

素数表

心静かに「写素数」を

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)

素数は無限にある (紀元前3世紀 ユークリッドの「原論」に証明)

素数定理 (1896年 アタマール と, ド・ラ・バレ・プーサンが証明)

$x \rightarrow \infty$ のとき

$\frac{x \text{ 以下の素数の個数}}{\left(\frac{x}{\log(x)} \right)} \rightarrow 1$

$\frac{x}{\log(x)}$ よりも $\int_2^x \frac{1}{\log(t)} dt$ の方が「 x 以下の素数の個数」

を良く近似する

その心は, x あたりでは数が素数であることの

「確率」が $\frac{1}{\log(x)}$ くらい.

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

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

$4n+1$ の形の素数	5	13	17	29	37	41	53	61	73	89	97		
$4n+\frac{2}{3}$ の形の素数	3	7	11	19	23	31	43	47	59	67	71	79	83

$3n+1$ の形の素数	7	13	19	31	37	43	61	67	73	79	97		
$3n+2$ の形の素数	2	5	11	17	23	29	41	47	53	59	71	83	89

$8n+1$ の形の素数	17	41	73	89	97		
$8n+3$ の形の素数	3	11	19	43	59	67	83
$8n+5$ の形の素数	5	13	29	37	53	61	
$8n+7$ の形の素数	7	23	31	47	71	79	

ディリクレの素数定理 (19世紀なかば)

a, b も互いに素な自然数とするとき

$an+b$ の形の素数は無限にある

タオ-グリーンの定理 (2004年)

素数からなる, どんな長さの等差数列も存在する

長さ4の, 素数の等差数列 11, 17, 23, 29

長さ6の, 素数の等差数列 7, 37, 67, 97, 127, 157

- $n^2 + 1$ の形の素数 $2 = 1^2 + 1, 5 = 2^2 + 1, 17 = 4^2 + 1, 37 = 6^2 + 1$
 $101 = 10^2 + 1, 197 = 14^2 + 1, \dots$
- $2^n - 1$ の形の素数 $3 = 2^2 - 1, 7 = 2^3 - 1, 31 = 2^5 - 1, \dots$
(メルセンヌ素数)
- $2^n + 1$ の形の素数 $3 = 2^1 + 1, 5 = 2^2 + 1, 17 = 2^4 + 1, 257 = 2^8 + 1, \dots$
(フェルマー素数)

正 N 角形がコンパスと定規で作図可能

$$\Leftrightarrow N = (2 \text{ のべき}) \times \text{相異なるフェルマー素数の積}$$

- 双子素数 (p と $p+2$ がともに素数)

$$3 \text{ と } 5, 5 \text{ と } 7, 11 \text{ と } 13, 17 \text{ と } 19, 29 \text{ と } 31, \dots$$

- 四つ子素数 ($p, p+2, p+6, p+8$ がいずれも素数)

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

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

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

これらのものは、それぞれ無限個あるだろうと思われるが
証明されていない

自然界の神秘は数の世界の神秘に凝縮し、

数の世界の神秘は素数の世界の神秘に凝縮する。

円周率 π と素数のふしぎな関係

$$\frac{\pi}{4} = \frac{1}{1+\frac{1}{3}} \times \frac{1}{1-\frac{1}{5}} \times \frac{1}{1+\frac{1}{7}} \times \frac{1}{1+\frac{1}{11}} \times \frac{1}{1-\frac{1}{13}} \\ \times \frac{1}{1-\frac{1}{17}} \times \frac{1}{1+\frac{1}{19}} \times \frac{1}{1+\frac{1}{23}} \times \dots$$

(4でわると1余る素数 p については $\frac{1}{1-\frac{1}{p}}$ を、

4でわると3余る素数 p については $\frac{1}{1+\frac{1}{p}}$ を
かけてゆく。)

素数の歌

素数の歌はとんからり
とんからりんりん らりるれろ
耳を澄ませば聞こえます
楽しい歌が聞こえます

素数の歌はちんからり
ちんからりんりん らりるれろ
声を合わせて歌います
素数の国の愛の歌

素数の歌はころころり
ころりんころりん ころころり
心やさしい星の子の
願いのように澄んだ歌

素数の歌はひいひやらら
ひいひやららんらん らりるれろ
うさぎも鹿も聞いてます
森のふしぎな笛の音

素数の歌はほろんほろり
ほろりん ほろりん ほろほろり
素数は夢を見ています
あしたの夢を歌います

フェルマー (1601-1665)



Wikipediaより引用

http://ja.wikipedia.org/wiki/%E7%94%BB%E5%83%8F:Pierre_de_Fermat.jpg

「
$$x^n + y^n = z^n \quad (n \geq 3)$$

は自然数の解をもたない。

私はこのことの真に驚嘆すべき証明
を発見したが、この余白はそれを記すには
狭すぎる。」

フェルマーの他の定理 (類体論の「玄関」)

定理

4でわると1余る素数 p は

$$p = x^2 + y^2 \quad (x, y \text{ は整数})$$

の形に書ける.

$$5 = 2^2 + 1^2, \quad 13 = 3^2 + 2^2, \quad 17 = 4^2 + 1^2 \quad \text{など.}$$

4でわると3余る素数は, そのようにならない.

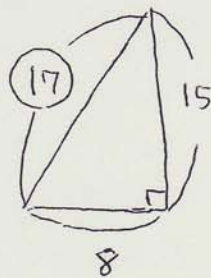
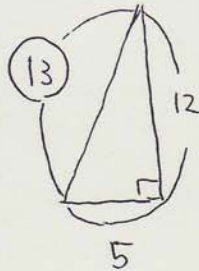
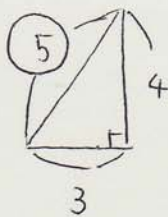
定理

4でわると1余る素数 p は

$$p^2 = x^2 + y^2 \quad (x, y \text{ は整数})$$

の形の式をみたら, つまり p は,

3辺の長さが整数の直角三角形の斜辺となる



など.

4でわると3余る素数は, そのようにならない.

定理 (フェルマーが発見した, 類体論の「玄関」)

素数 p について

(1) $p = x^2 + y^2$ となる整数 x, y がある

$\Leftrightarrow$ p を 4 でわると 1 余る. または, $p=2$.
同値

(2) $p = x^2 - 2y^2$ となる整数 x, y がある

$\Leftrightarrow$ p を 8 でわると 1 または 7 余る. または $p=2$.
同値

(3) $p = x^2 + 2y^2$ となる整数 x, y がある

$\Leftrightarrow$ p を 8 でわると 1 または 3 余る. または $p=2$.
同値

(4) $p = x^2 + 3y^2$ となる整数 x, y がある

$\Leftrightarrow$ p を 3 でわると 1 余る. または $p=3$.
同値

(5) $p = x^2 - 5y^2$ となる整数 x, y がある

$\Leftrightarrow$ p を 5 でわると 1 または 4 余る. または $p=5$.
同値

例. 4 でわると 1 余る素数が $x^2 + y^2$ と書ける様子
ふしぎにも

$$\begin{aligned} 5 &= 2^2 + 1^2, & 13 &= 3^2 + 2^2, & 17 &= 4^2 + 1^2, & 29 &= 5^2 + 2^2 \\ 37 &= 6^2 + 1^2, & 41 &= 5^2 + 4^2, & 53 &= 7^2 + 2^2, & 61 &= 6^2 + 5^2 \\ 73 &= 8^2 + 3^2, & 89 &= 8^2 + 5^2, & 97 &= 9^2 + 4^2 \end{aligned}$$

例. 8 でわると 1 または 7 余る素数が $x^2 - 2y^2$ と書ける様子
ふしぎにも

$$\begin{aligned} 7 &= 3^2 - 2 \times 1^2, & 17 &= 5^2 - 2 \times 2^2, & 23 &= 5^2 - 2 \times 1^2 \\ 31 &= 7^2 - 2 \times 3^2, & 41 &= 7^2 - 2 \times 2^2, & 47 &= 7^2 - 2 \times 1^2 \\ 71 &= 11^2 - 2 \times 5^2, & 73 &= 9^2 - 2 \times 2^2, & 79 &= 9^2 - 2 \times 1^2 \\ 89 &= 11^2 - 2 \times 4^2, & 97 &= 13^2 - 2 \times 6^2 \end{aligned}$$

8 でわると 1 または 3 余る素数か $x^2 + 2y^2$ と書ける様子
ふしぎにも

$$\begin{aligned} 3 &= 1^2 + 2 \times 1^2, & 11 &= 3^2 + 2 \times 1^2, & 17 &= 3^2 + 2 \times 2^2 \\ 19 &= 1^2 + 2 \times 3^2, & 41 &= 3^2 + 2 \times 4^2, & 43 &= 5^2 + 2 \times 3^2 \\ 59 &= 3^2 + 2 \times 5^2, & 67 &= 7^2 + 2 \times 3^2, & 73 &= 1^2 + 2 \times 6^2 \\ 89 &= 9^2 + 2 \times 2^2, & 97 &= 5^2 + 2 \times 6^2 \end{aligned}$$

3 でわると 1 余る素数か $x^2 + 3y^2$ と書ける様子
ふしぎにも

$$\begin{aligned} 7 &= 2^2 + 3 \times 1^2, & 13 &= 1^2 + 3 \times 2^2, & 19 &= 4^2 + 3 \times 1^2 \\ 31 &= 2^2 + 3 \times 3^2, & 37 &= 5^2 + 3 \times 2^2, & 43 &= 4^2 + 3 \times 3^2 \\ 61 &= 7^2 + 3 \times 2^2, & 67 &= 8^2 + 3 \times 1^2, & 73 &= 5^2 + 3 \times 4^2 \\ 79 &= 2^2 + 3 \times 5^2, & 97 &= 7^2 + 3 \times 4^2 \end{aligned}$$

5 でわると 1 または 4 余る素数か $x^2 - 5y^2$ と書ける様子
ふしぎにも

$$\begin{aligned} 11 &= 4^2 - 5 \times 1^2, & 19 &= 8^2 - 5 \times 3^2, & 29 &= 7^2 - 5 \times 2^2 \\ 31 &= 6^2 - 5 \times 1^2, & 41 &= 11^2 - 5 \times 4^2, & 59 &= 8^2 - 5 \times 1^2 \\ 61 &= 9^2 - 5 \times 2^2, & 71 &= 14^2 - 5 \times 5^2, & 79 &= 22^2 - 5 \times 9^2 \\ 89 &= 13^2 - 5 \times 4^2 \end{aligned}$$

類体論の大きな流れ

フェルマーの研究 1630年頃～



平方剰余の相互法則 (ガウス 1796年)



クンマー、ヒルベルトらの貢献

類体論の完成 (高木貞治 1920年)

谷山志村予想など、保型形式論を用いて
類体論を越える動き

非可換類体論を予想として定式化
(ラングランズ 1970年頃)

大発展時代への突入 (1994年～)

1994年 ワイルスカ

谷山志村予想を大部分解決し
フェルマーの最終定理を証明

2006年 テイラーら

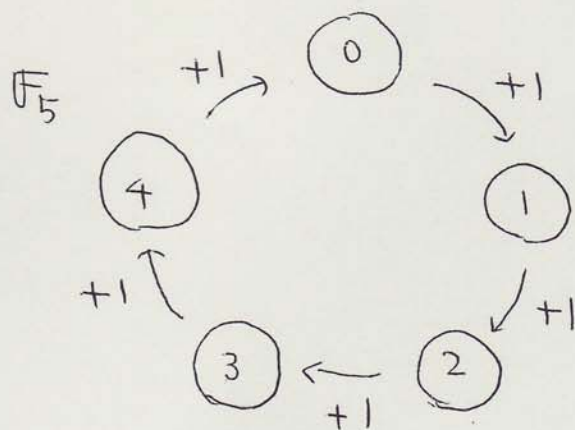
佐藤テイト予想を大部分証明



(非可換類体論完成へ向かっている)

5 でわった余りの世界 $\mathbb{F}_5$

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



$\mathbb{F}_5$ では $5 = 0, 6 = 1, 7 = 2, 8 = 3, \dots, 10 = 0, \dots$

$$4 + 2 = 6 = 1 \quad (\text{だから } 1 - 2 = 4)$$

$$4 \times 2 = 8 = 3 \quad (\text{だから } 3 \div 2 = 4)$$

素数 p でわった余りの世界 $\mathbb{F}_p$

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

そこでは 四則演算ができる。

定理 (平方剰余の相互法則の一部. 類体論の「玄関」)

(1) $\mathbb{F}_p$ に -1 の平方根がある

$\Leftrightarrow$ p を 4 でわると 1 余る. または, $p=2$
同値

(2) $\mathbb{F}_p$ に 2 の平方根がある

$\Leftrightarrow$ p を 8 でわると 1 または 7 余る. または, $p=2$.
同値

(3) $\mathbb{F}_p$ に -2 の平方根がある

$\Leftrightarrow$ p を 8 でわると 1 または 3 余る. または $p=2$.
同値

(4) $\mathbb{F}_p$ に -3 の平方根がある

$\Leftrightarrow$ p を 3 でわると 1 余る. または $p=3$.
同値

(5) $\mathbb{F}_p$ に 5 の平方根がある

$\Leftrightarrow$ p を 5 でわると 1 または 4 余る. または $p=5$.
同値

例1 4でわると1余る素数 p について $\mathbb{F}_p$ に -1 の平方根がある様子

$$2^2 \equiv -1 \pmod{5} \quad 5^2 \equiv -1 \pmod{13}$$

8でわると1または7余る素数 p について $\mathbb{F}_p$ に 2 の平方根がある様子

$$3^2 \equiv 2 \pmod{7} \quad 6^2 \equiv 2 \pmod{17}$$

8でわると1または3余る素数 p について $\mathbb{F}_p$ に -2 の平方根がある様子

$$1^2 \equiv -2 \pmod{3} \quad 3^2 \equiv -2 \pmod{11}$$

3でわると1余る素数 p について $\mathbb{F}_p$ に -3 の平方根がある様子

$$2^2 \equiv -3 \pmod{7} \quad 7^2 \equiv -3 \pmod{13}$$

5でわると1または4余る素数 p について $\mathbb{F}_p$ に 5 の平方根がある様子

$$4^2 \equiv 5 \pmod{11} \quad 9^2 \equiv 5 \pmod{19}$$

平方剰余の相互法則

p と q を相異なる, 2 でない素数とする.

(1) $\mathbb{F}_p$ に q の平方根があること

(2) $\mathbb{F}_q$ に p の平方根があること

という (互いに無関係のように見える) ふたつのことを考える.

次の (*) の場合を除いて

$$(1) \quad \Longleftrightarrow \quad (2) \\ \text{同値}$$

となる.

(*) p を 4 でわった余りも q を 4 でわった余りも 3 の場合

(*) の場合には $(1) \Longleftrightarrow ((2) \text{ でない})$
同値

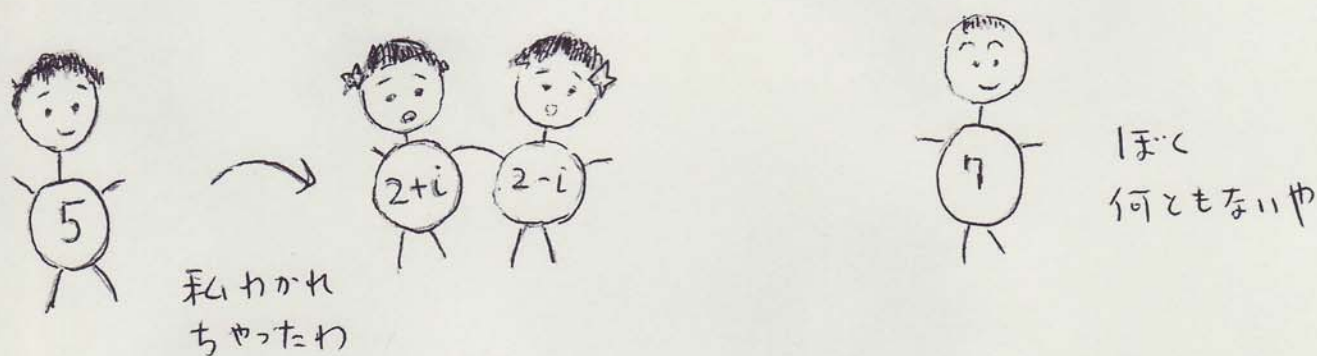
$((1) \text{ でない}) \Longleftrightarrow (2)$ となる
同値

類体論は、数の世界が広がるときの
素数の分解の様子をあらわす

有理数の世界 $\mathbb{Q}$ が $i = \sqrt{-1}$ の入った数の世界 $\mathbb{Q}(i)$ に
広がるとき、4 でわると 1 余る素数は 2 つに分裂し

$$\begin{aligned} (例) \quad 5 &= 2^2 + 1^2 = (2+i)(2-i), & 13 &= 3^2 + 2^2 = (3+2i)(3-2i) \\ 17 &= 4^2 + 1^2 = (4+i)(4-i), & 29 &= 5^2 + 2^2 = (5+2i)(5-2i) \end{aligned}$$

4 でわると 3 余る素数は分裂しない

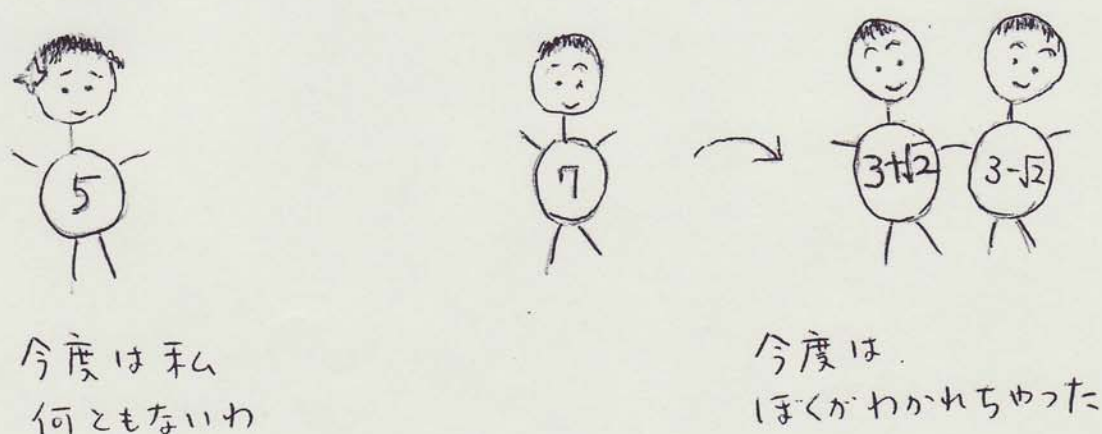


$\mathbb{Q}$ が $\mathbb{Q}(\sqrt{2})$ に広がるとき、

8 でわると 1 または 7 余る素数は 2 つに分裂し

$$\begin{aligned} (例) \quad 7 &= 3^2 - 2 \times 1^2 = (3+\sqrt{2})(3-\sqrt{2}), & 17 &= 5^2 - 2 \times 2^2 = (5+2\sqrt{2})(5-2\sqrt{2}) \\ 23 &= 5^2 - 2 \times 1^2 = (5+\sqrt{2})(5-\sqrt{2}), & 31 &= 7^2 - 2 \times 3^2 = (7+3\sqrt{2})(7-3\sqrt{2}) \end{aligned}$$

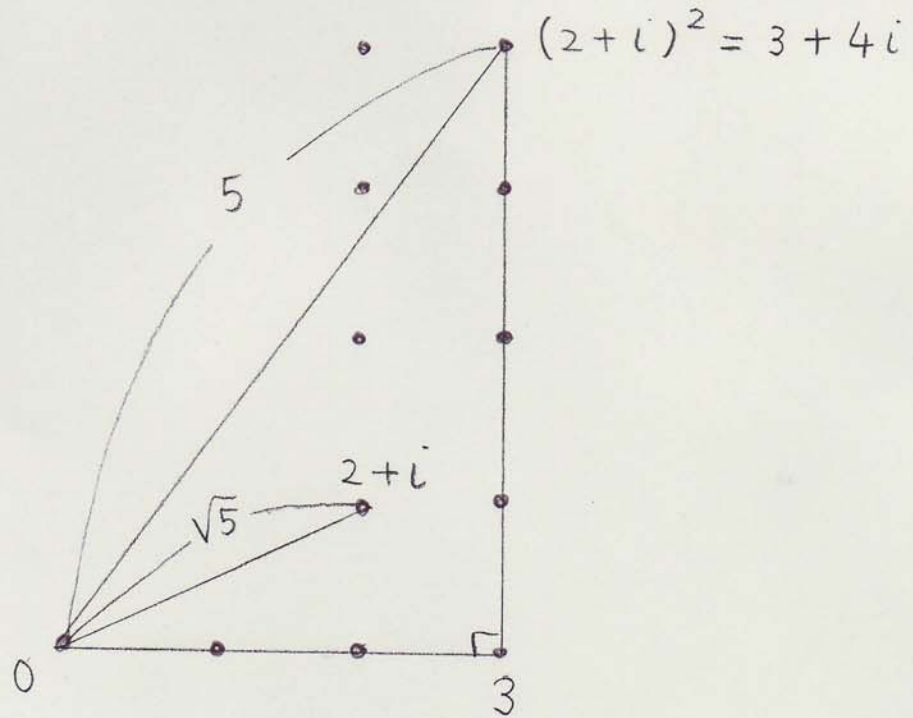
8 でわると 3 または 5 余る素数は分裂しない



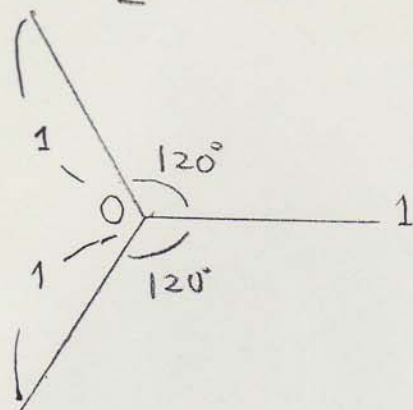
$$5 = 2^2 + 1^2 = (2+i)(2-i)$$

という 5 の分解から,

3, 4, 5 の直角三角形が生まれる様子



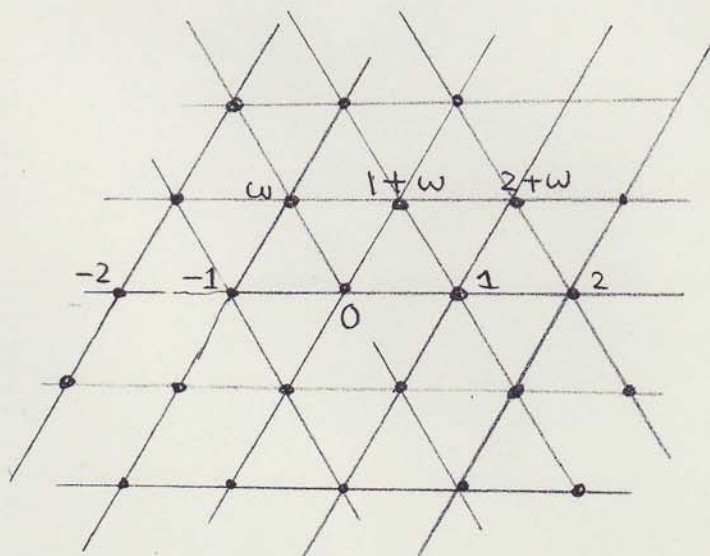
$$\omega = \frac{-1 + \sqrt{3}i}{2}$$



$$\omega^3 = 1$$

$$\omega^2 = \frac{-1 - \sqrt{3}i}{2}$$

ω の世界 $\{a + b\omega \mid a, b \text{ は整数}\}$



ω の世界では

3でわると1余る素数が2つに分裂し

3でわると2余る素数が分裂しない

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

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

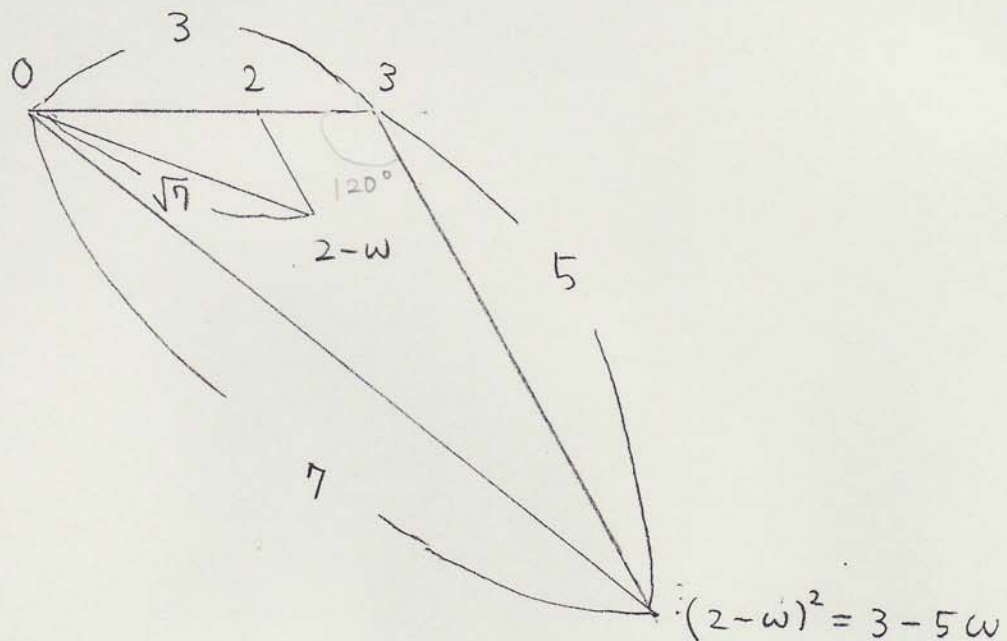
$$19 = (3 - 2\omega)(3 - 2\omega^2)$$

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

という 7 の分解から

7, 5, 3 の 3 角形 (120° の角を持つ)

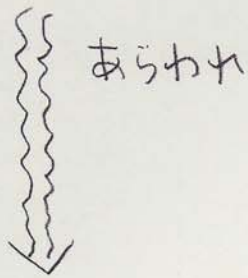
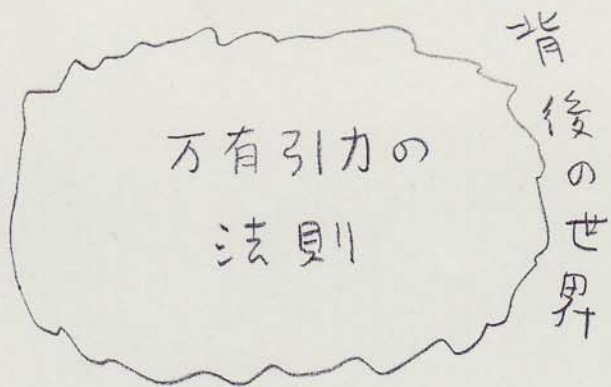
が生まれる様子



3 でわると 1 余る素数は

3 辺が整数で 120° の角をもつ 3 角形の
 120° の角の対辺にあらわれる

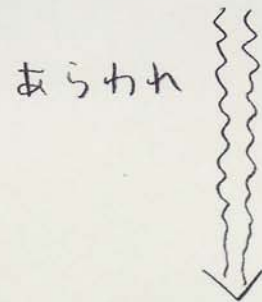
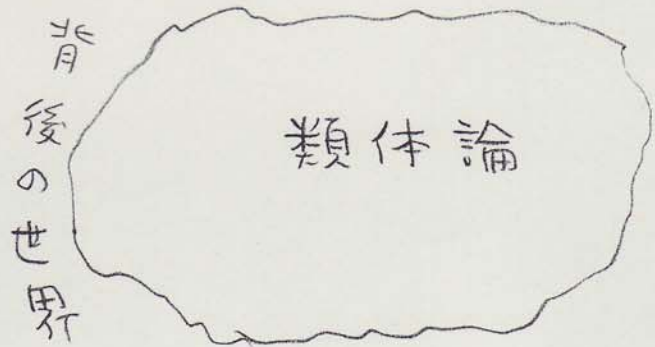
3 でわると 2 余る素数は そうならない



地球とリンゴが
ひき合う



リンゴが
木から落ちる



120°の角を持つ
7, 5, 3の3角形が
あらわれる



七五三の行事
ができる



高木貞治

Teiji Takagi

1925年ごろ

京都府(Kyoto Pref.)

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

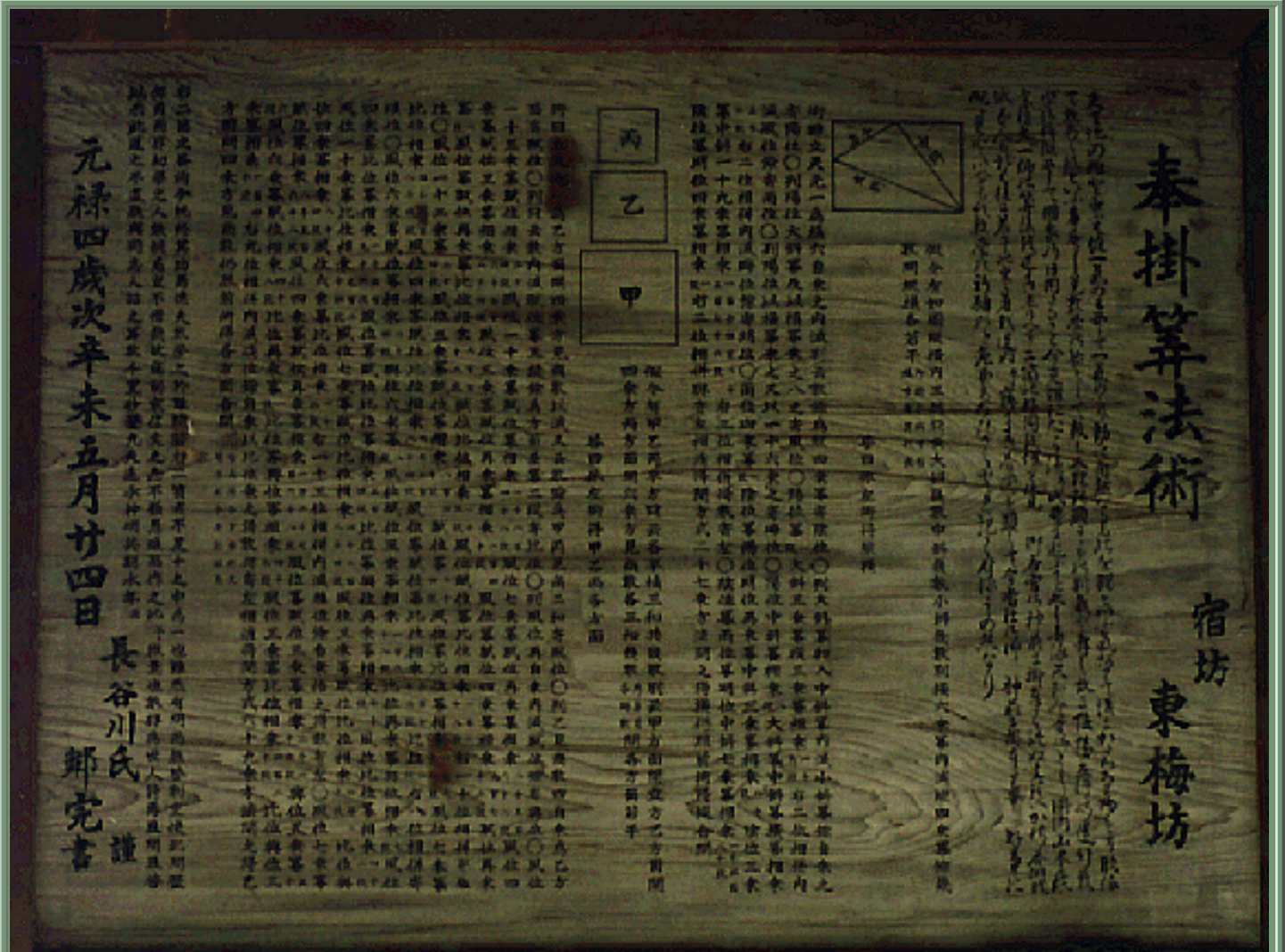
完全な形で現存する日本最古の算額.

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

京都府(Kyoto Pref.)

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

愛媛県(Ehime Pref.)

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

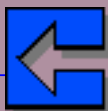
75.2 × 91.1cm

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](#)

非可換類体論の一部となる、ふしぎな事実

例 1. $\mathbb{F}_p$ における $x^3 = 2$ の解の個数

p	2	3	5	7	11	13	17	19	23	29	31
解の個数 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} が 3 である様子

$$4^3 = 64 = 31 \times 2 + 2 \equiv 2 \pmod{31}, \quad 7^3 = 343 = 31 \times 11 + 2 \equiv 2 \pmod{31}$$

大変ふしぎなこと；

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

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

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

$$\text{と} \sum_{n=1}^{\infty} a_n q^n = a_1 q + a_2 q^2 + a_3 q^3 + \dots \text{とあくと}$$

$$(a_1 = 1, a_2 = 0, a_7 = -1 \text{ など})$$

$$N_p - 1 = a_p$$

がすべての素数 p について成り立っている。

例 2 $\mathbb{F}_p$ における $y^2 = x^3 + 1$ の解 (x, y) の個数

p	2	3	5	7	11	13	17	19	23	29	31
解の個数 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

(N_5 が 5 である様子)

$\mathbb{F}_5$ における解は $2^2 = 2^3 + 1$ など

$(2, 2), (2, 3), (0, 1), (0, 4), (4, 0)$ の 5 個)

大変ふしぎなこと:

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

これを $\sum_{n=1}^{\infty} a_n q^n$ と書いてみると

$$p - N_p = a_p$$

がすべての素数 p について成り立っている

例 3 $\mathbb{F}_p$ における $y^2 + y = x^3 - x^2$ の解 (x, y) の個数

p	2	3	5	7	11	13	17	19	23
解の個数 N_p	4	4	4	9	10	9	19	19	24
$p - N_p$	-2	-1	1	-2	1	4	-2	0	-2

大変ふしきなこと

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

$$\text{を } \sum_{n=1}^{\infty} a_n q^n \text{ と書いてみると}$$

$$p - N_p = a_p$$

かすべての素数 p について成りたっている

まとめ: 方程式 $x^3 = 2$, $y^2 = x^3 + 1$, $y^2 + y = x^3 - x^2$ 楕円曲線

か 素数の海を渡ってゆくとき, ふしきな音楽

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

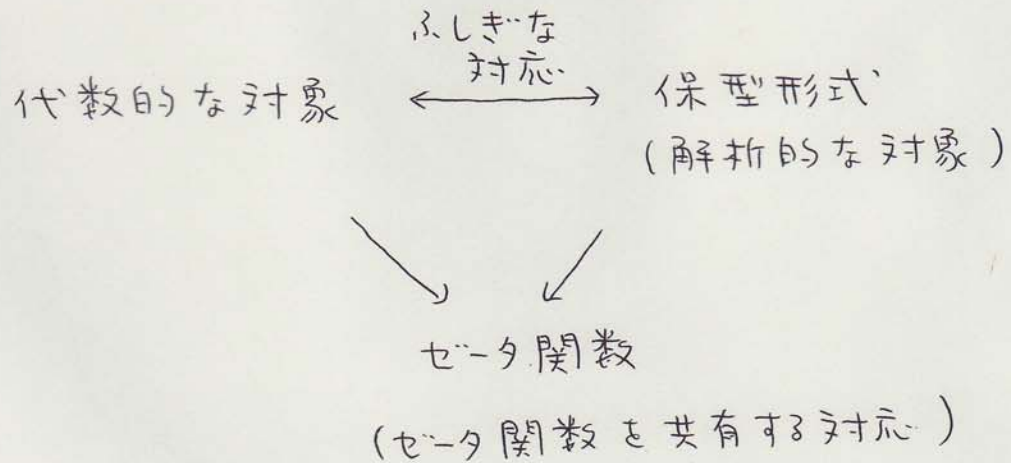
を奏でる.

保型形式

非可換類体論は

($x^2=2$ や $x^3=2$ や $y^2=x^3+1$ や $\mathbb{Q}(i)$ や $\mathbb{Q}(\sqrt{2})$ などの)

代数的な対象が素数の海を渡ってゆくときに奏でる
ふしきな音楽を聞きとるもの。



いろいろなものが素数の海を渡っていく

素数の海は私達のふるさとである

フェルマーの最終定理は 1994年に, ワイルズにより

谷山志村予想の大きな部分を解決することで

証明された。 — 楕円曲線と保型形式のふしぎな関係



Wikipediaより引用

http://en.wikipedia.org/wiki/Andrew_Wiles

$a^n + b^n = c^n$ $n \geq 3$ に解があったとする。

楕円曲線

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

を考えると, この楕円曲線は

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

$C - A, C - B, B - A$ が全部 n 乗数

という異常な楕円曲線になる。

この楕円曲線 $\longleftrightarrow$ 保型形式
谷山志村予想

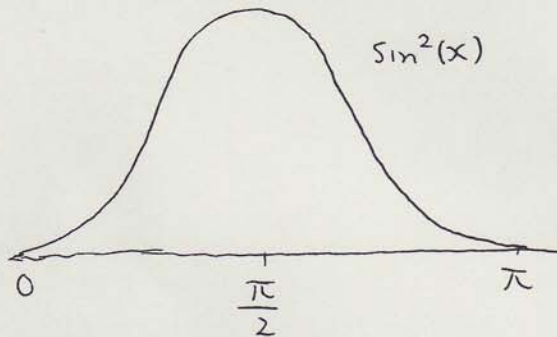
とすると, 楕円曲線が異常すぎて, この保型形式は異常な存在しない保型形式になる。

佐藤 テイト予想 (1963年3月頃 佐藤 幹夫)

有理数係数の楕円曲線を考え、その N_p , $a_p = p - N_p$ を考える。 $|a_p| < 2\sqrt{p}$ (ハセの定理) となる。

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

で角 θ_p を定めると、いろいろな素数 p についての θ_p は、 p が動くとき $\sin^2(x)$ の形に分布する。



2006年に、この予想の大きい部分が、テイラー達により

この楕円曲線の n 個の積 $(n=1, 2, 3, \dots)$ $\longleftrightarrow$ (GL_{n+1}) の保型形式、
非可換類体論

という関係の考察により証明された。

