Hasse-Minkowski の定理から Legendre の定理を導く

MATHEMATICS.PDF

2012-01-20

目 次

参考文献

[1] 加藤和也, 黒川信重, 斎藤毅: 数論 1, 岩波書店, 1996.

[2] 斎藤秀司: 整数論, 共立出版, 1997.

1　Legendre の定理と Hasse-Minkowski の定理

［定理 1.1（Legendre の定理）］ a, b, c を, どの二つをとっても互いに素な 0 でない整数であるとする. このとき,

- a, b, c は同一符号でない.
- a を割るすべての奇素数 p に対し, $\left(\dfrac{-bc}{p}\right) = 1$.
- b を割るすべての奇素数 p に対し, $\left(\dfrac{-ca}{p}\right) = 1$.
- c を割るすべての奇素数 p に対し, $\left(\dfrac{-ab}{p}\right) = 1$.

をすべて満たすならば, 方程式 $ax^2 + by^2 + cz^2 = 0$ は自明でない整数解をもつ.

今回, Legendre の定理を, 次の Hasse-Minkowski の定理から導く.

［定理 1.2（Hasse-Minkowski の定理）］ a, $b \in \mathbb{Q}^\times$ に対し, 次の二つの条件は同値である.

(i) 方程式 $ax^2 + by^2 = 1$ が $\mathbb{Q}$ において自明でない解をもつ.

(ii) 任意の素数 p および $p = \infty$ に対し, 方程式 $ax^2 + by^2 = 1$ が $\mathbb{Q}_p$ において自明でない解をもつ. ただし, $\mathbb{Q}_\infty = \mathbb{R}$ とする.

Hasse-Minkowski の定理の証明については, 加藤, 黒川, 斎藤 [1] 命題 2.20 あるいは斎藤 [2] 系 7.26 を参照のこと.

2　Hilbert 記号

p を素数または ∞ とし, $\mathbb{Q}_p$ を p 進整数環 ($p = \infty$ のときは $\mathbb{Q}_\infty = \mathbb{R}$) とする. a, $b \in \mathbb{Q}_p$ に対し,

$$(a,b)_p = \begin{cases} 1, & \text{方程式 } ax^2 + by^2 = 1 \text{ が } \mathbb{Q}_p \text{ において自明でない解をもつとき} \\ -1, & \text{そうでないとき} \end{cases}$$

とおく. 記号 $(a,b)_p$ を Hilbert 記号という.

[定理 2.1（積公式）] $a,\ b \in \mathbb{Q}^{\times}$ とする．このとき, $(a,b)_p$ は有限個の p を除いて 1 に等しく,

$$\prod_p (a,b)_p = 1$$

が成り立つ. この積で, p は ∞ と素数全体を走る.

積公式の証明については, 加藤, 黒川, 斎藤 [1] 定理 2.5 を参照のこと.

3　いくつかの補題

[補題 3.1] $a,\ b$ は 0 でない実数であり, $a > 0$ または $b > 0$ であるとする．このとき, 方程式

$$ax^2 + by^2 = 1$$

は自明でない実数解をもつ.

[証明] $a > 0$ と仮定しても一般性を失わない. $by_1^2 < 1$ を満たす 0 でない実数 y_1 を一つ選び,

$$x_1 = \sqrt{\frac{1 - by_1^2}{a}}$$

とおけば, $(x,y) = (x_1, y_1)$ が自明でない実数解である. □

[補題 3.2] p を素数, $a,\ b,\ r$ を整数とし, $\gcd(a,p) = \gcd(b,p) = 1$ とする．このとき, 合同式

$$ax^2 + by^2 \equiv r \pmod{p}$$

は $x,\ y$ について整数解をもつ.

[証明] まず, $a = 1$ の場合を証明する. すなわち, 合同式

$$x^2 + by^2 \equiv r \pmod{p}$$

が $x,\ y$ について整数解をもつことを証明する.

$p = 2$ の場合. $\gcd(b, 2) = 1$ より, $b \equiv 1 \pmod 2$ となる. $r \equiv 0 \pmod 2$ のとき, $(x, y) = (0, 0)$ が整数解の 1 つである. $r \equiv 1 \pmod 2$ のとき, $(x, y) = (1, 0)$ が整数解の 1 つである.

p が奇素数の場合. y^2 $(0 \leq y \leq (p-1)/2)$ は, どの 2 つも p を法として合同ではない. $\gcd(b, p) = 1$ より, $r - by^2$ $(0 \leq y \leq (p-1)/2)$ も, どの 2 つも p を法として合同ではない. ところが, これらの個数が $(p+1)/2$ 個であるにもかかわらず, 0 から $p-1$ までの整数のうち, p の平方非剰余であるものは $(p-1)/2$ 個しかない. ゆえに, ある整数 y_0 が存在して, $r - by_0^2$ は p の平方剰余になる. すなわち, ある整数 x_0 が存在して, $r - by_0^2 \equiv x_0^2 \pmod p$. このとき, $(x, y) = (x_0, y_0)$ は与えられた合同方程式の整数解である.

次に, 一般の場合について, $\gcd(a, p) = 1$ より, 1 次合同式 $ax \equiv b \pmod p$ は x についての整数解 b' をもつ. $\gcd(b, p) = 1$ より, $\gcd(b', p) = 1$ である. 同様に, 1 次合同式 $ax \equiv r \pmod p$ は x についての整数解 r' をもつ. 与えられた合同方程式の両辺を a で割ると,

$$x^2 + b'y^2 \equiv r' \pmod p$$

となり, $a = 1$ の場合に帰着する. □

[補題 3.3] p を奇素数, a, b, c を整数とし, a, b, c はいずれも p と互いに素であるとする. このとき, 方程式

$$ax^2 + by^2 + cz^2 = 0$$

は $\mathbb{Z}_p$ において自明でない解をもつ.

[証明] $z_0 \in \mathbb{Z}$ で p と互いに素なものを任意に一つとり, $r = -cz_0^2$ とおき, 補題 3.2 を適用すると, ある x_0, $y_0 \in \mathbb{Z}$ が存在して,

$$ax_0^2 + by_0^2 \equiv -cz_0^2 \pmod{p\mathbb{Z}}.$$

よって,

$$ax_0^2 + by_0^2 \equiv -cz_0^2 \pmod{p\mathbb{Z}_p}.$$

c は p と互いに素であるから, $c \in \mathbb{Z}_p^\times$. すなわち, $\mathbb{Z}_p$ における c の逆元 c^{-1} が存在する. 上式の両辺に c^{-1} を掛けたのち, $a' = -ac^{-1}$, $b' = -bc^{-1}$ とおくと,

$$-(a'x_0^2 + b'y_0^2) \equiv z_0^2 \pmod{p\mathbb{Z}_p}.$$

ゆえに, $-(a'x_0^2 + b'y_0^2) \in (\mathbb{Z}_p^\times)^2$. すなわち, ある $z_1 \in \mathbb{Z}_p^\times$ が存在して,

$$-(a'x_0^2 + b'y_0^2) = z_1^2.$$

両辺に $-c$ を掛けて移項すると,

$$ax_0^2 + by_0^2 + cz_1^2 = 0.$$

したがって, $(x, y, z) = (x_0, y_0, z_1)$ は方程式 $ax^2 + by^2 + cz^2 = 0$ の $\mathbb{Z}_p$ における自明でない解である. □

[補題 3.4] p を奇素数とし, a, b, c をどの二つをとっても互いに素な 0 でない整数であるとする. また,

- p が a を割るならば, $\left(\dfrac{-bc}{p}\right) = 1$.
- p が b を割るならば, $\left(\dfrac{-ca}{p}\right) = 1$.
- p が c を割るならば, $\left(\dfrac{-ab}{p}\right) = 1$.

がすべて成立するものとする. このとき, 方程式

$$ax^2 + by^2 + cz^2 = 0$$

は $\mathbb{Z}_p$ において自明でない解をもつ.

[証明] a, b, c はどの二つも互いに素だから, p が a, b, c のいずれも割らない場合と, a のみを割る場合を証明すれば十分である. 前者の場合は, 補題 3.3 より明らか. 後者の場合, $\left(\dfrac{-bc}{p}\right) = 1$ であるから, ある $z_0 \in \mathbb{Z}_p^\times$ が存在して, $z_0^2 = -bc$ となる. 両辺に c を掛け, $y_0 = c^2$ とおくと, $cz_0^2 = -by_0^2$ となる. ゆえに, $by_0^2 + cz_0^2 = 0$. このとき, $(x, y, z) = (0, y_0, z_0)$ は方程式 $ax^2 + by^2 + cz^2 = 0$ の $\mathbb{Z}_p$ における自明でない解である. □

4 Legendre の定理の証明

[定理 1.1（Legendre の定理, 再掲)] a, b, c を, どの二つをとっても互いに素な 0 でない整数であるとする. このとき,

- a, b, c は同一符号でない.
- a を割るすべての奇素数 p に対し, $\left(\dfrac{-bc}{p}\right) = 1$.
- b を割るすべての奇素数 p に対し, $\left(\dfrac{-ca}{p}\right) = 1$.
- c を割るすべての奇素数 p に対し, $\left(\dfrac{-ab}{p}\right) = 1$.

をすべて満たすならば, 方程式 $ax^2 + by^2 + cz^2 = 0$ は自明でない整数解をもつ.

[証明] 補題 3.4 より, p が奇素数ならば, 方程式 $ax^2 + by^2 + cz^2 = 0$ は $\mathbb{Z}_p$ における自明でない解 $(x, y, z) = (x_0, y_0, z_0)$ をもつ. $z_0 \neq 0$ であるとすれば, $(X, Y) = (x_0/z_0, y_0/z_0)$ は方程式 $(-a/c)X^2 + (-b/c)Y^2 = 1$ の $\mathbb{Q}_p$ における自明でない解である.

また, a, b, c は同一符号でないという仮定より, $-a/c > 0$ または $-b/c > 0$ である. 補題 3.1 より, $(-a/c)X^2 + (-b/c)Y^2 = 1$ は $p = \infty$ の場合にも自明でない解をもつ. よって, Hilbert 記号についての等式 $(-b/a, -c/a)_p = 1$ が $p = 2$ 以外の場合にいえる.

ところが, Hilbert 記号の積公式により, $p = 2$ の場合も $(-b/a, -c/a)_2 = 1$ でなければならない. すなわち, $(-a/c)X^2 + (-b/c)Y^2 = 1$ は $\mathbb{Q}_2$ においても自明でない解をもつ.

したがって, 任意の素数 p および $p = \infty$ に対し, $(-a/c)X^2 + (-b/c)Y^2 = 1$ は $\mathbb{Q}_p$ において自明でない解をもつ. よって, Hasse-Minkowski の定理により, $(-a/c)X^2 + (-b/c)Y^2 = 1$ は自明でない有理数解 $(X, Y) = (X_1, Y_1)$ をもつ. ある x_1, y_1, $z_1 \in \mathbb{Z}$, $z_1 > 0$ によって $X_1 = x_1/z_1$, $Y_1 = y_1/z_1$ と表せば, $(x, y, z) = (x_1, y_1, z_1)$ は方程式 $ax^2 + by^2 + cz^2 = 0$ の自明でない整数解である. □

[注意 4.1] 定理 1.1 の逆もいえて, 条件は必要十分である. 以下, それを証明する.

方程式 $ax^2 + by^2 + cz^2 = 0$ が自明でない整数解 (x_1, y_1, z_1) をもつとする.

a, b, c が同一符号ならば実数解は自明なものしかない. よって, 自明でない整数解が存在すれば, a, b, c は同一符号にならない.

係数の平方因子を整数解に押しやることにより, a, b, c は平方因子をもたないと仮定してもよい. さらに, $ax_1^2 + by_1^2 + cz_1^2 = 0$ の両辺を x_1, y_1, z_1 の公約数で割って $\gcd(x_1, y_1, z_1) = 1$ なるものが得られる. このとき, c が平方因子を持たないことにより, x_1, y_1 の共通の素因子は z_1 を割るので, そのような共通の素因子は存在しない. 他の組み合わせについても同様である. こうして, x_1, y_1, z_1 が二つずつ互いに素であるような整数解がとれる.

さて, a を割る任意の奇素数 p に対して,

$$by_1^2 + cz_1^2 \equiv 0 \pmod{p}$$

が成り立つ. 両辺に b を掛けて移項すると,

$$b^2y_1^2 \equiv -bcz_1^2 \pmod{p}.$$

a, b, c は互いに素であり, y_1, z_1 は共通の素因子をもたないことから, b, c, y_1, z_1 は p と互いに素である. ゆえに,

$$\left(\frac{-bc}{p}\right) = \left(\frac{-bcz_1^2}{p}\right) = 1.$$

同様にして, 残りの二つの条件も得られる.