Prime Numbers

素数表

Write Prime Numbers With a Serene Mind

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71
73 79 83 89 97 (25個)

101 103 107 109 113 127 131 137 139 149 151 157 163 167 173
179 181 191 193 197 199 (21個)

211 223 227 229 233 239 241 251 257 263 269 271 277 281
283 293 (16個)

307 311 313 317 331 337 347 349 353 359 367 373 379 383
389 397 (16個)

401 409 419 421 431 433 439 443 449 457 461 463 467 479
487 491 499 (17個)

503 509 521 523 541 547 557 563 569 571 577 587 593 599
(14個)

601 607 613 617 619 631 641 643 647 653 659 661 673 677
683 691 (16個)

701 709 719 727 733 739 743 751 757 761 769 773 787 797
(14個)

809 811 821 823 827 829 839 853 857 859 863 877 881 883
887 (15個)

907 911 919 929 937 941 947 953 969 971 977 983 991 997
(14個)

1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091
1093 1097 (16個)

1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 (12個)

1201 1213 1217 1223 1229 1231 1237 1249 1259 1277 1279 1283 1289 1291
1297 (15個)

1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 (11個)

1409 1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487

1489 1493 1499 (17個)

1511 1523 1531 1543 1549 1553 1559 1567 1571 1579 1583 1597 (12個)

1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697

(14個)

1709 1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 (12個)

1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879 1889 (12個)

1901 1907 1913 1931 1933 1949 1951 1973 1979 1987 1993 1997 1999 (13個)

Prime numbers are infinite. (B.C.3 Proved by Euclid in "The Elements" .

Prime number theorem (1896 Proved by Hadamard and de la Vallee Poussin.)

When $x \to \infty$

$$\frac{\text{number of primes smaller than } x}{\left(\frac{x}{\log(x)}\right)} \longrightarrow 1$$

Compared to $\frac{x}{\log(x)}$, $\int_2^x \frac{1}{\log(t)}\,dt$ approximates "number of primes smaller than x" better.

This means, around x, "probability" of a number being a prime is about $\frac{1}{\log(x)}$

$$\frac{1}{\log 1000} = 0.144\cdots$$

$$\frac{1}{\log 2000} = 0.131\cdots$$

$4n+1$ type primes 5 13 17 29 37 41 53 61 73 89 97

$4n+3$ type primes 3 7 11 19 23 31 43 47 59 67 71 79 83

$3n+1$ type primes 7 13 19 31 37 43 61 67 73 79 97

$3n+2$ type primes 2 5 11 17 23 29 41 47 53 59 71 83 89

$8n+1$ type primes 17 41 73 89 97

$8n+3$ type primes 3 11 19 43 59 67 83

$8n+5$ type primes 5 13 29 37 53 61

$8n+7$ type primes 7 23 31 47 71 79

Dirichlet's Prime Number Theorem

(mid-19th Century)

When a, b Co Primes,

$an+b$ type primes exist infinitely.

Green-Tao Theorem (2004)

They are arbitrarily long arithmetic progressions of prime numbers.

arithmetic progression of prime numbers
with common difference 4 11, 17, 23, 29

arithmetic progressions of prime numbers 7, 37, 67, 97, 127, 157
with common difference 30

- n^2+1 type primes $\quad 2=1^2+1,\ 5=2^2+1,\ 17=4^2+1,\ 37=6^2+1$
  $101=10^2+1,\ 197=14^2+1,\ \cdots\cdots$

- 2^n-1 type primes $\quad 3=2^2-1,\ 7=2^3-1,\ 31=2^5-1,\ \cdots$
  (Mersenne primes)

- 2^n+1 type primes $\quad 3=2^1+1,\ 5=2^2+1,\ 17=2^4+1,\ 257=2^8+1,\ \cdots$
  (Fermat primes)

An n-sided regular polygon can be constructed with a compass and a straightedge

$\Leftrightarrow$ $N = (\text{power of } 2) \times$ the product of 2 distinct Fermat primes.

- Twin primes (p & $p+2$ are both primes)

  3 & 5, 5 & 7, 11 & 13, 17 & 19, 29 & 31, $\cdots\cdots$

- Prime quadruplets (p, $p+2$, $p+6$, $p+8$ are all primes

  (5, 7, 11, 13), (11, 13, 17, 19), (101, 103, 107, 109),

  (191, 193, 197, 199), (821 823 827 829) (1481, 1483, 1487, 1489)

  (1871, 1873, 1877, 1879) (2081, 2083, 2087, 2089), $\cdots$

These numbers could exist infinitely,

but it is not yet proved if they do.

The Mystery of nature is condensed into the mystery of numbers.

The Mystery of numbers is condensed into the mystery of nature.

mysterious relationship between

circle ratio π and prime numbers

$$\frac{\pi}{4} = \frac{1}{1+\frac{1}{3}} \times \frac{1}{1-\frac{1}{5}} \times \frac{1}{1+\frac{1}{7}} \times \frac{1}{1+\frac{1}{11}} \times \frac{1}{1-\frac{1}{13}}$$

$$\times \frac{1}{1-\frac{1}{17}} \times \frac{1}{1+\frac{1}{19}} \times \frac{1}{1+\frac{1}{23}} \times \cdots\cdots$$

For a prime number p whose remainder is 1 when divided by 4,

multiply $\frac{1}{1-\frac{1}{p}}$

For a prime number p whose remainder is 3 when divided by 4,

multiply $\frac{1}{1+\frac{1}{p}}$

Prime Numbers Song

The song of prime numbers sounds Tonnkarari,
Tonkara rinrin ruririrurero
We can hear if we keep our ears open,
We can hear their joyful song.

The song of prime numbers sounds Chinnkarari,
Chinnkara rinrin ruririrurero
Prime numbers sing together in harmony
The song of love in the land of prime numbers.

The song of prime numbers sounds Korokororo,
Kororin kororin korokororo
Star child with a kind heart
The song is pure like his wish in the heart.

The song of prime numbers sounds Piihyarara,
Piihyara ranran rarirurero
Rabbits and deers are listening the song.
Mysterious sound of whistle in the woods.

The song of prime numbers sounds Ponnpororo,
Pororin pororin poropororo
Prime numbers are seeing dreams,
They sing the dreams for tomorrow

Pierre de Fermat (1601-1665)

$$x^n + y^n = z^n \qquad (n \geqq 3)$$

Had no solutions in non-zero integers.

I have a truly marvelous proof of this proposition which this margin is too narrow to contain.

Fermat's other theorems (Entrance into class field theory)

Theorem

A prime number p whose remainder is 1 when divided by 4

$$p = x^2 + y^2 \qquad (x,\ y : \text{integer})$$

could be written as above.

$5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$ etc.

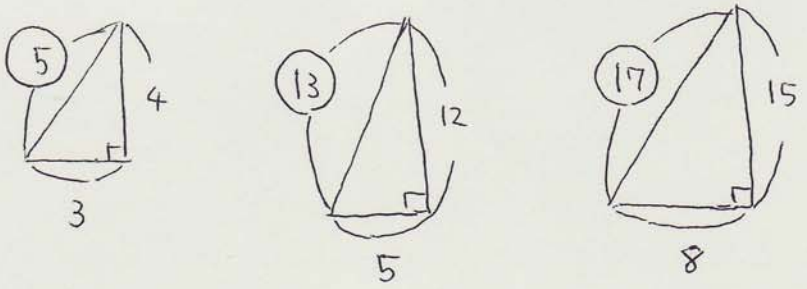
This does not stand for a number whose remainder is 3.

Theorem

A prime number p whose remainder is 1 when divided by 4

$$p^2 = x^2 + y^2 \qquad (x,\ y : \text{integer})$$

satisfies the formula above. This means that p could be a hypotenuse of a right triangle length of whose 3 sides are integers.



This does not stand for a prime whose remainder is 3.

Theorems (The entrance into the class field theory that Fermat discovered)

For a prime number P,

(1) $P = x^2 + y^2$ Integers x, y that satisfy the expression exist.

$\Longleftrightarrow$ equivalent

remainder is 1 when P is divided by 4, or P=2

(2) $P = x^2 - 2y^2$ Integers x, y that satisfy the expression exist.

$\Longleftrightarrow$ equivalent

remainder is 1 or 7 when P is divided by 8, or P=2

(3) $P = x^2 + 2y^2$ Integers x, y that satisfy the expression exist.

$\Longleftrightarrow$ equivalent

remainder is 1 or 3 when P is divided by 8, or P=2

(4) $P = x^2 + 3y^2$ Integers x, y that satisfy the expression exist.

$\Longleftrightarrow$ equivalent

remainder is 1 when P is divided by 3, or P=3

(5) $P = x^2 - 5y^2$ Integers x, y that satisfy the expression exist.

$\Longleftrightarrow$ equivalent

remainder is 1 or 4 when P is divided by 5, or P=5

Ex.

A prime whose remainder is 1 when divided by 4 somehow could be expressed as $x^2 + y^2$

$5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$

$37 = 6^2 + 1^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$, $61 = 6^2 + 5^2$

$73 = 8^2 + 3^2$, $89 = 8^2 + 5^2$, $97 = 9^2 + 4^2$

A prime whose remainder is 1 or 7 when divided by 8 somehow could be expressed as $x^2 - 2y^2$

$7 = 3^2 - 2\times1^2$, $17 = 5^2 - 2\times2^2$, $23 = 5^2 - 2\times1^2$

$31 = 7^2 - 2\times3^2$, $41 = 7^2 - 2\times2^2$, $47 = 7^2 - 2\times1^2$

$71 = 11^2 - 2\times5^2$, $73 = 9^2 - 2\times2^2$, $79 = 9^2 - 2\times1^2$

$89 = 11^2 - 2\times4^2$, $97 = 13^2 - 2\times6^2$

A prime whose remaider is 1 or 3 when divided by 8
could somehow be expressed as x^2+2y^2

$3=1^2+2\times1^2$, $11=3^2+2\times1^2$, $17=3^2+2\times2^2$
$19=1^2+2\times3^2$, $41=3^2+2\times4^2$, $43=5^2+2\times3^2$
$59=3^2+2\times5^2$, $67=7^2+2\times3^2$, $73=1^2+2\times6^2$
$89=9^2+2\times2^2$, $97=5^2+2\times6^2$

A prime whose remainder is 1 when divided by 3
could somehow be expressed as x^2+3y^2

$7=2^2+3\times1^2$, $13=1^2+3\times2^2$, $19=4^2+3\times1^2$
$31=2^2+3\times3^2$, $37=5^2+3\times2^2$, $43=4^2+3\times3^2$
$61=7^2+3\times2^2$, $67=8^2+3\times1^2$, $73=5^2+3\times4^2$
$79=2^2+3\times5^2$, $97=7^2+3\times4^2$

A prime whose remainder is 1 or 4 when divided by 5
could somehow be expressed as x^2-5y^2

$11=4^2-5\times1^2$, $19=8^2-5\times3^2$, $29=7^2-5\times2^2$
$31=6^2-5\times1^2$, $41=11^2-5\times4^2$, $59=8^2-5\times1^2$
$61=9^2-5\times2^2$, $71=14^2-5\times5^2$, $79=22^2-5\times9^2$
$89=13^2-5\times4^2$

The Stream of Class Field Theory

Fermat's studies, from the 1630s

↓

Law of quadratic reciprocity (Gauss, 1796)

↓ contribution by Kummer, Hilbert

Completion of class field theory Sadaharu Takagi (1920)

↓

Actions to exceed class field theory were taken using modular theorems such as "Taniyama-Shimura conjecture"

Non-commutative class field theory was formulated. (Langlands, around 1970)

Entry into the period of development (1994～)

1994. Wiles solved most of Taniyama-Shimura conjecture and proved Fermat's last theorem

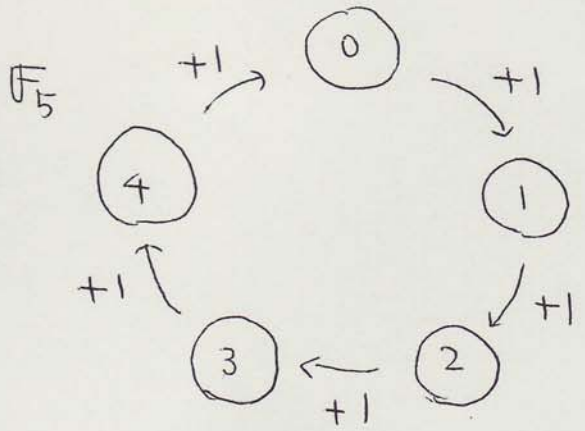
2006. Taylor proved most of Sato-Tate conjecture

↓

Non-commutative class field theory is yet to be completed.

Remainders when divided by 5: $\mathbb{F}_5$

$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$



In $\mathbb{F}_5$ $\quad 5 = 0,\ 6 = 1,\ 7 = 2,\ 8 = 3,\ \cdots,\ 10 = 0,\ \cdots$

$4 + 2 = 6 = 1$ (So, $1 - 2 = 4$)

$4 \times 2 = 8 = 3$ (So, $3 \div 2 = 4$)

The world of remainders when divided by a prime P: $\mathbb{F}_p$

$\mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}$

Four arithmetic operations are possible here.

Theorems (one of the law of quadratic reciprocity,
the entrance into class field theory)

(1) $\mathbb{F}_p$ has a square-root of -1.

$\Longleftrightarrow$ The remainder is 1 when P is divided by 4, or P=2
equivalent

(2) $\mathbb{F}_p$ has a square-root of 2.

$\Longleftrightarrow$ The remainder is 1 or 7 when P is divided by 8, or P=2
equivalent

(3) $\mathbb{F}_p$ has a square-root of -2.

$\Longleftrightarrow$ The remainder is 1 or 3 when P is divided by 8, or P=2
equivalent

(4) $\mathbb{F}_p$ has a square-root of -3.

$\Longleftrightarrow$ The remainder is 1 when P is divided by 3, or P=3
equivalent

(5) $\mathbb{F}_p$ has a square-root of 5.

$\Longleftrightarrow$ The remainder is 1 or 4 when P is divided by 5, or P=5
equivalent

Ex. For a prime P whose remainderis 1 when divided by 4, $\mathbb{F}_p$ has a square root of -1.

$2^2 \equiv -1 \mod 5$ $\quad$ $5^2 \equiv -1 \mod 13$

For a prime P whose remainderis 1 or 7 when divided by 8, $\mathbb{F}_p$ has a square root of 2.

$3^2 \equiv 2 \mod 7$ $\quad$ $6^2 \equiv 2 \mod 17$

For a prime P whose remainderis 1 or 3 when divided by 8, $\mathbb{F}_p$ has a square root of -2.

$1^2 \equiv -2 \mod 3$ $\quad$ $3^2 \equiv -2 \mod 11$

For a prime P whose remainderis 1 when divided by 3, $\mathbb{F}_p$ has a square root of -3.

$2^2 \equiv -3 \mod 7$ $\quad$ $7^2 \equiv -3 \mod 13$

For a prime P whose remainderis 1 or 4 when divided by 5, $\mathbb{F}_p$ has a square root of 5.

$4^2 \equiv 5 \mod 11$ $\quad$ $9^2 \equiv 5 \mod 19$

Law of Quadratic Reciprocity

When p and q are different primes and not 2,

(1) $\mathbb{F}_p$ has a square root of q

(2) $\mathbb{F}_q$ has a square root of p

Suppose these conditions above (which seems indifferent to each other) Except in case of $(*)$,

we have (1) $\Longleftrightarrow$ (2)
equivalent

$(*)$ When both remainders of p divided by 4 and q divided by 4 are 3.

In case of $(*)$ (1) $\Longleftrightarrow$ ((2) not)
equivalent

((1) not $\Longleftrightarrow$ (2))
equivalent

Class Field Theory Expresses How Primes are Split When the World of Numbers Enlarges.

When the world of rational number $\mathbb{Q}$ enlarges into $i = \sqrt{-1}$ containing world, $\mathbb{Q}(i)$

A prime whose remainder is 1 when divided by 4 splits into 2 numbers.

(Ex. $5 = 2^2 + 1^2 = (2+i)(2-i)$, $13 = 3^2 + 2^2 = (3+2i)(3-2i)$

$17 = 4^2 + 1^2 = (4+i)(4-i)$, $29 = 5^2 + 2^2 = (5+2i)(5-2i)$)

A prime whose remainder is 3 when divided by 4 does not split.

I got split.

I' m ok.

When $\mathbb{Q}$ enlarges into $\mathbb{Q}(\sqrt{2})$

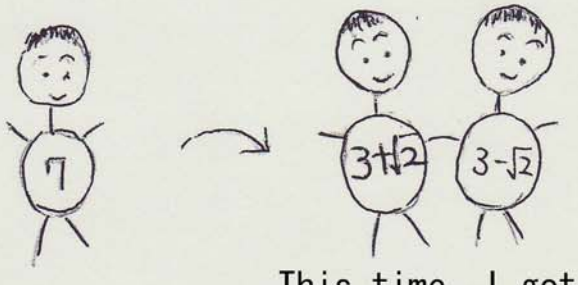
a prime whose remainder is 1 or 7 when divided by 8 splits into 2 numbers.

(Ex. $7 = 3^2 - 2\times 1^2 = (3+\sqrt{2})(3-\sqrt{2})$, $17 = 5^2 - 2\times 2^2 = (5+2\sqrt{2})(5-2\sqrt{2})$

$23 = 5^2 - 2\times 1^2 = (5+\sqrt{2})(5-\sqrt{2})$, $31 = 7^2 - 2\times 3^2 = (7+3\sqrt{2})(7-3\sqrt{2})$)

A prime whose remainder is 3 when divided by 8 does not split.

Now, I' m ok.

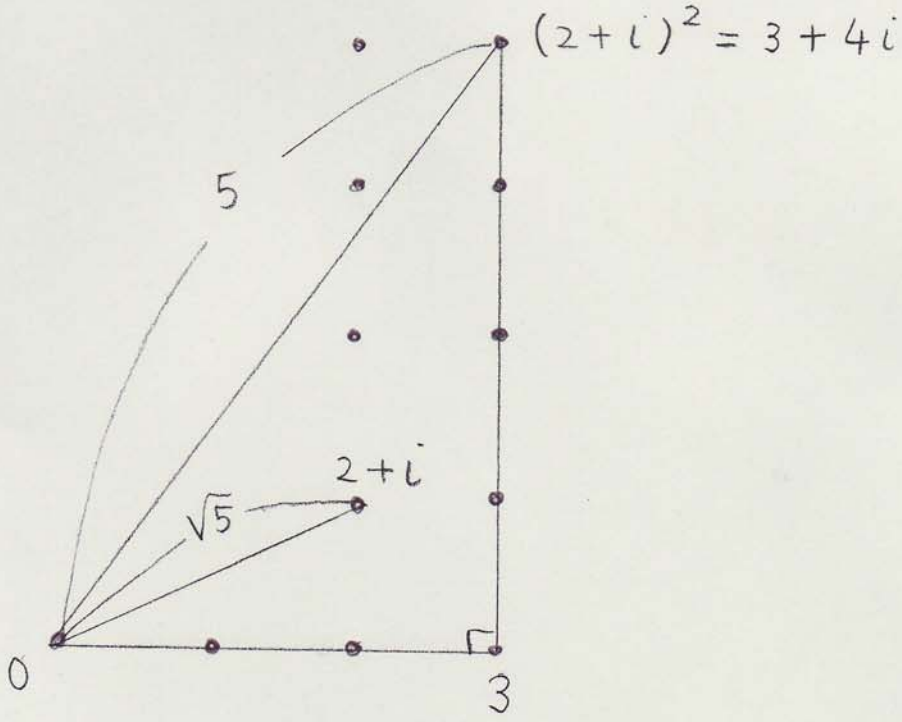


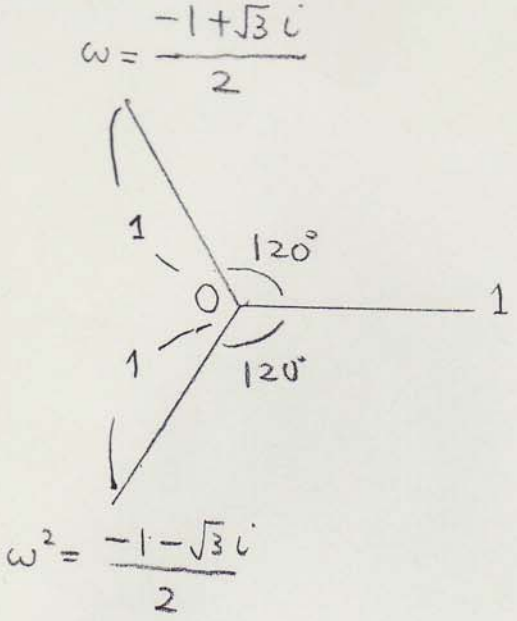
This time, I got split.

$$5 = 2^2 + 1^2 = (2+i)(2-i)$$

From splitting of 5,

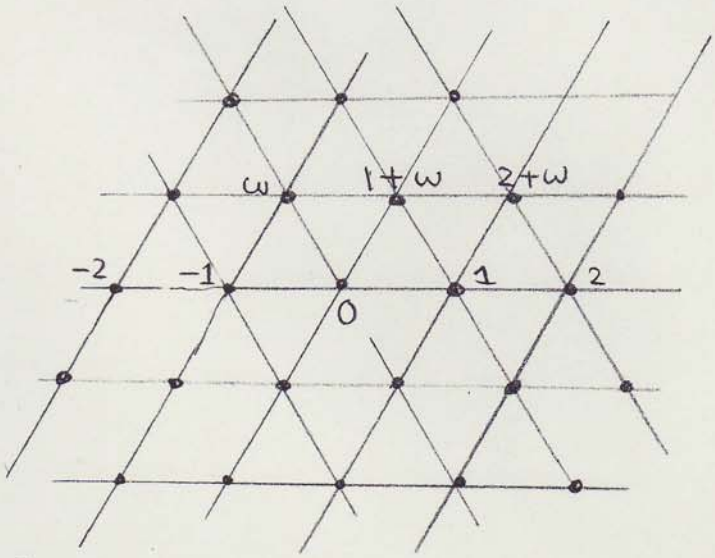
3, 4, 5 right triangle is born.





$\omega^3 = 1$

The world of ω $\{a + b\omega \mid a, b : \text{integers}\}$



In the world of ω the prime whose remainder is 1 when divided by 3 splits into 2 numbers, and the prime whose remainder is 2 when divided by 3 does not split.

$7 = (2-\omega)(2-\omega^2)$

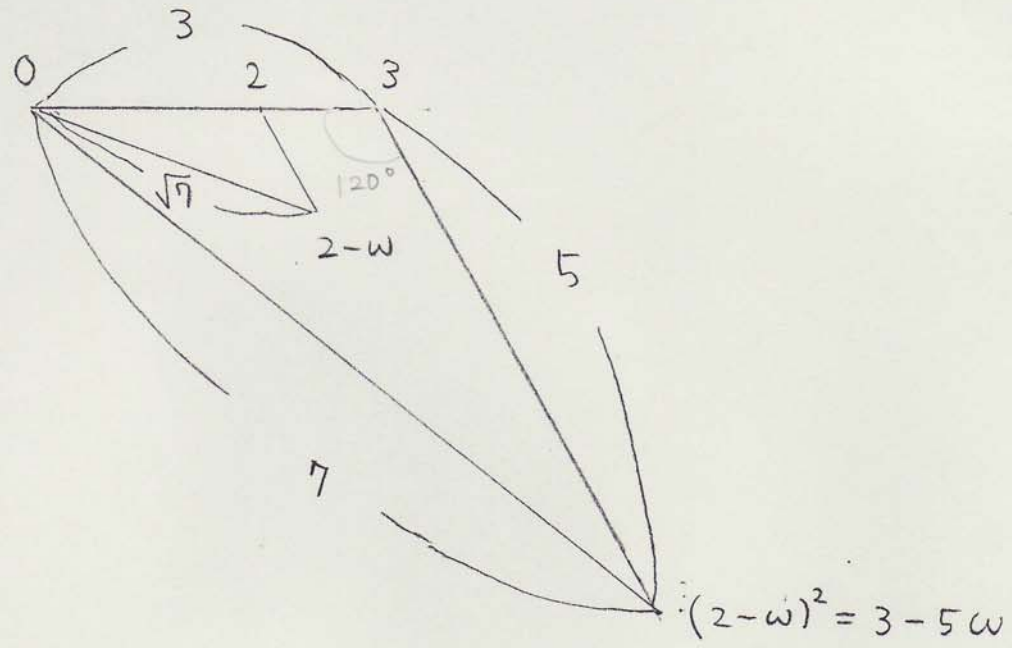
$13 = (3-\omega)(3-\omega^2)$

$19 = (3-2\omega)(3-2\omega^2)$

$$7 = (2-\omega)(2-\omega^2)$$

From the splitting of 7,

7, 5, 3 triangle with an angle of 120° is born



A prime whose remainder is 1 when divided by 3

appears at the opposite side of 120° angle

of a triangle with 120° angle and whose sides are integers.

This does not happen with a prime whose remainder is 2 when divided by 3.

The World Behind

law of universal gravitation

expression

The earth and an apple pull each other.

The apple falls from a tree,

The World Behind

class field theory

expression

120°-angle 7, 5, 3 triangle appears.

The Seven-Five-Three Festival

高貞治

Teiji Takagi

1925年ごろ

京都府 (Kyoto Prefecture)

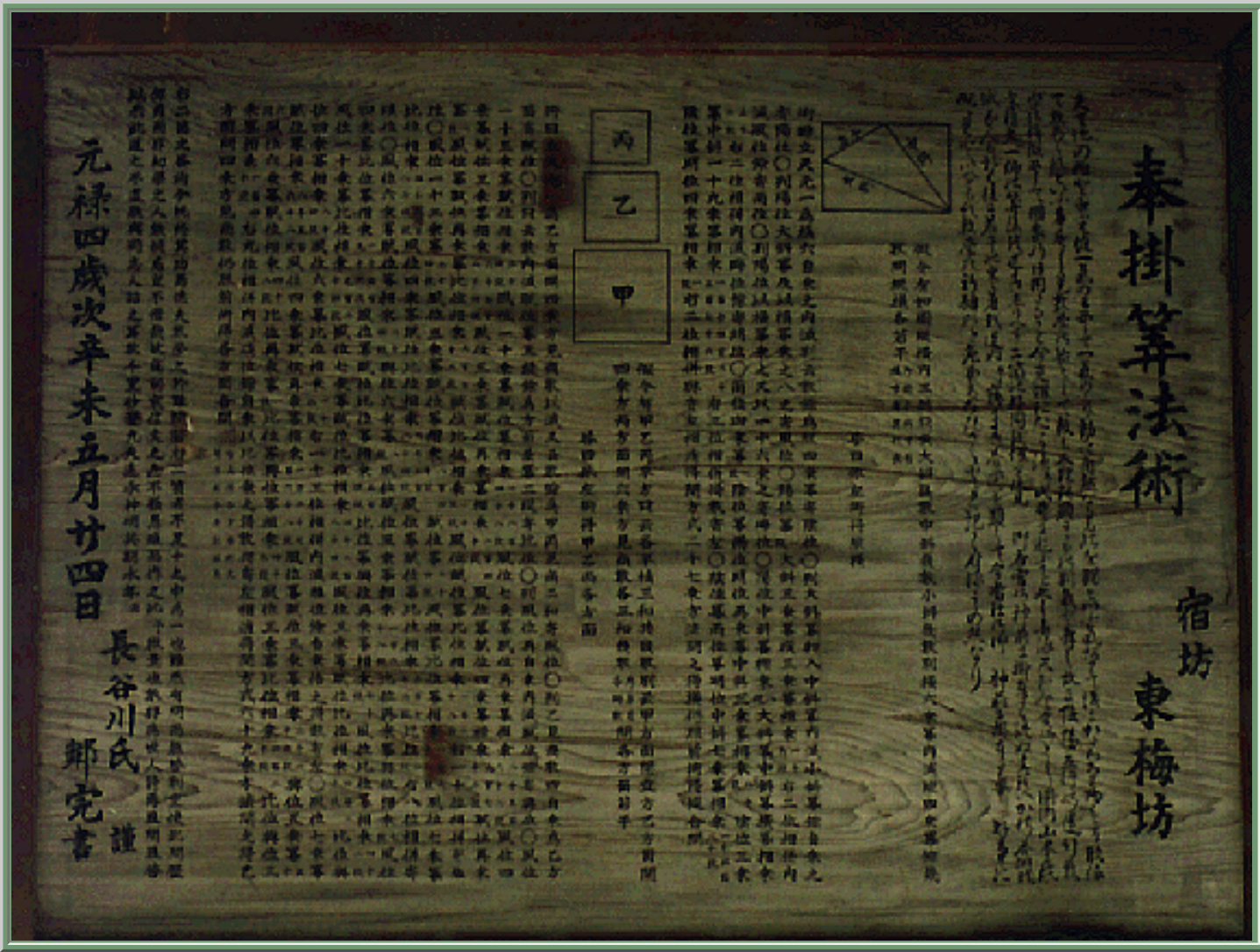
北野天満宮1

DATA:
京都市上京区　北野天満宮
貞亨3年(1686)　今西小右衛門重之　飯田武助正成　奉納
95×190cm
昭和57年　松崎利雄氏発見　山本了三，吉田柳二氏調査
完全な形で現存する日本最古の算額.
算額の上に別の絵馬が画かれ，その絵具の剥落した部分から算額の一部があらわれている.
参考文献：近畿の算額［近畿数学史学会著］大阪教育図書　1992

Home Page 八坂神社 天満宮2

京都府(Kyoto Prefecture)

八坂神社



DATA:
京都市東山区　八坂神社
元禄4年(1691)　長谷川鄰完　奉納
93×123.5cm
昭和50年　日本数学史学会近畿支部　復元
御香宮の遺題を解答した算額
参考文献：近畿の算額［近畿数学史学会著］大阪教育図書　1992

Home Page 御香宮2 天満宮1

愛媛県(Ehime Prefecture)

伊佐爾波神社18(Isaniwa Shrine No.18)

DATA:
松山市　伊佐爾波神社
明治6年(1873)12月　高阪金次郎峻則　奉納
75.2×91.1cm
参考文献：愛媛の算額［浅山秀博・武田三千雄著］自家版 1982
　　九州・四国の現存算額探訪必携［米光　丁著］自費出版　平成4年

Home Page 伊佐爾波神社17 伊佐爾波神社19

算法少女

遠藤 寛子 著

父から和算を学ぶ町娘あきは、算額に誤りを見つけ声を上げた。と、若侍が…。和算への誘いとして定評の少年少女向け歴史小説。箕田源二郎・絵

シリーズ:ちくま学芸文庫
定価:945円（税込）
Cコード:0141
整理番号:エ-11-1
刊行日: 2006/08/09
判型:文庫判
ページ数:272
ISBN:4-480-09013-4
JANコード:9784480090133

在庫 問合せ

遠藤 寛子
エンドウ ヒロコ

この著作者の本

算法少女

この著作者の本の一覧をみる

著作者からのメッセージ

「算法少女」この不思議の書をめぐって　遠藤寛子［全文を読む］

この本の内容

父・千葉桃三から算法の手ほどきを受けていた町娘あきは、ある日、観音さまに奉納された算額に誤りを見つけ声をあげた…。その出来事を聞き及んだ久留米藩主・有馬侯は、あきを姫君の算法指南役にしようとするが、騒動がもちあがる。上方算法に対抗心を燃やす関流の実力者・藤田貞資が、あきと同じ年頃の、関流を学ぶ娘と競わせることを画策。はたしてその結果は…。安永４（１７７５）年に刊行された和算書『算法少女』の成立をめぐる史実をていねいに拾いながら、豊かに色づけた少年少女むけ歴史小説の名作。江戸時代、いかに和算が庶民の間に広まっていたか、それを学ぶことがいかに歓びであったかを、いきいきと描き出す。

この本への感想投稿

本書をお読みになったご意見・ご感想などをお寄せください。
投稿されたお客様の声は、弊社HP、また新聞・雑誌広告などに掲載させていただくことがございます。
※は必須項目です。おそれいりますが、必ずご記入をお願いいたします。

ご意見、ご感想 *

A mysterious Fact Which is a Part of Non-Commutative Class Field Theory

Ex 1. Inside $\mathbb{F}_p$ number of answers for $x^3 = 2$

p	2	3	5	7	11	13	17	19	23	29	31
number of answers N_p	1	1	1	0	1	0	1	0	1	1	3
$N_p - 1$	0	0	0	-1	0	-1	0	-1	0	0	2

(N_{31} is 3

$4^3 = 64 = 31 \times 2 + 2 \equiv 2 \mod 31$, $7^3 = 20^3 \equiv 2 \mod 31$)

The very mysterious thing is ...

Suppose $q \prod_{n=1}^{\infty} (1-q^{6n})(1-q^{18n})$

$= q(1-q^6)(1-q^{18})(1-q^{12})(1-q^{36})(1-q^{18})(1-q^{54}) \cdots$

$= q - q^7 - q^{13} - q^{19} + q^{25} + 2q^{31} \cdots$

is $\sum_{n=1}^{\infty} a_n q^n = a_1 q + a_2 q^2 + a_3 q^3 + \cdots$

($a_1 = 1$, $a_2 = 0$, $a_7 = -1$ etc.)

$N_p - 1 = a_p$

stands for all primes p.

ex. 2 in $\mathbb{F}_p$, how many $y^2 = x^3 + 1$ are contained?

answers to

P	2	3	5	7	11	13	17	19	23	29	31
# of answers N_p	2	3	5	11	11	11	17	11	23	29	35
$p - N_p$	0	0	0	-4	0	2	0	8	0	0	-4

When N_5 is 5

answers in $\mathbb{F}_5$ are, for example, $2^2 = 2^3 + 1$

$(2, 2), (2, 3), (0, 1), (0, 4), (4, 0)$ 5 answers are contained.

The mystery :

$$q \prod_{n=1}^{\infty} (1 - q^{6n})^4 = q - 4q^7 + 2q^{13} + 8q^{19} - 5q^{25} - 4q^{31} \cdots$$

Express above as $\sum_{n=1}^{\infty} a_n q^n$.

$$p - N_p = a_p$$

This stands for all primes P.

Ex. 3 In $\mathbb{F}_p$, how many anseres for $y^2+y=x^3-x^2$ are there?

p	2	3	5	7	11	13	17	19	23
number of answers N_p	4	4	4	9	10	9	19	19	24
$p-N_p$	-2	-1	1	-2	1	4	-2	0	-2

The mystery:

$$q\prod_{n=1}^{\infty}\{(1-q^n)(1-q^{11n})\}^2$$
$$=q-2q^2-q^3+2q^4+q^5+2q^6-2q^7-2q^9-2q^{10}+q^{11}$$
$$-2q^{12}+4q^{13}+4q^{14}-q^{15}-4q^{16}-2q^{17}+4q^{18}+2q^{20}$$
$$+2q^{21}-2q^{22}-q^{23}-4q^{25}\cdots$$

If above is expressed $\sum_{n=1}^{\infty} a_n q^n$

$$p-N_p=a_p$$

is true for all primes p

When the equation $x^3=2$, $y^2=x^3+1$, $y^2+y=x^3-x^2$ elliptic curve cross the sea of prime numbers, a mysterious music is played.

$$q\prod_{n=1}^{\infty}(1-q^{6n})(1-q^{18n}),\quad q\prod_{n=1}^{\infty}(1-q^{6n})^4,\quad q\prod_{n=1}^{\infty}\{(1-q^n)(1-q^{11n})\}^2$$

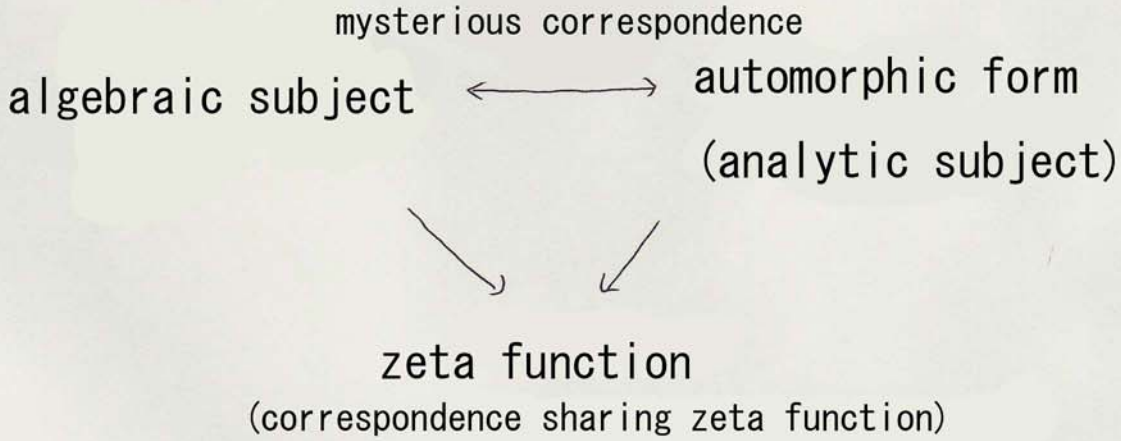
automorphic form

Non-Commutative Class Field Theory:

($x^2=2$, $x^3=2$, $y^2=x^3+1$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ etc.)

like listening to mysterious music that

algebraic subjects play as they cross the sea of primes.



Various things cross the sea of primes.

The sea of primes is our home.

Fermat's last theorem was proved by Wiles in 1994 by solving most of Taniyama-Shimura conjecture.

A strange relationship between elliptic curve and automorphic form

$a^n + b^n = c^n$ Suppose $n \geqq 3$ had an answer.

Then, an elliptic curve

$$y^2 = (x - a^n)\, x\, (x + b^n)$$

becomes an irregular elliptic curve

$$y^2 = (x - A)(x - B)(x - C)$$

which $C - A$, $C - B$, $B - A$ are all power of n.

This elliptic curve $\longleftrightarrow$ Automorphic form

Taniyama-Shimura conjecture

This elliptic curve is so abnormal that the automorphic form becomes an abnormal form that does not exist.

Sato-Tate Conjecture (Mikio Sato, March, 1963)

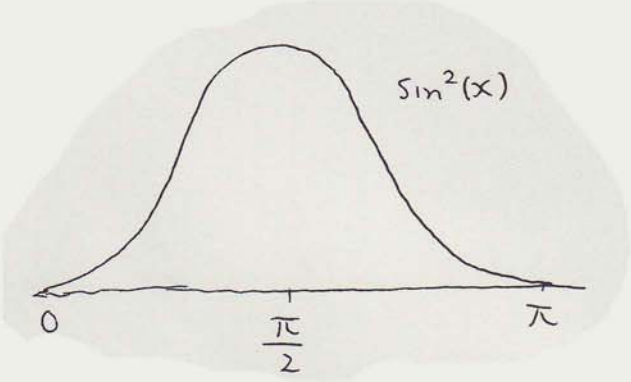
Suppose an elliptic curve with a rational coefficient,

and its N_p, $a_p = p - N_p$

Then, $|a_p| < 2\sqrt{p}$ (Theorem of Hase)

$a_p = 2\sqrt{p}\cos(\theta_p)$ $\quad 0 \leq \theta_p \leq \pi$

Suppose an angle θ_p that satisfies conditions above, θ_p for various primes P is distributed in a shape of $\sin(x)$ when P moves.



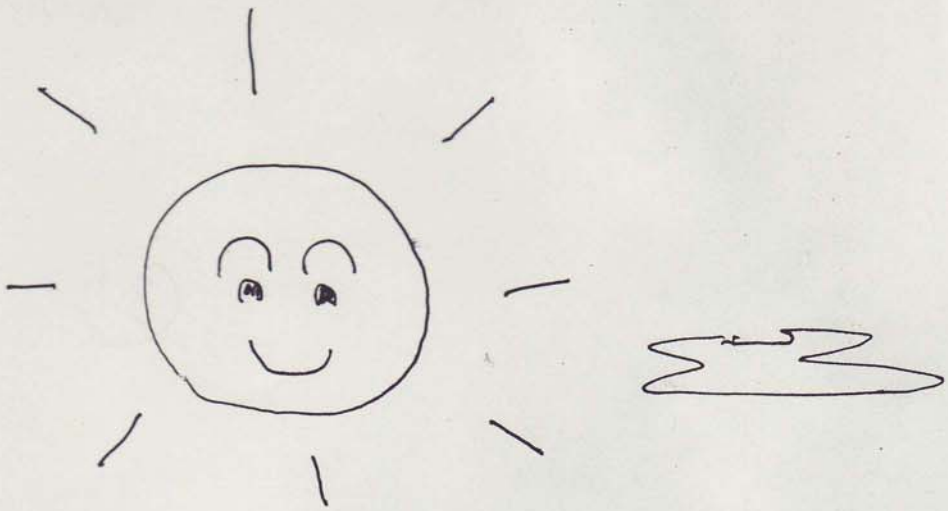
In 2006, a large part of this conjecture was proved by Taylor et al.

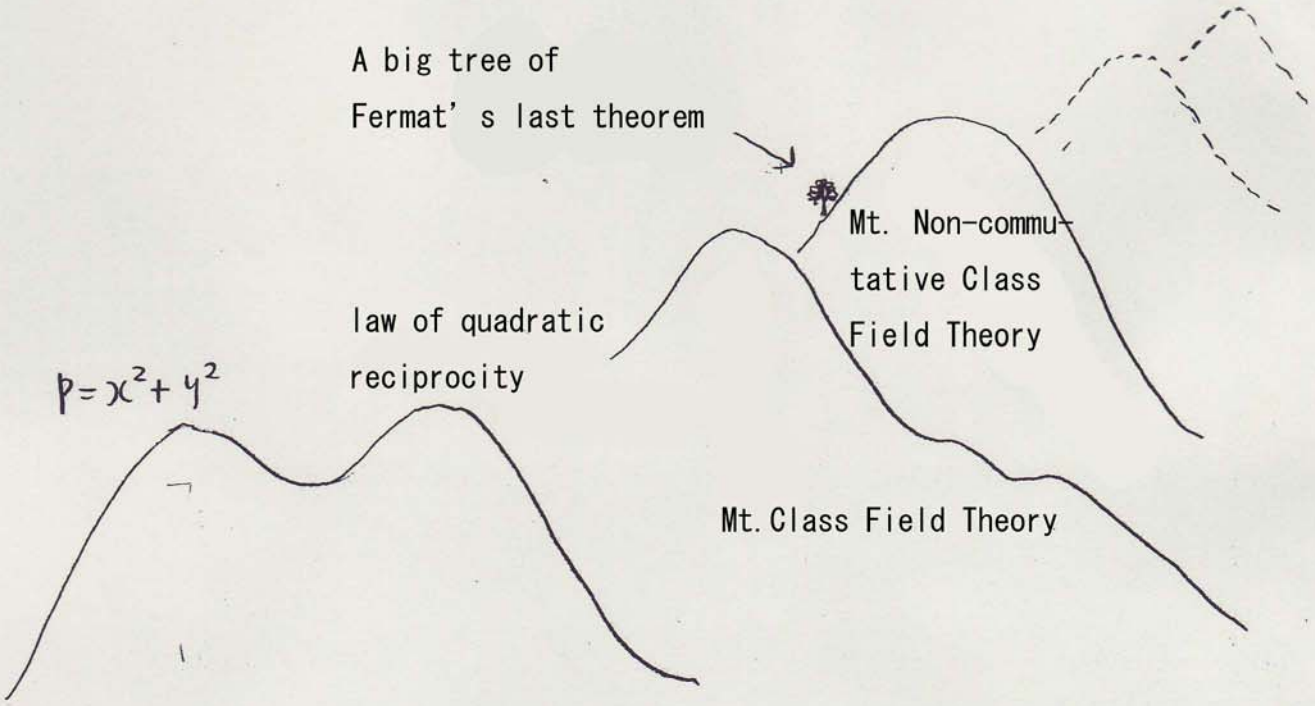
in supposition of the relationship below.

product of n elliptic curves $\longleftrightarrow$ (GL_{n+1} の) automorphic form

non-commutative

($n = 1, 2, 3, \cdots$) class field theory




A big tree of
Fermat's last theorem
Mt. Non-commu-
tative Class
Field Theory
law of quadratic
reciprocity
$p=x^2+y^2$
Mt. Class Field Theory