

格子の整数論

東大 理 和田秀男

まずはじめに「 π 」の問題を考えよう。

問題. $x^2 - 3y^2 = \pm 1$ となる最小の整数解 (x, y) を求めよ。

これはまず左辺を因数分解して

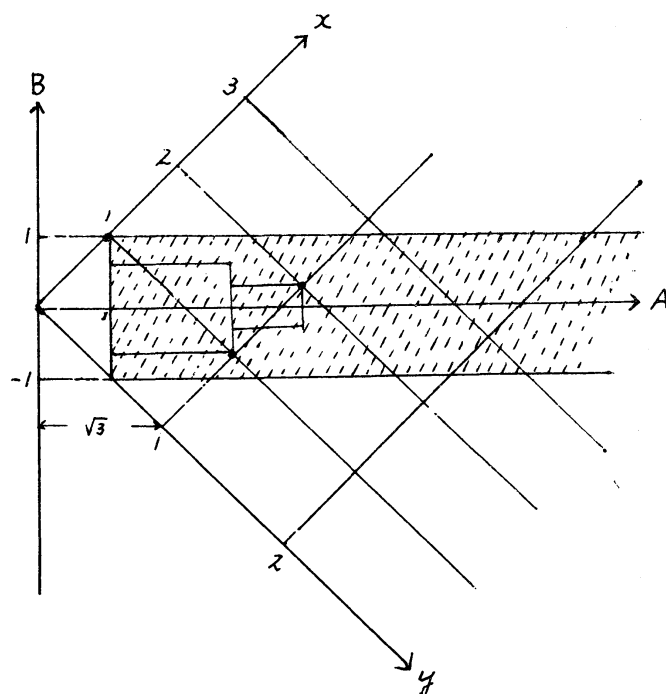
$$(x + \sqrt{3}y)(x - \sqrt{3}y) = \pm 1$$

とする. $A = x + \sqrt{3}y$, $B = x - \sqrt{3}y$ とおけば, $1 < A$,

$|B| < 1$ と思って良

い. つまり左図の点線の部分にある格子点を求めれば良い。

その中で $A \cdot B = \pm 1$ となるものを「 π 」がす。上記の問題の場合は最初の点は $(1, 1)$, 2 番目の点は $(2, 1)$ である。そして



$(1 + \sqrt{3})(1 - \sqrt{3}) = -2$, $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ であるから、 $(2, 1)$ が答である。

他の整数解は、 $(2 + \sqrt{3})^n = x_n + \sqrt{3}y_n$ としたときの (x_n, y_n) である。

同様に $x^2 - 2311y^2 = \pm 1$ の最小整数解を求めると、96番目の点となり

$$\begin{cases} x = 400892050972310899724010277137604913515533179720 \\ y = 8339259190601108963913338322963746423187510147 \end{cases}$$

となる。こゝの計算は $\sqrt{3}$ (x は $\sqrt{2311}$) を連分数展開すること、言い変えたものである。そして x/y は $\sqrt{3}$ (x は $\sqrt{2311}$) に非常に近い値なのである。つまり $\frac{x_n}{y_n} \xrightarrow{n \rightarrow \infty} \sqrt{3}$ となるが、その収束が速いのである。

$A = x + \sqrt{3}y$ の代りに $A = x + \sqrt[3]{3}y + (\sqrt[3]{3})^2z$ とおくと、どのようなことが言えるだろうか。 $\theta = \sqrt[3]{3}$ とおけば、

$$|A'|^2 = |A''|^2 = A'A''$$

$$= (x - y\theta)^2 + (y\theta - z\theta^2)^2 + (x - y\theta)(y\theta - z\theta^2)$$

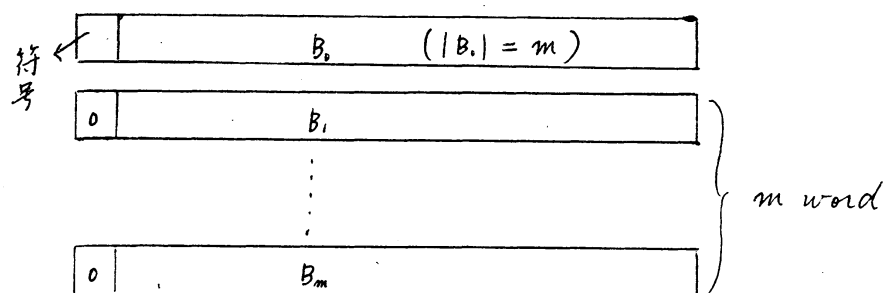
$$AA'A'' = x^3 + 3y^3 + 9z^3 - 9xyz$$

であるから、同様な(3次元格子点での)考察により

$$x^3 + 3y^3 + 9z^3 - 9xyz = \pm 1$$

の最小の整数解は、 $(x, y, z) = (4, 3, 2)$ となり

$$(4 + 3\theta + 2\theta^2)^3 = 52 + 36\theta + 25\theta^2$$



で 符号 及び以下いくつかの word で 1つの数を表わそうかと

いう値を入れ. $B_1, \dots, B_m$ で

$$B^* = B_m \cdot p^{m-1} + B_{m-1} \cdot p^{m-2} + \dots + B_1, \quad (p=2^{23}), (B_0 \text{ 正のとき})$$

$$\text{又/又 } B^* = -(B_m \cdot p^{m-1} + B_{m-1} \cdot p^{m-2} + \dots + B_1); \quad (B_0 \text{ 負のとき})$$

という数を表わすわけである。

$$B^* = B_m \cdot p^{m-1} + \dots + B_n \cdot p^{n-1} + \dots + B_1$$

$$C^* = C_n \cdot p^{n-1} + \dots + C_1$$

$$\text{のとき, } B^* \div C^* = D^* \text{ 余り } E^*$$

を計算するにはまず $0 < d < 2^{23}$ なる数と 正の整数 α を適当に求めて

$$|B^* - C^* \cdot d \cdot 2^\alpha|$$

がなるべく小さくなるようにすることを考える。

$$|B^* \cdot 2^\alpha - C^* \cdot 2^\alpha \cdot d \cdot 2^\alpha| = 2^\alpha \cdot |B^* - C^* \cdot d \cdot 2^\alpha|$$

であるから $|B^* - C^* \cdot d \cdot 2^\alpha|$ を小さくすることと

$|B^* \cdot 2^\alpha - C^* \cdot 2^\alpha \cdot d \cdot 2^\alpha|$ を小さくすることとは同じことである。

よって $0 \leq \alpha (< 23)$ なる整数を適当に求め、 B^*, C^* に 2^α

を乗ずることにより

$$2^{22} \leq C_n < 2^{23}$$

と書いてはつかえない。

$$|B^* \cdot 2^\beta - C^* \cdot d \cdot 2^{\beta+\rho}| = 2^\beta |B^* - C^* \cdot d \cdot 2^\rho|$$

であるから B^* の代りに $B^* \cdot 2^\beta$ に対する d, ρ を求めても良い。

(ただし、そのようにして求めた ρ は β 以上でなければならぬ。 $\rho \geq 23$ のときは心配ない。 $\rho < 23$ のときは $\beta = 0$ としておけば良い。) よって適当に $0 \leq \beta < 23$ なる整数を求め

$$\frac{1}{2} C_n \leq B_m < C_n$$

と書いてはつかえない。

このように標準化した上で d を何にしたら良いかといえは

$$(B_m \cdot p + B_{m-1}) \div C_n = d_0 \text{ 余り } r, \quad 0 \leq r < C_n$$

としたときの d_0 が最適である。なぜならは、

$$\begin{aligned} & |B^* - C^* \cdot d_0 \cdot p^{m-n-1}| \\ &= |(B_m p + B_{m-1} - C_n d_0) p^{m-2} + (B_{m-2} p^{m-3} + \dots + B_1) \\ &\quad - (C_{n-1} p^{n-2} + \dots + C_1) \cdot d_0 \cdot p^{m-n-1}| \end{aligned}$$

ここで

$$\begin{aligned} 0 &\leq (B_m p + B_{m-1} - C_n d_0) \cdot p^{m-2} + (B_{m-2} p^{m-3} + \dots + B_1) \\ &< r \cdot p^{m-2} + p^{m-2} < p^{m-1} \end{aligned}$$

$$0 \leq (C_{n-1} p^{n-2} + \dots + C_1) \cdot d_0 \cdot p^{m-n-1} < p^{n-1} \cdot p \cdot p^{m-n-1} = p^{m-1}$$

であるから

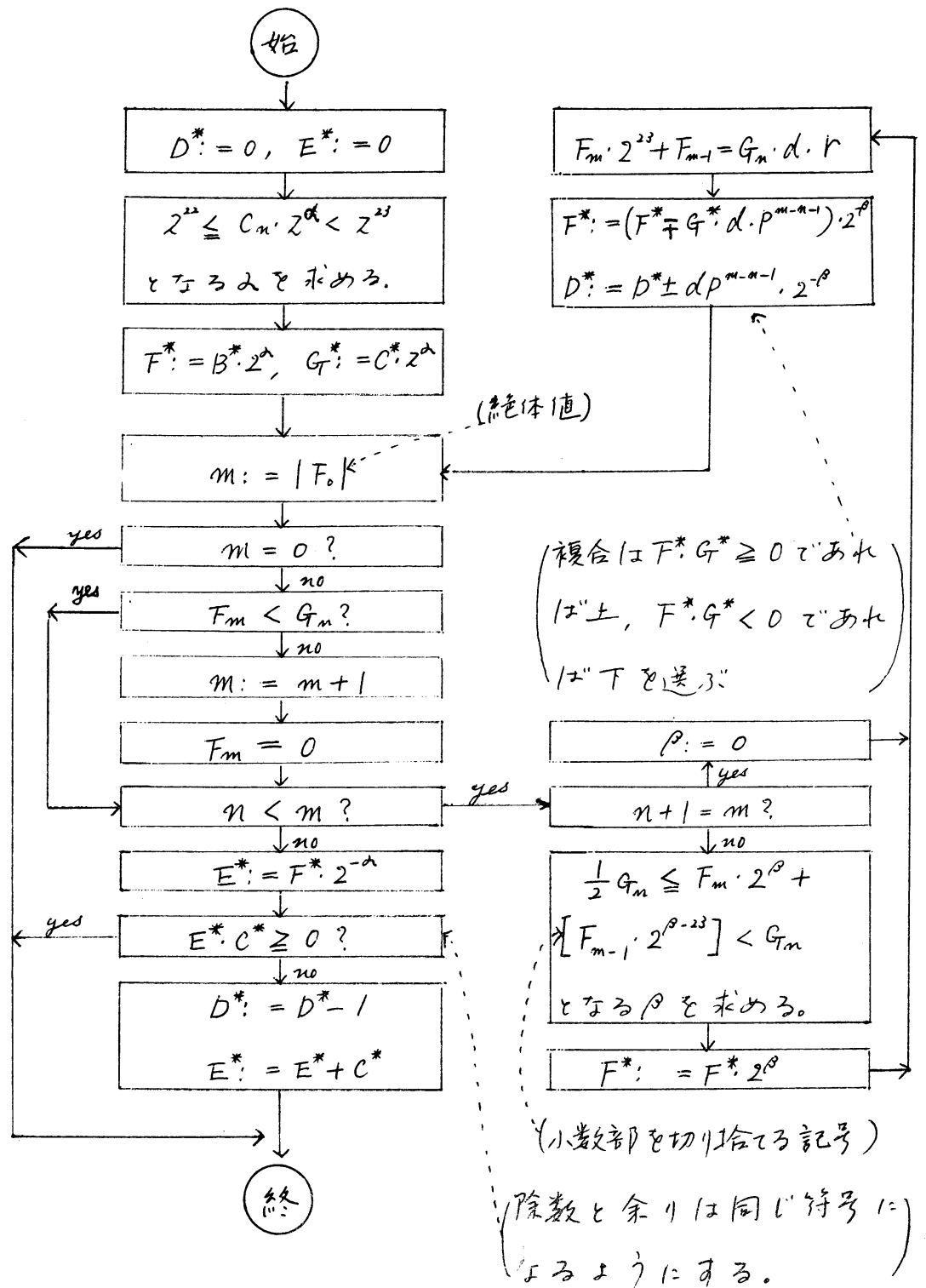
$$|B^* - C^* \cdot d_0 \cdot p^{m-n-1}| < p^{m-1}$$

である。つまり $d_0 \cdot p^{m-n-1}$ を最初の商に立てることにより B^* は

$$B^* - C^* \cdot d_0 \cdot p^{m-n-1} = \pm (B'_{m-1} p^{m-2} + \dots + B'_1)$$

となる。

以上の原理より、つぎのような流水図で除法が出来る。



$B^* \div C^* = D^*$ 余り E^* の流れ図