RSA暗号計算 NO.2
多数桁因数分解の方法

2007年5月

後　保範　(東京工芸大学)

目次

1. 多数桁の因数分解の種類

(1) 古典的な因数分解
  (a) 試行割算法 (原始的手法)
  (b) ρ 法 (モンテカルロ法)
  (c) フェルマー法
  (d) 2次ふるい法(QS)
  (e) Pollardのρ-1法
(2) 最近の解法
  (a) MPQS(複数多項式2次ふるい法)
  (b) GNFS(一般数体ふるい法)
  (c) MBPS(多重基底多項式ふるい法)
  (d) ECM(楕円曲線法)

2. 試行割算法(原始的手法)

計算法 (nの因数分解)
(1) $n^{1/2}$より小さい素数で次々試行割算を実施する。

欠点: 演算量が$O(n^{1/2})$以上で遅い

2.1 試行割算法の例

n=8051の因数分解の例
(1) n mod(2) = 1,　n mod(3) = 2
　n mod(5) = 1,　n mod(7) = 1
　…..
　n mod(79) = 72,　n mod(83) = 0
(2) n = 83×97と因数分解

3. ρ 法 (モンテカルロ法)

計算法 (nの因数分解)
(1) 変換多項式 (例: $x_{k+1} = x_k^2 + 1 \bmod(n)$)
　及び 初期値(例: $x_0 = 2$)を選定
(2) x_kを変換式でk=1,2,3,…と計算
(3) $2^h \le k < 2^{h+1}$となるhで$j = 2^h - 1$とする
(4) p=GCD(x_k-x_j, n)で1以外なら素因数
(5) q=n/pでn=p×qと分解

3.1 ρ 法の例

n=8051の因数分解の例

(1) $x_{k+1} = x_k^2 + 1 \bmod(n)$, $x_0 = 1$ を選定

(2) $x_1=2$, $GCD(x_1-x_0,n) = 1$

$x_2=5$, $x_3=26$, $x_4=677$,

$x_5=7474$, $GCD(x_5-x_3,n) = 1$

$x_6=2839$, $GCD(x_6-x_3,n) = 97$

(3) $p=n/97=83$, $q=97$でn=p×qと因数分解

7

4. フェルマー法

計算法 (nの因数分解)

(1) $t = n^{1/2}$の整数部+1とする。

(2) $t^2 - n = s^2$(完全平方)となるまで、tを1ずつ増加させながら繰り返す。

(3) $p = t - s$, $q = t + s$でn=p×qと因数分解

pとqが近い値のとき強力な因数分解法

8

4.1 フェルマー法の例

n = 92296873の因数分解の例

(1) $t = n^{1/2} + 1 = 9607 + 1 = 9608$

(2) $9608^2 - n = 16791 = 129.58^2$

9609, 96010, 96011, 96012とテスト

$9613^2 - n = 112896 = 336^2$: 決定

(3) p=9613-336= 9277,

q=9613+336= 9949 でn=p×qと分解

9

5. 2次ふるい法(QS)

QSの基本的な考え方(合成数nの因数分解)

$X_1^2 - n = P_1^2 \cdot P_2^0 \cdot P_3^0 \cdot P_4^1$

$X_2^2 - n = P_1^0 \cdot P_2^1 \cdot P_3^3 \cdot P_4^1$

$X_3^2 - n = P_1^1 \cdot P_2^1 \cdot P_3^1 \cdot P_4^2$

$X_4^2 - n = P_1^1 \cdot P_2^0 \cdot P_3^2 \cdot P_4^0$

$\Longrightarrow (X_1X_2X_3X_4)^2 = (P_1^2P_2^1P_3^3P_4^2)^2 \bmod n$

$\Longrightarrow X^2 = P^2 \bmod n \Longrightarrow n = (X+P)\cdot(X-P)$

10

5.1 2次ふるい法の例(1/4)

- n=1042387を因数分解する

(1) P_kはnの平方剰余より8個の素数を選ぶ

$\{P_k\} = \{2, 3, 11, 17, 19, 23, 43, 47\}$

(2) $t^2 > n$ となる整数tより順に下記を行う

$1021^2 - 1042387 = 54 = 2 \cdot 3^3$

$1022^2 - 1042387 = 2097 = 3^2 \cdot 233$

$1023^2 - 1042387 = 4142 = 2 \cdot 19 \cdot 109$

11

5.1 2次ふるい法の例(2/4)

- $\{P_k\}$の積に分解されたもの

$1021^2 - n = 54 = 2^1 \cdot 3^3$

$1027^2 - n = 12342 = 2^1 \cdot 3^1 \cdot 11^2 \cdot 17^1$

$1030^2 - n = 18513 = 3^2 \cdot 11^2 \cdot 17^1$

$1061^2 - n = 83334 = 2^1 \cdot 3^1 \cdot 17^1 \cdot 19^1 \cdot 43^1$

$1112^2 - n = 194157 = 3^5 \cdot 17^1 \cdot 47^1$

$1129^2 - n = 232254 = 2^1 \cdot 3^3 \cdot 11^1 \cdot 17^1 \cdot 23^1$

$1148^2 - n = 275517 = 3^2 \cdot 11^3 \cdot 23^1$

$1175^2 - n = 338238 = 2^1 \cdot 3^2 \cdot 19^1 \cdot 23^1 \cdot 43^1$

$1217^2 - n = 438702 = 2^1 \cdot 3^1 \cdot 11^1 \cdot 17^2 \cdot 23^1$

$1390^2 - n = 889713 = 3^2 \cdot 11^2 \cdot 19^1 \cdot 43^1$

$1520^2 - n = 1268013 = 3^1 \cdot 17^1 \cdot 23^2 \cdot 47^1$

12

5.1 2次ふるい法の例(3/4)

- ベキが2を法として従属な行は1,2,3で
  $(1021 \cdot 1027 \cdot 1030)^2 = (2 \cdot 3^3 \cdot 11^2 \cdot 17^2)^2 \mod n$
  n= 1042387から
  $1021 \cdot 1027 \cdot 1030 = 1080024010 = 111078 \mod n$
  $2 \cdot 3^3 \cdot 11^2 \cdot 17^2 = 111078$
  従って
  $111078^2 = 111078^2$
  これは自明のため解ではない

13

5.1 2次ふるい法の例(4/4)

- ベキが2を法として従属な行は5,11で
  $(1112 \cdot 1520)^2 = (3^3 \cdot 17 \cdot 23 \cdot 47)^2 \mod n$
  n=1042387から
  $(1690240)^2 = (647853)^2 = (496179)^2 \mod n$
  従って
  $(647853+496179) \cdot (647853-496179) = 0 \mod n$
  $1144032 \cdot 151674 = 101645 \cdot 151674 = 5 \cdot 29 \cdot 701$
  $\cdot 2 \cdot 51 \cdot 1487 = 0 \mod n$, $701 \cdot 1487 = 1042387$

14

6. Pollardの ρ -1法の例

- n=540143を因数分解する。
  B=8とする。
  $k = B! = 8! = 1 \cdot 2 \cdot \ldots \cdot 8 = 840$
  $2^k = 2^{840} = 53047 \mod n$
  $GCD(53047-1, n) = 421$ $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$
  $n = 540143 = 421 \cdot 1283$
- ρ -1法の性質
  nの素因数pの総てに対してp-1が大きな素数だけしか持たないと効率が悪い。

15

6.1 Pollardの ρ -1法のベース

- n=p•qに素因数分解されるとする。
  任意の整数 α, β に対して下記が成立する。
  $\alpha^{\beta(p-1)} = 1 \mod p$
  即ち、適当な整数mで下記が成立する。
  $\alpha^{\beta(p-1)} = m \cdot p + 1 \mod n$
  従って、下記が成立する。
  $GCD(\alpha^{\beta(p-1)}-1, n) = GCD(m \cdot p, n) = p$

==> (p-1)が小さな整数の積だと効率が良い

16

7. 最近の素因数分解

(1) 複数多項式2次ふるい法
(MPQS : Multipolynomial Quadratic Sieve)
(2) 一般数体ふるい法
(GNFS : General Number Field Sieve)
(3) 多重基底多項式ふるい法
(MBPS : Multiple Base Polynomial Sieve)
(4) 楕円曲線法
(ECM : Elliptic Curve Method)

17

7.1 各方式の特色

因数分解の各方式の特色
(1) 合成数の桁数に依存: MPQS,GNFS,MBPS
素因数の桁数に依存: 楕円曲線法
(2) 合成数の10進桁数での優位性
MPQS:約100桁まで、GNFS:約100桁以上
現在の世界記録は200桁(GNFS)
MBPS:最近発見した解法、MPQS,GNFSより高速と思われるが検証はこれから
(3) 素因数桁が短いと楕円曲線法が優位
現在の世界記録は素因数66桁

18