

数学特別講義 XX

整数係数 2 次形式

コスキヴィルタ ジャンステファン

埼玉大学

2020 年 11 月 6 日

参考書

Cox, David A., Primes of the form $p = x^2 + ny^2$



(wikipedia)

フェルマーの定理

まず, $n = 1$ の場合を考える.

定理 (フェルマー)

奇素数 p に対し,

$$p = x^2 + y^2 \text{ と表すことができる} \iff p \equiv 1 \pmod{4}.$$



ピエール・ド・フェルマー
(1607 年 - 1665 年)



マラン・メルセンヌ
(1588 年 - 1648 年)

チェック

```
test := proc(n, m)
local a, b, x, y, v;
a := floor(sqrt(m));
b := floor(sqrt(m/n));
v := 0;
for x from 0 to a do for y from 0 to b do
if  $x^2 + n*y^2 = m$  then v := 1; break;
end if; end do; end do; v; end proc;

test_prime := proc(n, N)
local L, P, i;
P := [seq(ithprime(i), i = 1 .. N)]; L := [];
for i to N do if test(n, P[i]) = 1 then
L := [op(L), P[i]]; end if; end do; L; end proc;
```

素数	$p = x^2 + y^2$?	$p \equiv 1 \pmod{4}$?
3	×	×
5	$5 = 1^2 + 2^2$	○
7	×	×
11	×	×
13	$13 = 2^2 + 3^2$	○
17	$17 = 1^2 + 4^2$	○
19	×	×
23	×	×
29	$29 = 2^2 + 5^2$	○
31	×	×
37	$37 = 1^2 + 6^2$	○
41	$41 = 4^2 + 5^2$	○
43	×	×
47	×	×
53	$53 = 2^2 + 7^2$	○
59	×	×

$$n = 2, 3$$

定理 (フェルマー)

奇素数 p に対し,

$$p = x^2 + 2y^2 \iff \begin{cases} p \equiv 1 \pmod{8} \\ p \equiv 3 \pmod{8} \end{cases} \quad \text{または}$$

$$p = x^2 + 3y^2 \iff \begin{cases} p = 3 \\ p \equiv 1 \pmod{3} \end{cases} \quad \text{または}$$

二次形式

一般に, **2元2次形式** (binary quadratic form) とは,

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{C}$$

の形の多項式という. 特に, $a, b, c \in \mathbb{Z}$ とき, **整2次形式** (integral quadratic form) という.

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad M_f := \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

$\Delta_f := b^2 - 4ac$ は, f の**判別式**と呼ぶ.

もちろん, $x^2 + ny^2$ は整2元2次形式である.

同値関係

f を整 2 次形式とし, $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ とする. このとき,

$$(A \cdot f)(x, y) = f(rx + ty, sx + uy)$$

また整 2 次形式である. 整 2 次形式 f, g に対し, $g = A \cdot f$ ($A \in \mathrm{GL}_2(\mathbb{Z})$) ならば, f, g が互いに **同値 (equivalent)** であるといい, $f \sim g$ と書く.

$g = A \cdot f$ となる $A \in \mathrm{SL}_2(\mathbb{Z})$ が存在するとき, f, g は **properly equivalent** であるといい, $f \approx g$ で表す.

注意

$$f \sim g \implies \Delta_f = \Delta_g$$

定義

自然数 Δ により,

$$h(\Delta) = \#\{ \text{判別式 } \Delta \text{ の 2 次形式の同値類} \}$$

とおき, 類数と呼ぶ.

$$h(\Delta) \in \mathbb{N}? \quad h(\Delta) = \infty?$$

表現される整数

定義

$m \in \mathbb{Z}$ とする. 2次形式 f は m を表現するとは, $m = f(x, y)$ となる $x, y \in \mathbb{Z}$ が存在するときをいう. さらに互いに素 x, y が存在するとき, m が原始的に表現されるという.

$f \sim g \implies f, g$ は同じ整数を表現する.

補題

f が $m \in \mathbb{Z}$ を原始的に表現する $\iff f \sim mx^2 + b'xy + c'y^2$ ($b', c' \in \mathbb{Z}$)

$f = x^2 + ny^2$ の性質 :

- ① $\Delta_f = -4n$. 特に, $\Delta_f < 0$.
- ② 原始形式である. 一般に, 整 2 次形式 $ax^2 + bxy + cy^2$ は原始であるとは, $\gcd(a, b, c) = 1$ ときにいう. その性質は同値な形式の間で保たれる.
- ③ 簡約 2 次形式である. 簡約形式とは,

$$|b| \leq a \leq c \quad \text{かつ} \quad \left(|b| = a \text{ または } a = c \quad \text{ならば} \quad b \geq 0 \right)$$

を満たす 2 次形式 $ax^2 + bxy + cy$ をいう.

定理

任意の 2 次形式 f に対し, $f \approx g$ となる簡約形式 g が一意に存在する.

$ax^2 + bxy + cy^2$ 簡約ならば, $a \leq \frac{|\Delta|}{2}$ となる. よって, $h(\Delta)$ は有限である.

判別式 Δ	簡約 2 次形式	$h(\Delta)$
-4	$x^2 + y^2$	1
-8	$x^2 + 2y^2$	1
-12	$x^2 + 3y^2$	1
-20	$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$	2
-28	$x^2 + 7y^2$	1
-56	$x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2$	4

素数の話に戻ろう. 自然数 n を固定する.

補題

$p \nmid n$ となる奇素数 p に対し, 以下は同値である.

- ① 判別式 $-4n$ の f が存在し, p を原始的に表現する.
- ② $\exists k \in \mathbb{Z}, -n \equiv k^2 \pmod{p}$.

証明

① $\Rightarrow$ ②: p が判別式 $-4n$ の形式 f に原始的に表現されるとする. このとき, $f \sim px^2 + b'xy + c'y^2$. よって, $-4n = b'^2 - 4pc'$ である. 特に, b' は偶数であり, $b' = 2k$ と書ける $\Rightarrow -n \equiv k^2 \pmod{p}$.

② $\Rightarrow$ ①: $-n = k^2 + pd$ ならば, $-4n = (2k)^2 + 4pd$ である. 2 次形式 $f = px^2 + (2k)xy - dy^2$ の判別式は $-4n$ であり, f は p を原始的に表現する.

$$\exists k \in \mathbb{Z}, -n \equiv k^2 \pmod{p}$$

ならば, $-n$ は p を法とする **平方剰余** であるという.

定義

p を奇素数とし, a を整数とする.

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } p \nmid a \text{ かつ } \exists k \in \mathbb{Z}, a \equiv k^2 \pmod{p} \\ -1 & \text{if } p \nmid a \text{ かつ } \nexists k \in \mathbb{Z}, a \equiv k^2 \pmod{p} \\ 0 & \text{if } p \mid a \end{cases}$$

とおき, **ルジャンドル記号**と呼ぶ.



系

$h(-4n) = 1$ とする.

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p} \right) = 1$$

例えば、 $n = 1, 2, 3$ の場合はこの仮定が成り立つ.

平方剰余の相互法則

どのように $\left(\frac{a}{p}\right)$ を計算できるか？ まず、整数 a の素因数分解を、
 $a = \epsilon p_1^{\alpha_1} \dots p_m^{\alpha_m}$ ($\epsilon \in \{\pm 1\}$) とする。そして、

$$\left(\frac{a}{p}\right) = \left(\frac{\epsilon}{p}\right) \prod_{\alpha_i \text{ 奇数}} \left(\frac{p_i}{p}\right)$$

である。よって、素数 q に対し、 $\left(\frac{q}{p}\right)$ を計算するだけで十分である。

定理

互いに異なる奇素数 p, q に対し、次が成り立つ。

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

$$n = 3$$

$n = 3$ とする. 素数 $p > 3$ に対し,

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}} (-1)^{\frac{3-1}{2} \times \frac{p-1}{2}} = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3} \\ -1 & \text{if } p \equiv -1 \pmod{3} \end{cases}$$

である. $h(-12) = 1$ なので, $p > 3$ に対し,

$$p = x^2 + 3y^2 \iff p \equiv 1 \pmod{3}$$



$$n = 7$$

同様に, 奇素数 $p \neq 7$ に対し,

$$\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 2, 4 \pmod{7} \\ -1 & \text{if } p \equiv 3, 5, 6 \pmod{7} \end{cases}$$

である. $h(-28) = 1$ なので, 奇素数 $p \neq 7$ に対し,

$$p = x^2 + 7y^2 \iff p \equiv 1, 2, 4 \pmod{7}$$

$h(-4n) > 1$ の場合

$n = 5$ とする. この場合に, $h(-20) = 2$. 判別式 -20 の簡約形式は

$$x^2 + 5y^2, \quad 2x^2 + 2xy + 3y^2$$

である. よって, 奇素数 $p \neq 5$ に対し,

$$\begin{aligned} \begin{cases} p = x^2 + 5y^2 \text{ または} \\ p = 2x^2 + 2xy + 3y^2 \end{cases} &\iff \left(\frac{-5}{p} \right) = 1 \\ &\iff p \equiv 1, 3, 7, 9 \pmod{20}. \end{aligned}$$

$h(-4n) > 1$ の場合

$n = 5$ とする. この場合に, $h(-20) = 2$. 判別式 -20 の簡約形式は

$$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$$

である. よって, 奇素数 $p \neq 5$ に対し,

$$\begin{aligned} \begin{cases} p = x^2 + 5y^2 \text{ または} \\ p = 2x^2 + 2xy + 3y^2 \end{cases} &\iff \left(\frac{-5}{p} \right) = 1 \\ &\iff p \equiv 1, 3, 7, 9 \pmod{20}. \end{aligned}$$



それはオイラーが予想した.

種 (genus) の理論

カール・フリードリヒ・ガウス



$$\begin{cases} p = x^2 + 5y^2 \text{ または} \\ p = 2x^2 + 2xy + 3y^2 \end{cases} \iff p \equiv 1, 3, 7, 9 \pmod{20}.$$

$H = \{1, 9\} \subset (\mathbb{Z}/20\mathbb{Z})^\times$ は部分群である.
 $\{3, 7\}$ は $\{1, 9\}$ による剰余類である.

$$C(-4n) := \{ \text{判別式 } -4n \text{ の原始形式} \} / \sim$$

この集合は自然な群の構造を持ち, $x^2 + ny^2$ は $C(-4n)$ の単位元である.
また,

$$H = \left\{ \overline{m} \in (\mathbb{Z}/4n\mathbb{Z})^\times \mid \begin{array}{l} \gcd(m, 4n) = 1, \\ x^2 + ny^2 \text{ が } m \text{ を表現する} \end{array} \right\}$$

は $(\mathbb{Z}/4n\mathbb{Z})^\times$ の部分群である.

$f \in C(-4n)$ ならば, f が表現する $(\mathbb{Z}/4n\mathbb{Z})^\times$ の剰余類全体は H による剰余類 xH である. $f \mapsto xH$ で定まる写像は群準同型

$$C(-4n) \longrightarrow (\mathbb{Z}/4n\mathbb{Z})^\times / H$$

である。