L-007

仮想格子点を考慮した素因数分解の検討

Study of the prime factorization considering the virtual grid point

赤堀 晋作† 永瀬 宏† 津田 伸生† 郭 清蓮†
Akahori Shinsaku Ngase Hiroshi Tsuda Nobuo Kaku Seiren

1. はじめに

インターネットで広く利用されている暗号に RSA 暗号鍵がある．RSA 暗号鍵とは 1970 年代に発明された．素因数分解の難しさを利用した公開鍵暗号方式の一つである．RSA 暗号鍵の安全性を高めるためには，桁数の大きい合成数をふたつの素数を分解するのにかかる時間が長いことが良い．

1990 年代に RSA 暗号鍵における合成数の素因数分解の方法として，格子点探索法が提案された．格子点探索法の探索の効率を高めることで，RSA 暗号鍵の安全性を高めることができる．

昨年度，最新の計算機で格子点探索法を用いて，RSA 暗号鍵の安全性と探索の効率化を高める実験を行った．しかし，双曲線 xy=N 上における探索直線の傾きが整数の形のみ適応されていた．探索の進行に伴い，探索間隔が減ってしまうという問題点があることがわかった．

そこで本研究では，平面上で非整数の座標値を持つ仮想格子点を用いることにより，探索直線の傾きが非整数の場合でも適応できるよう検討する．探索が広い範囲で，より高速に計算できるように改良する．

2. 格子点探索法

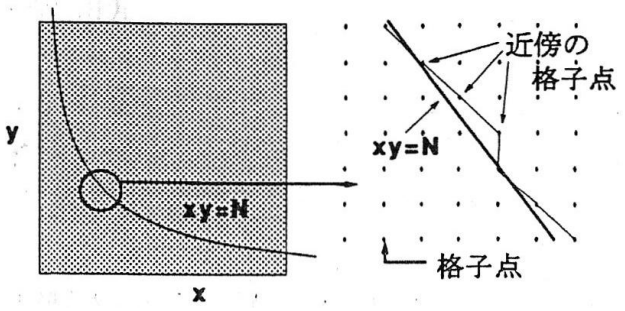

図 1 双曲線の近傍の格子点

xy 平面上で x，y 座標が整数であるような格子点は無数に存在する．格子点の中で双曲線 xy=N の最近傍にあ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．RSA 暗号の実用としては合成数 N の場合，例として 10 進数の 650 桁というような大きな合成数が用いられる．その合成数 N における双曲線 xy=N を拡大すると，ほぼ直線のように見える．近傍格子点列からなる直線と双曲線の傾きがほぼ平行のときには，直線と曲線は交差しにくく，交点も稀にしか存在しない．

格子点探索法とはこのような交点を取り出し，それが格子点上に存在すれば因数，位置しなければ非因数として素因数分解していく方法である．詳しい手順については参考文献[2]を参照．

† 金沢工業大学大学院 工学研究科
Kanazawa Institute of Technology

3. 仮想格子点

初期格子点(n,m)の座標値の傾き m/n が整数から離れている時，順探索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，探索間隔が長くすることができる．

例えば，傾きが 1.5 のとき、図 2 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．双曲線の近傍の格子点を結ぶと，この直線 Q は双曲線とほぼ平行になって探索間隔が長くなる．ただし，双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ため，整数か非整数かを調べる必要がある．

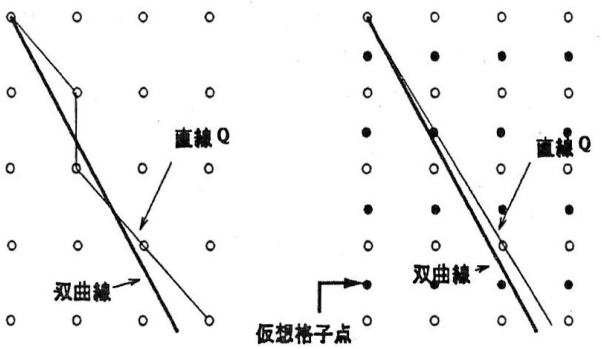

図 2 仮想格子点の考慮

仮想格子点探索の手順を次に示す．

① 探索の初期格子点の座標 n,m を次の式を満たすように選ぶ．

$nm > N$, $n(m - 1/s) < n$,

$R + t/s \leqq m/n < R + (t + 1) / s$ (1)

(R,s,t は整数)

② 初期格子点(n, m)を通り，傾き $\beta = (R + t/s)$とする直線 Q_2と，双曲線 xy=N の交点を求め，この交点から初期格子点までの探索間隔 k_0 を求める．

③ $x_1y_1 = N$ のとき，y_1が整数ならば x_1, y_1が因数である．y_1 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 $x_1y_1 < N$ のとき，$x_1(y_1 + v/s) \geqq N$ となる最小の整数 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，$(x_1, (y_1 + v/s))$を次の初期格子点として②に戻る．

4. 仮想格子点の存在領域

仮想格子は整数格子の間に，y 軸方向に複数個挿入する．その結果，非整数の直線 Q の傾きが実現可能となる．具体的には挿入個数と傾きの関係は，表 1 のようになる．

表 1　挿入個数と傾きの関係

挿入個数	傾き（非整数で-1 以下）
1	-3/2　-5/2　-7/2　…
2	-4/3　-5/3　-7/3　…
3	-5/4　-7/4　-9/4　…
…	……

例として直線 Q の傾きが非整数の-3/2 のときの x 座標軸の値を求めると，

$$xy=N \text{ より } \quad y'=\frac{-N}{x^2}=\frac{-3}{2} \text{ から } \quad x=\frac{\sqrt{2}\sqrt{N}}{\sqrt{3}}$$

$$y=\frac{\sqrt{3}\sqrt{N}}{\sqrt{2}} \qquad (2)$$

となる．すなわち，x が(2)式を満たすような値の近傍に位置するとき，仮想格子点を導入する効果が現れると予想される．他の非整数の傾きについても，同様である．

上記(2)式で初期格子点を選ぶ場合，x は整数，y は整数または小数部が 0.5 となる数である．ただし，xy≧N である必要がある．このような初期値(n, m)を選んだとき，双曲線の近傍の直線 Q は，

$$x=n-k \quad y=m+\frac{3}{2}k \qquad (3)$$

と表現できる．この直線 Q と双曲線 xy=N との交点は，

$$xy=N \qquad (4)$$

について，(3)(4)式を連立させて，求めることができる．その結果，

$$x=\frac{(m+\frac{3}{2}n)-\sqrt{(m+\frac{3}{2}n)^2-6N}}{3} \qquad (5)$$

が得られる．すなわち，x 軸上では初期値 n に対して，次の探索点は(5)式のように求まる．具体的な探索では，x,y の値は整数である必要がある．したがって，(5)式でもとまる交点が仮想格子点でなく，本来の整数格子点に合致したときが因数解となる．以上の原理に基づく探索プログラムを現在作成中であり，結果が得られ次第，別途報告したい．

5. 仮想格子を使わない場合の探索間隔

すでに 2 で述べているが，(2)式をほぼ満たすような x の値の付近では仮想格子を用いない順探索では，探索の様子が図 3 に示すようになる．合成数 N に対して，$N^{\frac{1}{2}}$から探索を開始する場合，探査曲線 Q の傾きは-1 である．したがって図 3 の場合，x 軸上での探索間隔は 2~3 とほぼ全数探索に近い状態まで探索スピードが劣化する．これに対して仮想格子を使った場合は，$N^{\frac{1}{2}}$付近での探索と同様，探索間隔は$N^{\frac{1}{4}}$程度を予想しているが，詳細は今後明らかにしていきたい．

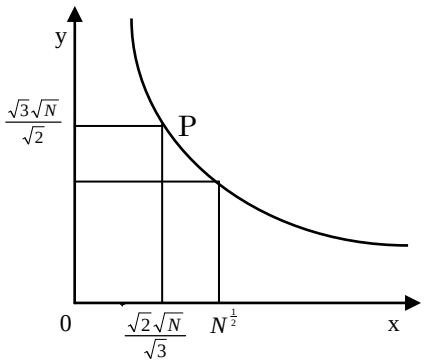

図 3　仮想格子を用いない順探索

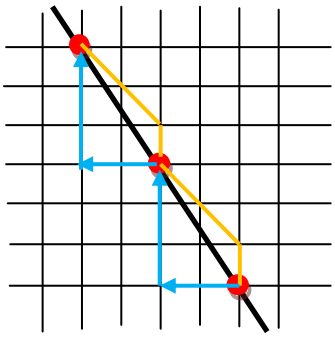

図 4　図 3 における P の拡大図

6. まとめと今後の展開

冒頭にも述べたように，格子点探索法はすでに 20 年以上前に提案されている．その間，仮想格子点ならびに剰余類探索の概念も提案されている．本学では昨年より，この研究を再開して多倍長計算に基づく基本格子探索法を実装し，さらに剰余類探索についても実装を行い，すでに報告済みである．今回，仮想格子点を使った探索についてそのアルゴリズムと高速化が予想される探索位置を明らかにした．今後はアルゴリズムの実装を進めると同時に，マルチプロセッサーでの計算にも対応していきたい．

謝辞

本研究を進めるにあたり，多倍長計算ならびに基本格子点探索法の昨年度までの成果を提供いただいた，和田拓也氏に深謝します．

参考文献

[1]永瀬宏，井上清一，高長早織，“準均一な探索間隔を有する格子点探索法”，信学技報，ISEC97-4 (1997-05).

[2]和田拓也，津田伸生，永瀬宏，“PC クラスタを用いた格子点探索法による RSA 暗号鍵の安全性評価”，情報処理学会，1ZA-3

-