〔公　開〕

ＴＲ－Ｃ－０１１２

格子点探索法による素因数分解高速化手法

力石　徹也
Tetsuya　CHIKARAICHI

１９９５　　３．３１

ＡＴＲ通信システム研究所

格子点探索法による素因数分解高速化手法

Prime Factorization Method by searching Near Points of Solution Curve xy=N

力石徹也

Tetsuya Chakaraishi

ＡＴＲ通信システム研究所

ATR Communnication Systems Research Laboratories

１９９５年３月３１日

目次

１．はじめに

素因数分解の困難さに安全性の基礎を置く暗号・認証方式が数多く提案されている。RSA暗号、Fiat-Shamir零知識証明等がその例である。これらの暗号・認証方式が安心して使用できるためには、第３者による暗号の解読や偽証明が素因数分解と同等の困難さであることが証明され、素因数分解が計算量的に困難であるような合成数の桁数についての指針が与えられることが必要である。このうち、暗号・認証方式と素因数分解の計算量的な関係については専門書に譲るとして、ここでは後者の素因数分解の困難さについて論じる。

「RSA暗号のブロック長はどの程度であれば安全か」というような具体的な問題の解は、個々の素因数分解のアルゴリズムに依存する。最も単純、かつ明解な方法は合成数Ｎを素数で順に割る、という試行割算法である。但し、この方法は最悪$N^{1/2}$回の探索となり、１０進２００桁程度の合成数を用いる現在のRSA暗号は、解読不可能である。

今日では、専門的には素因数分解は準指数的な計算量であると言われている(1)。簡単に言えば、２００桁の合成数であれば、概ね$N^{1/8}$回の探索で済むことになる。このような計算量で素因数分解できるアルゴリズムは、楕円曲線法や２次ふるい法である。これらの手法を用いて、かつ多数の計算機を使用すれば、１５５桁の合成数が素因数分解できるまでになっている。

これらは概ね、「一定の規則で整数を次々と生成して、各整数と合成数の公約数を求める」という手法をとる。素因数を含む可能性の高い整数Ｌを生成する方法が、技術的なポイントである。例えば楕円曲線法では、ある種となる整数xと、数多くの素数の積からなる合成数Ｍとの積Mxを因数とする楕円関数の値を整数Ｌに用いる。整数ｘを振らせて、自明でない公約数が存在するかどうかを調べるのである。これらの手法を$N^{1/8}$オーダよりさらに高速化することは、興味あるテーマであるが、種xの選択法や選択範囲、整数Ｌを生成するアルゴリズム自体の改良法等の解決すべき問題がある。

本稿では試行割算法に近い、新しい素因数分解の方法を提案する。試行割算法では、因数の探索範囲が１から$N^{1/2}$までと決まっているので、研究の方向としては総当たり探索でない、効率的な因数探索法を見つけることに専念すればよい。この探索を効率化するには、幾何学的な手法が有効である。すなわち素因数分解は幾何学的はｘ、ｙを座標軸とする解平面上で、双曲線xy=Nが整数座標からなる講師点を通過する箇所を求めることに相当する。そこで双曲線xy=Nの近傍に位置するような格子点だけを取り出して、座標値の積を計算して合成数に一致すれば、それが因数である。この方法（これを格子点探索法と呼ぶことにする）により、最大、$N^{1/4}$の幅で因数を探索できる。従来の試行割算法やフェルマー法(1)等と比較すると高速である。さらに格子点探索法を高速化するために、仮想格子点を設定する方式と合成数の素数に対する剰余値から、格子点の中でも因数の候補となり得るもののみを選択し、これらの間引きされた格子点の中で、双曲線の近傍にあるものを探索する方式を提案する。

第２章では格子点探索法の基本的な方式の説明を行う。第３章では仮想格子点を導入した方式を説明し、第４章で剰余類を導入した方式を説明する。

2．格子点探索法

本章では格子点探索法の基本的な方式について述べる。

2－1　近傍点の探索

任意の合成数Nに対して、xy=Nなる整数解x，yはNの因数である。xあるいはyが合成数となる場合は、2数への因数分解を繰り返す。このようにして最終的に素因数を求めることができる。従ってここは2数への因数分解、xy=Nのタイプの問題のみ扱う。

（1）探索の考え方

解平面上でx，y座標が整数であるような点は格子状に無数に存在する。これらの格子点の中で解曲線xy=Nの最近傍に位置する点列のみを取り出すと、図1に示すような直線が引ける。実用的な暗号では、Nとして例えば10進200桁というような大きな合成数が用いられるので、双曲線を拡大してみると、ほぼ直線のように見える。従って近傍の格子点列からなる直線と解曲線の接線の傾きがほぼ並行なときには、直線と曲線は交差しない。すなわち解曲線と直線の交点は稀にしか存在しない。このような交点を取り出して、それが格子点上にあるかどうかを調べる、という方法で探索を進める。

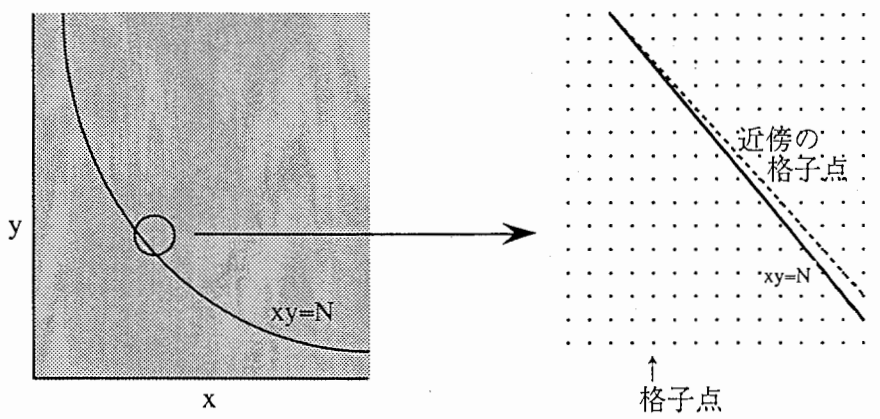


図1　解曲線の近傍の格子点

（2）交点の抽出

上述した近傍の格子点列を数式を用いて厳密に定義する。いま2つの整数n、mを次のように選ぶ。

$$nm > N$$

$$n(m-1) < N$$

$$n < m \qquad (1)$$

座標値が (1) 式を満たすような格子点を通る直線、並びにこの直線を平行移動した直線からなる直線群を次に定義する。

$$x = n - k$$

$$y = m + \beta k + \iota \qquad (2)$$

ここでk (≧0)、ι、βは整数で

$$\beta \triangleq \lfloor m/n = \alpha \rfloor \leqq \alpha \qquad (3)$$

（$\lfloor x \rfloor$はxを超えない最大の整数）

とする。(2) 式からパラメータkを消去すると

$y=-\beta(x-n)+m+\iota$ (4)

となる。これは格子点（n、m）を通り、傾きが$-\beta$の直線をy軸方向にιだけシフトした直線群を表す。このように選んだ直線群は次のような性質を持つ。

〔定理1〕 直線群 (4) のうち、$\iota \leqq -1$とした直線P上のx＜nの格子点は全て曲線より下にあり、xy=Nを満たすことはない。

〔証明〕 まず$\iota=-1$のときを考える。直線P上の格子点（x、y）＝（n－k、m+βk－1）に対して、合成数と積xyの誤差は

$g(k) \triangleq N-xy$

$=\beta k^2+(m-\beta n-1)k-N-n(m-1)$ (5)

である。(5) 式は軸が

$$-\frac{m-\beta n-1}{2\beta} \leqq \frac{1}{2\beta} \leqq \frac{1}{2}$$

となる放物線である。さらに

$g(0)=N-n(m-1)>0$

$g(1)=\beta+(m-\beta n-1)+N-n(m-1)$

$=\beta-1+(m-\beta n)+N-n(m-1)$

>0

$g(k)>0 \quad k \geqq 1$

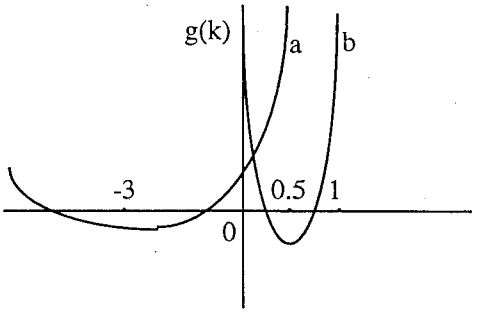


図2　誤差曲線N-xy

である。よって直線g(k)は軸が負のとき図2の曲線a、軸が正のとき図2の曲線bのようになり、いずれの場合も

$g(k)>0 \quad k=0、1、2、\cdots$

が言える。$\iota<-1$のときは積xyが$\iota=-1$の場合に比べて減少する。従って、$\iota<-1$のときもg(k)＞0　k=0, 1, 2,…が言える。□

以下では、解曲線xy=Nの近傍の格子点（x、y）のうち、座標値の積がxy≧Nとなるような点のみを選択することにする。従って定理1より、$\iota \geqq 0$の場合のみを考える。

〔定理2〕 直線群 (4) のうち、$\iota \geqq 0$とした直線Q上の点 (x, y) = (n-k, m+βk) に対して、xy=Nとなるkの値（≧0）が存在する。

〔証明〕 合成数と積xyの誤差を

$f(k) \triangle N-xy \qquad k \geqq 0$

とすると、

$f(k)=\beta k^2+k(m-n\beta)+N-nm$

$=\beta[k+(m-n\beta)/2\beta]^2+\cdots$

軸：$-(m-n\beta)/2\beta \leqq 0$

$f(0)=N-nm<0$

$f(k)=2\beta k+(m-n\beta)>0$

すなわちf(k)は下に凸の放物線である。f(0)＜0、f(∞)＞0、f(k)は単調増加なので、あるkの値に対してf(k)=0、すなわちxy=Nとなる。

一般に $\iota > 0$ のときも、同様に $f(k) = 0$ となる k が存在することを証明できる。□

探索の初期格子点の座標 n、m を (1) 式のように選ぶと、この格子点の付近では、解曲線 x、y=N と交差する様な直線群（$\iota \geqq 0$）の中で、$xy \geqq N$、かつ積 xy が最小となるのは $\iota = 0$ のときである。すなわち、定理１、２より $\iota = 0$ とした直線 Q が解曲線の最近傍にある。両者の交点は $f(k0) = 0$ となる。k0 から求まる。

$$k_0 = \frac{-(m-n\beta)+\sqrt{(m-n\beta)^2+4\beta(nm-N)}}{2\beta} \qquad (6)$$

この交点が格子点になっているときのみが因数である。交点の座標値が非整数のときは、直線上で交点の次に現れる格子点（座点と呼ぶ）を求め、その座標 (x, y) の座標値 y を更新して、次の初期格子点とする。すなわち合成数 N の因数を探索する手順（後述する方法と区別するため順方向探索と呼ぶ）は次のようになる。

〔探索手順１〕

① 探索の初期格子点の座標 n、m を (1) を満たすように選ぶ。

② (3) より n、m から β を求めて、(6) より k　を計算する。k_0 が整数ならば $(n-k_0、m+\beta k_0)$ が因数である。

③ k_0 が小数部を持つときは

$$(x_1, y_1) = (n - \lceil k_0 \rceil,\ m + \beta \lceil k_0 \rceil)$$

（$\lceil k_0 \rceil$ は k_0 より大きい最小の整数）

により、探索の底点となる格子点を求める。底点では $xy < N$ なので、次の初期格子点を (x_1, y_1+1) として、② から繰り返す。□

（３）探索間隔の解析

探索手順1で底点の x 座標と次の底点の x 座標値の差分をここでは探索間隔と呼ぶことにする。解曲線の近傍の格子点を結ぶ直線 Q と解曲線（局所的には直線状に見える）がほぼ並行になったときは探索間隔が長く、それ以外の区間では探索間隔が短くなる、という性質がある。従って、直線 Q の傾きと解曲線の接線の傾きが問題になる。

直線 Q の傾きは (4) より $-\beta(=-\lfloor m/n \rfloor)$ である。定義により $\lfloor m/n \rfloor$ は m/n を超えない最大の整数であるから、

$$-m/n \leqq -\beta < -m/n+1$$

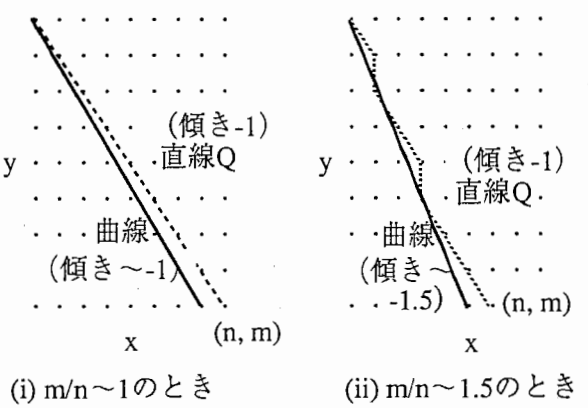
が成り立つ。

一方、解曲線の座標 x における接線の傾きは $-N/x^2 = -y/x$ （$\because N = xy$）である。ここで n、m が大きな値のときには、(n,m) の近傍にある格子点 (x, y) について、

$$\beta = -\frac{y}{x} = -\frac{m+\varepsilon_1}{n-\varepsilon_2} \fallingdotseq -\frac{m}{n}$$

（$\varepsilon_1 << m$, $\varepsilon_2 << n$）

となる。従って、$m \sim \beta n$ のときには、直



(i) m/n～1のとき　(ii) m/n～1.5のとき

図３　直線Qと解曲線

線Qと解曲線がほぼ平行になる。幾何学的には、このときに探索間隔が最大になると予想される（図３）。

このことは数値的にも容易に確かめることができる。すなわち、手順１で探索間隔k_0の値には次の性質がある。

$$1 \leqq \lceil k_0 \rceil \leqq \left\lceil \sqrt{\frac{nm-N}{\beta}} \right\rceil \qquad (7)$$

（右側の等号は$m=\beta n$のとき）

k_0は$m \fallingdotseq \beta n$のとき、すなわちmがnの整数倍になる毎にほぼ最大になる。このときのkの値は (7) 式から、nm-N、βの値に依存する。

このうちnm-Nの値については、次のような幾何学的な考察から推定できる。まず探索の初期値n、mが$m \fallingdotseq \beta n$の関係にあるとき、既に述べたように直線Qと解曲線（の接線）はほぼ平行である。従って、直線Qとの解曲線の交点の近傍にある底点 (n, m) は解曲線にほぼ接するように存在する。すなわち$n'\ m' \fallingdotseq N$が言える。従って、次の探索の初期値n'、m'+1について、

$$n' \ (m'+1) - N \sim n \qquad (8)$$

が言える。探索の初期値では、(1) よりnm-N＜nであるが、以上の考察から、$m \fallingdotseq \beta n$の関係が成り立つ範囲ではnm-N$\fallingdotseq$nと考えられる。

一方、βの値はn、$m \fallingdotseq N^{1/2}$では$\beta \fallingdotseq 1$であり、nが減少するにつれてβは増大する。探索間隔の最大値（$m \fallingdotseq \beta n$が成り立つときの値、nm-N$\fallingdotseq$nと考える）をnの関数として表示すると、(7) から図４のような傾向を示す。

これより、n、$m \fallingdotseq N^{1/2}$のときに探索間隔が$N^{1/4}$と最も長いが、nが減少すると、探索間隔が短くなってしまう。従って、本手法は基本的に因数が$N^{1/2}$の近傍にあるときに有効である。例えばNが10^{200}程度の値とすると、

$n=10^{100}$：探索間隔$=10^{50}$

$n=10^{98}$：探索間隔$=10^{47}$

……

$n=10^{66}$：探索間隔$=1$

となる。nが10^{100}から10^{98}まで、すなわち全探索区間10^{100}の99%は10^{47}の探索間隔で進む（但し、mとnが整数比という条件が成り立つ部分）。一方、nが小さい値のときは全数探索となってしまうので、最悪10^{66}回以上の探索が必要である。有限回の探索で打ち切るのが現実的であるから、その場合、因数が見つからないこともあり得る。この意味では確率的アルゴリズムとなっている。

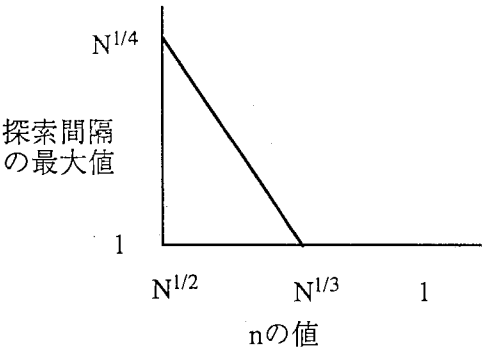


図４　探索間隔と探索点の関係

一方m／n$\fallingdotseq \beta$が成り立たない、すなわちm／nが図３ (ij) のように小数部を持つときに探索間隔が短くなり、(7) に示すように最悪では全数探索が必要になる。この場合の対策については後述する（３．仮想格子点）。

2－2　逆方向探索

初期格子点の座標値の比m／nが整数値より僅かに小さいとき（例えばm/n=1.99のような場合)、探索手順1では探索間隔が短いが、手順の若干の変更で探索間隔を長くすることができる。

いま解曲線の近傍の格子点からなる直線群（(2) に対応）を次のように定義しなおす。

$$x=n+k$$

$$y=m-\gamma\ k+\iota \qquad (9)$$

ここで

$$\gamma \triangleq \lceil m/n \rceil \qquad (10)$$

とする。(4) と同様に

$$y=\gamma\ (x-n)+m+\iota \qquad (11)$$

となる方程式が得られる。このとき、定理1、2と同様の性質が成り立つ。

〔系1〕 直線群 (11) のうち、$\iota \leqq -1$ とした直線P上のx＜nの格子点は全て曲線より下にあり、xy=Nを満たすことはない。(証明略)

〔系2〕 直線群 (11) のうち、$\iota \geqq 0$ とした直線Q上の格子点 $(x, y) = (n+k, m-\gamma k)$ に対して、xy=Nとなるkの値（≧0）が存在する。(証明略

これより、探索手順1とは逆に初期格子点 (n, m) からxを増加する方向に探索すれば、探索間隔が長くなる。

〔探索手順2〕

①探索の初期格子点の座標n, mを (1) を満たすように選ぶ。

②整数zがあって、

$$m/n < z \qquad (12)$$

$$z-m/n=\varepsilon << 1$$

のとき、(10) からγを求める。さらに (6)（ただしβはγと置き換える）からk_0を計算する。

③ (x_1, y_1)

$$=(n+\lceil k_0 \rceil,\ m-\gamma\lceil k_0 \rceil)$$

により、探索の底点となる格子点を求める。底点ではxy＜Nなので、次の初期格子点を (x_1, y_1+1) として②から繰り返す。□

3．仮想格子点

3－1　仮想格子点の考え方

初期格子点の座標値の比m/nが整数から離れているとき、探索手順1、2では探索間隔が短いが、仮想的な格子点を考慮することで、探索間隔を長くすることができる。

例えばm/n≒1.5のとき、図5のようにy軸方向に1/2だけ平行移動した格子点を追加する。解曲線の近傍の格子点を結ぶと、この直線Qは解曲線（局所的には直線状）とほぼ平行になって探索間隔が長くなる。ただし解曲線上の格子点が見つかっても、座標値が整数とは限らないので、整数か否かの検査は必要である。一般にm/n≒R+t/s（R, s, tは整数）のときはw/s (w=1, 2,…s-1) 平行移動した格子点を追加する。

以下、探索手順1と同様に順方向の探索を行う場合について、詳細を述べる。まず整

数値を座標とする格子点に、w/sだけy軸方向に平行移動した格子点を追加した点群wを考える。

wの中で改めて初期格子点 (n, m) を次のように選ぶ。

$$nm > N$$
$$n\ (m-1/s) < N$$
$$R+t/s \leqq m/n < R+\ (t+1)\ /s$$
(n, R, s は整数)　　(13)

解曲線の近傍にある、Wの点を結ぶ直線群を

$$x=n-k$$
$$y=m+\ (R+t/s)\ k+\ \iota\ /s \qquad (14)$$
$$(\ \iota\ =1, 2, \cdots)$$

とすると、定理1、2が成り立つ。

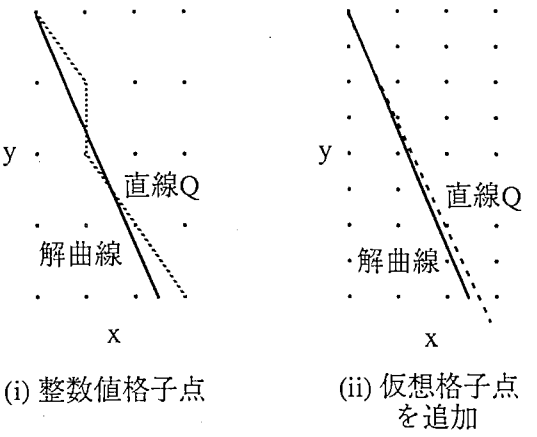


図5　仮想格子点の考慮

(14) で ι =0とした直線Qと、解曲線の交点は f (k_0) =N-xy=0 となる k_0 から求まる。

$$k_0=\frac{-[m-n(R+t/s)]+\sqrt{[m-n(R+t/s)]^2-4(R+t/s)(N-nm)}}{2(R+t/s)} \qquad (15)$$

〔探索手順3〕

①探索の初期格子点の座標n, mを (13) を満たすように選ぶ。

② (15) から k_0 を求め、底点 $(x_1, y_1) = (n-\lfloor k_0 \rfloor, m+\ (R+t/s)\lfloor k_0 \rfloor)$ を求める。

③$x_1 y_1$ =Nのとき、y_1 が整数ならばx　、y　が因数である。y　が非整数ならば次の初期格子点を $(x_1, y_1+1/s)$ として②に戻る。

④$x_1 y_1$ < Nのとき、$x_1\ (y_1 + v/s) \geqq N$ となる最小のvを求める。

⑤$x_1\ (y_1+v/s)$ =Nのとき、y_1+v/s が整数ならば、因数である。y_1+v/s が非整数ならば $(x_1, y_1+v/s+1/s)$ を次の初期格子点として②に戻る。

⑥$x_1\ (y_1+v/s)$ > Nのとき、$(x_1, y_1+v/s)$ を次の格子点として②に戻る。□

3－2　探索回数の解析

手順3で因数が見つかるまでの探索回数は、仮想格子点の密度sに依存する。これは次の2つの要因がある。

①総区間数との関係

仮想格子点の導入により、探索区間はs分割される。分割された各区間で初期格子点を求めて探索するので、最低限s回の探索は必要になる。例えば $N^{1/2}$ の幅で区切ると、$N^{1/4}$ 個の区間が生じる。従って、sの値として $N^{1/4}$ をとると、1探索区間内での探索の方法をいかに効率化しようと、全体の探索回数は $N^{1/4}$ 以上となる。

②探索間隔との関係

仮想格子点の近傍間隔は大きいとは言え、初期格子点の比m/nが整数の場合よりは小さい、という点がある。点群Wにおいては (7) に対応する式として

$$1 \leqq \lceil k_0 \rceil \leqq \left\lfloor \sqrt{\frac{nm-N}{R+t/s}} \right\rfloor \qquad (16)$$

（右側の等号は m= (R+t/s) n が成り立つとき）

が得られる。(13) より nm-N ＜ n/s なので、探索間隔は手順１と同様に求めることができて

$$k0=N^{1/4}/s^{1/2} \qquad (17)$$

となる。すなわち探索間隔はm/nが整数の場合と比べると探索間隔が $(1/s)^{1/2}$ に短縮する。

sの値は、およそ次のように目安を付けることができる。まず手順１のみでは、探索点の座標比m/nが整数値から離れたときに、探索幅k_0がどの程度、減少するかに着目する。前述した図５では１桁の整数について (6) からk_0を計算した。この例ではm/n=1～1、1の間で探索幅k_0が$N^{1/4}$のオーダを維持している。すなわち、区間〔m/n=1,m/n=2〕を1/10に分割するようなsの値は１０である。一方、合成数Nが２００桁の場合を考える。初期格子点n、mとその比は概算次のようである。

m/n=1.0　　$n=n_0 \times 10^{100}$

$m=n_0 \times 10^{100}+\varepsilon$

$(\varepsilon << n)$

m-n=1.1　　$n=0.95n_0 \times 10^{100}$

$m=1.05n_0 \times 10^{100}$

……

(6) 式の各要素、並びにk　の概算値は以下の通りである。

m/n=1.0　　$m-n\ \beta = \varepsilon$

$nm-N=n_0 \times 10^{100}$　　((8) より)

$k_0 \sim 10^{50}$

m n=1.1　　$m-n\ \beta =0.1n_0 \times 10^{100}$

$nm-N=0.95n_0 \times 10^{100}$　　((8) より)

$k_0 << n$

……

同様の計算をm/nが1～1、1の間についても行うことができる。この結果、大きな桁数の合成数Nに対しては、k_0が$N^{1/4}$を維持するようなsの値は$N^{1/4}$程度と大きいことが分かる。

そこでsの値を$N^{1/4}$にとり、今までに説明した$N^{1/4}$の探索幅を持つ格子点探索のアルゴリズムを適用したとき、仮想格子点の影響がどのように出るかを考察する。

① 総区間数と関係

全探索区間$N^{1/2}$を$N^{1/4}$毎に区切るので、総区間数は$N^{1/4}$である。$N^{1/4}$個の初期格子点から、各々$N^{1/4}$の探索幅をもつアルゴリズムを適用できれば、全体として$N^{1/4}$回の探索で因数を求められる。

② 探索間隔との関係

(17) 式から、探索幅は

$$\frac{N^{1/4}}{s^{1/4}}=\frac{N^{1/4}}{N^{1/8}}=N^{1/8}$$

と縮小する。

このようにsはk_0が$N^{1/4}$を維持するように$N^{1/4}$と大きな値を選んだが、仮想格子点が探索間隔に及ぼす影響から、結果的には$N^{1/8}$の探索間隔となった。従って、sは$N^{1/4}$より小さい値$N^{1/t}$ $(t>4)$ に選ぶ方がよい。また、一般に探索中の格子点の座標比m/nが非整数の区間で、つねに$s=N^{1/t}$にとる必要はない。例えばm/n≒1.5のときはs=2でよい。従ってsは格子点の位置によって1から$N^{1/t}$ $(t>4)$ の間に分布する。このとき探索間隔は$N^{1/4}$から$N^{1/v}$ $(4<v<8)$ の間に分布する。探索間隔を図式的に描くと図6のようになる。

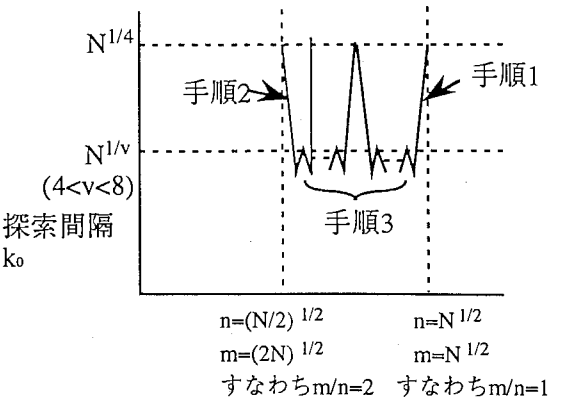


図6　仮想格子点を用いたときの探索間隔k0の因数値依存性

4．剰余類

これまでに述べた手順は、最大$N^{1/4}$の探索間隔となる。RSA暗号のようにN≒10^{200}程度の合成数では、10^{50}という大きな探索間隔である。しかしこれでも全体の探索区間である$N^{1/2}=10^{100}$を探索するには手順に示した底点の計算を10^{50}回以上、繰り返す必要がある。

そこで、これまでの手順をさらに高速化できるかどうかが、次の論点になる。ここでは、合成数Nをある素数で割った余りの値から、因数となり得る格子点を絞り込んで、その中でこれまでの手順を適用する手法を提案する。

4－1　剰余類の考え方

素数Pに対して、p個の剰余類Z_0、Z_1、Z_2、…Z_{p-1}が存在する。ここではZ_iとは$z=i \bmod p$となるような整数zの集合である。

いま合成数Nを2整数の積で表すことを考える。整数を任意に一つ選ぶと（この整数はある剰余類に属する）、他方の整数が属する剰余類が一意に定まる。NはZ_0に属さないと仮定すると（もしNがZ_0に属するならば、Nは素数pで割り切れ、因数分解ができたことになる）Nを2整数の積で表現したときの、剰余類の組合せは

$$\left.\begin{array}{l} N=z_1\ z_j \\ N=z_2\ z_k \\ \cdots\cdots \\ N=z_{p-1}\ z_l \end{array}\right\} \text{p-1通り} \qquad (18)$$

ただし　$z_t \in Z_t$

だけである。例えば合成数Nが$N=1 \bmod 3$のとき

$$N=(3a+1)\ (3b+1) \qquad (19)$$
$$N=(3a+2)\ (3b+2)$$

ただしa、bは整数

のような因数分解だけが考えられる。

ある素数pを選んで、Nのpに対する剰余から、(18) のように剰余類の組合せが定まる。そのうちの一つ、例えば

$N=z_i\ z_j \quad (z_i \in Z_i, z_j \in Z_j)$ (20)

のような剰余類の組合せを仮定する。このとき探索手順1では、初期格子点を

$nm>N, n\ (m-p)\ <N$ (21)

$n<m, \qquad n \in Z_i, m \in Z_j$

と選ぶ。また (2) に相当する直線群は

$x=n-pk$ (22)

$y=m+p\ \beta\ k+p\ \iota$

である。定理1、2は同様に成立ち、$\iota=0$ のときの (6) に相当する k_0 は

$(n-pk_0)\quad (m+p\ \beta\ k_0)=N$

から

$$k_0=\frac{-(m-\beta n)+\sqrt{(m-\beta n)^2+4\beta(nm-N)}}{2p\beta} \qquad (23)$$

となる。このときの探索間隔は

$$1 \leqq \lceil pk_0 \rceil \leqq \left\lceil \sqrt{\frac{nm-N}{\beta}} \right\rceil \qquad (24)$$

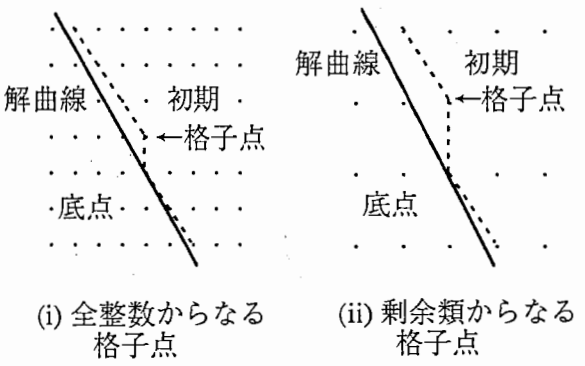
(右側の符号は $m=\beta n$ のとき)

である。

(24) の値域は、剰余類を考えないとき ((7) 式) と式の表現は同一であるが、平方根の中の分子の値が異なる。まず探索の直線群 (22) の傾き $-\beta$ は解曲線の接線の傾きとほぼ一致していると仮定する。これは、探索間隔を大きくとるための必須条件であり、仮想格子点を設ければ実現可能であることは既に述べた。このときそこ点は図7に示すように解曲線の近傍に存在する。次の初期格子点 (n, m) は格子間隔だけ m の値が増大する。素数pの剰余類を考慮すると、格子間隔は全整数からなる格子点の場合に比較してp倍である。すなわち (24) の nm-N の値は、素数 p の剰余類を考えることにり p 倍になる。このとき探索間隔 pk　は$\sqrt{\ }$ p 倍になる。

以上の考察から、格子点として素数pに対する剰余類をとると、格子点が整数の場合に比べて探索間隔が$\sqrt{\ }$ p 倍になる。従って、探索回数は整数の場合の $1/\sqrt{\ }$ p で済む。しかし剰余類に対する因数の表現は、(18) からp-1t通りある。これらの剰余類の表現の中で、どれが真の表現かを、合成数から判断することは困難である。従って、探索をp-1回繰り返さなければならず、全体の探索回数は逆に $(p-1)/\sqrt{\ }$ p 倍と増加する。

ところで、ある一つの素数に対する剰余類を考えたときは、探索回数が増大するが、複数の素数 p_1、p_2、…p_n に対して、それぞれの剰余類を考えてみてはどうだろうか。各剰余類で探索を行うと、それぞれの底点が求まる。しかし上記の議論から、底点は素数



(i) 全整数からなる格子点　(ii) 剰余類からなる格子点

図7　剰余類の考慮

p_iの値に依存して、異なる間隔で存在する。合成数の因数であれば、いかなる剰余類に対しても、底点の位置が一致しなければならない。従って、共通的な底点のみが、因数の候補となり得る。様々な剰余類を考えることで、因数の表現形式も増大するが、もし共通的な底点が長い間隔で生じるようであれば、効率のよい探索ができる可能性がある。

4－2　単一剰余類での探索

（1）考え方

因数が合成数のときは、その因数に対して同じアルゴリズムを繰り返す。ここでは説明の都合上、その概略を再掲する。

いまNのpに関する剰余をrとする。

$$N=r \mod p \quad r \neq 0 \qquad (25)$$

このときNは整変数a, bに関する1次式の積で表現できる。

$$N=(pa+c)(pb+d) \qquad (26)$$

ここでc、dは

$$cd=r \mod p \qquad (27)$$

を満たす整数である。なお、以下ではpa+cの整数の集合、すなわち剰余類を {c} で表す。cは代表元、pは法（mod数）である。また、'modpでは'という表現を用いるが、これはNを (26) 式のように剰余類の数の積と考えることを意味する。

pが素数なので、(26) 式の表現はp-1通りある。ここで剰余類の組合せを一つ選択して、その剰余類に属する整数を座標値とする点をxy平面上にプロットすると、それらは格子点状に分布する。

Nの因数を求めるには、格子点の描かれたxy平面に、双曲線xy=Nを描き、その曲線上にある格子点を探す。剰余類の選択が正しければ、格子点は曲線上に必ず存在する。このとき次の2つの問題が生じる。

(ｱ) 剰余類の正しい選択とは何か。またそのような選択が (25) 式の関係のみから行なえるか。

(ｲ) 双曲線上にある格子点をいかに早く探索するか。

まず（ｱ）の問題を考える。合成数Nがf個の異なる素因数N_1、N_2、N_fの積とすると、Nを2個の因数の積に分解する方法は多数（2^f-2通り）存在する。各分解方式に対して剰余類の組合せが定まり、それらの組合せの全体が正しい剰余類である。特にRSA暗号のように2個の素数の積である場合、(26) 式の剰余類の表現は一意的である。本報告に述べるアルゴリズムでも、簡単のための剰余類の表現が一意的なことを前提とする。このような正しい剰余類の表現（c、dの値）が事前に判定できれば、他の剰余類での不必要な探索をしないで済む。そこでこの判定が本報告の主要な課題となっている。なお、合成数Nが複数の素数の積である場合、Nが2つの合成数の積であると見做せば、本報告のアルゴリズムがそのまま適用できる。但し得られる結果は合成数なので、素数が得られるまで繰り返しアルゴリズムを適用する。

次に（ｲ）の問題を考える。図8はxy平面上に双曲線と格子点を描いたものである。双曲線の近傍には、合成数の因数候補となる格子点の列が存在する。この格子点列（直線）と双曲線の交点が格子点ならば、それが因数である。また交点が格子点でないならば、直線上の次の格子点（底点）を求める。次に、y軸方向にシフトした格子点（先頭点）を初

期値として、次の交点を求める。以上のアルゴリズムで、合成数が大きな整数のとき、双曲線は局所的に直線状である。双曲線（局所的には直線）の傾きが格子点列の傾きにほぼ等しければ、底点の生じる間隔が長くなる。これが直観的な格子点探索の原理である。

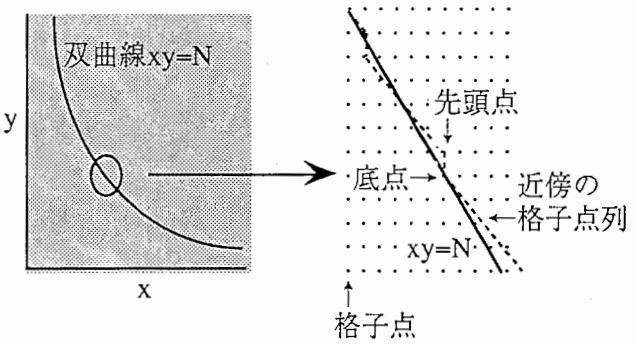


図８　格子点探索の原理

ところで底点から次の先頭点を求めるときのｙ軸方向のシフト量は格子点の間隔に等しい。上記のアルゴリズムのように剰余類を考えると格子点の間隔は素数の値である。従って大きな素数を選べばシフト量も大きく、底点間隔が拡大する。

（２）近傍格子点

合成数をN、素数をｐとする。(25)、(26) 式より剰余類の組合せを一つ選択する。格子点探索法では双曲線xy=Nの近傍にある格子点（n、m）にのみ着目する。すなわち座標n、mは

$$nm=N+\varepsilon_1 > N$$
$$n\ (m-p) < N \qquad (28)$$
$$n < m$$

を満たす整数とする。(28) 式よりε_1は

$$\varepsilon_1 < np \qquad (29)$$

を満たす整数である。

いま、近傍格子点（n、m）に隣接する近傍格子点を (n-p, m+p β) とする。ここでβは整数であって、(28) 式の定義から

$$(n-p)\ (m+p\beta) = N+\varepsilon_2 > N \qquad (30)$$
$$(n-p)\ (m+p\beta-p) < N$$

を満たさねばならない。(30) 式よりε_2は

$$\varepsilon_2 < np-p^2 \qquad (31)$$

を満たす整数である。

さて (28)、(30) 式からβは

$$\beta = \frac{\varepsilon_2-\varepsilon_1+pm}{np-p^2} \qquad (32)$$

と表現できる。(29)、(31)、(32) 式より

$$\frac{m-n}{n-p} < \beta < \frac{m+n-p}{n-p} \qquad (33)$$

が言える。

いま合成数Nが１０^{200}程度と大きい数であるとして、かつ

$$n, m >> p \qquad (34)$$

が成り立つものとする。このとき、(31) 式は

$$\frac{m}{n}-1<\beta<\frac{m}{n}+1$$

すなわち

$$\beta=\left\lfloor\frac{m}{n}\right\rfloor \quad (m/n\text{を越えない整数}) \qquad (35)$$

または

$$\beta=\left\lfloor\frac{m}{n}\right\rfloor+1 \qquad (36)$$

である。

(30)、(35)、(36) 式は近傍格子点の列が直線をなすことを意味する。このうち (35) 式は順方向探索 (x軸で負方向に探索) に対応する。また (36) 式では逆方向探索 (x軸で正方向に探索) に対応する。

ところで (34) 式のn、mの具体的な値が問題である。例えば$N=10^{200}$、p=3とすると

$$n=10^{67},\quad m=10^{133} \qquad (37)$$

程度までならば、(35)、(36) 式を満たす。すなわち

$$\frac{m}{n-p}=\frac{10^{133}}{10^{67}-3}\simeq 10^{66}=\beta$$

と (33) 式から、(35)、(36) 式が言える。nが10^{66}以下の場合、βを (32) 式で計算する必要がある。但し、このような場合は全探索区間、$N^{1/2}=10^{100}$の$1/10^{34}$を占めるに過ぎない。そこで以下ではnが大きい ((34) 式が成り立つ) ものとして議論を進める。またβとしては (35) 式を考える。

(3) 底点の位置とその間隔

格子点探索法の底点は、図7に示したように双曲線xy=Nの近傍の格子点を結ぶ直線上にあって、双曲線との交点と隣接する格子点である。本節ではこの底点を計算により求める。

まず探索の初期格子点 (先頭点) を求める。先頭点 (n、m) は双曲線の近傍格子点の中で、座標比m／nが整数に近いものを選ぶ。具体的には整数βに対して

$$m_0=\beta n_0 \qquad (38)$$

$$m_0 n_0=N$$

を満たす実数n_0、m_0を考えると、

$$n_0-p\leqq n\leqq n_0 \qquad (39)$$

からnを求める。また、(28)、(39) 式から

$$m_0\leqq m\leqq m_0+(\beta+1)p \qquad (40)$$

によりmを求める。このときmとβnの誤差は

$$m-\beta n\leqq m_0+(\beta+1)p-\beta(n_0-p)$$

表１　$p\iota+m-\beta n$の概算値

n	m	β	ι	p1+m-βn の最大値(ｵｰﾀﾞｰ)	p1+m-βn の支配項
$N^{1/2}$	$N^{1/2}$	1	0	p	m-βn
$N^{1/2}$	$N^{1/2}$	1	1	p	m-βn
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	1	$N^{1/8}$	$pN^{1/8}$	$p\iota$
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	1	$N^{3/8}$	$pN^{3/8}$	$p\iota$
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	1	$N^{1/2}$	$pN^{1/2}$	$p\iota$
$N^{1/2}$	$N^{1/2}$	2	0	p	m-βn
$N^{1/2}$	$N^{1/2}$	2	1	p	m-βn
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	2	$N^{1/8}$	$pN^{1/8}$	$p\iota$
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	2	$N^{3/8}$	$pN^{3/8}$	$p\iota$
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	2	$N^{1/2}$	$pN^{1/2}$	$p\iota$
:	:				
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	0	$pN^{1/4}$	m-βn
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	1	$pN^{1/4}$	m-βn
⋮	⋮	⋮			⋮
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	$N^{1/8}$	$pN^{1/4}$	m-βn
⋮	⋮	⋮			⋮
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	$N^{3/8}$	$pN^{1/4}$	m-βn
:	:				

表２　$4\beta(np\iota+nm-N)$の概算値

n	m	β	ι	4β(npι+nm-N) の最大値(ｵｰﾀﾞｰ)	4β(npι+nm-N) の支配項
$N^{1/2}$	$N^{1/2}$	1	0	$pN^{1/2}$	npι, nm-N
$N^{1/2}$	$N^{1/2}$	1	1	$pN^{1/2}$	npι, nm-N
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	1	$N^{1/8}$	$pN^{5/8}$	npι
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	1	$N^{3/8}$	$pN^{7/8}$	npι
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	1	$N^{1/2}$	pN	npι
$N^{1/2}$	$N^{1/2}$	2	0	$pN^{1/2}$	npι, nm-N
$N^{1/2}$	$N^{1/2}$	2	1	$pN^{1/2}$	npι, nm-N
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	2	$N^{1/8}$	$pN^{5/8}$	npι
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	2	$N^{3/8}$	$pN^{7/8}$	npι
⋮	⋮	⋮			⋮
$N^{1/2}$	$N^{1/2}$	2	$N^{1/2}$	pN	npι
:	:				
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	0	$pN^{7/8}$	nm-N
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	1	$pN^{7/8}$	nm-N
⋮	⋮	⋮			⋮
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	$N^{1/8}$	$pN^{7/8}$	nm-N
⋮	⋮	⋮			⋮
$N^{3/8}$	$N^{5/8}$	$N^{1/4}$	$N^{3/8}$	pN	npι
:	:				

$$= p+2\beta p \qquad (41)$$

である。

先頭点から底点を求めるには、(30)、(35) 式から

$$(n-pk_1)(m+p\beta k_1+p\iota)=N \qquad (42)$$

を解く。ここでι=0、1、2、…は底点から次の先頭点を求めるときに行う、y軸方向のシフトの回数である。

(18) 式をk_1について解くと、

$$k_1=\frac{-(pi+m-bn)}{2pb}+\frac{\sqrt{(pi+m-bn)^2+4b(npi+nm-N)}}{2pb} \qquad (43)$$

となる。このときn—pk　が、探索の初期値から数えてι＋１番目の交点のx座標である。底点は交点の近傍にあるので、ι＋１番目の底点のｘ座標も、ほぼn—pkである。また、x座標上で底点の生起間隔Ｉは、ほぼ

$$I_B=p\ (k_{1+1}-k1) \qquad (44)$$

である。

(43) 式で

$$(p\iota+m-\beta n)^2 >> 4\beta\ (np\iota+nm-N) \qquad (45)$$

のとき、$k_1 \fallingdotseq 0$、すなわち$I_B \fallingdotseq 0$となって全数探索が必要となる。格子点探索はこれ以外の場合に有効である。

表１、表２はβが (35) 式で与えられるような探索区間 ($n=N^{1/2}\sim N^{1/3}$) で、(43) 式の各項を概算評価したものである。ここで表１の$p\iota+m-\beta n$の評価では、初期条件 (28) 式、並びに (39) (40) 式が得られる。

$$0 < nm-N \leqq (\beta+1)\, pn_0 \qquad (46)$$

の関係を用いた。

これらの表から、探索区間には次の傾向が見られる。

(i) $n \fallingdotseq N^{1/2}$ のとき

座標比 m/n が整数に近い先頭点から探索を始めて、ι が小さい間（例えば $0 \leqq \iota \leqq N^{3/8}$）は、(43) 式の支配項は

$$4\beta\,(np\,\iota+nm-N) \fallingdotseq 4\beta\, np\,\iota \qquad (47)$$

である。従って

$$l_B=\frac{p\sqrt{4\beta np}\left(\sqrt{\iota+1}-\sqrt{\iota}\right)}{2p\beta}$$

$$=\sqrt{pn/\beta}\left(\sqrt{\iota+1}-\sqrt{\iota}\right)$$

$$\simeq\sqrt{p/\beta}\bullet N^{1/4}\bullet\iota^{-1/2} \qquad (48)$$

$$\geqq N^{1/16}$$

である。(48) 式より探索間隔は当初、$N^{1/4}$ で以降、徐々に短くなり、$N^{3/8}$ 個程度の底点を探索した段階では間隔が $N^{1/16}$ ほどになる。

ところで、探索区間 $n=N^{1/2} \sim 0$ で、$\beta = 1$ の区間は

$$N^{1/2} \geqq n \geqq \frac{N^{1/2}}{\sqrt{2}} \qquad (49)$$

である。このうち (47) 式が成り立つのは、最小

$$N^{1/2} \geqq n \geqq N^{1/2}-N^{3/8}\ N^{1/16}$$

$$=N^{1/2}-N^{7/16} \qquad (50)$$

の区間である。

ι が大きくなると ($N^{3/8} \leqq \iota$)、(43) 式の支配項は $p\,\iota + m - \beta\, n$ である。いま探索中の格子点を先頭点と見做して、先頭点の座標を改めて (n, m) とおく。このとき、底点までの間隔は (43) 式で $\iota = 0$ として、$m - \beta\, n$ が支配項であることを考慮すると、$k \fallingdotseq 0$ となる。すなわち、底点の探索が進むにつれて、やがて全数探索が必要となる。

(ii) $N^{1/3} \leqq n \leqq N^{1/2}$ のとき

先頭点の座標を (n, m) とおく。このとき底点までの間隔は、(43) 式で $\iota = 0$ として β (nm-N) が支配項であることを考慮すると、(46) 式から

$$l_B=\frac{p\sqrt{4\beta(nm-N)}}{2p\beta} \leqq \sqrt{pn} \qquad (51)$$

である。例えば $n=N^{3/8}$ では、$N^{3/16}$ の底点間隔である。また、n の減少とともに、探索間隔は短くなる。

これまでの解析で、単一剰余類での探索は次のように要約できる。

(ア) 因数の候補が $n \fallingdotseq N^{1/2}$ (N が１０^{200}ならば１００桁程度の数) で、かつ m／n 比が整

数に近いときは、探索間隔が$N^{1/4}$～$N^{1/16}$である。
(ｲ) それ以外では、探索間隔は$N^{1/4}$より小さく、最小では１、すなわち全数探索となる。
(ｳ) 探索間隔を表す (48)、(51) 式には、素数pが含まれており、この場合でも剰余類を考えることで、探索間隔が拡大する。

このうち、(ｱ) でm／n比が整数に近いときという制約は、仮想格子点の導入により緩和される。この結果、探索間隔をnの関数として描くと、多峰性のグラフとなる。いずれにせよ、全探索区間$N^{1/2}$を$N^{1/4}$回以上探索する必要がある。次節からは、格子点探索を一層、高速化するための技法を論じる。

４－３　複数剰余類での探索

（１）共通底点

合成数Nは剰余類 $\{c\}_p$の整数と、剰余類 $\{d\}_p$の整数の積で表される。このとき剰余類の選び方には$p-1$通りあることを４－１に述べた。いま２つの素数p_1、p_2を選び、Nの$\mathrm{mod}p_1$での表現を一つ、また$\mathrm{mod}p_2$での表現を一つ選んだとする。

それぞれの因数表現で格子点探索を行うと、底点の列

(n_{1j}, m_{1j})　　j=1, 2, …

(n_{2j}, m_{2j})

が得られる。これらの底点の中で、近傍にある２つの底点を$\mathrm{mod}p_1$と$\mathrm{mod}p_2$の共通底点と呼ぶことにする。すなわち、小さな整数εに対して

$$|n_{1j}-n_{2j}|<\varepsilon \qquad (52)$$
$$|m_{1j}-m_{2j}|<\varepsilon$$

が満たされるとき、共通底点である。

具体的なεの選び方や、共通底点の生起頻度は、底点の生起間隔に係わっているので、４－２と同様に各場合について以下に検討する。

(i) $n \lesssim N^{1/2}$のとき

最初の先頭点 (n, m) から数えて$\iota+1$番目の交点を与えるnの値は、ιが小さい間（$0 \leqq \iota \leqq N^{3/8}$のとき）は、(43)、(47) 式から

$$n-pk=n-\sqrt{\frac{np\iota}{\beta}} \qquad (53)$$

である。

いま (52) 式のように共通底点が与えられているとする。さらに

$$\iota_1=p_2L \qquad L=0, 1, 2, \cdots$$
$$\iota_2=p_1L \qquad (54)$$

として、$\mathrm{mod}p_1$でι_1+1番目の交点と、$\mathrm{mod}p_2$でι_2+1番目の交点を考える。このとき

$$\sqrt{\frac{np_1\ \iota_1}{\beta}}=\sqrt{\frac{np_2\ \iota_2}{\beta}} \qquad (55)$$

が成り立つ。すなわち各交点の近傍に次の共通底点がある。

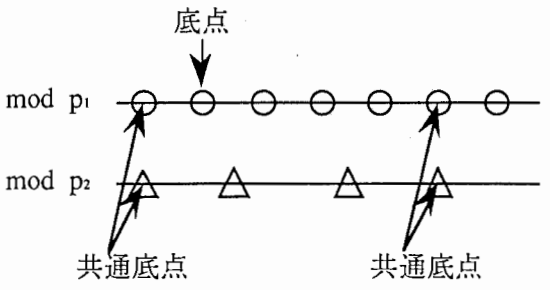


図９　共通底点（$p_1=3, p_2=5$）

共通底点は図９に示すように、ιの更新数に関して周期的に存在する。その周期は剰余類の法p_1、あるいはp_2である。

正確にはmodp_1のp_2個の底点間隔と、modp_2のp_1個の底点間隔がほぼ等しい。これらの周期の中に、底点の位置が最も近いものを共通底点と呼ぶのである。

〔例１〕　自明な例であるが、Ｎ＝１０^{200}をｎ＝１０^{100}から探索したときの底点の一部を図１０に示す。但し、mod1（全整数探索）ではN=ab、mod3（剰余類探索）ではN=(3a+1)　(3b+1)の両タイプについて格子点探索を行った。

mod1のときは、各kの値が底点間隔である。ι_1+1 (=t) 番目の底点のx座標は

$$10^{100}-\sum_{t=1}^{t2} k \qquad (56)$$

で与えられる。例えば３番目の底点のx座標は

$$10^{100}-1.73205\cdots\times 10^{50} \qquad (57)$$

である。

t = 1
k = 0000000000000000000000000000000000000000000000000
t = 2
k = 4142135623730950488016887242096990785696718753769 4
t = 3
k = 3178372451957822447257576172961742883731333784334 3
t = 4
k = 2679491924311227064725536584941276330571947461896 2
t = 5
k = 2360679774997896964091736687312762354406183596115 2
t = 6
k = 2134217652833884017881104059746151565253291210451 4
t = 7
k = 1962615682814124923043316789336903374431170242577
t = 8
k = 1826758136815995071017616947801357314290845676714 4
t = 9
k = 1715728752538099023966225515806038428606562492461 0
t = 10
k = 1622776601683793319988935444327185337195551393252 1

(1) N=ab

t = 1
k = 5773502691896257645091487805019574556476017512701 3
t = 2
k = 2391463117381002682232792444000063416743807422820 9
t = 3
k = 1935034190722739672675719750980362026780175064177 7
t = 4
k = 1547005383792515290182975610039149112952035025402 5
t = 5
k = 1362939103565540993747909055902182923157703992236 0
t = 6
k = 1232191136372894204086002576155648749586979736130 8
t = 7
k = 1133116692788516200609936736996380844251469835457 1
t = 8
k = 1054679302035053966021736518945914316491461281817 8
t = 9
k = 990576457134252280625902917019447722988402667059 3
t = 10
k = 936910507816764179957862678301347462330103961828 9

(2) N=(3a+1) (3b+1)

ｔ：本文中のι＋１（何番目の底点かを示す）
ｋ：t番目の先頭点（ｎ，ｍ）から底点までの格子数ｋ，(19)式

図１０　N=１０^{200}の因数探索

mod3のときは、3kの値が底点間隔である。ι_2+1 (=t) 番目の底点のx座標は

$$10^{100}-\sum_{t=1}^{t2} k \qquad (58)$$

で与えられる。例えば１番目の底点のx座標は

$$10^{100}-1.73205\cdots\times 10^{50} \qquad (59)$$

である。

(57)、(59) 式の例から分かるように、mod1の３番目毎の底点と、mod3の各底点の位置が等しく、これらは共通底点となっている。□

一方、n$\simeq$N$^{1/2}$でιが大きくなると（ι＞N$^{3/8}$)、探索間隔は徐々に減少して、やがて全数探索になる。このとき、底点の間隔は剰余類の法に等しい。この場合も、modp_1のp_2毎の底点、並びにmodp_2のp_1毎の底点がそれぞれ共通底点となる。

なお、全数探索にまでは到らない過渡的な段階（ιがN$^{3/8}$程度）での底点の位置についても、同様の共通底点があると予想している。これは (43) 式の評価で、ιの大小により支配項が変わるものの、いずれも共通底点の生起間隔が同一なことがその根拠である。

(ii) $N^{1/3} < n < N^{1/2}$ のとき

探索中のnの値が小さくなると、表1、表2に示したように、(43) 式で

$$k \fallingdotseq \frac{\sqrt{4\beta(np_\iota+nm-N)}}{2p\beta} \qquad (60)$$

が成り立つ。(50) 式でn、mは最初の先頭点の座標に対応した定数である。このときβも定数となり、ιのみが変数となる。従って$\iota+1$番目の底点を与える式n-pkに対して、(54)、(55) 式と同様の関係が成り立ち、共通底点が存在する。この場合も、$modp_1$のp_2毎の底点並びに$modp_2$のp_1毎の底点がそれぞれ共通底点となる。

（2）共通因子

格子点探索法は図8に示したように、双曲線xy=Nの近傍格子点に着目する。modpの剰余類を考えるときは、(26) 式により、格子点の座標は剰余類 $\{c\}_p$、$\{d\}_p$に属する整数である。複数の剰余類について各々、近傍格子点を求めたとき、格子点の座標が一致する場合があり、このような近傍格子点を共通因子と呼ぶことにする。具体例に基づきながら、共通因子の求め方を以下に示す。

〔例2〕 N=1315753 (=409 x 3217) とする。

(i) 剰余類の選択。

N=1 mod3 から N= (3a+1) (3b+1)

N=3 mod5 から N= (5a+1) (5b+3) (61)

を仮定する。

(ii) (4) 式を満たす先頭点（n、m）を求める。

$n \fallingdotseq N^{1/2}$（$\beta=1$）で、

mod3では（1147、1150）

mod5では（1146、1153）

が先頭点である。

(iii) mod3、mod5の近傍格子点で、x座標の値nが一致する箇所を求める。この例では

mod3では（1141、1156）

mod5では（1141、1158）

である。

(iv) mod3、mod5で近傍格子点（n、m）の座標は (42) 式で与えられる。これらが一致するとき、次式が満たされる。

$$n = 1141 - 3 \cdot 5k$$
$$m = 1156 + 3 \cdot 5k + 3\iota_3 \qquad (62)$$
$$= 1158 + 5 \cdot 3k + 5\iota_5$$

但し、ι_3、ι_5はそれぞれmod3、mod5で何番目の底点かを示す。

(62) 式を解くと、

mod 3				mod 5		
n	m	ι		n	m	ι
1147	1150	0	←先頭点	1146	1153	0
⋮				⋮		
1090	1207	0	←底点			
1090	1210	1				
				1071	1228	0
1066	1234	1		1071	1233	1
1066	1237	2				
1048	1255	2				
1048	1258	3		1041	1263	1
				1041	1268	2
1036	1270	3				
1036	1273	4		1036	1273	2
			共通因子			
1021	1288	4		1021	1288	2

図11 2組の剰余類の近傍格子点

$\iota_3=4+5L$ (63)

$\iota_5=2+3L$

である。(62)、(63) 式から、(61) 式の剰余類を選択したときの共通因子 (n_e、m_e) は

$n_e=11411-15k$

$m_e=11681+15k+15L$ (64)

で与えられる。

因みに mod3、mod5 の近傍格子点を図11に列挙する。□

いま、先頭点から底点まで ι が一定の区間を探索ブロックと呼ぶことにする。$modp_1$、$modp_2$ を考えたとき、共通因子は図11のように、特定の探索ブロック内で、周期的に生じる。一般にどの探索ブロックで共通因子が生じるかを論じることは、剰余類の選び方に依存するので難しいが、次のような説明はできる。

まず素数 p_1 として、$modp_1$ での剰余類 $\{r_1\}_{p1}$ を考える。但し、$\{r_1\}$ は

$z=r_1 \quad modp_1$ (65)

となるような整数 z の集合である。次に、素数 p_2 を $p_1<p_2$ のように選ぶ。そして (65) 式を満たす z を順に p_2 個列挙する。例えば

$$\begin{aligned} z_1&=r_1 \\ z_2&=r_1+p_1 \\ &\vdots \\ z_{p2}&=r_1+(p_2-1)\,p_1 \end{aligned} \qquad (66)$$

とする。このとき、(65) 式の z_i は完全剰余系となす。すなわち $modp_2$ の全ての剰余類、

$\{r_i\}_{p2} \quad i=1,\cdots,p_2$

を生成できる。

さて、いままでに述べた格子点探索法が、どのような剰余類を選択しているのか、以下に考察する。合成数 N の剰余類表現として

$N=\{c_1\}_{p1}\times\{d_1\}_{p1}$ (67)

$N=\{c_2\}_{p2}\times\{d_2\}_{p2}$ (68)

を選んだとする。

(i) 探索ブロック内

$modp_1$ で近傍格子点

$(n_1,m_1)\rightarrow(n_2,m_2)\rightarrow\cdots$

を探索するとき、(67) 式を満たし、かつ

$n_k=n_1-p_1k$ (69)

$m_k=m_1+p_1\,\beta\,k$

となっている。座標値 n_k は (66) 式のように生成され、p_2 回の探索毎に、(68) 式の剰余類 $\{c_2\}_{p2}$ の整数になる。一方、座標値 m_k は

① $\beta\neq p_2$ の倍数のときは、P_2 回の探索毎に (68) 式の剰余類 $\{d_2\}_{p2}$ の整数になる。このとき、n_k も (44) 式を満たせば共通因子である。

② $\beta=p_2$ の倍数のとき、m_k は $modp_2$ でつねに同一の剰余類に属する。従って、つねに (68) 式の剰余類 $\{d_2\}_{p2}$ の整数であるか、またつねに (68) 式を満たさないかのいずれかである。

(ii)　探索ブロック間

$modp_1$ における近傍格子点は、底点から先頭点を求めるときのy軸方向のシフトまで考慮すると

$$n_k=n_1-p_1k \qquad (70)$$

$$m_k=m_1-p_1\ \beta\ k+p_1\ \iota$$

である。(69) 式と比較して、追加される $p_1\ \iota$ は (66) 式のように $modp_2$ での完全剰余系を生成する。従って、p_2 回のy軸方向のシフト（p_2 番目の探索ブロック）毎に、$\{d_2\}_{p2}$ の整数が出現する。

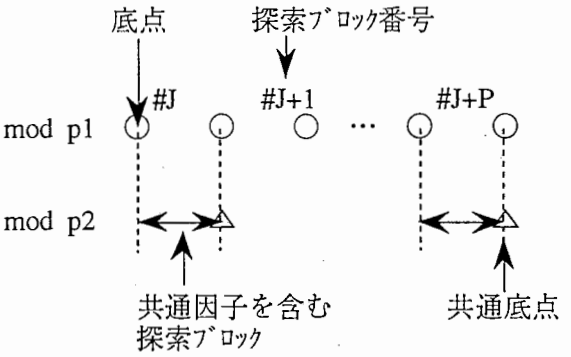


図１２　共通底点と共通ブロックの関係

（３）因数の探索

整数n、mが合成数Nの因数ならば、いかなる剰余類においても、(n、m) は共通底点、かつ共通因子である。逆に、合成数Nから剰余類表現を (67)、(68) 式のように選んだとき、その共通底点と共通因子が同一の探索ブロック内にあれば、その剰余類表現はおそらく正しい。

図１２に示すように、$modp_1$ の第Jブロックに $modp_2$ との共通因子があるとき、3.2の議論から、第J＋p_2 ブロックにも共通因子がある。一方、共通底点も p_2 ブロック毎にある。従って、共通因子と共通底点がつねに同一ブロックにある（同期状態とよぶ）か、ブロックが一致しない（非同期状態とよぶ）かのいずれかである。

以上の結果から、合成数Nから因数の剰余類表現を選んだとき、試行的に共通因子と共通底点を求め、それらの同期状態を判定して、その剰余類表現が正しいかどうかが判断できると考えられる。もし剰余類が一意的に選択できるならば、多数の素数、p_1、p_2、… p_H につついて、剰余類を考え、以上のアルゴリズムを適用することができる。格子点間隔が $p_1p_2\cdots p_H$ のとき、探索間隔は (68) 式から、全整数格子点の場合の $(p_1p_2\cdots p_H)^{1/2}$ 倍になるので、その効果は大きい。

５．まとめ

素因数をxy平面上の解曲線 xy=N と、その近傍の整数値をとる格子点列（直線）との交点から求める、という素因数分解の手法を提案した。この手法では解曲線の傾き（局所的には直線と見なせる）と格子点列の傾きが等しいときには$N^{1/4}$のオーダの間隔で探索が進む。しかしこれ以外の場合は、探索間隔が短縮する。そこで座標値が非整数の仮想的な格子点を追加して２直線を平行にするという手法を考えた。

RSA暗号に用いられるような２００桁程度の合成数を考えると、$N^{1/4}$～10^{50} となり、この探索間隔は大きいが、総探索回数も 10^{50} 回となり、一層の高速化が望まれる。そこで合成数の素数に対する剰余から、因数の形式を限定する、という方法を提案した。一般にmodpで剰余類を考えると、探索間隔は$\sqrt{P}$倍に拡大する。格子点探索法は格子点の座標比が整数に近いとき、$N^{1/4}$ の探索間隔である。世界水準であるO（$N^{1/8}$）を実現するには、$N^{3/8}$ の探索間隔が必要である。一方、剰余類の表現はp-１通りもあり、正しい表現を選択できるかが、剰余類上での探索ポイントとなっていた。本報告では、合成数を異

なる法のもとで、格子点探索したとき、格子点の位置が重なる（共通因子）箇所で、双曲線に最も接近する（共通底点）か否かで、因数がどの剰余類に属するかを推定できることを示した。これにより、探索間隔を拡大できるが、その効果は素数の値に依存する。従って将来的には、多くの素数を考えたときに、どの剰余類でも底点（解曲線と格子点列からなる直線の交点）となるような箇所のみを探索する、という方法が有望である。