第二回 ZK 数論セミナー
（テキスト：山本芳彦著，数論入門，§ 6.1,2）
暫定まとめ

佐藤隆

2009 年 5 月 18 日

整数 m，素数 p に対して，不定方程式 $x^2 + my^2 = p$ の整数解を求める．いくつかの例を結論から．

定理 0.1. 上の方程式が解を持つための必要十分条件は，以下．

(1) $m = 1$ のとき，$p = 2$ または $p \equiv 1 \mod 4$.
(2) $m = 2$ のとき，$p = 2$ または $p \equiv 1, 3 \mod 8$.
(3) $m = 3$ のとき，$p = 3$ または $p \equiv 1, 3 \mod 3$.
(4) $m = 5$ のとき，$p = 5$ または $p \equiv 1, 9 \mod 20$.
(5) $m = -2$ のとき，$p = 2$ または $p \equiv 1, 7 \mod 8$.
(6) $m = -3$ のとき，$p \equiv 1 \mod 12$.

必要性は mod とか平方剰余を使って証明できる．今後，十分性を一般的に証明するのが目標となる．

定理 0.2. $O = \mathbb{Z}[\sqrt{m}]$ $(m \in \mathbb{Z})$ が UFD のとき，素数 $p \in O$ の素元分解の様子は以下のようになる．

(1) $(\frac{m}{p}) = -1$ のとき，p は素元.
(2) $(\frac{m}{p}) = 0, 1$ のとき，$p = (a + b\sqrt{m})(a - b\sqrt{m})$ $(a, b \in \mathbb{Z})$ と素元分解される．

証明. O は UFD ゆえ，$p = \prod_{i=1}^{n} \pi_i$ と素元分解される．両辺のノルムをとると，$p^2 = \prod_{i=1}^{n} N(\pi_i)$．$N(\pi_i) \in \mathbb{Z} \setminus \{\pm 1\}$ に注意して，$i = 1, 2$ であることに注意しておく．

(1) $(\frac{m}{p}) = -1$ とする．もし，p が素元でないとすると，$i = 2$ で，$\pi_1 = a + b\sqrt{m}$ とおくと，$\pm p = N(\pi_1) = a^2 - mb^2$．いま，$p|b$ とすると，$p|a$ となり，$p^2|a^2 - mb^2 = p$ となり矛盾．よって，$(\frac{b}{p}) \neq 0$．いま，$p|a$ とすると，仮定より，$p \not| m$ であるから，$p|b$．同様にして，$(\frac{a}{p}) \neq 0$．よって，$(\frac{m}{p}) = (\frac{mb^2}{p}) = (\frac{a^2}{p}) = 1$．これは矛盾である．

(2) $(\frac{m}{p}) = 0, 1$ のとき，ある整数 x によって $m = x^2 \mod p$，すなわち，$p|(x^2 - m) = (x + \sqrt{m})(x - \sqrt{m})$ となる．一方，$p \not| (x \pm \sqrt{m})$ なので，p は素元ではない．よって，$i = 2$，$p = \pi_1\pi_2$，$\pm p = N(\pi_1) = N(\pi_2)$．$\pi_1 = a + b\sqrt{m}$ とすると，$\pm p = N(\pi) = a^2 + mb^2 = (a + b\sqrt{m})(a - b\sqrt{m})$．ここで，$N(a \pm b\sqrt{m}) = \pm p$ より $a \pm b\sqrt{m}$ は既約元[*1]，O が UFD ゆえ素元である[*2]．素元分解の一意性より，$\pi_2 = a - b\sqrt{m}$．結局，$p = (a + b\sqrt{m})(a - b\sqrt{m})$ と素元分解される．

□

初めの定理の証明の概略.

- $\mathbb{Z}[\sqrt{m}]$ が UFD であることを確かめる（PID であることを言うほうが簡単で，そうすれば UFD だとわかる．ただし，UFD にならない m もある）.
- 二つ目の定理より，m が p のもとで平方剰余であるかどうかで，不定方程式の解 (a, b) が存在するかが判定できる.
- 平方剰余であるかどうかを $\mod$ で表現すると，初めの定理の条件となる.

[*1] 命題 6.21

[*2] 「代数入門」p47, 問 9