcd(x^2 + xy + y^2, x) &= \gcd(x(x + y) + y^2, x)\\ &= \gcd(y^2, x)\\ &= 1.\end{aligned}$$

The latter is 1 because of, for example, the following argument. If p is a prime s.t.

$$p \mid y^2, x,$$

then $p \mid y, x$ while $\gcd(x, y) = 1$. So no such prime p can exist.

Consequently,

$$x^2 + xy + y^2 \leq g$$

Note that

$$\begin{aligned}&x^2 + y^2 \geq 2xy\\ \iff &x^2 - 2xy + y^2 \geq 0\\ \iff &(x - y)^2 \geq 0\end{aligned}$$

So

$$g \geq 3xy$$

Then

$$\begin{aligned}
\mid s-t \mid^3 &= g^3 \mid x-y \mid^3 \\
&\geq g^3 \\
&= g^2 \cdot g \\
&\geq 3g^2xy \\
&= 3(gx)(gy) \\
&= 3st \\
&\implies \mid s-t \mid \geq \sqrt[3]{3st}.
\end{aligned}$$

Note that we have shown an even stronger conclusion.

2.10.2 Counting primes

Theorem 14. *(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 14.1. *Order the primes $p_1 = 2 < p_2 = 3 < p_3 < \cdots$. Then*

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

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

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

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. □

Let

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

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

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

The following is the celebrated Prime Number Theorem.

Theorem 15. *(Hadamard, indep. de la Vallée Poussin late 1800s.)*

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

i.e.

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

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

Proof. We use strong induction on k.

$$\begin{aligned} p_1 &= 2 < 2^{2^1}, \\ p_2 &= 3 < 2^{2^2}. \end{aligned}$$

Assume it is true for $1 \leq k \leq n$.

Using

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

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 16.

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

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

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

From the previous proposition,

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

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

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

On the other hand,

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

and if $n > 3$, then

$$\begin{aligned} e^{n-1} &\geq 2^n && (2) \\ \iff \left(\frac{e}{2}\right)^n &\geq e \text{ (for } n > 3). \end{aligned}$$

Therefore, from (0), (1) and (2), we obtain for $n > 3$

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

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

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

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 17.

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

Corollary 17.1.

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

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

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

□

Notation. 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

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

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 $k \leq n$, $p_i \leq n$. Therefore,

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

is a factor of

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

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,

$$\prod_{p \text{ prime},\ p \leq n} \Big(\frac{1}{1-\frac{1}{p}}\Big) \geq \sum_{k=1}^{n} \frac{1}{k}.$$

In the following, p is always implicitly a prime number. We have this chain of (in)equalities:

$$\begin{aligned}
-\sum_{p\leq n}\log(1-\frac{1}{p}) &= \log\prod_{p\leq n}(1-\frac{1}{p})^{-1} \\
&\geq \log(\sum_{k=1}^{n}\frac{1}{k}) \\
&\geq \log\left(\int_1^n \frac{1}{t}\,dt\right) \\
&= \log(\log n).
\end{aligned}$$

On the other hand, it can be shown that

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

Indeed, recall the Taylor expansion

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

Using this, we obtain

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

Note that

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

I will show that

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

We have the inequalities

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

This settles inequality (5). Hence, we have

$$\sum_{p\ \mathrm{prime}\leq n}\frac{1}{p}+\frac{1}{2}>\log(\log n),$$

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

2.11 Oct 10, Counting primes continued

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,

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

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

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?

Question 1. *Let $x \in \mathbb{N}$, and let $m := \pi(x)$. Write $\{p \text{ prime} \leq x\} = \{p_1, \cdots, p_m\}$.*

How many natural number n such that $1 \leq n \leq x$ have all their prime divisors among $\{p_1, \cdots, p_m\}$?

Answer 1. *x. This is because every natural number $1 \leq n \leq x$ has all its prime divisors at most x and so among $\{p_1, \ldots, p_m\}$.*

Now, let us bound the number of such natural numbers, x, from above as follows. Given $1 \leq n \leq x$,

$$n = r^2 \cdot s,$$

where $r \in \mathbb{N}$, s is a product of distinct prime number. Every natural number n may be written in this form.

e.g. If

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

e.g.

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

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,

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

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

$$\begin{aligned} \frac{1}{2} \log x &\leq \pi(x) \log 2 \\ \Longrightarrow \pi(x) &\geq \frac{\log x}{2 \log 2} \end{aligned}$$

This lower bound is better than the lower bound $\log(\log(x))$. By the prime number theorem, for sufficiently large x,

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

Question 2. *Can we prove that for say $x \geq 6$ that there is a constant $c > 0$ s.t. $\pi(x) \geq \frac{cx}{\log x}$?*

This would be even better than the last lower bound we found for $\pi(x)$.

Consider the function

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

e.g.

$$\begin{aligned} \psi(8) &= \log 2 + \log 2 + \log 2 + \log 3 + \log 5 + \log 7 \\ &= \log(2^3 \cdot 3 \cdot 5 \cdot 7) \end{aligned}$$

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

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

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,

$$x(1-x)\leq\frac{1}{4}$$

$$\implies x^n(1-x)^n\leq(\frac{1}{4})^n$$

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

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

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

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

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

Theorem 18. *For $x \geq 6$, we have*

$$\pi(x) \geq \frac{x\log 2}{2\log x}.$$

2.12 Oct 12, Counting primes continued

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

$$\begin{aligned} 0.99 &< \frac{\pi(x)}{\frac{x}{\log x}}\\ \implies \pi(x) &> 0.99\frac{x}{\log x} \qquad \text{for } x \text{ large enough}\end{aligned}$$

Notation.

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

Observation.

$$\prod_{\substack{p\, prime \\ n<p\le 2n}} \Bigg| \binom{2n}{n}.$$

Note that

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

Any prime p s.t. $n < p \le 2n$ does not divide the denominator, while it divides the numerator.

Using the general fact that

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

we obtain

$$\prod_{n<p\le 2n} p \,\Bigg|\, \binom{2n}{n}.$$

This implies that

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

(Using general fact that $a, b \in \mathbb{N}, a \mid b \implies a \le b$)

Using

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

we have

$$\binom{2n}{n} \le 2^{2n}. \tag{2}$$

Combining (1) and (2), we obtain

$$\prod_{n<p\le 2n} p \le 2^{2n}.$$

Taking logs, we have

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

Let's introduce the function

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

(3) may be written as

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

$$\implies \theta(2n)-\theta(n)\le 2n\log 2, \tag{*}$$

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

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

Proof. We induct on r.

If $r=1$, then

$$\theta(2)=\log 2, \tag{4}$$

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

If we have

$$\theta(2^k)\le 2^{k+1}\log 2 \tag{5}$$

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

$$\begin{aligned}\theta(2^{k+1})&\le\theta(2^k)+2\cdot 2^k\log 2\\ &\overset{(5)}{\le} 2^{k+1}\log 2+2^{k+1}\log 2\\ &=2^{(k+1)+1}\log 2.\end{aligned}$$

The conclusion follows from induction. □

Given $x\ge 2$, choose $r\in\mathbb{N}$ s.t.

$$2^r\le x<2^{r+1}.$$

From this, we obtain

$$\begin{aligned}\theta(x)&\le\theta(2^{r+1})\\ &\le 2^{r+2}\log 2 \text{ (by lemma)}\\ &=4(\log 2)\cdot 2^n\\ &\le 4x\log 2.\end{aligned}$$

In particular,

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

The LHS of (6) is at least

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

(6) combined with (7) implies that

$$\frac{1}{2}(\log x)\big(\pi(x)-\pi(\sqrt{x})\big) \le 4x\log 2.$$

$$\begin{aligned}
\implies \pi(x)-\pi(\sqrt{x}) &\le \frac{8x\log 2}{\log x}\\
\implies \pi(x) &\le \frac{8x\log 2}{\log x} + \pi(\sqrt{x})\\
&\le \frac{8x\log 2}{\log x} + \sqrt{x}
\end{aligned}$$

Question. When is

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

If this is to be true, we must have

$$\frac{\log x}{\log 2} \le \sqrt{x}, \text{ i.e. } \sqrt{x}\log 2 - \log x \ge 0$$

Let

$$f(x) := \sqrt{x}\log 2 - \log x.$$

For which x is $f'(x) \ge 0$?

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

$$\begin{aligned}
f'(x)\ge 0 &\iff \frac{\log 2}{2\sqrt{x}} \ge \frac{1}{x}\\
&\iff \sqrt{x} \ge \frac{2}{\log 2}\\
&\iff x \ge \Big(\frac{2}{\log 2}\Big)^2 \text{ For } x \ge 8.32...
\end{aligned}$$

Therefore

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

for $x \geq 10$.

We conclude that

$$\pi(x) \leq \frac{8x \log 2}{\log x} + \sqrt{x} \leq \frac{9x \log 2}{\log x}$$

for $x \geq 10$. We can also check that the final inequality is also true for $2 \leq x < 10$. We have, therefore, proved the following theorem.

Theorem 19. *For $x \geq 2$ we have*

$$\pi(x) \leq \frac{9x \log 2}{\log x}.$$

This ends our discussion of analytic methods in counting primes. We now return to algebra. Recall the following.

Theorem 20. *(Fermat's Little Theorem) If p is a prime number and $n \in \mathbb{N}$ s.t. $p \nmid n$. (i.e. $\gcd(p, n) = 1$). Then $n^{p-1} \equiv 1 \pmod{p}$, i.e.*

$$p \mid n^{p-1} - 1.$$

Example. Let $p = 5$ and $n = 3$. Then

$$3^{5-1} \equiv 1 \pmod{5}.$$

Application. What is the last digit of 3^{1001}?

Answer. Though using Fermat's Little Theorem is overkill, let us use it to find the final answer. This will be a model for other problems that cannot be easily solved without using Fermat's Little Theorem.

We want to find $3^{1001} \pmod{10}$. By the division algorithm, we may write

$$3^{1001} = 10q + r,$$

where $q, r \in \mathbb{Z}$ with $0 \leq r \leq 9$.

$$\begin{aligned} r &\equiv 10q + r \\ &= 3^{1001} \\ &\equiv 1^{1001} \\ &= 1 \pmod{2}. \end{aligned}$$

Also,

$$\begin{aligned} r &\equiv 10q + r \\ &= 3^{1001} \\ &= 3^{1000} \cdot 3 \\ &= (3^4)^{250} \cdot 3 \\ &\equiv 1^{250} \cdot 3 \\ &\equiv 3 \pmod 5, \end{aligned}$$

where $3^4 \equiv 1 \pmod 5$ follows from Fermat's Little Theorem. The only $0 \le r \le q$ satisfying the above congruences modulo 2 and 5 is 3. Therefore, the last digit of 3^{1001} is 3.

Of course, the above is too complicated in this case, as we could do the following instead.

$$3^{1001} = 3^{1000} \cdot 3 = (3^2)^{500} \cdot 3 \equiv (-1)^{500} \cdot 3 \equiv 3 \pmod{10}.$$

However, what if we want to find

$$3^{1001} \pmod{51}?$$

In the next lecture, I will start giving a proof of Fermat's Little Theorem that is better, leads to generalizations (Euler's Theorem, for example), and motivates a part of abstract algebra known as *Group Theory*.

2.13 Oct 17, Chinese Remainder Theorem

Problem. What is the last digit of 3^{1001}?

Solution. The remainder of 3^{1001} divided by 10 is one of $0, 1, 2, \cdots, 9$.

$$\begin{aligned} & r \equiv 3^{1001} \pmod{10} \\ \Longrightarrow\ & r \equiv 3^{1001} \pmod 5 \text{ and } r \equiv 3^{1001} \pmod 2 \end{aligned}$$

By Fermat's Little Theorem,

$$3^{5-1} \equiv 1 \pmod 5.$$

Therefore,

$$\begin{aligned} r &\equiv 3^{1001} = 3^{4\cdot 250+1} \\ &= (3^4)^2 50 \cdot 3 \equiv 1^2 50 \cdot 3 \\ &\equiv 3 \pmod 5. \end{aligned}$$

We also have that

$$r \equiv 1 \pmod 2.$$

Warning. When dealing with powers when working mod n, you can't reduce the power mod n!

$$\begin{aligned} 3^5 &\equiv 3 \pmod 5 \\ 3^0 &\equiv 1 \pmod 5 \\ \implies 3^5 &\not\equiv 3^0 \pmod 5 \end{aligned}$$

Problem. What is the last digit of 2^{1002}?

Solution. We want to find

$$2^{1002} \pmod{10}.$$

By Fermat's Little Theorem, $2^4 \equiv 1 \pmod 5$.

Therefore, $2^{1002} \equiv (2^4)^{250} \cdot 2^2 \equiv 1^{250} \cdot 2^2 \equiv 4 \pmod 5$.

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 example,

$$2^{1002} \pmod{51}.$$

Lemma. Suppose $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Then

$$ax \equiv b \pmod n \qquad (\dagger)$$

has a solution if and only if

$$d := \gcd(a, n) \mid b.$$

In fact, modulo n, there are exactly d solutions.

Proof. Finding x s.t.

$$ax \equiv b \pmod n$$

is equivalent to solving the equation

$$\begin{aligned} &ax - b = ny, y \in \mathbb{Z} \\ \implies &ax - ny = b \qquad (*) \end{aligned}$$

This has integer solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ if and only if

$$d := \gcd(a, n) \mid b$$

(Essentially, Bézout's Theorem).

Recall that if (x_0, y_0) is a solution of $(*)$, then <u>all</u> integer solutions are of the form

$$\begin{array}{l} x = x_0 + \frac{n}{d}t \\ y = y_0 - \frac{a}{d}t \end{array}, t \in \mathbb{Z}$$

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 (†).

Why are they distinct modulo n?

Assume to the contrary that

$$n \Bigm| (x_0 + \frac{in}{d}) - (x_0 + \frac{jn}{d}),$$

where $0 \le i, j \le d-1$ and $i \ne j$.

Then

$$n \Bigm| (i-j)\frac{n}{d}.$$

However, note that

$$\left|(i-j)\frac{n}{d}\right| \le \frac{d-1}{d} \cdot n < n.$$

n can't divide a natural number less than n.

If

$$x_0 + \frac{n}{d}t$$

is a solution, then we can use the division algorithm, to write

$$t = qd + r, 0 \le r \le d-1,$$

from which it follows that

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + \frac{nr}{d} + nq.$$

□

Corollary 20.1. *a, n as before. 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* mod n.

2.13.1 Chinese Remainder Theorem.

Theorem 21. *Chinese Remainder Theorem*

Suppose $n_1, n_2, \cdots, n_k$ are natural numbers s.t.

$$\forall i \neq j, \gcd(n_i, n_j) = 1.$$

Also, let $a_1, \cdots a_k \in \mathbb{Z}$.

Then the system of congruences

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has a unique solution modulo $n_1 n_2 \cdots n_k$.

Suppose

$$\begin{cases} r \equiv 3 \pmod 5 \\ r \equiv 1 \pmod 2. \end{cases}$$

Then $r \equiv 3 \pmod{10}$ was the unique solution mod $10 = 2 \cdot 5$.

Proof. Why must a solution exist?

Let

$$N_1 = \frac{n_1 \cdots n_k}{n_1}$$
$$\vdots$$
$$N_k = \frac{n_1 \cdots n_k}{n_k}$$

Note that

$$\gcd(N_1, n_1) = \cdots = \gcd(N_k, n_k) = 1.$$

By the corollary, there are $x_1, \cdots, x_k \in \mathbb{Z}$ s.t.

$$N_1 x_1 \equiv 1 \pmod{n_1}$$
$$\vdots$$
$$N_k x_k \equiv 1 \pmod{n_k}$$

Then let

$$x = a_1 N_1 x_1 + \cdots + a_k N_k x_k.$$

Then since $n_1 | N_2, \ldots, N_k$,

$$\begin{aligned} x &\equiv a_1 N_1 x_1 + 0 + \cdots + 0 \pmod{n_1} \\ &\equiv a_1 \cdot 1 \pmod{n_1} \\ &= a_1 \pmod{n_1}. \end{aligned}$$

Similarly, we can show that $x \equiv a_2 \bmod N_2, \ldots, x \equiv a_k \bmod n_k$.

To show uniqueness of the solution modulo $n_1 \cdots n_k$, 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,

$$\begin{aligned} n_1 &\mid x' - x'' \\ n_2 &\mid x' - x'' \\ &\vdots \\ n_k &\mid x' - x''. \end{aligned}$$

Since for every $i \neq j$, $\gcd(n_i, n_j) = 1$,

$$n_1 \cdots n_k \,\Big|\, x' - x'',$$

i.e.

$$x' \equiv x'' \pmod{n_1 \cdots n_k}.$$

This means that x' and x'' are the same modulo n, as required. □

Problem. 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 s.t.

$$N_1 x_1 = 15 x_1 \equiv 1 \pmod{2}$$

Note that $15x_1 \equiv x_1 \pmod{2}$. So $x_1 = 1$ is a solution. We also want x_2 s.t.

$$N_2 x_2 = 10 x_2 \equiv 1 \pmod{3}.$$

Again,

$$1 \equiv 10x_2 \equiv x_2 \pmod{3},$$

and so we can take $x_2 = 1$.

Finally, we want x_3 s.t.

$$N_3x_3 = 6x_3 \equiv 1 \pmod{5} \implies x_3 \equiv 1 \pmod{5}.$$

Therefore, we can take $x_3 = 1$.

Then

$$\begin{aligned} x &= a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 \\ &= 1 \cdot 3 \cdot 5 \cdot 1 + 2 \cdot 2 \cdot 5 \cdot 1 + 3 \cdot 2 \cdot 3 \cdot 1 \\ &= 15 + 20 + 18 = 53. \end{aligned}$$

Therefore, $x \in \mathbb{Z}$ s.t.

$$x \equiv 53 \equiv 23 \pmod{30}$$

are all the solutions.

Problem. There are 17 thieves who rob a bank. They try to divide the dollar equally amongst themselves, but 3 dollar remains. Along the way, one of them dies. When they return to the hiding place, they try a gain, but 10 dollars 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 minimum number of dollars they stole?

Solution. 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

$$\begin{aligned} N_1 &= 16 \cdot 15 \\ N_2 &= 17 \cdot 15 \\ N_3 &= 17 \cdot 16 \end{aligned}$$

We want to find $x_1, x_2, x_3 \in \mathbb{N}$ s.t.

$$\begin{aligned} 16 \cdot 15x_1 &= N_1x_1 \equiv 1 \pmod{17} \\ 17 \cdot 15x_2 &= N_2x_2 \equiv 1 \pmod{16} \\ 17 \cdot 16x_3 &= N_3x_3 \equiv 1 \pmod{15}. \end{aligned}$$

$$\begin{aligned} & 1 \equiv 16 \cdot 15x_1 \equiv (-1) \cdot (-2)x_1 \pmod{17} \\ \iff & 2x_1 \equiv 1 \pmod{17} \\ \implies & x_1 \equiv 18x_1 = 9 \cdot 2x_1 \equiv 9 \pmod{17} \end{aligned}$$

Take $x_1 = 9$.

$$\begin{aligned} & 1 \equiv 17 \cdot 15x_2 \equiv 1 \cdot (-1)x_2 \pmod{16} \\ \implies & x_2 \equiv -1 \equiv 15 \pmod{16} \end{aligned}$$

Take $x_2 = 15$.

$$\begin{aligned} & 1 \equiv 17 \cdot 16x_3 \equiv 2 \cdot 1x_3 \equiv 2x_3 \pmod{15} \\ \implies & x_3 \equiv 16x_3 \equiv 8(2x_3) \equiv 8 \pmod{15} \end{aligned}$$

Take $x_3 = 8$.

Then all solutions are congruent to

$$\begin{aligned} x &= a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 \\ &= 3 \cdot 16 \cdot 15 \cdot 9 + 10 \cdot 17 \cdot 15 \cdot 15 + \underbrace{0}_{=a_3} \cdots \end{aligned}$$

modulo $17 \cdot 16 \cdot 15$.

Equivalently,

$$d \equiv 3930 \pmod{4080}$$

The smallest such $d \in \mathbb{N}$ is $\underline{3930}$.

Another solution:

$$\begin{cases} d \equiv 3 \pmod{17} \\ d \equiv 10 \pmod{16} \\ d \equiv 0 \pmod{15} \end{cases}$$

From the last equation,

$$d = 15x \text{ for some } x \in \mathbb{Z}$$

From the second equation,

$$\begin{aligned} & 15x = d \equiv 10 \pmod{16} \\ \iff & -x \equiv 10 \pmod{16} \\ \iff & x \equiv -10 \equiv 6 \pmod{16} \end{aligned}$$

This implies that

$$\begin{aligned}
&x = 16y + 6 \text{ with } y \in \mathbb{Z}\\
\implies &d = 15x = 15(16y + 6)\\
\implies &d = 15 \cdot 16y + 90
\end{aligned}$$

From the first equation,

$$15 \cdot 16y + 90 = d \equiv 3 \pmod{17}.$$

Therefore,

$$\begin{aligned}
&15 \cdot 16y \equiv 3 - 90 \pmod{17}\\
\implies &2y \equiv -87 \pmod{17}\\
\implies &2y \equiv -2 \pmod{17}\\
\implies &y \equiv -1 \equiv 16 \pmod{17}\\
\implies &y = 17z + 16 \text{ with } z \in \mathbb{Z}.
\end{aligned}$$

Then

$$\begin{aligned}
d &= 15 \cdot 16y + 90\\
&= 15 \cdot 16(17z + 16) + 90\\
&= 15 \cdot 16 \cdot 17z + (15 \cdot 16^2 + 90).
\end{aligned}$$

2.14 Oct 21

Recall the following proposition:

Proposition 18. *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* <u>*unique*</u> *solution modulo n.*

Moral of this proposition is that you can "invert" a modulo if and only if $\gcd(a, n) = 1$.

e.g.

$$5x \equiv 1 \pmod{3}.$$

If $x \equiv 2 \pmod{3}$, then

$$5x \equiv 5 \cdot 2 = 10 \equiv 1 \pmod{3}$$

When $\gcd(a, n) = 1$, we can speak of a^{-1} mod n. In the above situation, $5^{-1} \equiv 2 \pmod{3}$.

e.g.

$$7x \equiv 1 \pmod 9.$$

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 the Euclidean algorithm, then solving $7x \equiv -1 \pmod 9$ is more or less the same as solving

$$7x - 1 = 9y \iff 7x - 9y = 1$$

2.14.1 New proof of Fermat's Little Theorem

Consider a prime p and the numbers

$$1, 2, 3, \cdots, p-1.$$

If you take $x \in \mathbb{Z}$ s.t. $p \nmid x$, then

$$x = pq + r, \;\; 0 < r \leq p - 1$$

In order to prove that if $p \nmid a$ then

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

What we can do is consider

$$a, 2a, 3a, \cdots, (p-1)a \pmod p$$

Claim. $a, 2a, 3a, \cdots, (p-1)a$ 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 they are distinct modulo p.

None of them is divisible by p because $p \nmid a$ and $p \nmid i$ for any $1 \leq i \leq p-1$.

They are also all distinct modulo p.

Otherwise, we can find $1 \leq i, j \leq p-1$ s.t. $i \neq j$ and

$$ai \equiv aj \pmod p \tag{1}$$

However, $\gcd(a,p)=1$, so there exists a^{-1} (mod p), and so

$$\begin{aligned} i &\equiv 1\cdot i \equiv (a^{-1}a)\cdot i \equiv a^{-1}(a\cdot i) \\ &\equiv a^{-1}(a\cdot j) \equiv 1\cdot j \equiv j \pmod{p} \end{aligned}$$

Since $\gcd(a,p)=1$, there is an x s.t.

$$ax \equiv 1 \pmod{p}.$$

Multiply 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 $1 \le i, j \le p-1$, $i = j$. □

Now since $a, 2a, \cdots, (p-1)a$ are exactly $1, 2, \cdots, p-1$ modulo p.

We have

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

i.e.

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

Since p is a prime, $p \nmid (p-1)!$. Therefore, $(p-1)!$ is invertible modulo p.

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

as required.

We now discuss Euler's Theorem, a generalization of Fermat's Little Theorem.

Def. The Euler totient function φ is given by

$$\varphi(n) := \#\{a \in N \mid 1 \le a \le n \text{ and } \gcd(a,n)=1\}$$

e.g.

$$\begin{aligned} \varphi(3) &= \#\{1 \le a \le 3 \text{ s.t. } \gcd(a,3)=1\} \\ &= \#\{1,2\} \\ &= 2 \end{aligned}$$

More generally, if p is a prime number, then

$$\begin{aligned} \varphi(p) &= \#\{1 \le a \le p \mid \gcd(a,p)=1\} \\ &= \#\{1,2,\cdots,p-1\} \\ &= p-1. \end{aligned}$$

e.g.

$$\begin{aligned}\varphi(4) &= \#\{1 \leq a \leq 4 : \gcd(a,4) = 1\}\\ &= \#\{1,3\}\\ &= 2\end{aligned}$$

Euler generalized Fermat's Little Theorem as follows:

Theorem 22. *[Euler] If $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ s.t. $\gcd(a,n) = 1$, then*

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

If $n = p$ is a prime number, then

$$\gcd(a,p) = 1 \implies a^{\varphi(p)} \equiv 1 \pmod{p}$$

Proof of Euler's Theorem 22. Consider $\{a_1, \cdots, a_{\varphi(n)}\} = \{a \in \mathbb{N} \mid 1 \leq a \leq n, \gcd(a,n) = 1\}$.

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 that same as

$$a_1, \cdots, a_{\varphi(n)}.$$

Therefore,

$$(aa_1)\cdots(aa_{\varphi(n)}) \equiv a_1 \cdots a_{\varphi(n)} \pmod{n}$$

But then

$$a^{\varphi(n)} a_1 \cdots a_{\varphi(n)} \equiv a_1 \cdots a_{\varphi(n)} \pmod{n}$$

and so

$$n \Bigm| a_1 \cdots a_{\varphi(n)}(a^{\varphi(n)} - 1).$$

□

2.15 Oct 24

How to compute $\varphi(n)$ in general? Consider

$$\frac{\varphi(n)}{n} = \mathbb{P}[1 \leq a \leq n \mid \gcd(a,n) = 1].$$

Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factors of n.

Then the probability that $1 \leq a \leq n$ and $p_i \nmid a$ is $1 - \frac{1}{p_i}$. This is true for each p_i, and so

$$\begin{aligned}\frac{\varphi(n)}{n} &= (1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})\\ \implies \varphi(n) &= n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).\end{aligned}$$

e.g.

$$\begin{aligned}\varphi(3^3) &= 3^3(1-\frac{1}{3})\\ &= 3^2(3-1)\\ &= 18.\end{aligned}$$

Proof of proposition. An argument is probabilistic. Note that

$$\frac{\varphi(n)}{n} = \mathbb{P}[1 \le a \le n \mid \gcd(a,n)=1]$$

A number $1 \le a \le n$ is relatively prime to $n \iff p_1 \nmid a, p_2 \nmid a, \cdots, p_k \nmid a$. The probability that $p_i \nmid a$ is 1 minus the probability that $p_i \mid a$, i.e.

$$1 - \frac{n/p_i}{n} = 1 - \frac{1}{p_i}.$$

Go through all primes less or equal to n. Hence we can get

$$\begin{aligned}\frac{\varphi(n)}{n} &= (1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})\\ \implies \varphi(n) &= n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).\end{aligned}$$

as required. □

Problem.

$$\text{What is } 2^{1003} \equiv \pmod{45}?$$

Solution. $\gcd(2,45)=1$. By Euler's theorem,

$$2^{\varphi(45)} \equiv 1 \pmod{45}$$

$$\begin{aligned}\varphi(45) &= \varphi(3^2\cdot 5)\\ &= 3^2\cdot 5(1-\frac{1}{3})(1-\frac{1}{5})\\ &= 3^2\cdot 5(\frac{2}{3})(\frac{4}{5})\\ &= 3\cdot 2\cdot 4\\ &= 24.\end{aligned}$$

And so

$$2^{24} \equiv 1 \pmod{45}.$$

Question. How can we write

$$1003 = 24q + r,\ 0 \leq r \leq 23.$$

Solution. Take $q = 41, r = 19$. So

$$\begin{aligned} 2^{1003} &= 2^{24 \cdot 41 + 19} \\ &= (2^{24})^{41} \cdot 2^{19} \pmod{45} \\ &\equiv 2^{19} \pmod{45} \end{aligned}$$

Let's find $2^{19} \pmod{45}$. Then let's find

$$2^{19} \pmod{3^2}$$

and

$$2^{19} \pmod{5}.$$

$$2^{\varphi(3^2)} \equiv 1 \pmod{3^2} \text{ by Euler's theorem}$$

and

$$\varphi(3^2) = 3^2(1 - \frac{1}{3}) = 6.$$

$19 = 3 \cdot 6 + 1$ and so

$$2^{19} = 2^{3 \cdot 6 + 1} = (2^6)^3 \cdot 2 \equiv 2 \pmod{9}.$$

By FLT,

$$2^4 \equiv 1 \pmod{5}.$$

$19 = 4 \cdot 4 + 3$, and so

$$2^{19} = 2^{4 \cdot 4 + 3} = (2^4)^4 \cdot 2^3 \equiv 2^3 \equiv 3 \pmod{5}.$$

By the CRT (Chinese Remainder Theorem), there is a unique solution modulo 45 to

$$x \equiv 2 \pmod{9}$$

$$x \equiv 3 \pmod{5}$$

Let $N_1 = 5, N_2 = 9$.

Then we want to find x_1 and x_2 s.t.

$$5x_1 \equiv N_1 x_1 \equiv 1 \pmod{9} \tag{1}$$

$$9x_2 \equiv N_2 x_2 \equiv 1 \pmod{5} \tag{2}$$

Multiply (1) by 2 to get

$$x_1 \equiv 10x_1 \equiv 2 \pmod{9}.$$

Take $x_1 = 2$.

Note that $9 \equiv -1 \pmod{5}$ so (2) is equiv 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.

Theorem 23 (Wilson)**.** *If p is a prime number, then*

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

Recall the following: if $\gcd(a, p) = 1$, then

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

has a unique solution mod p.

Solution. Write

$$(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$$

Whenever $x \in \{1, 2, \cdots, p-1\}$ and $x^2 \not\equiv 1 \pmod{p}$, you can find a $y \in \{1, 2, \cdots, p-1\}$ s.t. $y \neq x$ and $xy \equiv 1 \pmod{p}$.

Which ones can't be paired with another number?

Exactly those x s.t.

$$x^2 \equiv 1 \pmod{p}$$

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,

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

Note that when $p = 2$, we have

$$(2-1)! = 1 \equiv -1 \pmod{2}.$$

Theorem 24. *Suppose p is an odd prime number. Then*

$$x^2 \equiv -1 \pmod{p}$$

has a solution if and only if

$$p \equiv 1 \pmod{4}.$$

2.16 Oct 26

Proof. By Wilson's theorem, we know that

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

Note that

$$(p-1)! = 1 \cdot 2 \cdots (\frac{p-1}{2}) \cdot (\frac{p+1}{2}) \cdots (p-1).$$

$$\begin{aligned}\frac{p+1}{2} &= p - \frac{p-1}{2} \equiv -(\frac{p-1}{2}) \pmod{p} \\ \frac{p+3}{2} &= p - \frac{p-3}{2} \equiv -(\frac{p-3}{2}) \pmod{p} \\ &\vdots \\ p-1 &= p-1 \equiv -1 \pmod{p}\end{aligned}$$

Consequently,

$$\begin{aligned}(p-1)! &\equiv 1\cdot 2\cdots(\frac{p-1}{2})\cdot(-1)\cdot(-2)\cdots(-(\frac{p-1}{2}))\\ &\equiv(-1)^{\frac{p-1}{2}}[1\cdot 2\cdots(\frac{p-1}{2})]^2 \pmod{p}.\end{aligned}$$

Since $p\equiv 1 \pmod{4}$, $\frac{p-1}{2}$ is even!

We have deduced that when $p\equiv 1 \pmod{4}$,

$$(p-1)!\equiv[(\frac{p-1}{2})!]^2 \pmod{p}.$$

By Wilson's theorem, this is $\equiv -1 \pmod{p}$.

One direction of the theorem is proved. □

When $p=5$, the proof boils down to the following computation:

$$\begin{aligned}-1 &\equiv (5-1)! = 1\cdot 2\cdot 3\cdot 4 \pmod{5}\\ &= (1\cdot 2)(5-2)(5-1)\\ &\equiv (1\cdot 2)(-2)(-1)\\ &\equiv (-1)^{\frac{5-1}{2}}(2!)^2 = 2^2 \pmod{5}\end{aligned}$$

The other direction say that if p is an odd prime number and

$$x^2\equiv -1 \pmod{p}$$

has a solution, then $p\equiv 1 \pmod{4}$. We need to introduce the notion of orders to prove this.

Def. Suppose $n\in\mathbb{N}$ and $a\in\mathbb{Z}$ s.t. $\gcd(a,n)=1$. Then the order of a modulo n is the smallest $k\in\mathbb{N}$ s.t.

$$a^k\equiv 1 \pmod{n}.$$

⋆ **Warning:** Fermat's Little theorem and Euler's Theorem do not necessarily provide the smallest power k for which $a^k\equiv 1 \pmod{n}$.

e.g. 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 25. *a,n as before. Then let $\operatorname{ord}_n(a)$ be the order of a modulo n. ($\operatorname{ord}_n(a)\in\mathbb{N}$ smallest such that $a^{\operatorname{ord}_n(a)}\equiv 1 \pmod{n}$)*

If $a^m\equiv 1 \pmod{n}$, then

$$\operatorname{ord}_n(a)\bigm| m.$$

Proof. Assume to the contrary that

$$\mathrm{ord}_n(a) \nmid m.$$

This assumption, combined with the division algorithm, implies that

$$m = \mathrm{ord}_n(a)q + r,\ q, r \in \mathbb{Z}, 0 < r < \mathrm{ord}_a(n)$$

We then have

$$\begin{aligned} 1 &\equiv a^m = a^{\mathrm{ord}_n(a)q+r} \pmod n \\ &= (a^{\mathrm{ord}_n(a)})^q \cdot a^r \pmod n \\ &\equiv 1^q \cdot a^r = a^r \pmod n. \end{aligned}$$

Since $0 < r < \mathrm{ord}_a(n)$, this contradicts the minimality of $\mathrm{ord}_n(a)$.

The conclusion follows. □

To prove the other direction, note that $x^2 \equiv -1 \bmod p$ implies that $x^4 \equiv 1 \bmod p$. Therefore, the order of x modulo p divides 4. Consequently, it is 1, 2, or 4. It is not 1 or 2 as $x^2 \equiv -1 \not\equiv 1 \bmod p$ (p is odd). The order of x is, therefore, 4. On the other hand, by Fermat's Little Theorem, we have $x^{p-1} \equiv 1 \bmod p$ (not that since $x^2 \equiv -1 \bmod p$, $\gcd(x, p) = 1$). By the previous theorem, we must have $4|p - 1$, that is, $p \equiv 1 \bmod 4$, as required.

2.16.1 Reformulation of Fermat's Little Theorem

Suppose p is a prime number.

Consider the sets

$$\begin{aligned} \overline{0} &= p\mathbb{Z} = \{\cdots, -2p, -p, 0, p, 2p, 3p, \cdots\} \\ \overline{1} &= 1 + p\mathbb{Z} = \{\cdots, 1-2p, 1-p, 1, 1+p, 1+2p, 1+3p, \cdots\} \\ &\vdots \\ \overline{p-1} &= (p-1) + p\mathbb{Z} \\ \overline{p} &= \overline{0} \end{aligned}$$

Recall the following:

$$\left\{ \begin{array}{l} a \equiv b \pmod p \\ c \equiv d \pmod p \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} a + c \equiv b + d \pmod p \\ ac \equiv bd \pmod p \end{array} \right.$$

So we have

$$\left\{ \begin{array}{l} \overline{a} \equiv \overline{b} \\ \overline{c} \equiv \overline{d} \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} \overline{a+c} \equiv \overline{b+d} \\ \overline{ac} \equiv \overline{bd} \end{array} \right.$$

From $\overline{0}, \overline{1}, \cdots, \overline{p-1}$, let's keep only those elements $\overline{a}$ s.t. there is an $\overline{x}$ satisfying

$$\overline{ax} = \overline{a}\,\overline{x} = \overline{1} \iff ax \equiv 1 \pmod{p}.$$

Note that for any $\overline{a} \in \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$,

$$\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}.$$

The "invertible" $\overline{a}$ are precisely those a a.t. $\gcd(a, p) = 1$.

Therefore, every element of

$$(\mathbb{Z}/p\mathbb{Z})^{\times} := \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$$

has an inverse. We also have that

$$(\overline{a} \cdot \overline{b})\overline{c} = \overline{abc} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$$

(associativity).

Def. A group $(G, *)$ is a set G with a binary operation

$$* : G \times G \to G$$

satisfying

1. There is a distinguished element $1 \in G$ s.t. for every $g \in G, 1{*}g = g{*}1 = g$.
2. $*$ is associative.

$$a * (b * c) = (a * b) * c \text{ for every } a, b, c \in G$$

3. For every $g \in G$ there is $x \in G$ such that

$$g * x = x * g = 1.$$

Theorem 26 (Lagrange)**.** *If G is a finite group with $|G|$ elements, then for every $g \in G$,*

$$g^{|G|} = 1.$$

e.g. 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 $\gcd(a, p) = 1$.

2.17 Oct 28

Suppose p is an odd prime and that

$$x^2 \equiv -1 \pmod{p}$$

has a solution. Then

$$p \equiv 1 \pmod{4}$$

Proof.

$$x^4 = (x^2)^2 \equiv (-1)^2 = 1 \pmod{p}$$

Therefore,

$$\mathrm{ord}_p(x) \mid 4 \implies \mathrm{ord}_p(x) = 1, 2, \text{ or } 4.$$

However, $x^2 \equiv -1 \not\equiv 1 \pmod{p}$ since p is odd.

Therefore, $\mathrm{ord}_p(x) = 4$.

On the other hand,

$$x^2 \equiv -1 \pmod{p} \implies \gcd(x, p) = 1.$$

Indeed, if $p \mid x$, then from $p \mid x^2 + 1$, we would obtain $p \mid 1$, a contradiction.

By Fermat's Little Theorem,

$$x^{p-1} \equiv 1 \pmod{p}.$$

Consequently,

$$4 = \mathrm{ord}_p(x) \mid p - 1 \implies p \equiv 1 \pmod{4}.$$

□

Valuations of n! (p-adic)

Question. For prime p, what is $v_p(n!)$?

Note that

$$n! = 1 \cdot 2 \cdots n$$

How many of $1, 2, 3, \cdots, n$ are divisible by p but not p^3?

Floor function definition. Given $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the largest integer $\leq x$.

e.g.

$$\lfloor 2.75 \rfloor = 2$$
$$\lfloor -1.25 \rfloor = -2$$

Lemma. The number of integers $1 \leq a \leq n$ s.t. $p \mid a$ is $\lfloor \frac{n}{p} \rfloor$.

Proof of Lemma. $p \mid a \iff \exists k \in \mathbb{Z}$ s.t.

$$a = pk.$$

We want this multiply to satisfy

$$1 \leq a = pk \leq n$$

Equivalently, we want

$$1 \leq k \leq \left\lfloor \frac{n}{p} \right\rfloor.$$

So we have $\lfloor \frac{n}{p} \rfloor$ choices for such k.

The conclusion follows. □

e.g. How many numbers among $\{1, 2, 3, 4, 5, 6, 7, 8\}$ 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 $a \in \{1, 2, \cdots, n\}$ 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 $a \in \{1, \cdots, n\}$ s.t. $v_p(a) = k$ 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 19. *p prime,*

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \cdots.$$

e.g.

$$v_2(5!) = \left\lfloor \frac{5}{2} \right\rfloor + \left\lfloor \frac{5}{2^2} \right\rfloor + \left\lfloor \frac{5}{2^3} \right\rfloor \cdots = 2 + 1 = 3$$

Another way of computing $v_p(n!)$ is as follows.

Write $n = a_k p^k + a_{k-1}p^{k-1} + \cdots + a_1 p^1 + a_0$, where $0 \leq a_i \leq p-1$. (base p expansion of n).

The proposition way 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, $s_p(n) = a_0 + \ldots + a_k$ is the sum of the digits of n in its base p expansion. Note that

$$\begin{aligned} \left\lfloor \frac{n}{p} \right\rfloor &= \left\lfloor \frac{a_k p^k + \cdots + a_1 p + a_0}{p} \right\rfloor \\ &= \left\lfloor a_k p^{k-1} + a_{k-1}p^{k-2} + \cdots + \frac{a_0}{p} \right\rfloor \\ &= a_k p^{k-1} + \cdots + a_2 + \underbrace{\left\lfloor \frac{a_0}{p} \right\rfloor}_{=0} \end{aligned}$$

$$\begin{aligned} \left\lfloor \frac{n}{p^2} \right\rfloor &= \left\lfloor \frac{a_k p^k + \cdots + a_1 p + a_0}{p^2} \right\rfloor \\ &= \left\lfloor a_k p^{k-2} = a_{k-1}p^{k-3} + \cdots + \frac{a_1 p + a_0}{p^2} \right\rfloor \\ &= a_k p^{k-2} + \cdots + a_2 + \underbrace{\left\lfloor \frac{a_1 p + a_0}{p^2} \right\rfloor}_{=0} \end{aligned}$$

Continuing in this fashion, we end with

$$\left\lfloor \frac{n}{p^k} \right\rfloor = a_k$$

Note that $\lfloor np^{k+1} \rfloor = 0$ and also for higher powers of p. Summing these, we obtain using geometric sums of the form

$$1 + p + p^2 + \ldots + p^a = \frac{p^{a+1} - 1}{p-1}$$

that

$$\begin{aligned}
v_p(n!) &= a_k(1+p+\ldots+p^{k-1})+a_{k-1}(1+p+\ldots+p^{k-2})+\ldots+a_k \\
&= a_k\left(\frac{p^k-1}{p-1}\right)+a_{k-1}\left(\frac{p^{k-1}-1}{p-1}\right)+\ldots+a_1\left(\frac{p-1}{p-1}\right) \\
&= \frac{(a_kp^k+a_{k-1}p^{k-1}+\ldots+a_1p)-(a_k+a_{k-1}+\ldots+a_1)}{p-1} \\
&= \frac{(a_kp^k+a_{k-1}p^{k-1}+\ldots+a_1p+a_0)-(a_k+a_{k-1}+\ldots+a_1+a_0)}{p-1} \\
&= \frac{n-s_p(n)}{p-1}
\end{aligned}$$

e.g.

$$\begin{aligned}
v_2(5!) &= \frac{5-s_2(5)}{2-1} \\
&= \frac{5-2}{2-1} \\
&= 3.
\end{aligned}$$

Problem. $n \in \mathbb{N}$. Then

$$n! \,\Bigg|\, \prod_{k=0}^{n-1}(2^n-2^k).$$

Proof. Recall that

$$a \mid b \iff \text{for every prime } p, v_p(a) \le v_p(b).$$

Therefore, it suffices to show that for every prime p,

$$v_p(n!) \le v_p\bigg(\prod_{k=0}^{n-1}(2^n-2^k)\bigg)$$

For $p \le 2$, we have

$$\begin{aligned}
&v_2\bigg(\prod_{k=0}^{n-1}(2^n-2^k)\bigg) \\
&\ge v_2(2^n-2^{n-1}) \\
&= v_2(2^{n-1}) \\
&= n-1.
\end{aligned}$$

On the other hand

$$\begin{aligned} v_2(n!) &= \frac{n - s_2(n)}{2-1} \\ &\leq \frac{n-1}{2-1} \\ &= n-1. \end{aligned}$$

Now suppose p is an odd prime. Since p is odd, $\gcd(z, p) = 1$.

By Fermat's Little Theorem, therefore, (if $1 \leq j(p-1) \leq n$)

$$2^{p-1} \equiv 1 \pmod{p} \implies 2^{j(p-1)} \equiv 1 \pmod{p} \text{ for any } j \in \mathbb{N}.$$

First note that

$$\begin{aligned} v_p(n!) &= \frac{n - s_p(n)}{p-1} \\ &\leq \left\lfloor \frac{n-1}{p-1} \right\rfloor. \end{aligned}$$

On the other hand,

$$2^{k(p-1)} \equiv 1 \pmod{p} \implies p \;\Big|\; 2^{k(p-1)} - 1.$$

Also, for p odd,

$$\begin{aligned} &v_p\Big(\prod_{k=0}^{n-1} (2^n - 2^k) \Big) \\ =&v_p\Big(2^0 \cdot 2^1 \cdots 2^{k-1} \prod_{k=0}^{n-1} (2^{n-k} - 1) \Big) \\ =&\underbrace{v_p\Big(2^{\frac{n(n-1)}{2}}\Big)}_{=0} + \sum_{k=1}^{n} v_p(2^k - 1). \end{aligned}$$

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. $1 \leq k = j(p-1) \leq n$.

The number of such j is at least $\lfloor \frac{n}{p-1} \rfloor$, 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

Hence,

$$\begin{aligned}
&v_p\left(\prod_{k=0}^{n-1}(2^n-2^k)\right)\\
&\geq \sum_{k=1}^{n} v_p(2^k-1)\\
&\geq \sum_{j\in\mathbb{N}:1\leq j(p-1)\leq n}^{n} v_p(2^k-1)\\
&\geq \sum_{j\in\mathbb{N}:1\leq j(p-1)\leq n}^{n} 1\\
&= \left\lfloor\frac{n}{p-1}\right\rfloor\\
&\geq \left\lfloor\frac{n-1}{p-1}\right\rfloor\\
&\geq v_p(n!)
\end{aligned}$$

We have deduced that for every odd prime p as well that $v_p(n!) \leq v_p\left(\prod_{k=0}^{n-1}(2^n-2^k)\right)$. 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!

2.18 Nov 2

2.18.1 A Taste of Group Theorem

Recall the following definition:

Def. 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 1.

$$\begin{aligned} G &= \mathbb{R}^\times := \mathbb{R}\backslash\{0\} \\ * &= \text{multiplication} \\ e &= 1 \quad (\text{for any } x \in \mathbb{R}\backslash\{0\},\ x \cdot 1 = 1 \cdot x = x) \end{aligned}$$

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 2.

$$\begin{aligned} G &= \mathbb{Z} \\ * &= + \\ e &= 0 \quad (\text{for any } x \in \mathbb{Z},\ x + 0 = 0 + x = x) \end{aligned}$$

It is clearly associative, and for any $x \in \mathbb{Z}$,

$$x + (-x) = (-x) + x = 0$$

Example 3.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\} \begin{cases} \overline{0} = \overline{n} \\ \overline{-1} = \overline{n-1} \end{cases}$$

$$* = + \text{ modulo } n.$$

For instance

$$\begin{aligned} \overline{1} + \overline{2} = \overline{1+2} = \overline{3} \\ \overline{n-1} + \overline{1} = \overline{n} = \overline{0} \end{aligned}$$

$+$ modulo n is associative:

$$\begin{aligned} \overline{a} + \left(\overline{b} + \overline{c}\right) = \overline{a} + \overline{b+c} = \overline{a+b+c} \\ \left(\overline{a} + \overline{b}\right) + \overline{c} = \overline{a+b} + \overline{c} = \overline{a+b+c} \end{aligned}$$

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 4.

$$(\mathbb{Z}/p\mathbb{Z})^{\times} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\} \qquad p \text{ prime}$$
$$* = \text{multiplication modulo } p$$

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 5.

$$\{1 \leqslant a \leqslant n : \gcd(a, n) = 1\} = \left\{a_1, \cdots a_{\varphi(n)}\right\}$$

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 27 (Lagrange)**.** *If G is a finite group, then for every $x \in G$ of size $|G|$*

$$\underbrace{x^{|G|}}_{\underbrace{x * x * \cdots * x}_{|G| \ times}} = e$$

Example 1.

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 2.

$$GL_2(\mathbb{R}) := \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \text{ such that } \det(A) = ad - bc \neq 0 \right\}$$

$$* = \text{ matrix multiplication}$$

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

Note that $GL_2(\mathbb{R})$ is closed under matrix multiplication because $\det(AB) = \det(A)\det(B)$, and so if $\det(A) \neq 0 \neq \det(B)$, then $\det(AB) \neq 0$, that is, $AB \in GL_2(\mathbb{R})$.

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,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

2.18.2 Applications of Group Theory to Combinations

Problem. Consider an 8 × 8 board filled by checkers as follows:

×		×		×		×	
	×		×		×		×
×						×	
	×						×
×						×	
	×						×
×		×		×		×	
	×		×		×		×

Figure 2: 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 flipting along the verticle line, b represents flip 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

$$a^2 = b^2 = c^2 = e$$

$$ab = c, bc = a, ca = b$$

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 $(1,1)$.

Color the squares of the board using the elements of G as above.

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 3: Coloring

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 become, 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, they could be some other algebraic gadget, they could be 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.

2.19 Nov 4

2.19.1 A little bit of group theory and their special function

Answer: Impossible.

$$G = \{a, b, c, e\}$$
$$a^2 = b^2 = c^2 = e$$
$$ab = c, bc = a, ca = b$$

$$G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{(0,0),(1,0),(0,1),(1,1)\}$$

Define I as the product of all elements in squares with checker pieces.

In the initial position,

$$I = e.$$

If exactly one chip, then the invariant is a, b, or $c \neq e$.

Problem. Suppose we have a 4×11 rectangle.

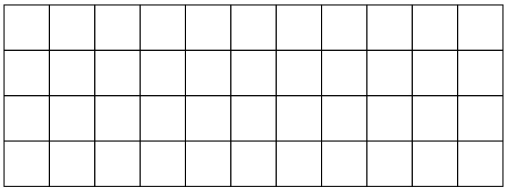


Figure 4: 4×11 rectangle

Is it possible to tile the 4×11 rectangle using the following L-shaped pieces?

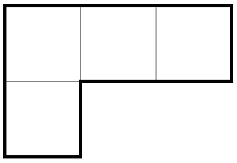


Figure 5: L shape piece

Special Functions

Def. Suppose $n \in \mathbb{N}$. Then

$$\tau(n) := \sum_{d|n, d\in\mathbb{N}} 1 = \text{number of positive divisors of } n$$

e.g.

$$\tau(10) = \tau(2^1 \cdot 5^1)$$

I can have 0 or 1 2's in the divisor. I can have 0 or 1 5's in the divisor. $\tau(10) = 2 \cdot 2 = 4$.

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,

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

e.g.

$$\begin{aligned}\tau(200) &= \tau(2^3 \cdot 5^2) \\ &= (3+1)(2+1) \\ &= 12.\end{aligned}$$

Note that

$$\tau(2^3)\tau(5^2) = (3+1)(2+1) = 12$$

Proposition 20. *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.

e.g. $\tau(2^3) = 4$

$\tau(2)\tau(2^2) = (1+1)(2+1) = 6 \neq 4 = \tau(2^3)$

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 $\gcd(m,n) = 1$,

$$\{p_1, \cdots, p_k\} \cap \{q_1, \cdots, q_l\} = \emptyset$$

It then follows that

$$\tau(mn) = \tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}) = (\alpha_1{+}1) \ldots (\alpha_k{+}1)(\beta_1{+}1) \ldots (\beta_l{+}1) = \tau(m)\tau(n),$$

as required. □

□

Definition. For $n \in \mathbb{N}$,

$$\sigma(n) = \sum_{d|n,\ d \in \mathbb{N}} d$$

is the sum of the positive divisors of n.

Question. How to compute this (if we know the prime fact. of n)?

Proposition 21. *If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \geq 1, p_i$ distinct primes, then*

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right) \cdot \left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right)$$

e.g.

$$\begin{aligned}\sigma(20) &= \sigma(2^2 \cdot 5) \\ &= \sum_{\substack{0 \leq \alpha \leq 2 \\ 0 \leq \beta \leq 1}} 2^\alpha 5^\beta \\ &= (\sum_{0 \leq \alpha \leq 2} 2^\alpha)(\sum_{0 \leq \beta \leq 1} 5^\beta) \\ &= (1 + 2 + 2^2)(1 + 5)\end{aligned}$$

Proof of proposition.

$$\begin{aligned}\sigma(n) &= (1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k}) \\ &= \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right) \cdot \left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right).\end{aligned}$$

□

e.g.

$$\begin{aligned}\sigma(20) &= \sigma(2^2 \cdot 5^1) \\ &= (\frac{2^3-1}{2-1})(\frac{5^2-1}{5-1}) \\ &= 7 \cdot (\frac{24}{4}) \\ &= 7 \cdot 6 \\ &= 42.\end{aligned}$$

Lemma. For $r \neq 1$,

$$a + ar + ar^2 + \cdots + ar^k = \frac{a(r^{k+1}-1)}{r-1}.$$

Proof. Let $S = a + ar + ar^2 + \cdots + ar^k$.

Then $rS = ar + ar^2 + \cdots ar^k + ar^{k+1}$.

$$\begin{aligned}rS - S &= ar^{k+1} - a \\ (r-1)S &= a(r^{k+1} - 1) \\ \overset{r \neq 1}{\Longrightarrow} \quad S &= \frac{a(r^{k+1}-1)}{r-1}.\end{aligned}$$

□

Proposition 22. *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 $\gcd(m,n) = 1$,

$$\{p_1, \cdots, p_k\} \cap \{q_1, \cdots, q_l\} = \emptyset$$

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, $\sigma(2^2) \neq \sigma(2)\sigma(2)$.

2.20 Nov 7, Special functions Continued

Problem. (Gauss' Lemma) For $n \in \mathbb{N}$,

$$n = \sum_{d|n} \varphi(d).$$

Solution. 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,

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

e.g. 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

$$\begin{aligned} 6 &= 1 + 1 + 2 + 2 \\ &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) \\ &= \sum_{d \mid 6} \varphi(d) \end{aligned}$$

Problem. 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 $1 \leq a \leq n$ 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, $2a_i = n \overset{\gcd(a_i,n)=1}{\implies} a_i = 1 \implies n = 2$.)

Summing $(*)$, we obtain

$$2 \sum_{\substack{1 \leq a \leq n \\ \gcd(a,n)=1}} a = n\varphi(n)$$

$$\implies \sum_{\substack{1 \leq a \leq n \\ \gcd(a,n)=1}} a = \frac{n\varphi(n)}{2}$$

□

Def. An <u>arithmetic</u> function is any function

$$f : \mathbb{N} \to \mathbb{R} \text{ (or } \mathbb{C}).$$

Def. A <u>multiplicative</u> function is an arithmetic function $f : \mathbb{N} \to \mathbb{C}$ s.t. for any $m, n \in \mathbb{N}$ satisfying $\gcd(m,n) = 1$,

$$f(mn) = f(m)f(n).$$

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

$$\tau(n) = \sum_{d \mid n} 1$$

and

$$\sigma(n) = \sum_{d \mid n} d.$$

Proposition 23. *If $f : \mathbb{N} \to \mathbb{C}$ is multiplicative, then*

$$g(n) := \sum_{d \mid n} f(d)$$

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,

$$g(mn) = \sum_{d \mid mn} f(d).$$

Since $\gcd(m, n) = 1, d = \gcd(m, d)\gcd(n, d)$.

From this, it can be seen that

$$\sum_{d \mid mn} f(d) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2). \tag{1}$$

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

$$g(n) := \sum_{d|n} f(d).$$

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.

2.21 Nov 9

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 about f. Can we recover f given g?

$$\begin{aligned}
&g(1) = \sum_{d|1} f(d) = f(1)\\
&g(2) = \sum_{d|2} f(d) = f(1) + f(2) = g(1) + f(2)\\
&\implies f(2) = g(2) - g(1)\\
&g(3) = \sum_{d|3} f(d) = f(1) + f(3) = g(1) + f(3)\\
&\implies f(3) = g(3) - g(1)\\
&g(4) = \sum_{d|4} f(d) = f(1) + f(2) + f(4)\\
&\qquad = g(1) + (g(2) - g(1)) + f(4)\\
&\implies f(4) = g(4) - g(2).
\end{aligned}$$

Can we recover $f(n)$ for every $n \in \mathbb{N}$ if we know $g(n)$ for every $n \in \mathbb{N}$?

Answer: Yes.

2.21.1 Möbius Inversion

Def. The möbius function $\mu : \mathbb{N} \to \mathbb{R}$ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 \cdots p_r, p_i \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Proposition 24. *μ is a multiplicative function, i.e. if $m, n \in \mathbb{N}$ s.t.* $\gcd(m, n) = 1$*, 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 s.t. $p^2 \mid m$ or $p^2 \mid n$, then $\mu(m) = 0$ or $\mu(n) = 0$, respectively. Furthermore, $p^2 \mid mn \implies \mu(mn) = 0$ as well.

It remains to consider the case where $m = p_1 \cdots p_r$, $n = q_1 \cdots q_l$, p_i distinct, q_j distinct.

Since $\gcd(m, n) = 1$,

$$\{p_1, \cdots, p_r\} \cap \{q_1, \cdots, q_l\} = \emptyset$$

Therefore,

$$\begin{aligned} \mu(mn) &= \mu(p_1 \cdots p_r q_1 \cdots q_l) = (-1)^{r+l} \\ &= (-1)^r (-1)^l \\ &= \mu(p_1 \cdots p_r)\mu(q_1 \cdots q_l) \\ &= \mu(m)\mu(n) \end{aligned}$$

□

Proposition 25. *For every* $n \in \mathbb{N}$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Proof. Recall from last class that since μ is multiplicative, so is

$$e(n) := \sum_{d|n} \mu(d)$$

Therefore, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \geq 1, p_i$ distinct primes, then

$$e(n) = e(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = e(p_1^{\alpha_1})e(p_2^{\alpha_2}) \cdots e(p_k^{\alpha_k}).$$

If $n = 1$, then

$$e(1) = \sum_{d|1} \mu(d) = \mu(1) = 1.$$

If suffices to show that if $n = p^\alpha$, $\alpha \geq 1$, p prime, then

$$e(p^\alpha) = 0$$

Computing this, we have

$$\begin{aligned} e(p^\alpha) &= \sum_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \underbrace{\mu(p^2) + \cdots + \mu(p^\alpha)}_{=0} \\ &= 1 + (-1)^1 = 0 \end{aligned}$$

□

Def. 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 28 (Möbius Inversion Formula)**.** *If $f : \mathbb{N} \to \mathbb{C}$ and for every $n \in \mathbb{N}$*

$$g(n) := \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(\frac{n}{d})g(d).$$

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

$$\sum_{d|n} \mu(\frac{n}{d})g(d) = \sum_{d|n} \mu(d)g(\frac{n}{d}).$$

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).

Def. (Dirichlet Convolution)

Given $f, g : \mathbb{N} \to \mathbb{C}$,

$$\begin{aligned}(f * g)(n) :=& \sum_{d|n} f(d)g(\frac{n}{d}) \\ =& \sum_{\substack{d_1 d_2 = n \\ d_1, d_2 \in \mathbb{N}}} f(d_1)g(d_2) \\ =& (g * f)(n)\end{aligned}$$

In the language of Dirichlet convolutions,

$$\sum_{d|n} f(d) = \sum_{d|n} f(d)I(\frac{n}{d}) = f * I$$

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 26. *Given $f, g : \mathbb{N} \to \mathbb{C}$,*

$$
\begin{aligned}
&(1) f * g = g * f \\
&(2) (f * g) * h = f * (g * h). && \text{(Associativity)} \\
&(3) f * e = f
\end{aligned}
$$

Proof. (1) is clear.

For (2), note that

$$
\begin{aligned}
((f * g) * h)(n) &= \sum_{\substack{d_1 d_2 = n \\ d_1 d_2 \in \mathbb{N}}} (f * g)(d_1) h(d_2) \\
&= \sum_{\substack{u v d_2 = n \\ u, v, d_2 \in \mathbb{N}}} f(u) g(v) h(d_2)
\end{aligned}
$$

You can similarly show that

$$
(f * (g * h))(n) = \sum_{\substack{u, v, d_2 \in \mathbb{N} \\ u v d_2 = n}} f(u) g(v) h(d_2)
$$

For (3), note that

$$
(f * e)(n) = \sum_{d|n} f(\frac{n}{d}) e(d) = f(n)
$$

□

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,

$$
f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d).
$$

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. Show that for every $n \in \mathbb{N}$,

$$1 = \sum_{d|n} \mu(\frac{n}{d})\tau(d).$$

Solution. By definition,

$$\tau(n) = \sum_{d|n} 1.$$

By Möbius inversion,

$$1 = \sum_{d|n} \mu(\frac{n}{d})\tau(d)$$

Problem. 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

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$$

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.

$$n = \sum_{d|n} \mu(\frac{n}{d})\sigma(d).$$

$$\sigma(n) = \sum_{d|n} d.$$

2.22 Nov 14

2.22.1 Möbius Inversion continued

Recall that Gauss' Lemma states that for every $n \in \mathbb{N}$,

$$id(n) = n = \sum_{d|n} \varphi(d).$$

By Möbius inversion,

$$\begin{aligned}\varphi(n) &= \sum_{d|n} id(\frac{n}{d})\mu(d) \\ &= \sum_{d|n} \frac{n}{d}\mu(d) \\ &= n\sum_{d|n} \frac{\mu(d)}{d}\end{aligned}$$

$\frac{\mu(d)}{d}$ 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

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big)$$

The idea of the proof is the same idea I used to show that

$$\sum_{d|n} \mu(d) = \left\{ \begin{array}{ll} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{array} \right. .$$

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,

$$\begin{aligned}\varphi(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) &= p_1^{\alpha_1}\Big(1-\frac{1}{p_1}\Big)p_2^{\alpha_2}\Big(1-\frac{1}{p_2}\Big)\cdots p_k^{\alpha_k}\Big(1-\frac{1}{p_k}\Big)\\ &= p_1^{\alpha_1}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

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

$$\begin{aligned}g(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) &= g(p_1^{\alpha_1})\cdots g(p_k^{\alpha_k})\\ &= \left(\sum_{d|p_1^{\alpha_1}}\frac{\mu(d)}{f(d)}\right)\cdots\left(\sum_{d|p_k^{\alpha_k}}\frac{\mu(d)}{f(d)}\right)\\ &= \left(\frac{\mu(1)}{f(1)}+\frac{\mu(p_1)}{f(p_1)}+\underbrace{\frac{\mu(p_1^2)}{f(p_1^2)}+\cdots+\frac{\mu(p_1^{\alpha_1})}{f(p_1^{\alpha_1})}}_{=0}\right)\\ &\qquad\cdots\left(\frac{\mu(1)}{f(1)}+\frac{\mu(p_k)}{f(p_k)}+\underbrace{\frac{\mu(p_k^2)}{f(p_k^2)}+\cdots+\frac{\mu(p_k^{\alpha_k})}{f(p_k^{\alpha_k})}}_{=0}\right)\\ &= \left(\frac{1}{f(1)}-\frac{1}{f(p_1)}\right)\cdots\left(\frac{1}{f(1)}-\frac{1}{f(p_k)}\right)\end{aligned}$$

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.

2.22.2 Multiplicative version of Möbius inversion

Theorem 29. *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

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

$$\begin{aligned}\overset{\text{Möbius inversion}}{\Longrightarrow}\ \log f(n) &= \sum_{d|n}\mu(\frac{n}{d})\log g(d)\\ &= \sum_{d|n}\log g(d)^{\mu(\frac{n}{d})}\\ &= \log\prod_{d|n}g(d)^{\mu(\frac{n}{d})}\\ \overset{exp.}{\Longrightarrow}\ f(n) &= \prod_{d|n}g(d)^{\mu(\frac{n}{d})}.\end{aligned}$$

□

Problem. 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 $n\in\mathbb{N}$,

$$a_n=\prod_{d|n}b_d.$$

2.22.3 Quadratic reciprocity

Recall the following theorem.

Theorem 30. *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?

Def. (Legendre Symbol)

Suppose $a \in \mathbb{Z}$, p prime (almost always odd).

Then

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ has } \underline{\text{no}} \text{ solution} \\ 1 & \text{otherwise} \end{cases}$$

Def. $a \in \mathbb{Z}$ is a quadratic residue mod p if

$$x^2 \equiv a \pmod{p}$$

has a solution. Otherwise, a is a quadratic non-residue.

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

$$4 \,\Big|\, p-1 \implies 2 \,\Big|\, \frac{p-1}{2} \implies (-1)^{\frac{p-1}{2}} = 1.$$

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 31. *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

$$p \,\Big|\, a^{\frac{p-1}{2}}.$$

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. □

2.23 Nov 16

2.23.1 Continuation of Quadratic residues

Remarks 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.

Quadratic residues

Recall the def of the Legendre symol. If p is a prime, $a \in \mathbb{Z}$, then

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \textit{if } p \mid a \\ -1 & \textit{if } x^2 \equiv a \pmod{p} \textit{ has } \underline{\textit{no}} \textit{ solution} \\ 1 & \textit{otherwise} \end{cases}$$

Theorem 32 (Euler's criterion)**.** *If p is an* <u>*odd*</u> *prime, then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Proposition 27. *If p* <u>*odd*</u> *prime and $p \nmid a$, then*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \iff x^2 \equiv a \pmod{p} \textit{ has a solution}$$

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 $j \in S$ s.t.

$$ij \equiv a \pmod{p}.$$

j must be unique. If you choose j, then by uniqueness again, it will be paired with i.

Since a is not a square mod p, $j \neq i$. This gives us a pairing between the numbers

$$1, 2, \cdots, p-1.$$

We have a total of $\frac{p-1}{2}$ pairs s.t. 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 33. *$a, b \in \mathbb{Z}, p$ odd prime, we have the following properties:*

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,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

$$\implies p \,\middle|\, \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) - \left(\frac{b}{p}\right)$$

Since

$$-1 \leq \left(\frac{ab}{p}\right),\ \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \leq 1$$

$$\implies \left|\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right| \leq 2.$$

p odd $\implies p \geq 3$.

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,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

e.g. Consider mod 5.

The possible squares mod 5 are

$$\begin{aligned}0^2 &\equiv 0 \pmod 5\\ 1^2 &\equiv 1 \pmod 5\\ 2^2 &\equiv 4 \pmod 5\\ 3^2 &\equiv 4 \pmod 5\\ 4^2 &\equiv 1 \pmod 5\end{aligned}$$

0, 1, 4 are the only quadratic residues mod 5.

2, 3 are the quadratic non-residues.

$$\left(\frac{2\cdot 3}{5}\right) = 1.$$

$$\left(\frac{2}{3}\right), \left(\frac{3}{5}\right) = -1 \implies \left(\frac{2}{5}\right)\left(\frac{3}{5}\right) = 1.$$

$$\left(\frac{4\cdot 2}{5}\right) = \left(\frac{8}{5}\right) = \left(\frac{3}{5}\right) = -1$$

$$\left(\frac{4}{5}\right) = 1, \ \left(\frac{2}{5}\right) = -1.$$

Proposition 28. *If* $a \equiv b \pmod p$*, then*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

e.g.

$$\left(\frac{2}{5}\right) = -1, \text{ and } 2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1 \pmod 5).$$

So

$$\left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} \pmod 5,$$

as predicted by Euler's criterion.

e.g.

$$\left(\frac{1002}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

e.g.

$$\left(\frac{1004}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1.$$

e.g.

$$\left(\frac{57}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

e.g.

$$\left(\frac{55}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{\frac{7-1}{2}} = -1.$$

2.23.2 Quadratic Reciprocity of Gauss

If you have two odd prime p, q, quadratic reciprocity will tell us that studying

$$x^2 \equiv p \pmod{q}$$

is intimately related to studying

$$x^2 \equiv q \pmod{p}$$

Theorem 34. *If p, q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

$$\left(\iff \text{for } p, q \text{ odd primes, } \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)\right).$$

e.g.

$$\begin{aligned}\left(\frac{3}{17}\right) &= (-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)\\ &= \left(\frac{17}{3}\right)\\ &= \left(\frac{2}{3}\right)\\ &= \left(\frac{-1}{3}\right)\\ &= (-1)^{\frac{3-1}{2}}\\ &= -1.\end{aligned}$$

e.g.

$$\begin{aligned}\left(\frac{15}{19}\right) &= \left(\frac{3}{19}\right)\left(\frac{5}{19}\right)\\ &= (-1)^{\frac{3-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{3}\right)(-1)^{\frac{5-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{5}\right)\\ &= -\left(\frac{19}{3}\right)\left(\frac{19}{5}\right)\\ &= -\left(\frac{1}{3}\right)\left(\frac{4}{5}\right)\\ &= -1.\end{aligned}$$

This computation demonstrates the general procedure. Of course, we could also do the computation as follows without using quadratic reciprocity:

$$\left(\frac{15}{19}\right) = \left(\frac{-4}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{4}{19}\right) = (-1)^{\frac{19-1}{2}} = -1.$$

2.24 Nov 18

$$\begin{aligned}\left(\frac{17}{19}\right) &= \left(\frac{-2}{19}\right)\\ &= \left(\frac{-1}{19}\right)\left(\frac{2}{19}\right)\\ &= (-1)^{\frac{19-1}{2}}\left(\frac{2}{19}\right)\\ &= -\left(\frac{2}{19}\right)\end{aligned}$$

Proposition 29. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(If x is odd, then $8 \mid x^2 - 1$)

Continuing 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

$$\begin{aligned}19^2 - 1 &= (19-1)\,(19+1)\\ &= 18 \cdot 20\\ &= 2^3 \cdot 3^2 \cdot 5\end{aligned}$$

and so

$$\frac{19^2-1}{8} = 45$$
$$(-1)\cdot(-1)^{\frac{19^2-1}{8}} = (-1)\cdot(-1) = 1$$

Another 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

$$\left(\frac{2}{17}\right) = \left(\frac{-15}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{3}{17}\right)\left(\frac{5}{17}\right) = \dots$$

Problem. 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 30. *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

$$p_1, \cdots, p_k.$$

Note that there is at least one such prime, 5, for example. Consider

$$N := (2p_1 \cdots p_k)^2 + 1 > 1$$

There is an odd prime $p \mid N$,

$$\begin{aligned}p \mid N &\implies (2p_1 \cdots p_k)^2 + 1 \equiv 0 \pmod{p}\\ &\implies x^2 \equiv -1 \pmod{p} \text{ has a solution}\\ &\implies \left(\frac{-1}{p}\right) = 1 \implies p \equiv 1 \pmod 4.\end{aligned}$$

In the final implication, I used that p must be odd. It is also clear that

$$p \notin \{p_1, \cdots, p_k\}.$$

Contradiction. □

Theorem 35. *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. 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,

$$\begin{aligned} 3 = 1^2 + 1 \cdot 1 + 1^2 \qquad & x = 1, y = 1 \\ \implies 3 \text{ is of this form.} & \end{aligned}$$

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

$$\begin{aligned} 4p &= 4x^2 + 4xy + 4y^2 \\ &= \left((2x)^2 + 2 \cdot (2x)\, y + y^2\right) + 3y^2 \\ &= (2x + y)^2 + 3y^2 \\ &\implies (2x + y)^2 \equiv -3y^2 \pmod{p} \qquad (2) \end{aligned}$$

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. Therefore, $p \nmid y$, and so there is a z such that

$$yz \equiv 1 \pmod{p}.$$

Consequently, (2) implies that

$$\begin{aligned} z^2 (2x+y)^2 &\equiv -3y^2z^2 \\ &\equiv -3 \pmod{p} \end{aligned}$$

This means that -3 is a quadratic residue modulo p, i.e.

$$\begin{aligned} &\overset{p\neq 3}{\implies} \left(\frac{-3}{p}\right) = 1 \\ &\implies p \equiv 1 \pmod{3}. \end{aligned}$$

The final conclusion follows from two problems ago.

Problem. 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

$$-1 \equiv \left(2^{\frac{n}{2}}\right)^2 \pmod{p}$$

$$\implies 1 = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \implies p \equiv 1 \pmod{4}$$

In particular,

$$p \not\equiv -1 \pmod{8}.$$

Assume now that n is odd. In this case

$$\frac{n+1}{2} \in \mathbb{Z},$$

and so

$$\begin{aligned} \left(2^{\frac{n+1}{2}}\right)^2 &= 2^{n+1} \\ &\equiv -2 \pmod{p}. \end{aligned}$$

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,

$$\begin{aligned}\frac{p-1}{2} &= \frac{(8k-1)-1}{2}\\ &= 4k-1 \quad \text{is odd.}\end{aligned}$$

These computations imply that if $p \equiv -1 \bmod 8$, then $\left(\frac{-2}{p}\right) \neq 1$. Therefore, again, we cannot have $p \equiv -1 \bmod 8$.

The conclusion follows.

Theorem 36. *If $a > 1$ is a natural number that is not a square, then*

$$\left(\frac{a}{p}\right) = -1$$

for ∞ many primes p.

Problem. 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 f are rational.

2.25 Nov 21

Proposition 31. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Lemma. (Gauss) Suppose p is an odd prime and $a \in \mathbb{Z}, p \nmid a$. Consider the numbers

$$1, 2, 3, \cdots, \frac{p-1}{2}$$

and

$$a, 2a, 3a, \cdots, a\left(\frac{p-1}{2}\right).$$

Reduce these numbers and choose remainders in

$$-\frac{p-1}{2} \leq r < \frac{p-1}{2}$$

after division by p.

Let l be the number of such remainders that are < 0. Then

$$\left(\frac{a}{p}\right) = (-1)^l.$$

Reminder on division algorithm: Given $x \in \mathbb{Z}$, then we may write

$$x = bp + r, \text{ where } 0 \leq r < p, b \in \mathbb{Z}$$

In stead, you can write

$$x = cp + s, \text{ where } -\frac{p-1}{2} \leq s < \frac{p-1}{2}$$

Proof of lemma. Let the remainder of ai mod p lying in $-\frac{p-1}{2} \leq r < \frac{p-1}{2}$ be denoted by a_i.

Then it is clear that

$$1 \leq |a_i| \leq \frac{p-1}{2}$$

for every i.

We claim that for every pair $i \neq j$, $|a_i| \neq |a_j|$.

Indeed, if $|a_i| = |a_j|$, then

$$a_i = \pm a_j \tag{$*$}$$

Since

$$a_i \equiv ai \pmod{p}, a_j \equiv aj \pmod{p},$$

$(*) \implies p \mid a(i-j)$ or $p \mid a(i+j)$

Since $p \nmid a$, this means $p \mid i-j$ or $p \mid i+j$. Since $-\frac{p-1}{2} \leq i, j < \frac{p-1}{2}$, this is only possible if

$$i = j.$$

Therefore, the $|a_i|$ are distinct.

Therefore,

$$(-1)^l a_1 \ldots a_{\frac{p-1}{2}} = |a_1| \cdots |a_{\frac{p-1}{2}}| = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!, \tag{1}$$

and so

$$a_1 \dots a_{\frac{p-1}{2}} = (-1)^l \left(\frac{p-1}{2}\right)!$$

On the other hand,

$$a_1 \cdots a_{\frac{p-1}{2}} \equiv (a)(2a) \cdots \left(\left(\frac{p-1}{2}\right) a\right) \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p \qquad (2)$$

Combining (1) and (2), we obtain

$$(-1)^l \left(\frac{p-1}{2}\right)! \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p$$

$$\overset{p \nmid \left(\frac{p-1}{2}\right)!}{\Longrightarrow} (-1)^l \equiv a^{\frac{p-1}{2}} \text{ (mod } p), \qquad (3)$$

By Euler's criterion,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Combining with (3), we obtain

$$\left(\frac{a}{p}\right) \equiv (-1)^l \pmod p$$

$$\overset{\substack{p \text{ odd} \\ \text{i.e. } p \geq 3}}{\Longrightarrow} \left(\frac{a}{p}\right) = (-1)^l.$$

□

We can use this to prove the proposition that for odd p,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Indeed, if we consider

$$1, 2, 3, \cdots, \frac{p-1}{2},$$

it is easy to see that exactly for

$$1 \leq j \leq \left\lfloor \frac{p}{4} \right\rfloor,$$

we have $2j$ leaving positive remainder, and that for

$$\left\lfloor \frac{p}{4} \right\rfloor < j \leq \frac{p-1}{2},$$

$2j$ has negative remainder in $[-\frac{p-1}{2}, \frac{p-1}{2})$

$$\implies l = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

It is an exercise to show that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \bmod 2,$$

from which the conclusion would follow.

Problem. Find all odd primes p s.t.

$$\left(\frac{7}{p}\right) = 1.$$

Solution. Clearly, if $p = 7$, then this is not satisfied. Therefore, assume $p \neq 7$. Applying quadratic reciprocity,

$$\left(\frac{7}{p}\right) = (-1)^{\frac{7-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right).$$

There are two main cases:

1. $(-1)^{\frac{p-1}{2}} = -1$ and $\left(\frac{p}{7}\right) = -1$.
2. $(-1)^{\frac{p-1}{2}} = 1$ and $\left(\frac{p}{7}\right) = 1$.

The nonzero quadratic residues mod 7 are

$$\begin{gathered} 1^2 \equiv 1 \pmod 7 \\ 2^2 \equiv 4 \pmod 7 \\ 3^2 \equiv 2 \pmod 7 \\ 4^2 \equiv 3^2 \equiv 2 \pmod 7 \\ \vdots \end{gathered}$$

$\implies$ nonzero quadratic residues: $1, 2, 4$, and quadratic non-residues: $3, 5, 6$.

1.

$$\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 3 \pmod 7 \end{cases} \implies p \equiv 3 \ (\mathrm{mod}\ 28)$$

$$\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 5 \pmod 7 \end{cases} \implies p \equiv 19 \ (\mathrm{mod}\ 28)$$

$$\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 6 \pmod 7 \end{cases} \implies p \equiv 27 \ (\mathrm{mod}\ 28)$$

2.

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 7 \end{cases} \implies p \equiv 1 \text{ (mod 28)}$$

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 2 \pmod 7 \end{cases} \implies p \equiv 9 \text{ (mod 28)}$$

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 4 \pmod 7 \end{cases} \implies p \equiv 25 \text{ (mod 28)}$$

Therefore we have

$$p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}.$$

Problem. If $p = x^2 - 7y^2$ is a prime ($x, y \in \mathbb{Z}$), what can say about p?

Solution. Let us assume for now that $p \neq 7$. Reducing mod p, we must have

$$x^2 \equiv 7y^2 \text{ (mod } p).$$

$p \nmid y$; otherwise $p \mid x, y \implies p^2 \mid x^2 - 7y^2 = p$ which is a contradiction.

Therefore, there is a z s.t.

$$zy \equiv 1 \text{ (mod } p).$$

Multiplying by z^2, we obtain

$$(xz)^2 = z^2x^2 \equiv 7y^2z^2 = 7(yz)^2 \equiv 7 \text{ (mod } p)$$

$$\overset{p\neq 7}{\implies} \left(\frac{7}{p}\right) = 1 \implies p \equiv 1, 3, 9, 19, 25, 27 \text{ (mod 28)}.$$

What about $p = 7$? Can we write $7 = x^2 - 7y^2$ for some $x, y \in \mathbb{Z}$?

No. Indeed, if this were possible, then

$$\begin{aligned} & 7(1 + y^2) = x^2 \\ \implies & 7 \mid x \\ \implies & x = 7x_1 \text{ for some } x_1 \in \mathbb{Z}. \\ \implies & 7(1 + y^2) = (7x_1)^2 = 49x_1^2 \\ \implies & 1 + y^2 = 7x_1^2 \equiv 0 \text{ (mod 7)} \\ \implies & 1 = \left(\frac{-1}{7}\right) = (-1)^{\frac{7-1}{2}} = -1 \end{aligned}$$

Thus there is a contradiction.

3 Final Review

3.1 Nov 29

Induction $\Leftarrow$ Well ordering principle

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

Combinatorial identities.

$$\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1} \qquad \text{(Pascal's identity)}$$

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

Example. $\sum_{k=0}^{n} k(k-1)(k-2)\binom{n}{k}=n(n-1)(n-2)2^{n-3}$

$$\begin{aligned}\binom{n}{k}&=\frac{n}{k}\binom{n-1}{k-1}\\&=\frac{n(n-1)}{k(k-1)}\binom{n-2}{k-2}\\&=\frac{n(n-1)(n-2)}{k(k-1)(k-2)}\binom{n-3}{k-3}\end{aligned}$$

We could also prove such identities by giving arguments.

Newton's binomial theorem:

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

In particular,

$$\begin{aligned}(1+x)^n&=\sum_{k=0}^{n}\binom{n}{k}x^k\\n(1+x)^{n-1}&=\sum_{k=0}^{n}k\binom{n}{k}x^{k-1}\\n(n-1)(1+x)^{n-2}&=\sum_{k=0}^{n}k(k-1)\binom{n}{k}x^{k-2}\\n(n-1)(n-2)(1+x)^{n-3}&=\sum_{k=0}^{n}k(k-1)(k-2)\binom{n}{k}x^{k-3}\end{aligned}$$

We briefly touched on Fermat's Little Theorem.

Theorem 37. *If p is a prime, $a \in \mathbb{Z}$, s.t. $p \nmid a$, then*

$$p \mid a^{p-1} - 1 \text{ , } i.e. \ a^{p-1} \equiv 1 \pmod{p}$$

In general, $a^p \equiv a \pmod{p}$ for any $a \in \mathbb{Z}$

The first used that if p is a prime, then

$$p \left| \binom{p}{k} \right. \text{ for any } 1 \leq k \leq p-1$$

We discussed gcd's.

The foundation was

Theorem 38 (Bézout)**.** *If $a, b \in \mathbb{Z}$, at least one of which is nonzero, then*

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

has integral solutions.

In particular,

$$ax + by = 1 \text{ has integer integral solutions } \iff \gcd(a, b) = 1.$$

In relation to gcd and lcm, we talked about p-adic valuations.

If $\begin{cases} m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \geq 0 \\ n = p_1^{\beta_1} \cdots p_k^{\beta_k}, \beta_i \geq 0 \end{cases}$, then $\gcd(m, n) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}$.

We also had the Euclidean algorithm for computing gcds.

This method was useful for solving equations of the form

$$ax + by = c.$$

Theorem 39. *If $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$. such that*

$$ax_0 + by_0 = c,$$

Then <u>*all*</u> *solutions are given by*

$$\begin{cases} x = x_0 - \frac{b}{\gcd(a,b)} t \\ y = y_0 + \frac{a}{\gcd(a,b)} t \end{cases}, \ t \in \mathbb{Z}$$

Theorem 40. *For $a, b \in \mathbb{N}$,*

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

Problem. If $a, b \in \mathbb{N}$ s.t. $\gcd(a, b) = 1$, then show that

$$\operatorname{lcm}(a^2 + b^3, b^5 + a^2 b + b^4) = b(a^2 + b^3)(b^4 + a^2 + b^3).$$

3.2 Nov 30

There is a class of problems had to do with the non-existence of integer solutions.
Problem. Show that

$$x^2 + y^2 = 4000z^2 + 3 \tag{*}$$

has no integer solutions.

Solution. Replace mod 4 to obtain

$$x^2 + y^2 \equiv 3 \pmod 4 \tag{**}$$

If an integer solution (x, y, z) to $(*)$ were to exist, then $(**)$ would have solutions. Modulo 4, the quad residues are 0 and 1 and so

$$x^2 + y^2 \equiv 0, 1, \ \textit{or}\ 2 \pmod 4$$

Proposition 32. *If x is odd, then*

$$x^2 \equiv 1 \pmod 8.$$

Proof. Write $x = 2k + 1, k \in \mathbb{Z}$, then

$$\begin{aligned} x^2 &= 4k^2 + 4k + 1 \\ &= 4k(k+1) + 1 \\ &\equiv 1 \pmod 8 \end{aligned}$$

□

Problem. Are there <u>odd</u> integers x, y, z, w, u, v s.t.

$$x^2 + y^2 + z^2 + w^2 + u^2 = 80!v^2 + 7?$$

Solution. For any odd $a \in \mathbb{Z}$, $a^2 \equiv 1 \pmod 8$.

If a solution exists, then

$$x^2 + y^2 + z^2 + w^2 + u^2 \equiv 5 \pmod 8,$$

while the right hand side is $\equiv 7 \pmod 8$.

You could also do this modulo 4, since an odd number squared is also 1 modulo 4. The right hand side would be 3 modulo 4, while the left hand side would be 1 modulo 4. (Sorry for forgetting that the numbers are odd when saying in class that modulo 4 it would not have worked! A memory lapse.) If we only had three variables on the left hand side, then modulo 4 would not have worked while modulo 8 would have worked.

Problem. Are there integer solutions to

$$x^2 + y^2 - 11^2 z^2 = 583?$$

Solution. Reducing modulo 11, we obtain

$$x^2 + y^2 \equiv 0 \pmod{11}$$
$$\implies x^2 \equiv -y^2 \pmod{11}.$$

Claim. $11 \nmid y$.

Assume to the contrary that $11 \mid y$. Then

$$\begin{aligned} & x^2 \equiv -y^2 \equiv 0 \pmod{11} \\ & \implies 11 \mid x, y \\ & \implies 11^2 \mid x^2 + y^2 - 11^2 z^2 = 583 = 11 \cdot 53, \end{aligned}$$

a contradiction.

Therefore, there is a $w \in \mathbb{Z}$ s.t.

$$yw \equiv 1 \pmod{11},$$

and so

$$(xw)^2 \equiv -(yw)^2 \equiv -1 \pmod{11}$$
$$\implies \left(\frac{-1}{11}\right) = 1$$

However,

$$\left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = (-1)^5 = -1$$

Problem. Let $a_1 = 5, a_2 = 19$ and $a_n = a_{n-1} + 2a_{n-2}$ for $n \geq 2$.

Show that for every n,

$$\gcd(a_n, a_{n+1}) = 1.$$

Solution. We apply induction on n. If $n = 1$, then we have

$$\gcd(a_1, a_2) = \gcd(5, 19) = 1.$$

Now suppose

$$\gcd(a_k, a_{k+1}) = 1.$$

For $n = k+1$, we have

$$\begin{aligned}
&\gcd(a_{k+1}, a_{k+2}) \\
&= \gcd(a_{k+1}, a_{k+1} + 2a_k) \\
&= \gcd(a_{k+1}, (a_{k+1} + 2a_k) - a_{k+1}) \\
&= \gcd(a_{k+1}, 2a_k) \\
&= \gcd(a_{k+1}, a_k),
\end{aligned}$$

which is 1 by the inductive hypothesis.

Problem. Suppose p and q are distinct prime numbers. Then show that

$$\sqrt{p} + \sqrt{q} + \sqrt{pq}$$

is irrational.

We know that if $\sqrt{p}$ is rational, then

$$\sqrt{p} = \frac{x}{y}, x, y \in \mathbb{N}$$
$$\implies py^2 = x^2$$

Apply v_p to obtain

$$v_p(p) + 2v_p(y) = v_p(py^2) = v_p(x^2) = 2v_p(x).$$

Solution. Assume to the contrary that

$$\begin{aligned}
&\sqrt{p} + \sqrt{q} + \sqrt{pq} = \frac{x}{y},\ x, y \in \mathbb{N} \\
&\implies \sqrt{q} + \sqrt{pq} = \frac{x}{y} - \sqrt{p} \\
&\overset{square}{\implies} q + 2q\sqrt{p} + pq = \frac{x^2}{y^2} - \frac{2x}{y}\sqrt{p} + p \\
&\implies \sqrt{p} = \frac{\frac{x^2}{y^2} + p - 1 - pq}{2q + \frac{2x}{y}} \in \mathbb{Q}.
\end{aligned}$$

If you want to show divisibility, say

$$a \mid b,$$

then by unique prime factorization, it suffices to show that for all primes p,

$$v_p(a) \le v_p(b).$$

Recall that

$$\begin{aligned}
v_p(\gcd(a_1, \cdots, a_n)) &= \min\{v_p(a_1), \cdots, v_p(a_n)\}, \\
v_p(\operatorname{lcm}(a_1, \cdots, a_n)) &= \max\{v_p(a_1), \cdots, v_p(a_n)\}.
\end{aligned}$$

Theorem 41. *e and π are irrational.*

We discussed counting primes.

Theorem 42 (PNT)**.**

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

Theorem 43 (Euler)**.** *If $n \in \mathbb{N}, a \in \mathbb{Z}, \gcd(a, n) = 1$, then*

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

Problems involving Euler's theorem:

Find $2^{1000} \pmod{100}$ and $3^{1000} \pmod{100}$.

If you want to find

$$a^m \pmod{n},$$

write $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Then compute

$$a^m \pmod{p_i^{\alpha_i}}$$

for each i.

$$\begin{cases} a^m \equiv a_1 \pmod{p_1^{\alpha_1}} \\ \qquad \vdots \\ a^m \equiv a_k \pmod{p_k^{\alpha_k}} \end{cases}$$

$$\begin{aligned} \varphi(p^\alpha) &= p^{\alpha-1}(p-1) \\ \varphi(p^2) &= p(p-1) \end{aligned}$$

3.3 Dec 2

Problem. Find the last two digits of 7^{1000}.

Solution. We need to find $7^{1000} \pmod{100}$.

$$\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = 2(2-1)5(5-1) = 40.$$

Since $1000 \equiv 0 \pmod{40}$, $7^{1000} \equiv 7^0 = 1 \pmod{100}$.

Answer: 01

If we want to use the CRT, we would have to compute

$$\left.\begin{array}{l} 7^{1000} \equiv 1 \pmod{2^2} \\ 7^{1000} \equiv 1 \pmod{5^2} \end{array}\right\} \implies 7^{1000} \equiv 1 \pmod{100},$$

where the last implication follows from the uniqueness part of the CRT.

Problem. Find the last two digits of 6^{83}.

Solution. We need to compute $6^{83} \pmod{100}$.

$\gcd(6, 100) = 2 \neq 1$, so we need to apply CRT.

$$6^{83} \equiv 0 \pmod{4}.$$

It remains to find

$$6^{83} \pmod{25}.$$

$$\varphi(25) = 5(5-1) = 20 \text{ and } 83 \equiv 3 \bmod 20.$$

Therefore,

$$6^{83} \equiv 6^3 = 216 \equiv 16 \bmod 25.$$

Both 16 and 6^{83} are solutions to the system

$$\begin{cases} x \equiv 0 \bmod 4 \\ x \equiv 16 \bmod 25. \end{cases}$$

By the uniqueness part of the CRT, we obtain $6^{83} \equiv 16 \bmod 100$, and so the last two digits of 6^{83} are 16 in this order.

Theorem 44 (Lagrange)**.** *If G is a finite group of order $|G|$, then for every $g \in G$,*

$$g^{|G|} = e.$$

Euler's theorem = Lagrange's theorem applied to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Special functions

1. φ
2. $\tau(n) = \sum_{d|n} 1$
3. $\sigma(n) = \sum_{d|n} d$
4. μ

Proposition 33. *If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \alpha_i \geq 1, p_i$ distinct primes, then*

$$\begin{aligned}\tau(n) &= (\alpha_1 + 1) \cdots (\alpha_k + 1)\\ \sigma(n) &= (1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k})\\ &= \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)\end{aligned}$$

Problem. What is the sum of all divisors of 90 that are divisible by 3?

Solution. The prime factorization of 90 is $2 \cdot 3^2 \cdot 5$. Therefore, the answer is

$$\begin{aligned}&(1 + 2)(3 + 3^2)(1 + 5)\\ =&3 \cdot 12 \cdot 6\\ =&216.\end{aligned}$$

You could write this as

$$\begin{aligned}\sum_{\substack{0 \leq \alpha \leq 1\\ 1 \leq \alpha_2 \leq 2\\ 0 \leq \alpha_3 \leq 1}} 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} &= \left(\sum_{0 \leq \alpha_1 \leq 1} 2^{\alpha_1}\right)\left(\sum_{1 \leq \alpha_2 \leq 2} 3^{\alpha_2}\right)\left(\sum_{0 \leq \alpha_1 \leq 1} 5^{\alpha_3}\right)\\ &= (1 + 2)(3 + 3^2)(1 + 5)\\ &= 216\end{aligned}$$

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1\\ (-1)^r & \text{if } n = p_1 \cdots p_r, p_i \text{ distinct primes}\\ 0 & \text{otherwise}\end{cases}$$

Möbius Inversion formula

Suppose $f, g : \mathbb{N} \to \mathbb{R}$. Then for every n,

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d).$$

Problem. Show that

$$n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d)$$

Solution. By Möbius inversion, this is equivalent to showing

$$\sigma(n) = \sum_{d|n} d$$

for every n.

This is true by definition.

Problem. Show that

$$\varphi(n) = \sum_{d|n} \mu(\frac{n}{d})d = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Solution. By Gauss' Lemma,

$$n = \sum_{d|n} \varphi(d).$$

By Möbius inversion, we obtain the result.

Proposition 34. *If $f : \mathbb{N} \to \mathbb{R}$ is multiplicative, i.e. if $m, n \in \mathbb{N}$ s.t.* $\gcd(m, n) = 1$*, then $g : \mathbb{N} \to \mathbb{R}$ given by*

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

is multiplicative.

Problem. Compute

$$\sum_{d|n} \frac{\varphi(d)}{d^2}$$

in terms of the prime factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Solution. $f(1) = \frac{\varphi(1)}{1^2} = 1$.

$d \mapsto \frac{\varphi(d)}{d^2}$ is a multiplicative function, and so f is a multiplicative function.

Therefore for $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 1$, if suffices to compute each $f(p^\alpha)$; p prime:

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$$

$$\begin{aligned}
f(p^\alpha) &= \sum_{d|p^\alpha} \frac{\varphi(d)}{d^2} \\
&= \frac{\varphi(1)}{1^2} + \frac{\varphi(p)}{p^2} + \cdots + \frac{\varphi(p^\alpha)}{p^{2\alpha}} \\
&= 1 + \frac{p-1}{p^2} + \frac{p(p-1)}{p^4} + \cdots + \frac{p^{\alpha-1}(p-1)}{p^{2\alpha}} \\
&= 1 + (p-1)\left[\frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^{\alpha+1}}\right] \\
&= 1 + \frac{p-1}{p^{\alpha+1}}\left[1 + p + \cdots + p^{\alpha-1}\right] \\
&= 1 + \frac{p-1}{p^{\alpha+1}}\left(\frac{p^\alpha - 1}{p-1}\right) \\
&= 1 + \frac{p^\alpha - 1}{p^{\alpha+1}}
\end{aligned}$$

So

$$f(n) = \begin{cases} 1 & \text{if } n = 1 \\ \left(1 + \frac{p_1^{\alpha_1}-1}{p_1^{\alpha_1}}\right)\cdots\left(1 + \frac{p_k^{\alpha_k}-1}{p_k^{\alpha_k}}\right) & \text{if } n \text{ has prime factorization } p_1^{\alpha_1}\cdots p_k^{\alpha_k} \end{cases}.$$

Quadratic reciprocity Problem. What can you say about primes of the form

$$p = x^2 + 2xy + 4y^2?$$

Solution.

$$x^2 + 2xy + 4y^2 = (x+y)^2 + 3y^2.$$

Therefore,

$$(x+y)^2 \equiv -3y^2 \pmod{p}. \qquad (*)$$

Note that $p = 3$ is such a prime, take $x = -1, y = 1$.

Let's assume $p \neq 3$.

If $p \mid y$, then $(*)$ implies that $p \mid x$.

Therefore,

$$p^2 \mid x^2 + 2xy + 4y^2 = p,$$

a contradiction.

Therefore, $p \nmid y$, and so there is a z s.t. $zy \equiv 1 \pmod{p}$, and so

$$(z(x+y))^2 \equiv -3(zy)^2 \equiv -3 \pmod{p}$$

$$\implies \left(\frac{-3}{p}\right) = 1$$

$$\begin{aligned}
1 &= \left(\frac{-3}{p}\right) \\
&= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} \\
&= \left(\frac{p}{3}\right) \\
&\implies p \equiv 1 \pmod 3.
\end{aligned}$$

In the third equality, we used quadratic reciprocity in addition to

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

We conclude that $p = 3$ or $p \equiv 1 \bmod 3$.