Amazing Stories Of Number Theory And How It Is Applied In Online Shopping

Tong Liu

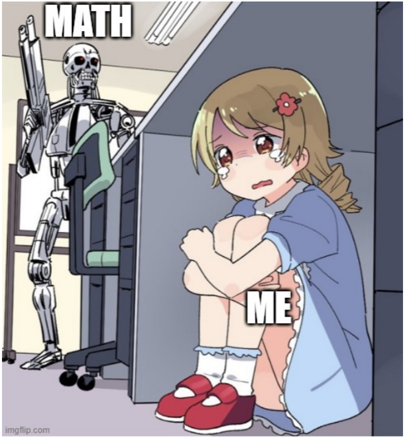
Public Lecture

June 18th 2023

What do you think about mathematics?

Hard, abstract, ...?

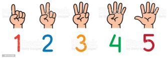
Something like.....


MATH
ME
imgflip.com

It could be, but it is also very fun and useful....

Natural numbers

By counting fingers,



our ancestors found natural numbers:

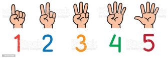
$$\mathbb{N} = \{1, 2, 3, 4, 5, ..\}$$

They also found addition and multiplication:

2 rows $\times$ 3 cavemen = 6 cavemen in total.

Natural numbers

By counting fingers,



our ancestors found natural numbers:

$$\mathbb{N} = \{1, 2, 3, 4, 5, ..\}$$

They also found addition and multiplication:

2 rows $\times$ 3 cavemen = 6 cavemen in total.

Division and remainder

Division is a little tricky: a is not always divisible by b, it could have a *remainder* r

$$a = q \times b + r, \quad 0 \leq r < b.$$

Example

$a = 10$ and $b = 3$. Then $10 = 3 \times 3 + 1$. So $r = 1$.

In the case that $r = 0$, $a = q \times b$ is a multiple of b. We say that a has a *factor* b.

For example, $a = 20$ has factors $1, 2, 4, 5, 10, 20$.

But not all numbers are created equally: Some numbers have many factors, while other numbers do not...

Division and remainder

Division is a little tricky: a is not always divisible by b, it could have a *remainder* r

$$a = q \times b + r, \quad 0 \leq r < b.$$

Example

$a = 10$ and $b = 3$. Then $10 = 3 \times 3 + 1$. So $r = 1$.

In the case that $r = 0$, $a = q \times b$ is a multiple of b. We say that a has a *factor* b.

For example, $a = 20$ has factors $1, 2, 4, 5, 10, 20$.

But not all numbers are created equally: Some numbers have many factors, while other numbers do not...

Definition

If $p > 1$ and has only factors 1 and p, then p is called *prime*.

For example, $p = 2, 3, 5, 7, 11, \cdots$

Believe it or not, primes are the main subjects that is studied in number theory, why?

1. It is fun !
2. It develops math that is very useful for science and daily life.
3. Also.....

Primes

Definition

If $p > 1$ and has only factors 1 and p, then p is called *prime*.

For example, $p = 2, 3, 5, 7, 11, \cdots$

Believe it or not, primes are the main subjects that is studied in number theory, why?

1. It is fun !
2. It develops math that is very useful for science and daily life.
3. Also.....

Primes

Definition

If $p > 1$ and has only factors 1 and p, then p is called *prime*.

For example, $p = 2, 3, 5, 7, 11, \cdots$

Believe it or not, primes are the main subjects that is studied in number theory, why?

1. It is fun !
2. It develops math that is very useful for science and daily life.
3. Also.....

It could make you RICH!

Prime factorization

Theorem (Prime factorization)

For any natural number $n > 1$, n can be uniquely factorized into

$$n = p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_s^{m_s}$$

with p_i being prime.

So primes are the building blocks of integers.

Example

$700 = 2^2 \times 5^2 \times 7$

Prime factorization

Theorem (Prime factorization)

For any natural number $n > 1$, n can be uniquely factorized into

$$n = p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_s^{m_s}$$

with p_i being prime.

So primes are the building blocks of integers.

Example

$700 = 2^2 \times 5^2 \times 7$

How many primes are there?

Euclid
(325–265 BC)

Theorem (Euclid)

There are infinitely many primes.

Proof.

Suppose there are only *finite* many primes $p_1, \ldots, p_m$. Then $N = p_1 \times \cdots \times p_m + 1$ can not have a correct prime factorization. Contradiction! $\square$

Twin primes conjecture

We see the gap between primes $p_{m+1} - p_m$ is at least 2 (why not 1?). The pair of primes (p, q) so that $q - p = 2$ is called *twin prime*. For example, $(5, 7)$, $(11, 13)$, $(17, 19)$.

Conjecture

There are infinitely many twin primes.

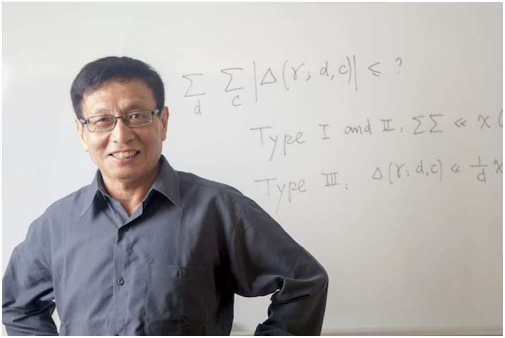
Conjecture here means that we do believe it is correct but we do not know how to confirm it purely by logic (prove).

This is a hard conjecture because the gap of prime $p_{m+1} - p_m$ can be arbitrarily large. For example, given any (large) m. The number sequence

$$m! + 2, m! + 3, \cdots, m! + m$$

has no primes! Here $m! = m \times (m-1) \times (m-2) \times \cdots \times 1$.

Work of Yitang Zhang



Yitang Zhang obtained Ph.D. in Purdue in 1991. He worked in fast food chains for a while. But he never gave up thinking math. In 2013, he proved ...

A big step to the twin primes conjecture

Theorem

There is a big number B so that there are infinite many prime pairs (p_m, p_{m+1}) with gap $p_{m+1} - p_m \leq B$.

If $B = 2$ then Zhang proved the twin primes conjecture. But he can only show such B exists and this is still a great achievement. So far B was improved to be 246 in 2014.

Zhang used **Calculus** invented by

to count primes!

Example

let $\pi(x) =$ number of primes $p \leq x$. Calculus shows that

$$\pi(x) \text{ approximates } \frac{x}{\ln x}$$

Conjecture (1+1)

Any even number $n > 2$ can be written as a sum of two primes:

$$n = p + q.$$

Example

4= 2+2, 6= 3+3, 8 = 3+5, 10 = 5+5 , 12= 7+5 , 14= 7+7, 16 = 11+5, 18= 13+5...

In 1973, Jingrun Chen (1933 – 1996) proved that

Theorem (1+2)

For any sufficient large even number n,

$$n = p + q \text{ or } n = p + q_1 q_2$$

where p, q, q_1, q_2 are primes.

Goldbach's Conjecture

Conjecture (1+1)

Any even number $n > 2$ can be written as a sum of two primes:

$$n = p + q.$$

Example

4= 2+2, 6= 3+3, 8 = 3+5, 10 = 5+5 , 12= 7+5 , 14= 7+7, 16 = 11+5, 18= 13+5...

In 1973, Jingrun Chen (1933 – 1996) proved that

Theorem (1+2)

For any sufficient large even number n,

$$n = p + q \text{ or } n = p + q_1 q_2$$

where p, q, q_1, q_2 are primes.

Goldbach's Conjecture

Conjecture (1+1)

Any even number $n > 2$ can be written as a sum of two primes:

$$n = p + q.$$

Example

4= 2+2, 6= 3+3, 8 = 3+5, 10 = 5+5 , 12= 7+5 , 14= 7+7, 16 = 11+5, 18= 13+5...

In 1973, Jingrun Chen (1933 – 1996) proved that

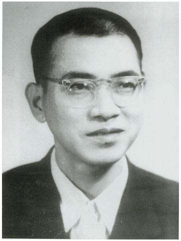
Theorem (1+2)

For any sufficient large even number n,

$$n = p + q \text{ or } n = p + q_1 q_2$$

where p, q, q_1, q_2 are primes.

Math Hero: Jingrun Chen



Jingrun Chen obtained this milestone work in a very difficult time in China. I am highly inspired by his work and life which has lead to devoting myself to mathematics.

Fermat's Last Theorem (FLT)

In 1637, Pierre de Fermat raised the following conjecture

Theorem (FLT)

For $n \geq 3$ (How about $n = 2$?), the equation

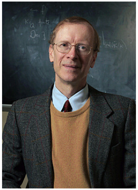
$$x^n + y^n = z^n \tag{1}$$

has no nonzero integral solution.

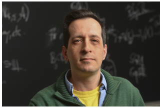
In 1637 in the margin of a copy of *Arithmetica*, Fermat claimed he had a proof that was too large to fit in the margin.

However, the first successful proof was given by Andrew Wiles in 1994.

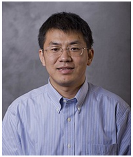
My connection to FLT



Sir Andrew Wiles



Prof. Brian Conrad



Me

Tools in FLT

To solve FLT, mathematicians develop tons of tools which greatly improved mathematics. Here we just mention:

1. Linear algebra
2. Galois group representation
3. Algebraic geometry

Matrix

Linear algebra is a game of

Actually, matrix is fundamental for AI (artificial intelligence), which humans are fighting against in the future (hopefully only in the movie).

Real Matrix

Real matrices in linear algebra look like:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \quad \begin{bmatrix} x \\ y \end{bmatrix}.$$

The key feature of matrices is that they can do *arithmetic*:

Example

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 2y \\ 3x + 4y \end{bmatrix}.$$

Évariste Galois

Évariste Galois was a French mathematician (1811 – 1832). He devoted himself to the French revolution of 1830. Just before his deadly duel, he finished his manuscripts, which could only be fully understood a decade later. These manuscripts laid the foundation of abstract algebra.

Root formula for algebraic equation

For quadratic equation $x^2 + bx + c = 0$, the formula of roots is

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

For cubic and quartic (degree 4) equations, there are also formulas, but extremely complicated. How about an equation of degree 5 or larger?

Theorem (Galois, Able)

There is no root formula (similar to that of quadratic equation) for an equation of degree 5 or larger.

Example

$x^5 - x - 1$

Root formula for algebraic equation

For quadratic equation $x^2 + bx + c = 0$, the formula of roots is

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

For cubic and quartic (degree 4) equations, there are also formulas, but extremely complicated. How about an equation of degree 5 or larger?

Theorem (Galois, Able)

There is no root formula (similar to that of quadratic equation) for an equation of degree 5 or larger.

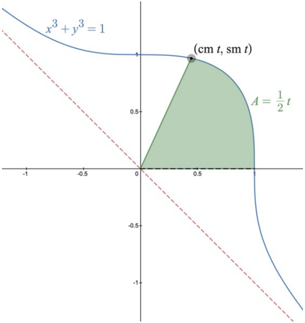
Example

$x^5 - x - 1$

Algebraic Geometry

If $x^n + y^n = z^n$ would have nontrivial solution, then $(\frac{x}{z}, \frac{y}{z})$ would be *rational* points of curve

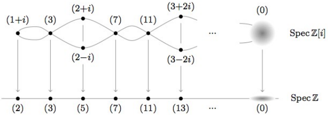
$$X^n + Y^n = 1 \qquad (2)$$



So FLT is equivalent to that the above curve has no rational points. But it is still very difficult from this point of view.

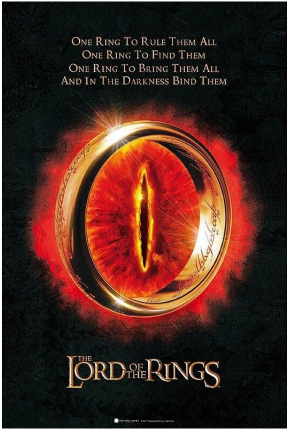
Modern algebraic geometry and Grothendieck

Starting from French mathematician Alexander Grothendieck (1928-2014), integer $\mathbb{Z}$ is regarded as a *curve* and primes are *points* in the curve.



Modern algebraic geometry heavily uses the theory of *rings*. For example, $\mathbb{Z}$ is a ring. So Grothendieck is regarded as

The Lord of Rings!



Who am I?

So if Grothendieck is the lord of rings, as a follower of Grothendieck, I must be

one of the ugly orcs!

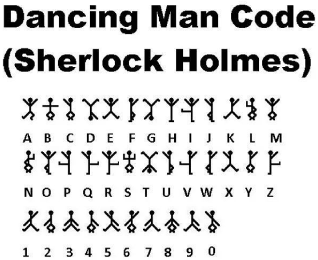
Risk of online shopping

Online shopping is enjoyable

But what if someone is in the middle to eavesdrop?

Classical encryption

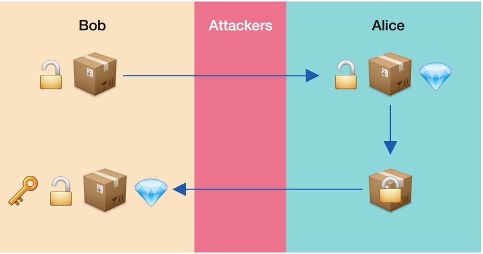
We must encrypt our message to communicate with the online store. But classical encryption always needs some pre-arrangement to make keys, for example,



But clearly it is not feasible to make pre-arrangement between us and online store. Note that evil attacker sits in the middle. He or she might know everything on our communication with online store!

Safebox and key

The idea of RSA is similar to the use of a safebox and key:



Here Bob= online store, Alice = us, and Diamond = our secret information to send, say, credit card number.

RSA algorithm

The key point of RSA: The safebox = (m, ℓ) where $m = pq$ with p, q being very LARGE primes. Pick ℓ so that $\ell, (p-1)(q-1)$ are relatively prime.

We write $z \equiv r \mod m$ if z is divided by m with remainder r. Let s be the secret message of Alice.

1. Bob sends (m, ℓ) to Alice;
2. Encryption: Alice computes

$$x = s^{\ell} \mod m$$

   and sends x back to Bob;
3. Decryption:
   1. Bob computes k so that $k\ell = 1 \mod (p-1)(q-1)$;
   2. Bob computes $x^k \mod m = s \mod m$ to find s.

A toy example

Pick $p = 5, q = 7$ and $\ell = 5$. Secret message $s = 3$. Note that $(p-1)(q-1) = 24$.

1. Bob sends $(35, 5)$ to Alice;
2. Encryption: Alice computes
$$x = 3^5 \mod 35 = 243 \mod 35 = 33 \mod 35$$
and sends 33 back to Bob;
3. Decryption:
    1. Bob computes $k = 5$ so that $k\ell = 25 = 1 \mod 24$;
    2. Bob computes $33^5 \mod 35$ to find $s = 3$.

Why RSA is safe ?

The Attacker can also see (m, ℓ) and $x = s^\ell \mod m$. But to know s then $k \mod (p-1)(q-1)$ is needed. Now here is the key point: From m, it is very hard to find prime factorization pq to compute $(p-1)(q-1)$.

Example

$703 = pq$ for two primes, what are p and q?

For RSA-2048 we use two 1,024-bit prime numbers, which have more then 250 digits! For now, public key cryptography is effectively impossible to breach. With existing computing technology, one estimate holds it would take at least 300 years to “brute force” an RSA 2048-bit key.

Thank all of you for help:

Ninghui Li,

Jiuluo Liu, Katie Liu, Kevin Liu,

Yue Yin