数理解析研究所講究録
第107巻 1971年 52-58

格子の整数論

東大 理　　和田秀男

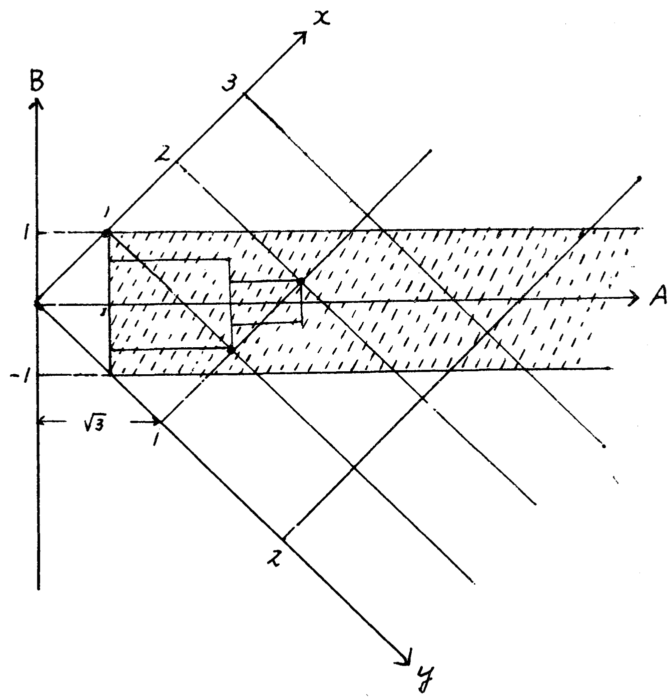
まずはじめにつぎの問題を考えよう。

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 $A\cdot B=\pm 1$ となるものをさがす。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 $x^2 - 2311y^2 = \pm 1$ の最小整数解をもとめると、96番目の点となり

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

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

$A = x + \sqrt{3}\,y$ の代りに $A = x + \sqrt[3]{3}\,y + (\sqrt[3]{3})^2 z$ 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

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

であるから2番目に小さな整数解は $(52, 36, 25)$ となる。2次元の場合と同様に x/y, y/z はともに $\theta \fallingdotseq 1.44225$ に非常に近い良い分数近似を与えている。このようなことを函数近似に利用出来ないであろうか。(連分数の拡張!)

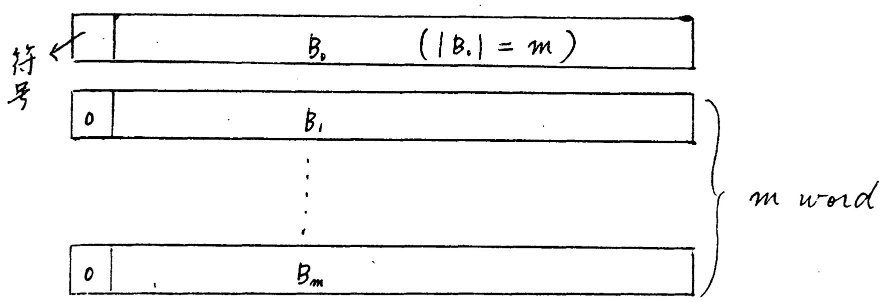
整数論において、3次元以上の格子の世界は謎多き、神秘の世界である。多くの不可思議な実例を、計算機が作り出すことを期待したい。又、これらの計算にはどうしても可変多倍長の四則計算が必要となる。これらが自由に行なえるシステムを、どの計算機も用意すべきではなかろうか。

つぎに多倍長除法の原理を記そう。
多倍長の数を多倍長で割るにはどうしたら能率良く出来るであろうか?
今、ここに24個のビットで1 wordをなしている計算機があったとしよう。1つのwordでは $P = 2^{23}$ より小さな数しか

a_0	a_1		a_{23}

符号($0 \to$ 正の数, $1 \to$ 負の数)

表わせないから、大きな数を表わすためにつぎのように $m+1$ 個で1つの数を表わすことにする。1番始めのword



で符号及び以下いくつのwordで1つの数を表わそうかという値を入れ、$B_1, \cdots, B_m$ で

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

又は $B^* = -(B_m \cdot P^{m-1} + B_{m-1} P^{m-2} + \cdots + B_1)$；（$B_0$負のとき）

という数を表わすわけである。

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

$$C^* = C_n P^{n-1} + \cdots + C_1$$

のとき、$B^* \div C^* = D^*$ 余り E^*

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

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

がなるべく小さくなるようにすることを考える。

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

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

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

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

と思ってさしつかえない。

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

であるから B^* の代りに $B^* \cdot 2^\beta$ に対する d, γ を求めても良い。(ただし、そのようにして求めた γ は β 以上でなければならない。$\gamma \geqq 23$ のときは心配ない。$\gamma < 23$ のときは $\beta = 0$ としておけば良い。) よって適当に $0 \leqq \beta < 23$ なる整数を求め

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

と思ってさしつかえない。

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ば、

$$(B_m \cdot P + B_{m-1}) \div C_n = d_0 \quad 余り\ r, \qquad 0 \leqq r < C_n$$

としたときの d_0 が最適である。なぜならば、

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

ここで

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

$$0 \leqq (C_{n-1} P^{n-2} + \cdots + C_1) \cdot d_0 \cdot P^{m-n-1} < P^{n-1} \cdot P \cdot P^{m-n-1} = P^{m-1}$$

であるから

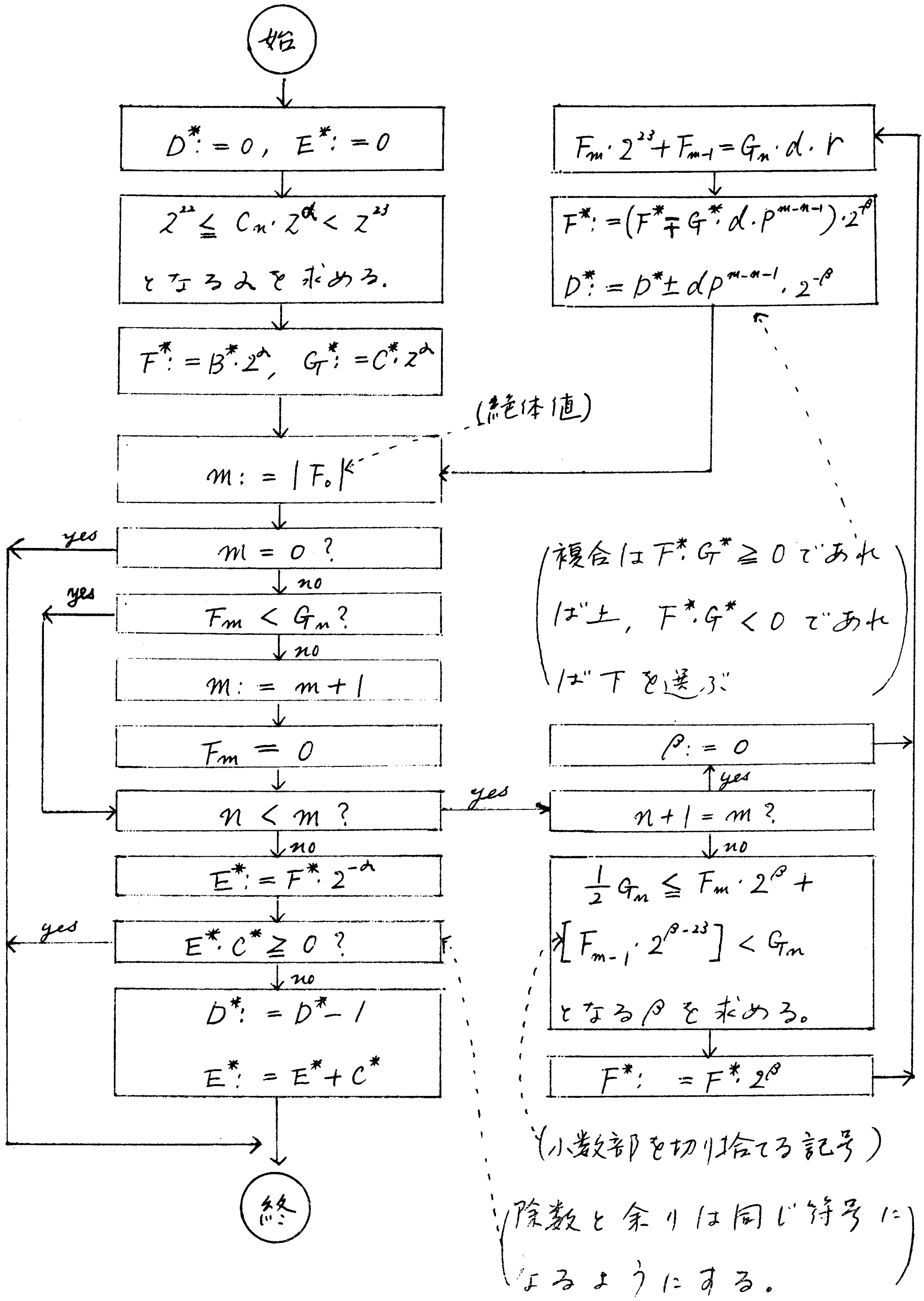
$$|B^* - C^* \cdot d_0 \cdot P^{m-n-1}| < P^{m-1}$$

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、

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

となる。

以上の原理より、つぎのような流れ図で除法が出来る。



$B^* \div C^* = D^*$ 余り E^* の流れ図