

# 数論入門<sup>1</sup>

担当：市川尚志<sup>2</sup>

## 1 自然数、整数についての基本的なこと

文献：高木貞治著「初等整数論講義」共立出版 (1931).

### 1.1 数の系列

- 自然数：1, 2, 3, 4, ...  $\Rightarrow$  足し算、掛け算ができる
- 整数：..., -2, -1, 0, 1, 2, ...  $\Rightarrow$  引き算ができる
- 有理数： $\frac{m}{n}$  ( $m$ ：整数、 $n$ ：自然数)  $\Rightarrow$  割り算ができる
- 実数：数直線上の点  $\Rightarrow$  極限がとれる
- 複素数： $a + b\sqrt{-1}$  ( $a, b$ ：実数)  $\Rightarrow$  方程式が解ける

### 1.2 主な数論の歴史

- Euclid(BC330?~BC275?) ... 素因数分解、素数が無限にあることの証明
- Diophantus(246?~330?) ... 合同数問題などの Diophantus 問題の研究
- Fermat(1601~1665) ... Fermat の小定理、Fermat 予想の提出
- Euler(1707~1783) ... Euler の定理、ゼータ値  $\sum_{n=1}^{\infty} 1/n^k$  の研究
- Gauss(1777~1855) ... 古典（初等）整数論の完成、素数分布の研究
- Jacobi(1804~1851) ... 関数論（保型形式）の整数論への応用
- Riemann(1826~1866) ... ゼータ関数  $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$  を用いた素数分布の研究
- 高木貞治(1875~1960) ... 代数的整数論における類体論の完成
- Wiles(1953~) ... 20世紀後半に発展した数論幾何を用い Fermat 予想を証明 (1995)

### 1.3 基本的な言葉（定義）

- 整数  $a$  と自然数  $b$  に対し、

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

を満たす整数  $q$  と  $r$  がただ一つずつ存在する ( $q$  は  $a/b$  を超えない最大の整数として得られる)。このとき、 $q$  を ( $a$  を  $b$  で割った) 商、 $r$  を余りという。

<sup>1</sup> <http://ichikawa.ms.saga-u.ac.jp/> からダウンロードできます

<sup>2</sup> 佐賀大学工学系研究科数理科学専攻 e-mail: ichikawn@cc.saga-u.ac.jp

- 上で  $r = 0$  のとき、

$$\left\{ \begin{array}{l} a \text{ は } b \text{ で割り切れる、 } a \text{ は } b \text{ の倍数である} \\ \text{または} \\ b \text{ は } a \text{ を割り切る、 } b \text{ は } a \text{ の約数である} \end{array} \right.$$

といい、 $b|a$  とかく (そうでないとき  $b \nmid a$  とかく)。

- 自然数は次の3つのタイプに分かれる：

$$\left\{ \begin{array}{l} 1 \quad : \text{ 正の約数を1つ持つ} \\ \text{素数} \quad : \text{ 正の約数を2つ (1と自分自身) 持つ} \\ \text{合成数} \quad : \text{ 正の約数を3つ以上持つ。} \end{array} \right.$$

- 整数  $a, b$  を割り切る自然数の中で最大のものを**最大公約数**といい、 $\gcd(a, b)$  と書く。  
 $\gcd(a, b) = 1$  のとき、 $a$  と  $b$  は互いに**素**であるという。
- 整数  $a, b$  で割り切れる自然数の中で最小のものを**最小公倍数**といい、 $\text{lcm}(a, b)$  と書く。

#### 1.4 Euclid の互除法 (最大公約数の求め方)

自然数  $a, b$  に対し、 $a_1 = a, a_2 = b$  として

$$\begin{aligned} a_1 \text{ を } a_2 \text{ で割った余りを } a_3 \quad (0 \leq a_3 < a_2), \\ a_2 \text{ を } a_3 \text{ で割った余りを } a_4 \quad (0 \leq a_4 < a_3), \\ \dots \end{aligned}$$

とすると、 $a_2 > a_3 > a_4 > \dots \geq 0$  より  $a_n = 0$  となる最小の自然数  $n$  が存在する。これを  $N$  とするとき、 $a$  と  $b$  との最大公約数  $\gcd(a, b)$  は  $a_{N-1}$  に等しい。

証明. 各  $n$  に対し  $a_n$  を  $a_{n+1}$  で割った商を  $q_{n+1}$  とすると、余りは  $a_{n+2}$  だから、

$$(*) \left\{ \begin{array}{l} a_1 - q_2 a_2 = a_3, \\ a_2 - q_3 a_3 = a_4, \\ \dots \dots \dots \\ a_{N-3} - q_{N-2} a_{N-2} = a_{N-1}, \\ a_{N-2} - q_{N-1} a_{N-1} = 0. \end{array} \right.$$

いま  $\gcd(a, b) = c$  とすると、 $a_1 = a = kc, a_2 = b = lc$  を満たす整数  $k, l$  が存在するから、  
(\*) より

$$\begin{aligned} a_3 &= a - q_2 b = kc - q_2 lc = (k - q_2 l)c : c \text{ の倍数} \\ a_4 &= a_2 - q_3 a_3 = \{l - q_3(k - q_2 l)\}c : c \text{ の倍数} \\ &\dots \dots \dots \\ a_{N-1} &= a_{N-3} - q_{N-2} a_{N-2} : c \text{ の倍数} \end{aligned}$$

よって  $a_{N-1} \geq c$  となる。一方 (\*) より

$$\begin{aligned} a_{N-2} &= q_{N-1}a_{N-1} : a_{N-1} \text{ の倍数} \\ a_{N-3} &= q_{N-2}a_{N-2} + a_{N-1} = (q_{N-2}q_{N-1} + 1)a_{N-1} : a_{N-1} \text{ の倍数} \\ &\dots\dots\dots \\ b = a_2 &= q_3a_3 + a_4 : a_{N-1} \text{ の倍数} \\ a = a_1 &= q_2a_2 + a_3 : a_{N-1} \text{ の倍数} \end{aligned}$$

よって  $a_{N-1}$  は  $a, b$  の公約数となるから  $a_{N-1} \leq c$ . 従って  $a_{N-1} = c = \gcd(a, b)$ . 証明終.

### 1.5 定理

整数  $a, b$  とその最大公約数  $\gcd(a, b)$  に対し、

$$na + mb = \gcd(a, b)$$

を満たす整数  $n, m$  が存在する。

注. これから次のことが分る：

$$ax + by = c \text{ が整数解 } x, y \text{ を持つ} \iff c \text{ が } \gcd(a, b) \text{ の倍数}$$

… 整数係数の方程式の整数解を求める問題 (Diophantus 問題) の一つ

証明. 1.4 の (\*) より

$$\begin{aligned} a_3 &= a_1 - q_2a_2 = a - q_2b, \\ a_4 &= a_2 - q_3a_3 = b - q_3(a - q_2b) = -q_3a + (1 + q_2q_3)b, \\ &\dots\dots\dots \end{aligned}$$

となるが、 $q_i$  が整数であることからそれらの和、差、積も整数になるので、各  $a_n$ , 特に  $a_{N-1} = \gcd(a, b)$  は、 $a$  と  $b$  に適当な整数をかけたものの和として表される。 証明終.

### 1.6 例

- 91 と 35 の最大公約数？

$$\begin{aligned} 91 &= 2 \times 35 + 21 \\ 35 &= 1 \times 21 + 14 \\ 21 &= 1 \times 14 + 7 \\ 14 &= 2 \times 7 + 0. \end{aligned}$$

よって  $\gcd(91, 35) = 7$  となり、定理 1.5 より

$$\begin{aligned} 7 &= 21 - 1 \times 14 = 21 - (35 - 1 \times 21) = -35 + 2 \times 21 \\ &= -35 + 2 \times (91 - 2 \times 35) = 2 \times 91 - (1 + 2 \times 2) \times 35 \\ &= 2 \times 91 + (-5) \times 35. \end{aligned}$$

のように最大公約数を表すことができる。

### 1.7 定理 (素数の重要な性質)

$p$  を素数、 $a$  と  $b$  を整数とするとき、 $p|ab$  (すなわち  $p$  が  $ab$  を割り切る) ならば、 $p|a$  または  $p|b$  が成り立つ。

証明.  $\gcd(p, a)$  は素数  $p$  の約数なので  $p$  または  $1$  に等しい。 $\gcd(p, a) = p$  のときは  $p|a$ 。 $\gcd(p, a) = 1$  のときは、上の定理より  $np + ma = 1$  を満たす整数  $n, m$  が存在し、この両辺に  $b$  をかけると  $npb + mab = b$  となり、左辺は仮定より  $p$  で割り切れるから  $p|b$ 。証明終。

### 1.8 定理 (素因数分解の一意性)

任意の自然数  $n$  は、

$$n = p^a \cdot q^b \cdot r^c \cdots; (p, q, r, \dots \text{は互いに異なる素数で、} a, b, c, \dots \text{は自然数})$$

とただ一通りに素因数分解ができる。

証明.  $n$  が 2 通りの素因数分解:

$$p_1^{a_1} \cdot q_1^{b_1} \cdot r_1^{c_1} \cdots = p_2^{a_2} \cdot q_2^{b_2} \cdot r_2^{c_2} \cdots$$

を持つとする。このとき、素数  $p_1$  は左辺、すなわち右辺を割り切るので、定理 1.7 より右辺に現れる素数  $p_2, q_2, r_2, \dots$  のいずれかを割り切る。もし  $p_1$  が  $p_2$  を割り切るとすると、 $p_2$  も素数なので  $p_1 = p_2$  となる。これで上式の両辺を割ると

$$p_1^{a_1-1} \cdot q_1^{b_1} \cdot r_1^{c_1} \cdots = p_2^{a_2-1} \cdot q_2^{b_2} \cdot r_2^{c_2} \cdots$$

となる。この操作を続けることにより、素因数分解が一通りであることが分る。証明終。

### 1.9 系 (素因数分解の応用)

2つの自然数  $n, m$  の素因数分解を

$$\begin{aligned} n &= p^a \cdot q^b \cdot r^c \cdots; (p, q, r, \dots \text{は素数で、} a, b, c, \dots \geq 0) \\ m &= p^{a'} \cdot q^{b'} \cdot r^{c'} \cdots; (p, q, r, \dots \text{は素数で、} a', b', c', \dots \geq 0) \end{aligned}$$

とするとき、

$$n|m \iff a \leq a', b \leq b', c \leq c', \dots$$

また  $\alpha \leq \beta$  のとき  $\min\{\alpha, \beta\} = \alpha$ ,  $\max\{\alpha, \beta\} = \beta$  と表すことにすると、

$$\begin{aligned} \gcd(n, m) &= p^{\min\{a, a'\}} \cdot q^{\min\{b, b'\}} \cdot r^{\min\{c, c'\}} \cdots, \\ \text{lcm}(n, m) &= p^{\max\{a, a'\}} \cdot q^{\max\{b, b'\}} \cdot r^{\max\{c, c'\}} \cdots. \end{aligned}$$

従って  $n \cdot m = \gcd(n, m) \cdot \text{lcm}(n, m)$  が成り立つ。

## 2 素数はどのように分布しているか？

文献：Don Zagier “The First 50 Million Prime Numbers” (1977), 和訳「最初の五千万の素数」

### 2.1 素数の不思議

- 大きな自然数が素数かどうかを判定するのは、一般には難しい  
1つの方法：自然数  $n$  が  $\sqrt{n}$  以下のすべての素数で割り切れないとき、 $n$  は素数  
例えば 1999 は  $\sqrt{1999} = 44.71\dots$  以下の素数：

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$$

のいずれでも割り切れないから素数であることが分る。同様に 1997, 2003 も素数。

- しかし素数の集まりを統計的に見ると“ある規則”に従っていることが分る。

### 2.2 定理 (Euclid) 素数は無限に存在する。

証明。背理法で示す。素数が有限個しかない、と仮定し、すべての素数を  $p_1, p_2, \dots, p_n$  と表すと

$$m = p_1 \times p_2 \times \dots \times p_n + 1$$

はすべての素数より大きく素数でなくなるから、いずれかの素数で割り切れる。一方  $m$  は  $p_1, p_2, \dots, p_n$  で割ると 1 が余り、いずれの素数でも割り切れないので矛盾が生じる。証明終。

### 2.3 素数定理

自然数  $x$  以下の素数の個数を  $\pi(x)$  で表す (例： $\pi(10) = 4, \pi(20) = 8$ ) と、

$x$	$\dots$	$10^4$	$10^5$	$10^6$	$10^7$	$10^8$	$10^9$	$10^{10}$
$x/\pi(x)$	$\dots$	8.1	10.4	12.7	15.0	17.4	19.7	22.0

$x$  が 10 倍になると  $x/\pi(x)$  は約  $2.3 \doteq \log_e 10$  増える (ただし  $e = \sum_{n=1}^{\infty} \frac{1}{n!} \doteq 2.718\dots$  : 自然対数の底)。この観察から次が推測できる：

Gauss の予想 (素数定理)  $x$  が大きくなると  $\frac{x}{\pi(x) \cdot \log_e(x)}$  は限りなく 1 に近づくだらう。

- Riemann: ゼータ関数  $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$  を導入し、 $\zeta(s)$  の零点についての予想 (Riemann 予想) を仮定して、素数定理を証明 (1858 年)  $\dots$  Riemann 予想は現在でも未解決。
- Hadamard (1865~1963), de la Vallée-Poussin (1866~1962) : Riemann 予想を使わずに、 $\zeta(s)$  を用いて素数定理を独立に証明 (1896 年)。

## 2.4 $\pi(x)$ を表す (近似) 式

- Legendre の式 :  $\frac{x}{\log_e(x) - 1.08366}$
- Gauss の式 :  $\text{Li}(x) = \int_2^x \frac{1}{\log_e(t)} dt \doteq \frac{1}{\log_e(2)} + \frac{1}{\log_e(3)} + \cdots + \frac{1}{\log_e(x)}$
- Riemann の式 :

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \text{Li}(\sqrt[n]{x}) = \text{Li}(x) - \frac{1}{2} \text{Li}(\sqrt{x}) - \frac{1}{3} \text{Li}(\sqrt[3]{x}) + \cdots;$$

ただし  $\mu(n) \stackrel{\text{def}}{=} \begin{cases} (-1)^r & (n \text{ が } r \text{ 個の異なる素数の積のとき}), \\ 0 & (\text{それ以外するとき}) \end{cases}$

$$= 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{(\log_e x)^n}{n!}; \quad \text{ただし } \zeta(n+1) = \sum_{m=1}^{\infty} \frac{1}{m^{n+1}}.$$

$x$	$\pi(x)$	$R(x)$	$\pi(x) - R(x)$
100,000,000	5,761,455	5,761,552	-97
200,000,000	11,078,937	11,079,090	-153
300,000,000	16,252,325	16,252,355	-30
400,000,000	21,336,326	21,336,185	141
500,000,000	26,355,867	26,355,517	350
600,000,000	31,324,703	31,324,622	81
700,000,000	36,252,931	36,252,719	212
800,000,000	41,146,179	41,146,248	-69
900,000,000	46,009,215	46,009,949	-734
1,000,000,000	50,847,534	50,847,455	79

## 2.5 双子素数

双子素数 (twin prime) とは、差が2である2つの素数の組のこと。無数に存在することが予想されているが、証明はされていない。ただし2014年12月現在、間隔が246以内である素数の組が無数に存在することが証明されている :

<https://www.quantamagazine.org/20141210-prime-gap-grows-after-decades-long-lull/>

### 3 数の合同と余りの計算

#### 3.1 合同の定義

自然数  $m$  と整数  $a, b$  に対し、

$$\begin{aligned} & a \text{ を } m \text{ で割った余りと } b \text{ を } m \text{ で割った余りが等しい} \\ \iff & a - b \text{ が } m \text{ で割り切れる} \end{aligned}$$

このとき  $a$  と  $b$  は  $m$  を法として合同であるといい、

$$a \equiv b \pmod{m}$$

と表す。

#### 3.2 合同式の性質

$a \equiv b \pmod{m}, c \equiv d \pmod{m}$  ならば

$$\begin{aligned} a + c &\equiv b + d \pmod{m}, \\ a - c &\equiv b - d \pmod{m}, \\ ac &\equiv bd \pmod{m}. \end{aligned}$$

証明. 仮定より  $a - b = km, c - d = lm$  を満たす整数  $k, l$  が存在するから、

$$\begin{aligned} (a \pm c) - (b \pm d) &= (a - b) \pm (c - d) = km \pm lm = (k \pm l)m \text{ (複号同順)}, \\ ac - bd &= (ac - bc) + (bc - bd) = ckm + blm = (ck + bl)m \end{aligned}$$

となり、 $k \pm l, ck + bl$  はいずれも整数なので題意が示された。 証明終。

つまり、等号と同じように両辺を足したり、引いたり、掛けたりしても、合同式が成り立つ。

#### 3.3 合同式の応用

- 1945 を 9 で割った余り (0 以上 9 未満の整数) を求めよ

$$\begin{array}{rclcl} 1000 & = & 1 \times 1000 & = & 1 + 1 \times \underline{999} & \equiv & 1 & \pmod{9} \\ 900 & = & 9 \times 100 & = & 9 + 9 \times \underline{99} & \equiv & 9 & \pmod{9} \\ 40 & = & 4 \times 10 & = & 4 + 4 \times \underline{9} & \equiv & 4 & \pmod{9} \\ +) & & 5 & & & \equiv & 5 & \pmod{9} \\ \hline 1945 & & & & & \equiv & 1 + 9 + 4 + 5 \equiv \mathbf{1} & \pmod{9} \end{array}$$

同様に 10 進法で表された 4 桁の数  $a b c d$  に対し、

$$a b c d \equiv a + b + c + d \pmod{9}$$

となるから、

$$\begin{aligned} a b c d \text{ が } 9 \text{ の倍数} &\iff a + b + c + d \text{ が } 9 \text{ の倍数} \\ a b c d \text{ が } 3 \text{ の倍数} &\iff a + b + c + d \text{ が } 3 \text{ の倍数} \end{aligned}$$

- 1945 を 11 で割った余り (0 以上 11 未満の整数) を求めよ

$$\begin{array}{r r r r r r} 1000 & = & -1 + 1001 & = & -1 + 91 \times 11 & \equiv & -1 & \text{mod}(11) \\ 900 & = & 9 + 9 \times 99 & = & 9 + 9 \times 9 \times 11 & \equiv & 9 & \text{mod}(11) \\ 40 & & & = & -4 + 4 \times 11 & \equiv & -4 & \text{mod}(11) \\ +) & 5 & & & & \equiv & 5 & \text{mod}(11) \\ \hline 1945 & & & & & \equiv & 9 & \text{mod}(11) \end{array}$$

同様に 10 進法で表された 4 桁の数  $a b c d$  に対し、

$$a b c d \equiv -a + b - c + d \pmod{11}$$

となるから、

$$a b c d \text{ が } 11 \text{ の倍数} \iff -a + b - c + d \text{ が } 11 \text{ の倍数}$$

- $2^{100}$  を 9 で割った余り (0 以上 9 未満の整数) を求めよ

$2^3 = 8 \equiv -1 \pmod{9}$  の両辺を 33 乗すると

$$2^{99} = (2^3)^{33} \equiv (-1)^{33} = -1 \pmod{9}$$

$$\therefore 2^{100} = 2 \cdot 2^{99} \equiv 2 \cdot (-1) = -2 \equiv 7 \pmod{9}$$

よって余りは 7。

- $3^{100}$  を 7 で割った余り (0 以上 7 未満の整数) を求めよ

$3^3 = 27 \equiv -1 \pmod{7}$  の両辺を 33 乗すると

$$3^{99} = (3^3)^{33} \equiv (-1)^{33} = -1 \pmod{7}$$

$$\therefore 3^{100} = 3 \cdot 3^{99} \equiv 3 \cdot (-1) = -3 \equiv 4 \pmod{7}$$

よって余りは 4。

別解.  $3^2 = 9 \equiv 2 \pmod{7}$  の両辺を 3 乗すると

$$3^6 = (3^2)^3 \equiv 2^3 = 8 \equiv 1 \pmod{7}$$

$$\therefore 3^{96} = (3^6)^{16} \equiv 1^{16} = 1 \pmod{7}$$

$$\therefore 3^{100} = 3^4 \cdot 3^{96} \equiv 3^4 = 81 \equiv 4 \pmod{7}$$

よって余りは 4。

## 4 平方数とその和

整数の2乗の形に表される数  $0, 1, 4, 9, 16, 25, 36, 49, \dots$  を平方数という。ここでは2つの平方数の和として表される自然数の性質について、すなわち、方程式

$$x^2 + y^2 = n$$

が整数解を持つ自然数  $n$  の性質について考える (Diophantus 問題の一つ)。

### 4.1 平方数の性質

- 整数  $a$  に対し、

$$\begin{cases} a : \text{偶数} & \Rightarrow a^2 \equiv 0 \pmod{4} \\ a : \text{奇数} & \Rightarrow a^2 \equiv 1 \pmod{4} \end{cases}$$

証明.  $a$  が偶数ならば  $a = 2n$  ( $n$ : 整数) の形に表され、 $n^2$  も整数となるから、

$$a^2 = 4n^2 \equiv 0 \pmod{4}.$$

また  $a$  が奇数ならば  $a = 2m + 1$  ( $m$ : 整数) の形に表されるから、

$$a^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1 \equiv 1 \pmod{4} \quad \text{証明終.}$$

- 整数  $a, b$  に対し、

$$\begin{cases} a, b : \text{偶数} & \Rightarrow a^2 + b^2 \equiv 0 \pmod{4} \\ a : \text{偶数}, b : \text{奇数} & \Rightarrow a^2 + b^2 \equiv 1 \pmod{4} \\ a : \text{奇数}, b : \text{偶数} & \Rightarrow a^2 + b^2 \equiv 1 \pmod{4} \\ a, b : \text{奇数} & \Rightarrow a^2 + b^2 \equiv 2 \pmod{4} \end{cases}$$

従って4で割った余りが3となる自然数は、2つの平方数の和として表されない。

- $n, m$  が2つの平方数の和として表されるとき、 $nm$  も同じ性質を持つ:

証明.  $n = a^2 + b^2, m = c^2 + d^2$  とすると、

$$nm = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (ac + bd)^2 + (ad - bc)^2$$

と表される。 証明終.

### 4.2 Euler の定理

4で割ると1余る素数  $p$  は、2つの平方数の和  $a^2 + b^2$  として表される。

注. 上式を  $p = (a + \sqrt{-1}b)(a - \sqrt{-1}b)$  と見ると、これは素数の分解法則を与えている (アーベル拡大における素数、素イデアルの分解法則を与える類体論の原型)  $\Rightarrow$  Hilbert(1862~1943), 高木により完成。

証明. まず 4 で割ると 1 余る素数  $p$  に対し、

$$n^2 + 1 \equiv 0 \pmod{p}$$

を満たす整数  $n$  が存在することが分る (「5 平方剰余」において証明する)。この  $n$  に対し、

$$(n + \sqrt{-1})(\alpha + \beta\sqrt{-1}) + p(\gamma + \delta\sqrt{-1}) \quad (\alpha, \beta, \gamma, \delta \text{ は整数})$$

の形の 0 でない複素数で、絶対値が最小になるもの ( $n + \sqrt{-1}$  と  $p$  との最大公約数にあたるもの) を  $a + b\sqrt{-1}$  とおくと、 $a, b$  は整数となる。いま  $\frac{n + \sqrt{-1}}{a + b\sqrt{-1}}$  及び  $\frac{p}{a + b\sqrt{-1}}$  の実部、虚部に一番近い整数をそれぞれ  $s, t$  及び  $u, v$  とすると、

$$\left| \frac{n + \sqrt{-1}}{a + b\sqrt{-1}} - (s + t\sqrt{-1}) \right| \leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{1}{\sqrt{2}} < 1.$$

$$\therefore |n + \sqrt{-1} - (a + b\sqrt{-1})(s + t\sqrt{-1})| < |a + b\sqrt{-1}|.$$

よって  $a + b\sqrt{-1}$  についての条件より左辺は 0 になるので、

$$n + \sqrt{-1} = (a + b\sqrt{-1})(s + t\sqrt{-1}), \text{ 同様に } p = (a + b\sqrt{-1})(u + v\sqrt{-1}).$$

上の右式より  $p^2 = (a^2 + b^2)(u^2 + v^2)$  だから  $a^2 + b^2$  は  $p^2$  の正の約数となる。ここで、

- もし  $a^2 + b^2 = 1$  ( $\Leftrightarrow (a, b) = (\pm 1, 0), (0, \pm 1)$ ) ならば

$$1 = (n + \sqrt{-1})(\alpha + \beta\sqrt{-1}) + p(\gamma + \delta\sqrt{-1})$$

を満たす整数  $\alpha, \beta, \gamma, \delta$  が存在するので、 $n - \sqrt{-1}$  を両辺にかけると

$$n - \sqrt{-1} = (n^2 + 1)(\alpha + \beta\sqrt{-1}) + p(n - \sqrt{-1})(\gamma + \delta\sqrt{-1}).$$

両辺の虚部を比べると  $-1 = (n^2 + 1)\beta + p(n\delta - \gamma) \equiv 0 \pmod{p}$  となるので矛盾。

- もし  $a^2 + b^2 = p^2$  ならば  $u^2 + v^2 = 1$  となるので、上式より

$$n + \sqrt{-1} = (a + b\sqrt{-1})(s + t\sqrt{-1}) = \frac{p(s + t\sqrt{-1})}{u + v\sqrt{-1}} = p(u - v\sqrt{-1})(s + t\sqrt{-1}).$$

両辺の虚部を比べると  $1 = p(ut - vs) \equiv 0 \pmod{p}$  となるので矛盾が生じる。

従って  $a^2 + b^2 = p$  となる。 証明終.

これらの結果を使うと次のことが分る (「初等整数論講義」 p.250~251) :

### 4.3 定理

1 より大きい平方数で割り切れない自然数  $n$  は、

$$n = 2^m p^a q^b r^c \cdots \quad (m, a, b, c, \dots \text{ は } 0 \text{ または } 1 \text{ で、 } p, q, r, \dots \text{ は } 4 \text{ で割ると } 1 \text{ 余る素数})$$

の形の素因数分解を持つとき、またそのときに限って、互いに素な 2 つの平方数の和として表される。

## 5 平方剰余

### 5.1 平方剰余の定義

奇素数 (すなわち 2 以外の素数)  $p$  と、 $p$  で割り切れない整数  $a$  に対し、 $n^2 \equiv a \pmod{p}$  を満たす整数  $n$  が存在するとき、 $a$  は  $p$  を法として平方剰余であるとい

$$\left(\frac{a}{p}\right) = 1$$

と表す。また平方剰余にならない  $a$  は平方非剰余であるとい

$$\left(\frac{a}{p}\right) = -1$$

と表す。(-) を Legendre の記号という。

### 5.2 平方剰余の求め方

奇素数  $p$  未満の自然数の 2 乗  $1^2, 2^2, \dots, (p-1)^2$  を  $p$  で割った余りと合同になる整数が、 $p$  を法とする平方剰余になる。例えば

$n$	1	2	3	4	5	6	...
$n^2$	1	4	9	16	25	36	...
$n^2 \pmod{3}$	1	1	0	1	1	0	...
$n^2 \pmod{5}$	1	4	4	1	0	1	...
$n^2 \pmod{7}$	1	4	2	2	4	1	...

となるから、

$$a \text{ が } 3 \text{ を法として平方剰余} \iff a \equiv 1 \pmod{3},$$

$$a \text{ が } 5 \text{ を法として平方剰余} \iff a \equiv 1, 4 \pmod{5},$$

$$a \text{ が } 7 \text{ を法として平方剰余} \iff a \equiv 1, 2, 4 \pmod{7}.$$

### 5.3 剰余についての基本定理 … 奇素数 $p$ に対し次が成り立つ :

$$(1) \left(\frac{a}{p}\right) = 1 \text{ ならば } (p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p}$$

$$\left(\frac{a}{p}\right) = -1 \text{ ならば } (p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$(2) (p-1)! \equiv -1 \pmod{p} \quad (\text{Wilson の定理})$$

$$(3) \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \quad (\text{Euler の規準})$$

- (4)  $p$  で割り切れない整数  $a$  に対し、 $a^{p-1} \equiv 1 \pmod{p}$  (Fermat の小定理)
- (5)  $p \equiv 1 \pmod{4} \iff \left(\frac{-1}{p}\right) = 1$  すなわち  $n^2 \equiv -1 \pmod{p}$  となる整数  $n$  が存在する  
(Euler の定理の証明 Step 1 で、第 1 補充法則と呼ばれている)
- (6)  $p$  で割り切れない整数  $a, b$  に対し、 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$

#### 5.4 Fermat の小定理 (4) の応用

- $3^{100}$  を 13 と 17 で割った余りをそれぞれ求めよ。

Fermat の小定理より  $3^{12} \equiv 1 \pmod{13}$  となるから、

$$3^{96} = (3^{12})^8 \equiv 1^8 \equiv 1 \pmod{13} \implies 3^{100} = 3^{96} \cdot 3^4 \equiv 3^4 = 81 \equiv 3 \pmod{13}.$$

また Fermat の小定理より  $3^{16} \equiv 1 \pmod{17}$  となるから、

$$3^{100} = (3^{16})^6 \cdot 3^4 \equiv 3^4 = 81 \equiv 13 \pmod{17}.$$

よって余りはそれぞれ 3, 13 となる。

#### 5.5 基本定理の証明の第 1 段階 : (1) $\implies$ (2)~(6)

- (1)  $\implies$  (2) の証明 :  $1 \equiv 1^2 \pmod{p}$  だから、(1) より

$$(p-1)! \equiv -1^{\frac{p-1}{2}} = -1 \pmod{p}.$$

- (1), (2)  $\implies$  (3) の証明 : 場合分けして示すと、

$$\left(\frac{a}{p}\right) = 1 \implies -a^{\frac{p-1}{2}} \stackrel{(1)}{\equiv} (p-1)! \stackrel{(2)}{\equiv} -1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$\left(\frac{a}{p}\right) = -1 \implies a^{\frac{p-1}{2}} \stackrel{(1)}{\equiv} (p-1)! \stackrel{(2)}{\equiv} -1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

- (3)  $\implies$  (4) の証明 :

$$a^{\frac{p-1}{2}} \stackrel{(3)}{\equiv} \left(\frac{a}{p}\right) = 1 \text{ または } -1 \pmod{p}$$

の両辺を 2 乗すると、 $a^{p-1} \equiv 1 \pmod{p}$ .

- (3)  $\implies$  (5) の証明 : (3) に  $a = -1$  を代入すると、

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

となるが、両辺は 1 または  $-1$  の値をとり、 $1 \not\equiv -1 \pmod{p}$  だから、

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (p \equiv 1 \pmod{4} \text{ のとき}) \\ -1 & (p \equiv 3 \pmod{4} \text{ のとき}). \end{cases}$$

- (3)  $\Rightarrow$  (6) の証明 :

$$\left(\frac{ab}{p}\right) \stackrel{(3)}{\equiv} (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \stackrel{(3)}{\equiv} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}$$

となるが、両辺は  $p$  を法として合同で  $\pm 1$  の値をとるので等しい。 証明終.

従って (2)~(6) はすべて (1) から従うので、(1) を証明すればよい。

## 5.6 補題 1 : (1) の証明の準備その 1.

$p$  未満の自然数  $r$  に対し、 $rs \equiv a \pmod{p}$  を満たす  $p$  未満の自然数がただ 1 つ存在する (これを  $r$  の配偶と呼び、 $r^*$  と書く)。

証明.  $r$  と  $p$  は互いに素だから、定理 1.5 より  $mr + np = 1$  を満たす整数が存在する。両辺に  $a$  をかけると  $amr + anp = a$  となるから  $amr \equiv a \pmod{p}$ 。よって  $am$  を  $p$  で割った余りを  $s$  とすれば、 $0 \leq s < p$  で  $am \equiv s \pmod{p}$  より

$$rs \equiv a \pmod{p}.$$

さらにもし  $s = 0$  ならば  $a \equiv 0 \pmod{p}$  となり  $p \nmid a$  に矛盾するから  $0 < s < p$ 。従って条件を満たす  $s$  が存在することが示された。

また  $p$  未満の自然数  $s, s'$  が共に条件を満たすとすると  $rs \equiv a \equiv rs' \pmod{p}$  より  $r(s - s') \equiv 0 \pmod{p}$  すなわち  $p \mid r(s - s')$  となる。一方  $p \nmid r$  だから定理 1.7 より  $p \mid (s - s')$  となるが  $-(p-2) \leq s - s' \leq p-2$  より  $s = s'$  となる。従って条件を満たす  $s$  がただ 1 つであることも示された。 証明終.

## 5.7 補題 2 : (1) の証明の準備その 2.

$\left(\frac{a}{p}\right) = 1$  のとき、 $r^* = r$  となる  $p$  未満の自然数はちょうど 2 つ存在して、その和は  $p$  になる。

証明. 仮定より  $n^2 \equiv a \pmod{p}$  を満たす整数  $n$  が存在するから、 $n$  を  $p$  で割った余りを  $r$  とすると、 $p \nmid a$  より  $0 < r < p$  で

$$r^2 \equiv n^2 \equiv a \pmod{p}$$

従って  $r^* = r$  となる。このとき  $p - r$  は  $r$  と異なる (もし  $p - r = r$  ならば  $p = 2r$  は素数でなくなる)  $p$  未満の自然数で、

$$(p - r)^2 = p^2 - 2pr + r^2 \equiv r^2 \equiv a \pmod{p}$$

より  $(p - r)^* = p - r$  を満たす。

また  $s^* = s$  となる  $p$  未満の自然数  $s$  をとると、 $s^2 \equiv a \equiv r^2 \pmod{p}$  より

$$s^2 - r^2 = (s - r)(s + r) \equiv 0 \pmod{p} \implies p \mid (s - r)(s + r)$$

よって定理 1.7 より  $p \mid (s - r)$  または  $p \mid (s + r)$  となるが、前者の場合  $s - r = 0$ 、後者の場合  $s + r = p$  となる。よって条件を満たす  $s$  は  $r, p - r$  のいずれかになる。 証明終.

## 5.8 基本定理の証明の第2段階：(1)の証明

まず  $\left(\frac{a}{p}\right) = 1$  のとき、 $p$  未満の自然数  $1, 2, \dots, p-1$  の中で  $r^* = r$  となるものを1つとると、補題2より  $r$  と  $p-r$  以外の  $p$  未満の自然数は自分と異なる配偶を持つから、それら配偶するものどうしの組  $\{s, s^*\}$  を単位として  $\frac{p-3}{2}$  個に分割される。 $s \cdot s^* \equiv a \pmod{p}$  となるから、

$$(p-1)! \equiv r(p-r) \cdot a^{\frac{p-3}{2}} \equiv -r^2 \cdot a^{\frac{p-3}{2}} \equiv -a \cdot a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}} \pmod{p}.$$

また  $\left(\frac{a}{p}\right) = -1$  のときは、 $r^* = r$  すなわち  $r^2 \equiv a \pmod{p}$  を満たすものはなく、 $1, 2, \dots, p-1$  を配偶するものどうしの組  $\{s, s^*\}$  を単位として  $\frac{p-1}{2}$  個に分割すると、 $s \cdot s^* \equiv a \pmod{p}$  より  $(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$ . 証明終.

## 5.9 補足

(7) 第2補充法則：

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & (p \equiv \pm 1 \pmod{8} \text{ のとき}), \\ -1 & (p \equiv \pm 3 \pmod{8} \text{ のとき}). \end{cases}$$

(8) 相互法則（証明は難しい）：異なる奇素数  $p, q$  に対し、

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

これらの法則（定理）を用いることにより、平方剰余が次のように簡単に計算できる：

$$\begin{aligned} \left(\frac{17}{23}\right) &\stackrel{(8)}{=} \left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) \stackrel{(6)}{=} \left(\frac{2}{17}\right) \left(\frac{3}{17}\right) \stackrel{(7)}{=} \left(\frac{3}{17}\right) \stackrel{(8)}{=} \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) \stackrel{(7)}{=} -1. \\ \left(\frac{365}{1847}\right) &\stackrel{(6)}{=} \left(\frac{5}{1847}\right) \left(\frac{73}{1847}\right) \stackrel{(8)}{=} \left(\frac{1847}{5}\right) \left(\frac{1847}{73}\right) = \left(\frac{2}{5}\right) \left(\frac{22}{73}\right) \\ &\stackrel{(6)}{=} \left(\frac{2}{5}\right) \left(\frac{2}{73}\right) \left(\frac{11}{73}\right) \stackrel{(7)}{=} -\left(\frac{11}{73}\right) \stackrel{(8)}{=} -\left(\frac{73}{11}\right) = -\left(\frac{7}{11}\right) \stackrel{(8)}{=} \left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) \\ &\stackrel{(6)}{=} \left(\frac{2}{7}\right)^2 = 1. \end{aligned}$$

## 6 整数論と暗号

文献：N. Koblitz, 櫻井幸一訳「数論アルゴリズムと楕円暗号理論入門」、シュプリンガー・フェアラーク東京 (1997)

### 6.1 素数判定

現代では大きな素数を使って作られた暗号が、電子情報の安全性のために用いられている。

- 大きな素数の記録 (1952 年以降は電子計算機による) :

発表年	1876	1951	1952	...	2013	2016
素数	$2^{127} - 1$	$(2^{148} + 1)/17$	$2^{521} - 1$	...	$2^{57885161} - 1$	$2^{74207281} - 1$
桁数	39	44	157	...	約 1743 万	約 2234 万

- $2^m - 1$  が素数ならば  $m$  も素数になる (逆は正しくない:  $2^{11} - 1 = 2047 = 23 \times 89$ )。よって素数  $p$  に対し、 $2^p - 1$  が素数になることが分れば大きな素数が得られる ( $2^p - 1$  と表される素数を Mersenne 型という)。
- 大きな自然数 (奇数)  $n$  が素数かどうか判定する方法 :

- $\sqrt{n}$  以下の自然数で割り切れるかどうかを調べる ... 非実用的  
 $\Rightarrow \sqrt{n}$  に比例して時間がかかり、すべての場合をチェックする必要がある。
- Fermat の小定理を用いた判定法 ...  $n$  と互いに素な自然数  $a$  に対し

$$(*) \quad a^{n-1} \equiv 1 \pmod{n}$$

が成り立つかどうかを調べる。

注. Fermat の小定理より、 $n$  が素数ならば (\*) は常に成立するので、(\*) が成り立たない  $a$  が 1 つでもあれば、 $n$  は素数でない。また (\*) が成り立たない  $a$  があれば、そのような  $a$  は全体の半分以上存在する。よって  $r$  個のランダムに選んだ  $a$  について (\*) が成り立てば、 $1 - (1/2)^r$  以上の確率で (\*) が常に成立し、 $n$  が素数である確率が増す。

- Solovay-Strassen の素数判定法 (1977) ... (2) より強力  
 $n$  と互いに素な自然数  $a$  に対し、

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}; \quad \left(\frac{a}{n}\right) : \text{Legendre 記号を拡張した Jacobi 記号}$$

が成り立つかどうかを調べる。

- AKS(Agrawal, Kayal, Saxena) 判定法 (2004) ... 素数判定の理論的完成  
Fermat の小定理に基づいた方法で、 $n$  の桁数の何乗かに比例する時間 (多項式時間) で、 $n$  が素数かどうか判定できる。

## 6.2 暗号と公開鍵暗号

- 暗号：メッセージ（平文）を別の形（暗号文）に偽装して、意図した受取人だけが偽装を取り払ってメッセージを読めるようにする方法
  - … 昔から戦争、外交などで使われてきた
  - … 現在では、インターネットショッピングにおける認証でも使われている
- ⇒ コンピューターの計算能力と数論に基づく「公開鍵暗号」
- 公開鍵暗号：暗号化するために必要な情報が公開されている暗号（この情報を公開鍵という）：

$$\begin{array}{ccc} & \text{暗号化} & \\ \text{平文} & \xrightarrow{\quad} & \text{暗号文;} \\ & \text{復号化} & \end{array} \left\{ \begin{array}{l} \text{暗号化： 公開鍵とコンピューターがあれば簡単} \\ \text{復号化： 復号化鍵がなければ膨大な計算量が必要} \end{array} \right.$$

公開鍵暗号の例として **RSA(Rivest, Shamir, Adleman)** 暗号と **ElGamal** 暗号を紹介する

## 6.3 RSA 暗号：大きな自然数の素因数分解の難しさを利用した暗号

1978年に発表されて広く使われている、最も古く有名な公開鍵暗号。

- user A は非常に大きな2つの素数  $p, q$  を用意し（これは A だけの秘密）、 $p, q$  の積  $n$ 、及び  $p-1, q-1$  と互いに素な自然数  $e$  を公開する
  - …  $n, e$  が公開鍵で  $p, q$  が復号化鍵となる。
- メッセージ  $P$ （： $n$ 未満の自然数）を user A に送るには、 $P^e \bmod(n)$  を暗号として A に送る。
- A は  $ed \equiv 1 \pmod{(p-1)(q-1)}$  を満たす自然数  $d$  を求めておくことにより、送られた暗号から、 $(P^e)^d = P^{ed} \equiv P \pmod(n)$  として  $P$  を復号できる。

## 6.4 RSA 暗号の例

- 公開鍵  $n(=pq) = 22, e = 7$  のとき、RSA 暗号  $C_1 = 3, C_2 = 5$  を解読して、メッセージ  $P_1, P_2$  を求めよ。

（解） $p = 2, q = 11$  より  $(p-1)(q-1) = 10$  だから、 $ed = 7d \equiv 1 \pmod{10}$  を満たす  $d$  は 3 になる。

$$\therefore P_1 = 3^3 = 27 \equiv \mathbf{5} \pmod{22}, \quad P_2 = 5^3 = 125 \equiv \mathbf{15} \pmod{22}.$$

## 6.5 ElGamal 暗号の準備

$p$  を素数とするとき、 $0 \leq a, b \leq p-1$  を満たす整数  $a, b$  と自然数  $n$  に対し、 $a \pm b$ ,  $a \times b$ ,  $a^n$  を  $p$  で割った余りを同じ記号で表す。

注.  $p$  が非常に大きな素数であっても、コンピューターを使えば  $a^n$  を求めるのは比較的簡単だが、 $a^n = b$  となる  $n$  を求めるのは大変 (離散対数問題)。

## 6.6 ElGamal 暗号 : 離散対数問題の難しさを利用した暗号

1985 年に発表され、これに基づいたデジタル署名標準が 1994 年に採用されている。

- 非常に大きな素数  $p$  と、 $p$  未満の自然数  $g$  を用意する。
- user A は  $p$  未満の自然数  $a$  を用意し (A だけの秘密)、 $g^a$  を計算して公開する  
 $\dots g^a$  が公開鍵で  $a$  が復号化鍵となる。
- メッセージ  $P$  ( $: p$  未満の自然数) を user A に送るには、整数  $k$  をランダムにとり

$$(\alpha, \beta) = (g^k, (g^a)^k \cdot P)$$

を暗号として A に送る ( $a$  を知らなくても計算できることに注意)。

- A は送られた暗号  $(\alpha, \beta)$  から、 $\alpha^a \cdot P = \beta$  を満たす  $p$  未満の自然数として  $P$  を復号できる。

## 6.7 ElGamal 暗号の例 $\dots$ 以下 $p = 13, g = 2$ とする

- 公開鍵  $g^a$  が 7 のとき、Elgamal 暗号  $(g^k, g^{ak}P) = (4, 3)$  を解読して、メッセージ  $P$  を求めよ。

(解)

$n$	1	2	3	4	5	6	7	8	9	10	11	12
$g^n$	2	4	8	3	6	12	11	9	5	10	7	1

より復号化鍵は  $a = 11$ .

$$\therefore g^{ak} = (g^k)^a = 4^{11} = 2^{22} = 2^{12} \cdot 2^{10} = 2^{10} = 10.$$

よって  $10 \cdot P = 3$  となるが、 $4 \cdot 10 = 1$  を用いると

$$P = 4 \cdot 3 = \mathbf{12}.$$

- 公開鍵  $g^a$  が 9 のとき、Elgamal 暗号  $(g^k, g^{ak}P) = (4, 2)$  を解読して、メッセージ  $P$  を求めよ。

(解) 上の表より復号化鍵は  $a = 8$  となるから、

$$g^{ak} = (g^k)^a = 4^8 = 2^{16} = 2^{12} \cdot 2^4 = 2^4 = 3.$$

よって  $3 \cdot P = 2$  となるが、 $9 \cdot 3 = 1$  を用いると

$$P = 9 \cdot 2 = \mathbf{5}.$$

## 7 数の組合せと保型形式

Zagier さんの言葉 : theory of modular forms ... get theorems without works

その例を以下に述べる。

### 7.1 例 1 (Jacobi の定理) .

自然数  $n$  に対し、 $r(n)$  を

$$a^2 + b^2 + c^2 + d^2 = n$$

を満たす整数の組  $(a, b, c, d)$  の個数とすると、 $r(n)$  は  $n$  の正の約数で 4 の倍数でないものすべての和の 8 倍に等しい。すなわち

$$(1) \quad r(n) = 8 \times \left( \sum_{0 < d|n, 4 \nmid d} d \right).$$

注. 上式の右辺 (=左辺) は常に正であることから、任意の自然数は 4 つの (0 を含む) 平方数の和として表されることが分る。

例えば  $n = 2$  のとき、条件を満たす  $(a, b, c, d)$  は

$$(a, b, c, d) = (\pm 1, \pm 1, 0, 0), (\pm 1, 0, \pm 1, 0), (\pm 1, 0, 0, \pm 1), \\ (0, \pm 1, \pm 1, 0), (0, \pm 1, 0, \pm 1), (0, 0, \pm 1, \pm 1)$$

で計  $4 \times 6 = 24$  個なので、(1) の左辺は 24。一方 2 の正の約数で 4 の倍数でないものは 1 と 2 だから、(1) の右辺は  $8 \times (1 + 2) = 24$  で左辺と一致する。

また  $n = 4$  のとき、条件を満たす  $(a, b, c, d)$  は

$$(a, b, c, d) = (\pm 2, 0, 0, 0), (0, \pm 2, 0, 0), (0, 0, \pm 2, 0), (0, 0, 0, \pm 2), \\ (\pm 1, \pm 1, \pm 1, \pm 1)$$

で計  $2 \times 4 + 2^4 = 24$  個なので、(1) の左辺は 24。一方 4 の正の約数で 4 の倍数でないものは 1 と 2 だから、(1) の右辺は  $8 \times (1 + 2) = 24$  で左辺と一致する。

### 7.2 例 2.

自然数  $k, n$  に対し、 $\sigma_k(n)$  を  $n$  の正の約数  $d$  すべてについての  $k$  乗  $d^k$  の和とする :

$$\sigma_k(n) \stackrel{\text{def}}{=} \sum_{0 < d|n} d^k.$$

このとき次が成り立つ：

$$(2) \quad \sigma_7(n) = \sigma_3(n) + 120 \sum_{i=1}^{n-1} \sigma_3(i) \sigma_3(n-i).$$

$$(3) \quad 11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{i=1}^{n-1} \sigma_3(i) \sigma_5(n-i).$$

例えば  $n = 2$  のとき

$$\left\{ \begin{array}{l} (2) \text{ の左辺} = 1^7 + 2^7 = 129 \\ (2) \text{ の右辺} = 1^3 + 2^3 + 120 \times 1^3 \times 1^3 = 129 : \text{左辺と一致} \end{array} \right.$$

$$\left\{ \begin{array}{l} (3) \text{ の左辺} = 11(1^9 + 2^9) = 11 \times 513 = 5643 \\ (3) \text{ の右辺} = 21 \times (1^5 + 2^5) - 10 \times (1^3 + 2^3) + 5040 \times 1^3 \times 1^5 \\ = 693 - 90 + 5040 = 5643 : \text{左辺と一致} \end{array} \right.$$

また  $n = 3$  のとき

$$\left\{ \begin{array}{l} (2) \text{ の左辺} = 1^7 + 3^7 = 2188 \\ (2) \text{ の右辺} = 1^3 + 3^3 + 120 \times \{1^3 \times (1^3 + 2^3) + (1^3 + 2^3) \times 1^3\} \\ = 1 + 27 + 120 \times 2 \times 9 = 2188 : \text{左辺と一致} \end{array} \right.$$

例 1, 2 の意味：違うやり方で定義された保型形式が実は一致する

これを (2) の場合について簡単に説明する。

### 7.3 (2) の略証.

4 以上の偶数  $k$  に対し、虚部が正となる複素数  $z$  の関数  $E_k(z)$  を

$$E_k(z) = \sum_{m,n} \frac{1}{(mz+n)^k} \quad (m, n \text{ はどちらかが } 0 \text{ でない整数全体を動く})$$

で定義すると、 $ad - bc = 1$  を満たす整数  $a, b, c, d$  に対して

$$E_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k E_k(z)$$

が成り立つ。この条件 (+アルファ) を満たす  $z$  の関数を、重さ  $k$  の保型形式 (関数)、またはモジュラー形式という。

$$E_4(z) : \text{重さ } 4 \text{ の保型形式} \Rightarrow E_4(z)^2 : \text{重さ } 8 \text{ の保型形式}$$

となるが、実は重さ 8 の保型形式は 1 次元しかない、すなわち定数倍を除いて一致することが知られているので、

$$E_4(z)^2 = cE_8(z)$$

を満たす定数  $c$  が存在する。一方  $q = e^{2\pi\sqrt{-1}z}$  とおくと

$$E_4(z) = \frac{\pi^4}{45} \left( 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n \right),$$

$$E_8(z) = \frac{\pi^8}{4725} \left( 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n)q^n \right).$$

よって  $E_4(z)^2, E_8(z)$  の  $q$  についての定数項は、それぞれ  $\left(\frac{\pi^4}{45}\right)^2, \frac{\pi^8}{4725}$  となるから、

$$c = \frac{4725}{45^2} = \frac{7}{3}.$$

これらを上式に代入すると、

$$\left( 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n \right)^2 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n)q^n.$$

上式の左辺、右辺における  $q^n$  の係数は、それぞれ

$$240\sigma_3(n) + 240^2 \sum_{i=1}^{n-1} \sigma_3(i)\sigma_3(n-i) + 240\sigma_3(n),$$

$$480\sigma_7(n)$$

となるから (2) が導かれる。 証明終.

#### 7.4 保型形式と数論.

保型形式は、現在数論の 1 分野として研究されており、さまざまなゼータ関数を生み出す有力な方法になっている。その大きな目標の一つは、数の範囲を広げたときに素数がどのように分解するか？を記述すること（非可換類体論の建設）である。

## 8 三辺の長さが自然数の直角三角形

Pythagorus の問題：三辺の長さが自然数になる直角三角形を求めよ、すなわち

$$a^2 + b^2 = c^2$$

を満たす自然数  $a, b, c$  をすべて求めよ。

### 8.1 定理

自然数  $a, b, c$  が  $a^2 + b^2 = c^2$  を満たすとき、

$$\begin{aligned} a &= l(m^2 - n^2), & b &= 2lmn, & c &= l(m^2 + n^2) \\ \text{または} \\ a &= 2lmn, & b &= l(m^2 - n^2), & c &= l(m^2 + n^2) \end{aligned}$$

を満たす自然数  $l, m, n$  で  $m > n$  となるものが存在する（逆に、このように表される自然数  $a, b, c$  は  $a^2 + b^2 = c^2$  を満たす）。

この定理の証明のために次の補題を示す：

### 8.2 補題

互いに素な自然数  $\alpha, \beta$  に対し、積  $\alpha\beta$  が平方数（整数の 2 乗となる数）ならば、 $\alpha$  と  $\beta$  は共に平方数となる。

証明.  $\alpha, \beta$  の素因数分解をそれぞれ

$$\alpha = p^a q^b r^c \dots, \quad \beta = s^l t^m u^n \dots$$

とすると、 $\alpha$  と  $\beta$  は互いに素だから、 $p, q, r, \dots$  と  $s, t, u, \dots$  の中に共通な素数はない。よって  $\alpha\beta$  の素因数分解は

$$\alpha\beta = p^a q^b r^c \dots s^l t^m u^n \dots$$

となる。一方仮定より、 $\alpha\beta = \gamma^2$  を満たす自然数  $\gamma$  が存在し、この  $\gamma$  は  $p, q, r, \dots, s, t, u, \dots$  を素因数に持つから、

$$\gamma = p^{a'} q^{b'} r^{c'} \dots s^{l'} t^{m'} u^{n'} \dots$$

とすると、

$$p^a q^b r^c \dots s^l t^m u^n \dots = \alpha\beta = \gamma^2 = p^{2a'} q^{2b'} r^{2c'} \dots s^{2l'} t^{2m'} u^{2n'} \dots$$

よって素因数分解の一意性より、

$$a = 2a', \quad b = 2b', \quad c = 2c', \quad \dots, \quad l = 2l', \quad m = 2m', \quad n = 2n', \quad \dots$$

となり、 $\alpha = (p^{a'} q^{b'} r^{c'} \dots)^2$  と  $\beta = (s^{l'} t^{m'} u^{n'} \dots)^2$  は平方数になる。 証明終。

### 8.3 定理の証明

$a, b, c$  の最大公約数を  $l$  とし、 $a = la', b = lb', c = lc'$  とすると、自然数  $a', b', c'$  の最大公約数は 1 で

$$(*) \quad (a')^2 + (b')^2 = (c')^2.$$

ここで  $a', b'$  が共に偶数であると仮定すると、(\*) より  $c'$  も偶数となり、 $a', b', c'$  がすべて 2 で割り切れることになり矛盾。また  $a', b'$  が共に奇数であると仮定すると、4.1 平方数の性質より

$$(a')^2 + (b')^2 \equiv 2 \pmod{4}$$

となるが、 $(c')^2$  は 4 を法として 0 または 1 と合同になるので、やはり (\*) に矛盾する。従って、 $a', b'$  のうち 1 つが奇数で残りの 1 つが偶数になる。

いま  $a'$  が奇数で  $b'$  が偶数であると仮定すると、(\*) より  $c'$  も奇数となるから、 $\frac{b'}{2}, \frac{c'+a'}{2}, \frac{c'-a'}{2}$  はいずれも自然数で、(\*) より

$$(\#) \quad \left(\frac{b'}{2}\right)^2 = \frac{(b')^2}{4} = \frac{(c')^2 - (a')^2}{4} = \left(\frac{c'+a'}{2}\right) \left(\frac{c'-a'}{2}\right).$$

いま  $\frac{c'+a'}{2}$  と  $\frac{c'-a'}{2}$  が互いに素でないと仮定すると、

$$\frac{c'+a'}{2} = sp, \quad \frac{c'-a'}{2} = tp$$

を満たす素数  $p$  と整数  $s, t$  が存在するから、 $c' = (s+t)p$  と  $a' = (s-t)p$  はいずれも  $p$  の倍数となり、(\*) より  $(b')^2$ 、従って  $b'$  も  $p$  の倍数となるので、 $a', b', c'$  の最大公約数が 1 であることに矛盾する。よって  $\frac{c'+a'}{2}$  と  $\frac{c'-a'}{2}$  が互いに素になるから、(\#) に 8.2 補題を適用すると、

$$\frac{c'+a'}{2} = m^2, \quad \frac{c'-a'}{2} = n^2$$

を満たす自然数  $m, n$  が存在する。よって

$$c' = m^2 + n^2, \quad a' = m^2 - n^2, \quad b' = \sqrt{(c')^2 - (a')^2} = \sqrt{4m^2n^2} = 2mn,$$

$$\therefore c = lc' = l(m^2 + n^2), \quad a = la' = l(m^2 - n^2), \quad b = lb' = 2lmn$$

となり、定理が成り立つことが示された。 $a'$  が偶数で  $b'$  が奇数である場合は、 $a'$  と  $b'$  を入れ替えて考えれば、 $a = 2lmn, b = l(m^2 - n^2), c = l(m^2 + n^2)$  と表される。証明終。

注. 上の証明の  $m, n$  は互いに素となり、1 つが偶数でもう 1 つが奇数になることが分る。

例.  $l = 1$  のとき 8.1 定理を使って直角三角形の例を作る :

$m$	$n$	$a = m^2 - n^2$	$b = 2mn$	$c = m^2 + n^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
...	...	...	...	...

## 9 Fermat 予想

Fermat 予想とは、Fermat が 1637 年頃に（本人は証明したと）書き記した次の主張：

3 以上の自然数  $n$  に対し、 $a^n + b^n = c^n$  を満たす自然数  $a, b, c$  は存在しない

### 9.1 定理 (Fermat)

Fermat 予想は  $n = 4$  のとき成り立つ。より強く

$$(*) \quad a^4 + b^4 = c^2$$

を満たす自然数  $a, b, c$  は存在しない。

**証明.** 背理法で示す。結論（主張）を否定すると  $(*)$  を満たす自然数の組  $a, b, c$  が存在することになるので、この中で  $c$  が最小になる解を 1 組とる。この解から、**Fermat** の降下法と呼ばれる方法により、 $c$  にあたる数がより小さくなる解を作って矛盾を導く。

まず  $a, b, c$  は互いに素（すなわち最大公約数が 1）となり、また必要なら  $a$  と  $b$  を入れ替えることによって  $a$  が奇数であるとしてよい。よって  $a^2 \equiv 1 \pmod{4}$  が成り立つ。 $(*)$  を書き換えた式：

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

に **8.1 定理** を適用すると

$$(1) \ a^2 = m^2 - n^2, \quad (2) \ b^2 = 2mn, \quad (3) \ c = m^2 + n^2$$

を満たす互いに素な自然数  $m, n$  が存在する。(2) に **8.2 補題** を適用することにより、

$$(A) \ m = 2\mu^2, n = \nu^2 \quad \text{または} \quad (B) \ m = \mu^2, n = 2\nu^2$$

を満たす自然数  $\mu, \nu$  が存在する。もし (A) の場合が起こるとすると、(1) より

$$a^2 + \nu^4 = 4\mu^4 \equiv 0 \pmod{4}$$

となるが、一方 **4.1 平方数の性質** より  $a^2 \equiv 1 \pmod{4}$ ,  $\nu^4 \equiv 0$  または  $1 \pmod{4}$  となるから矛盾が生ずる。よって (B) の場合だけが起こる。このとき (1) より

$$a^2 + 4\nu^4 = \mu^4 \quad \text{すなわち} \quad a^2 + (2\nu^2)^2 = (\mu^2)^2$$

となるから **8.1 定理** より

$$(4) \ a = \alpha^2 - \beta^2, \quad (5) \ 2\nu^2 = 2\alpha\beta, \quad (6) \ \mu^2 = \alpha^2 + \beta^2$$

を満たす互いに素な自然数  $\alpha, \beta$  が存在する。ここで (5) に **8.2 補題** を適用すると、

$$\alpha = (a')^2, \quad \beta = (b')^2$$

を満たす自然数  $a', b'$  が存在するから、 $c' = \mu$  とすると (6) より

$$(a')^4 + (b')^4 = (c')^2.$$

また (B) と (3) より

$$c' = \mu \leq \mu^4 = m^2 < m^2 + n^2 = c$$

となるから、(\*) の解  $a', b', c'$  で  $c' < c$  を満たすものが存在する。これは  $c$  の性質 (最小性) に矛盾する。 証明終.

注. 3 以上の自然数は 4 かまたは 3 以上の素数を約数に持つから、Fermat 予想を証明するには、すべての奇素数  $p$  に対し

$$a^p + b^p = c^p$$

を満たす自然数  $a, b, c$  が存在しないこと (これを  $p$  についての Fermat 予想と呼ぶ) を証明すればよいことになる。

## 9.2 Fermat 予想解決への歴史

- Euler (1770) :  $p = 3$  についての Fermat 予想を証明。
- Legendre (1825) :  $p = 5$  についての Fermat 予想を証明。
- Kummer (1850) : “正則な” 素数  $p$  についての Fermat 予想を証明 (注. 例えば 100 以下の素数の中では、37, 59, 67 以外が正則になる)。

方針.  $\zeta = \cos(2\pi/p) + \sqrt{-1} \sin(2\pi/p)$  : 円分数とにおいて上式を変形すると

$$a^p = c^p - b^p = (c - b)(c - \zeta b)(c - \zeta^2 b) \cdots (c - \zeta^{p-1} b)$$

となるが、 $a, b, c$  が自然数のとき、このような分解ができないことを示す。

⇒ 代数的整数論、円分体論が発展。

- Faltings (1983) : 高度に発達した数論幾何の諸結果を用い、すべての素数  $p$  について、 $a^p + b^p = c^p$  を満たす自然数の比  $a : b : c$  が有限になることを証明。
- Wiles and ... (1995) : すべての素数  $p$  についての Fermat 予想を証明。

方針. もし  $a^p + b^p = c^p$  を満たす奇素数  $p$  と自然数  $a, b, c$  が存在すると、方程式

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

によって定まる楕円曲線と呼ばれる空間は、右辺の解の差の積が  $p$  乗数になるという著しい性質を持つ。数論幾何の諸結果を用いて谷山-志村予想 (有理数体上の楕円曲線はモジュラーであろう) を証明することにより、このような空間が存在し得ないことを示す。

## 9.3 問. $a^2 + b^2 = c^4$ を満たす自然数 $a, b, c$ は存在するか?

答え.  $m > n$  となる自然数  $m, n$  に対し、 $a = m^2 - n^2$ ,  $b = 2mn$ ,  $c^2 = m^2 + n^2$  は  $a^2 + b^2 = (c^2)^2 = c^4$  を満たす (8.1 定理) から、 $m^2 + n^2 = c^2$  を満たす自然数  $m, n, c$  を求めればよい。

## 10 合同数問題と楕円曲線の数論

### 10.1 合同数

- 合同数 (congruent number) とは、三辺の長さが有理数 (すなわち、整数を 0 でない整数で割って得られる分数) となる直角三角形の面積として表される自然数のこと (注. 数の合同 (§3) とは関係なし)。

- 合同数問題 (Diophantus(246?~330?) による) とは、どのような自然数が合同数になるかを考える問題。

注. 合同数  $n$  が自然数  $m$  の平方  $m^2$  で割り切れるとき、 $n/m^2$  も合同数になるので、以下合同数としては 1 より大きい平方数で割り切れない (これを平方因子を持たないという) ものだけを考える。

- 合同数を作るには：

- 三辺の長さが自然数の直角三角形を作る (§8 を参照)。
- その面積を平方数で割って、平方因子を持たない自然数を作る。

$m$	$n$	$a = m^2 - n^2$	$b = 2mn$	$c = m^2 + n^2$	$S = ab/2$	合同数
2	1	3	4	5	$6 = 2 \cdot 3$	6
3	2	5	12	13	$30 = 2 \cdot 3 \cdot 5$	30
4	1	15	8	17	$60 = 2^2 \cdot 3 \cdot 5$	15
4	3	7	24	25	$84 = 2^2 \cdot 3 \cdot 7$	21
5	2	21	20	29	$210 = 2 \cdot 3 \cdot 5 \cdot 7$	210
5	4	9	40	41	$180 = 2^2 \cdot 3^2 \cdot 5$	5
...	...	...	...	...	...	...

- 実は、5 が最小の合同数になることが知られている。

- 定理. 2 は合同数にならない。

証明. 背理法で示す。もし 2 が合同数ならば

$$a^2 + b^2 = c^2, \quad \frac{ab}{2} = 2$$

を満たす正の有理数  $a, b, c$  が存在する。上式より  $b = 4/a$  となるから

$$c^2 = a^2 + b^2 = a^2 + \left(\frac{4}{a}\right)^2 = a^2 + \frac{16}{a^2}. \quad \therefore a^2 c^2 = a^4 + 2^4.$$

ここで有理数  $a, c$  を  $a = m/l, c = n/l$  ( $l, m, n$  は自然数) の形に表すと、上式より

$$\frac{m^2 n^2}{l^4} = \frac{m^4}{l^4} + 2^4. \quad \therefore (mn)^2 = m^4 + (2l)^4.$$

しかし 9.1 定理 で示したように、上式を満たす自然数  $m, n$  は存在しないので矛盾が生ずる。従って 2 は合同数ではない。 証明終.

## 10.2 合同数と楕円曲線

- いま自然数  $n$  が合同数ならば、

$$a^2 + b^2 = c^2, \quad \frac{ab}{2} = n$$

を満たす正の有理数  $a, b, c$  が存在する。このとき、

$$c^2 + 4n = a^2 + b^2 + 2ab = (a + b)^2, \quad c^2 - 4n = a^2 + b^2 - 2ab = (a - b)^2$$

となるから、 $x = c^2/4$  とおくと

$$x^3 - n^2x = x(x + n)(x - n) = \frac{1}{64}c^2(a + b)^2(a - b)^2 = \left\{ \frac{c(a + b)(a - b)}{8} \right\}^2.$$

よって次の対応が得られる：

$$(\sharp) \left\{ \begin{array}{l} \text{有理数を三辺に持つ面積 } n \text{ の直角三角形 } (a, b, c) \\ \downarrow \\ y^2 = x^3 - n^2x \text{ の有理数解 } (x, y) = \left( \frac{c^2}{4}, \frac{(a^2 - b^2)c}{8} \right). \end{array} \right.$$

- 楕円曲線 (elliptic curve) とは、重解を持たない  $x$  の 3 次式  $f(x)$  から定まる方程式  $y^2 = f(x)$  (の解集合) のこと。  $y^2 = x^3 - n^2x$  ( $n \neq 0$ ) はその例になっている。
- 楕円曲線  $y^2 = x^3 - 36x$  を使って、有理数を三辺に持つ直角三角形で面積が 6 になるものを作る。

- 面積 6 の直角三角形  $(a, b, c) = (4, 3, 5)$  に対し、 $(\sharp)$  より

$$(x, y) = \left( \frac{c^2}{4}, \frac{(a^2 - b^2)c}{8} \right) = \left( \frac{25}{4}, \frac{35}{8} \right) \text{ は、} y^2 = x^3 - 36x \text{ の解。}$$

- $(x, y) = \left( \frac{25}{4}, \frac{35}{8} \right)$  を通る  $y^2 = x^3 - 36x$  の接線と  $y^2 = x^3 - 36x$  との交点は、

$$\left( \frac{1,442,401}{140^2}, \frac{1,726,556,399}{140^3} \right) \left( \stackrel{??}{=} -2 \times \left( \frac{25}{4}, \frac{35}{8} \right) \right).$$

- $(\sharp)$  の対応の逆を使い

$$\begin{aligned} \frac{1442401}{140^2} &= \frac{1201^2}{140^2} = \frac{(c')^2}{4} = \frac{(a')^2 + (b')^2}{4}, \\ \frac{1726556399}{140^3} &= \frac{1201 \times 1437599}{140^3} = \frac{\{(a')^2 - (b')^2\} c'}{8} \end{aligned}$$

を満たす正の数  $a', b', c'$  を求めると、

$$a' = \frac{120}{7}, \quad b' = \frac{7}{10}, \quad c' = \frac{1201}{70}$$

となり、これは面積 6 の直角三角形の三辺となる。

- このようにして、有理数を三辺に持つ直角三角形で、同じ合同数を面積に持つものを沢山 (無限個) 作ることができる。

### 10.3 楕円曲線の数論

- 楕円曲線  $y^2 = x^3 + ax^2 + bx + c$  ( $a, b, c$  は有理数) の有理数解  $(x, y)$  の集合は、

$$P = (x_1, y_1), Q = (x_2, y_2) \quad (x_1 \neq x_2)$$

$$\Rightarrow P + Q = \left( \left( \frac{y_1 - y_2}{x_1 - x_2} \right)^2 - a - x_1 - x_2, \left( \frac{y_1 - y_2}{x_1 - x_2} \right) (x_1 - x_2) - y_1 \right)$$

: 直線  $PQ$  と楕円曲線との交点の、 $x$  軸に関する対称点

を加法として、無限遠点を単位元とする“アーベル群”になる。この群の“1次独立”な元の最大個数を、楕円曲線の階数 (**rank**) という。

- 久米教陽さん (平成 9 年佐大修士卒業) による例

面積 34 の 2 つの直角三角形  $(a, b, c) = \left( 24, \frac{17}{6}, \frac{145}{6} \right), \left( \frac{136}{15}, \frac{15}{2}, \frac{353}{30} \right)$  から (#) によって得られる  $y^2 = x^3 - 34^2x$  の 2 つの有理数解

$$\left( \frac{145^2}{12^2}, \frac{145 \times 20447}{12^3} \right), \left( \frac{353^2}{60^2}, \frac{353 \times 23359}{60^3} \right)$$

は、上記の加法について“1次独立”になる。よって  $y^2 = x^3 - 34^2x$  の階数は 2 以上。

- 楕円曲線の階数については、**Birch and Swinnerton-Dyer 予想** という次の予想：

楕円曲線の階数 (求めにくい) = そのゼータ関数の  $s = 1$  での位数 (求めやすい)

があり、これは現在でも証明されていない (証明した者には、賞金 100 万ドル!)。この予想が証明されれば、合同数問題について次の解答が得られる：

- (1) 自然数  $n$  を 8 で割った余りが 5, 6, 7 のいずれかであるとき、 $n$  は合同数になる (注.  $n$  が 8 で割った余りが 5, 7 になる素数か、または 4 で割った余りが 3 になる素数の 2 倍になるときは、Birch (1970 年) により成り立つことが証明されている)。
- (2) 任意の自然数  $n$  が合同数になるための必要十分条件が、Tunnel (1983 年) により次のように与えられている (注. 必要性は、Coates-Wiles の定理 (1977 年) により成り立つことが分る)：
  - \*  $n$  が奇数のときは、 $n = 2a^2 + b^2 + 8c^2$  を満たす整数の組  $(a, b, c)$  の個数が、 $n = 2a^2 + b^2 + 32c^2$  を満たす整数の組  $(a, b, c)$  の個数の 2 倍になること。
  - \*  $n$  が偶数のときは、 $\frac{n}{2} = 4a^2 + b^2 + 8c^2$  を満たす整数の組  $(a, b, c)$  の個数が、 $\frac{n}{2} = 4a^2 + b^2 + 32c^2$  を満たす整数の組  $(a, b, c)$  の個数の 2 倍になること。

## 11 終わりに … 現代の数論へ

### 数論 … 古く（紀元前）から始まり、今も活発に研究されている分野

- “数学者の王” と呼ばれる Gauss の言葉「数論は数学の女王である」  
その心は … 解析、幾何など数学の他分野の結果をどんどん使う “人使いの荒い” 分野
- 特に近年は、代数幾何学を仲立ちにしていろいろな空間の数論的性質を調べると共に、Galois 群、ゼータ関数など数論の基本的対象を研究する数論的幾何学が発展している。その主な成果は：

- Grothendieck（1960 年代）：現代代数幾何の思想と言葉を確立した。
- Mumford（1965 年）：モジュライ空間を代数幾何的に構成し、数論的幾何学における重要な道具を開発した。
- Deligne（1974 年）：Riemann 予想の幾何的類似である Weil 予想を一般的に証明し、その応用としてモジュラー（保型）形式に関する Ramanujan 予想：

$$q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \Rightarrow |\tau(p)| < 2p^{11/2} \quad (p: \text{素数})$$

を証明した。

- Faltings（1983 年）：Diophantus 問題の難問であった Mordell 予想：

種数が 2 以上の 2 元代数方程式  $f(x, y) = 0$  の有理数解は有限個

を証明した。

- Gross, Zagier（1986 年）：モジュラーな楕円曲線に対し、Birch and Swinnerton-Dyer 予想を部分的に解決した。
- Grothendieck, Drinfeld（1984, 1989 年）：モジュライ空間を用いて、絶対 Galois 群の幾何的表示を与えた。
- Wiles, ...（1995 年）：志村-谷山予想：

有理数体上の楕円曲線はモジュラーになる

を証明し、その応用として Fermat 予想を証明した。

- Lafforgue（2002 年）：Drinfeld の理論を発展させ、非可換類体論の 1 つの定式化である Langlands 予想：

Galois 群の表現はモジュラー形式から作ることができる

を関数体の場合に証明した。