計算量理論と公開鍵暗号と初等数論的な問題点

(熊本大学工学部数理工学科　角田法也)

- RSA暗号 -------- 素因数分解　>>　積

$$N = p \cdot q \qquad p \cdot q = N$$

NP　　P

- ElGamal暗号 ----- 離散対数問題 >> 累乗

$$y = g^x \bmod p \qquad g^x = y \bmod p$$

NP

$$3^{100} = 3^{2^6+2^5+2^2} = ((((3^2 \times 3)^2)^2)^2 \times 3)^2)^2$$

P

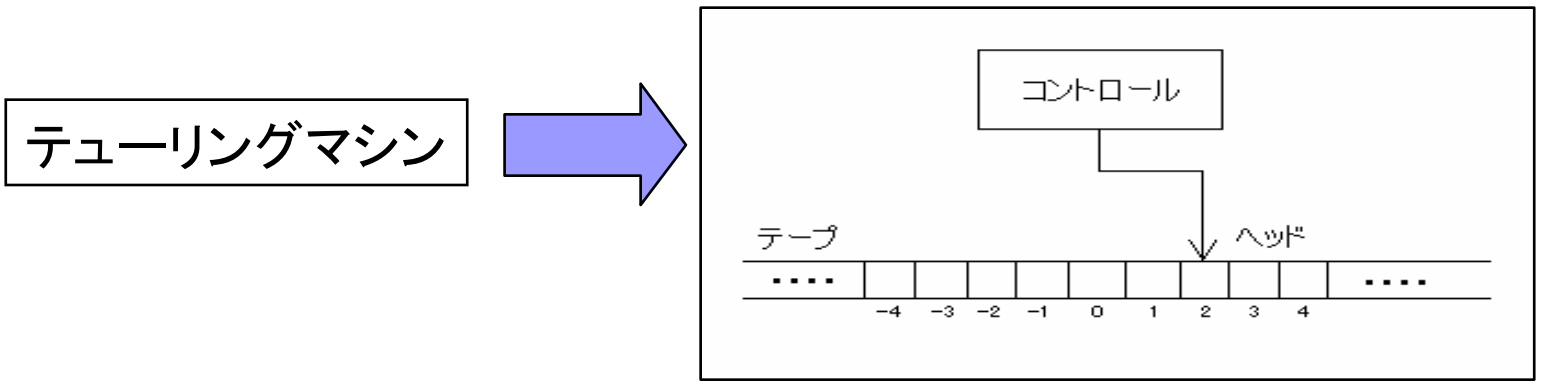
計算量の理論・クラスP

■計算プログラムを数学的に表現するため，テューリングマシンを用いる．（テューリングマシンは通常のコンピュータのモデル）．

■命令コマンドの実行ステップ数を「時間」と考えて，プログラムの時間複雑度は，同じ長さの入力のうち停止するまでの時間の最大値とする．（最悪計算量）

■プログラムが解く問題は，時間複雑度が「入力の長さ」の多項式でおさえられるとき，クラスPに属し多項式時間計算可能という．（Polynomial(多項式)のP)

■クラスPに属す問題はほとんど，高速に実行可能．



クラスNP・P=NP?問題

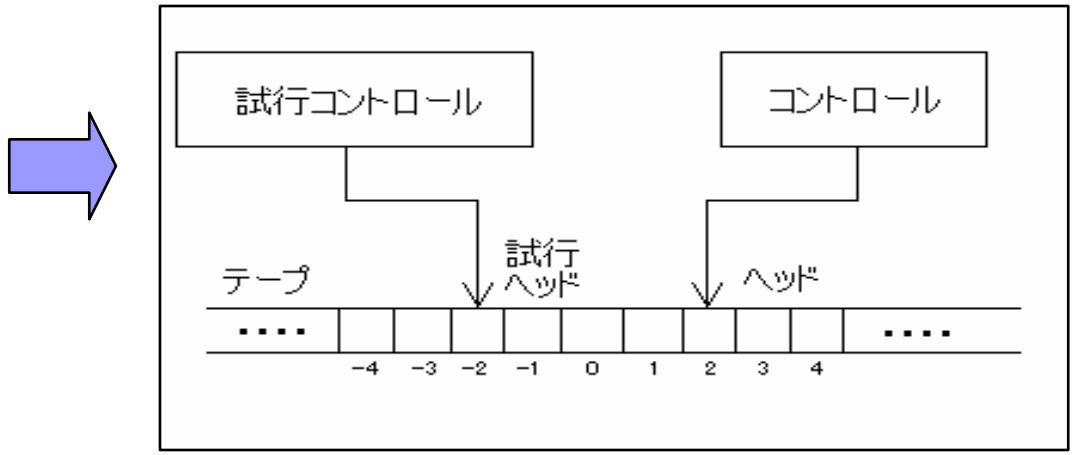
■非決定論的(Nondeterministicな)マシンは，テューリングマシンに試行コントロールと試行ヘッドが加わって，それらが任意に答を書いてのち，コントロールで確認計算をする．（答えを知っている人には早く計算ができるという意味）

■クラスNPとは，非決定論的マシンで多項式時間計算可能な問題の集合のこと

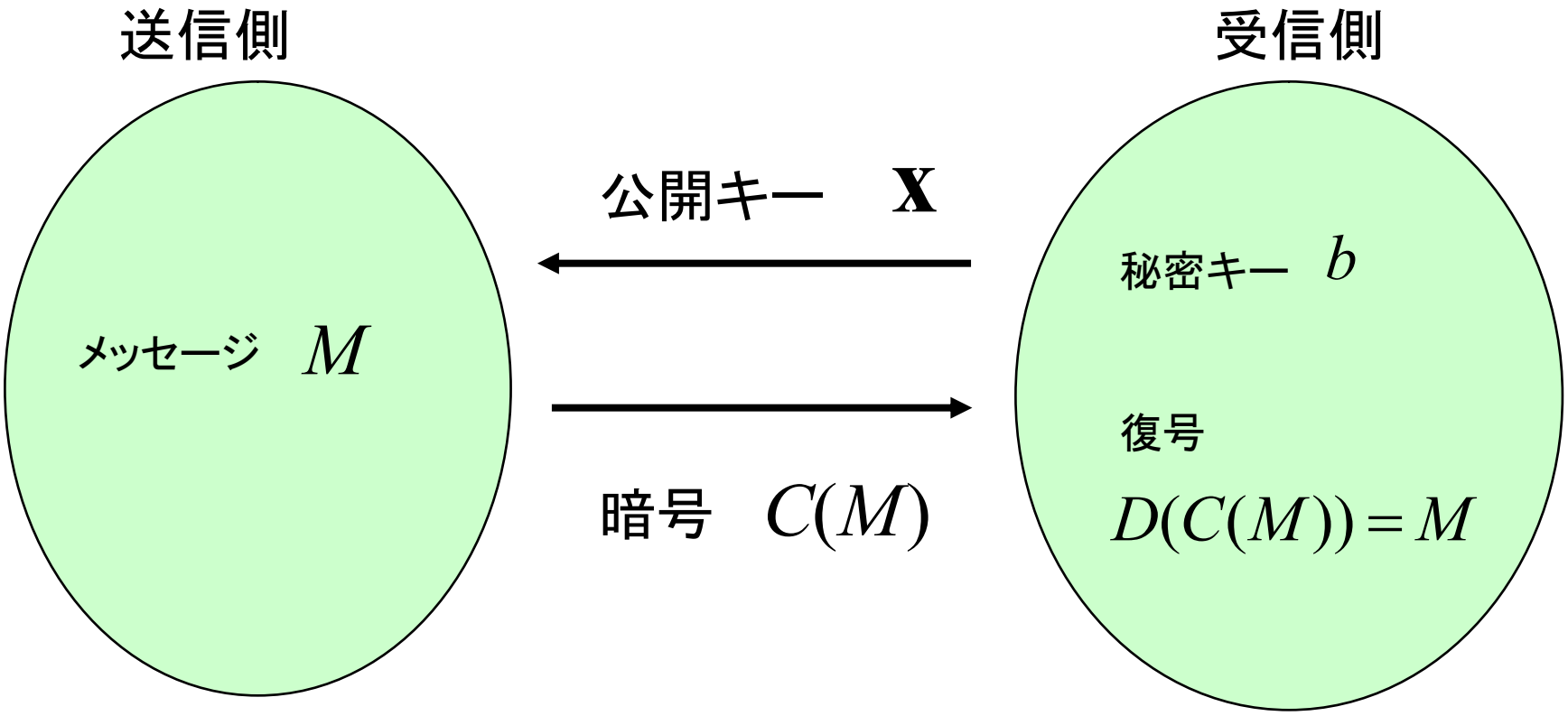
■例えば素因数分解は試行コントロールで素因数を書いて，チェックするのは多項式時間でできるのでNPに属すが，Pに属すかどうかは未解決．

■P=NP?問題は重要な未解決問題

非決定論的マシン



公開キー暗号



ポイント:

■通信の間に秘密キーを解読するのは計算量的に困難.

■ RSA　$N = p \cdot q (p \neq q$: 十進150桁くらいの素数)

(RSA modulus)

$$1 < e, d \in \mathbf{N}, e \cdot d = 1 (\mathrm{mod} \varphi(N) = (p-1)(q-1))$$

$\langle N, e \rangle$　公開キー

$\langle N, d \rangle$　秘密キー（受信側）

メッセージ:　$M \in (\mathbf{Z} / N\mathbf{Z})^*$

暗号化:　$C = M^e \mod N$

復号化:　$D(C) = C^d \mod N$

$$(= M^{ed} = M^{1 + k\varphi(N)} = M \mod N)$$

短い秘密キーの解読（連分数展開）

（定理）

$N = p \cdot q,\ q < p < 2q, d < \frac{1}{3} N^{\frac{1}{4}}, L = \varphi(N) = (p-1)(q-1),$

$ed = 1 \pmod{L}$ で与えられた $\langle N, e \rangle$ に対し、効率的に

d を復元できる。

$\exists k, ed - kL = 1,\ k < d < (1/3)\sqrt[4]{N}$ より

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{1-k(N-L)}{Nd}\right| \le \left|\frac{3k\sqrt{N}}{Nd}\right| \le \frac{1}{d\sqrt[4]{N}} < \frac{1}{3d^2} < \frac{1}{2d^2}$$

連分数近似により d を求めることができる。

連分数近似

$$\omega \in \mathrm{R},\quad \omega = k_0 + \frac{1}{\omega_1}\ (k_0 < \omega < k_0 + 1)$$

$$\omega = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \cdots \cfrac{1}{\omega_n}}}}$$

$$(k_m < \omega_m < k_m + 1)$$

$k_0 + \cfrac{1}{k_1 +}\ \cfrac{1}{k_2 +}\ \cfrac{1}{k_3 +}\cdots\cfrac{1}{\omega_n}$ で表すと $k_0 + \cfrac{1}{k_1 +}\ \cfrac{1}{k_2 +}\ \cfrac{1}{k_3 +}\cdots\cfrac{1}{k_{n-1}} = \cfrac{p_n}{q_n}$

ω の連分数近似

定理:

$$x \in \mathrm{R}: \qquad \left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$$

が成立すれば、p/q は x の連分数展開による 近似である。

```
> #------- RSA cryptosystem.  [ Attack of short secret key.]
p := 37989802934850283741982734609809809823745886554987234502934¥
       509809809810011892320457098702983712736 49 length(p)= 100
  q := 28948373770298375908109823740981237498001216782634987126401¥
       23649187263487987008172364287364198321571 length(q)= 100
> N:=p*q:L:=(p-1)*(q-1):d:=nextprime(16366279973659873264434274
89237458234872372837877);length(d);e:=d^(-1) mod L:
 d= 16366279973659873264434274892374582348723728379 99  length(d)= 49

> cf2:=cfrac(e/N,'quotients');
cf2=[0,4,1,6,5,2,5,1,2,1,8,6,1,1,121,4,2,5,2,1,2,6,1,8,2,2,2,5,2,2,3,2,3,6,1,2,1,2,12,1,41,
1,11,……,3,67,9,2, 1,2,2,4,1,1,3,1,109,1,7,2,25,4,3,9,3,2,105,5,4]
> nthconver(cf2,91);
d = 16366279973659873264434274892374582348723728379 99
> # Success!（発見に成功）
> ------------------------------
d1:=98989898439829384598349582849819347987129387493049
length(d)=50 ;e1:=d1^(-1) mod L:
> cf3:=cfrac(e1/N,'quotients');
cf3:=[0,2,3,2,3,1,3,92,1,1,2,57,2,2,1,10,1,2,1,4,1,4,1,3,1,2,11,1,5,19,2,1,1,1,1,7,1,1,1,3,
1,……,1,1,24,1,55,173,2,2,10,1,7,15,4,1,1,1,1,9,1,2,2,1,1,468,2]
> nthconver(cf3,99);length(nthdenom(cf3,99));
47206778532230854950720664128012479051029190886134 length=50
> # Failure.（発見に失敗）
```

- 先の定理で, $d < N^{0.292}$ のときは d が解読されることが知られている。
- Open Prob. $d < N^{0.5}$ のとき d は解読されるか？

離散対数問題を使ったElGamal暗号

公開: p, g, A

送信側

M 送りたいメッセージ

$A = g^a \pmod p$

受信側

秘密鍵 a で累乗する

秘密キーb で累乗する

$B = g^b \pmod p$

$C = M \cdot A^b \pmod p$

暗号
(B, C)

復号

$C \cdot (B^a)^{-1} \pmod p$

$= M \cdot g^{ab} \cdot (g^{ab})^{-1} \pmod p$

$= M$

ポイントは，２つの離散対数問題をペアにして送ること

安全素数(safe prime)

■　離散対数問題に対して「安全素数」をとらないとき，Pohlig-Hellmanの攻撃がかかりやすい．

定義

素数 $p\ (\geq 3)$ に対し $p-1=2\cdot t$ （ t は素数）のとき

p は安全素数という．

■安全素数に対する離散対数問題で解かれた記録は，　2005年6月，十進130桁の安全素数が現在最高．

■また，安全素数は無限に存在するかは知られていないが実用的には十分多く存在することを以下で見る．

安全素数を使わないときのPohlig-Hellmanの攻撃

概略:

離散対数問題 $\boxed{y = g^x \pmod p}$ に対し $p-1 = \prod_{j=1}^{k} q_j$ の素因数 q_j が小さな素数の場合を考える.

$g_j = g^{(p-1)/q_j}$, $y_j = y^{(p-1)/q_j}$ とおくと k 個の離散対数問題 $\boxed{y_j = g_j^{x(j)} \pmod p}$ が容易に解け, これらの解 $x(j) \pmod{q_j}$ が求まる. (g_j の位数が小さいから)

ここで, Chinese Remainder Theorem から, 連立方程式 $x = x(j) \pmod{q_j}, j = 1,\ldots,k$ を満たす $x \pmod{p-1}$ が求まり, これが離散対数問題の解となる.

ポイント:

Chinese Remainder Theorem での解を求める方法は十分高速である.

- 安全素数が無限にあるという予想はまだ証明されていない(200年前から？）

- 安全素数に対するSophie Germainの素数の世界記録が今年も更新されている（十進5万桁くらい）

p：安全素数　$p-1=2\cdot q$　(q：Sophie Germainの素数)

素数定理

$\pi(x)$ を x 以下の「素数の個数」とするとき

$$\pi(x) \sim \frac{x}{\log x}.$$

$f(x) \sim g(x)$ は $f(x)/g(x) \to 1 \ (x \to \infty)$ のこと.

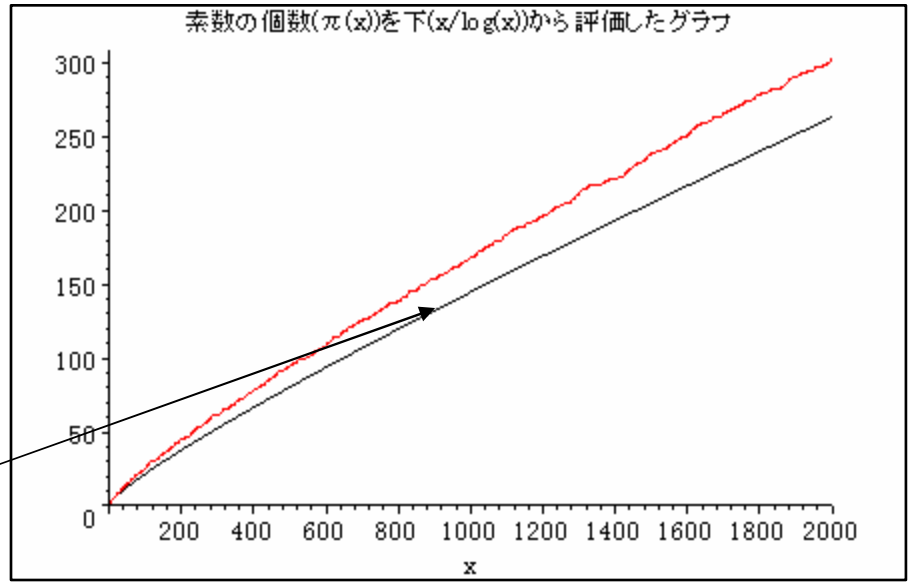
この意味は「x 以下の素数は x の桁数の定数倍でわった個数だけ十分多く存在する」こと

安全素数の個数調べに応用するには

【Rosser-Schoenfeldの定理】

$x \geq 17,$

$$\pi(x) > \frac{x}{\log x}.$$



安全素数の個数を下から評価する(1)

安全素数が無限にあるかどうか，知られていないので，予想値で下から評価する実験を行う.

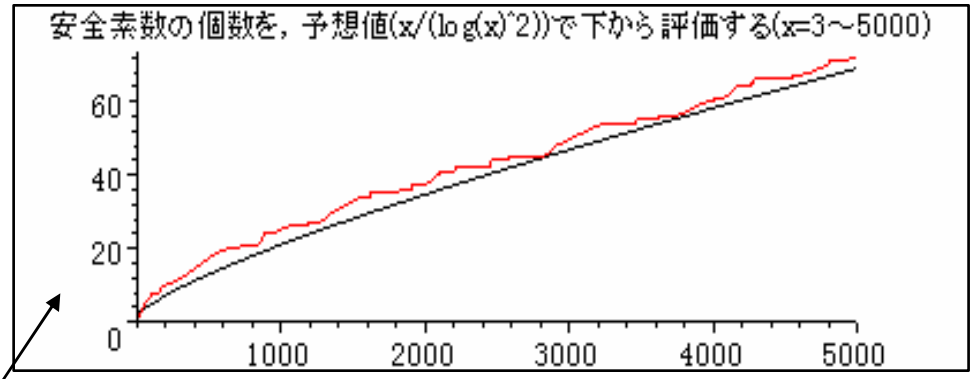
$\pi_{\mathrm{sp}}(x)$ を x 以下の安全素数の個数とする

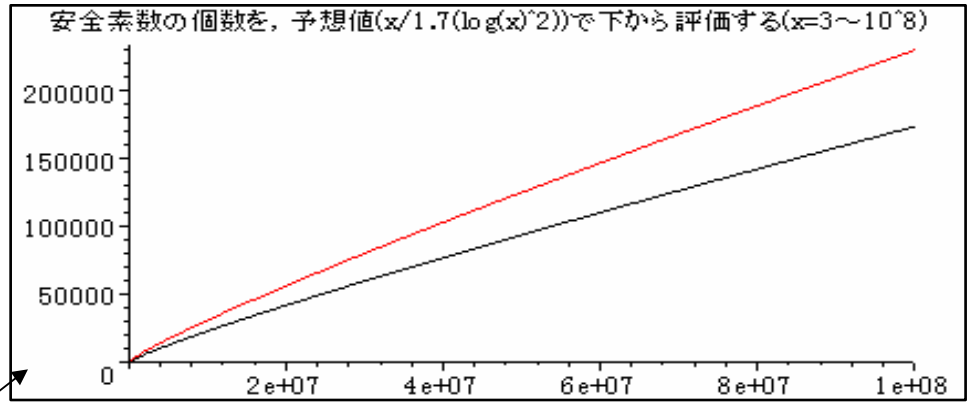
(1) 比較的小さな値での評価

予想値:

$$\pi_{\mathrm{sp}}(x) > \frac{x}{(\log x)^2}$$

$$\pi_{\mathrm{sp}}(x) > \frac{x}{1.7(\log x)^2}$$

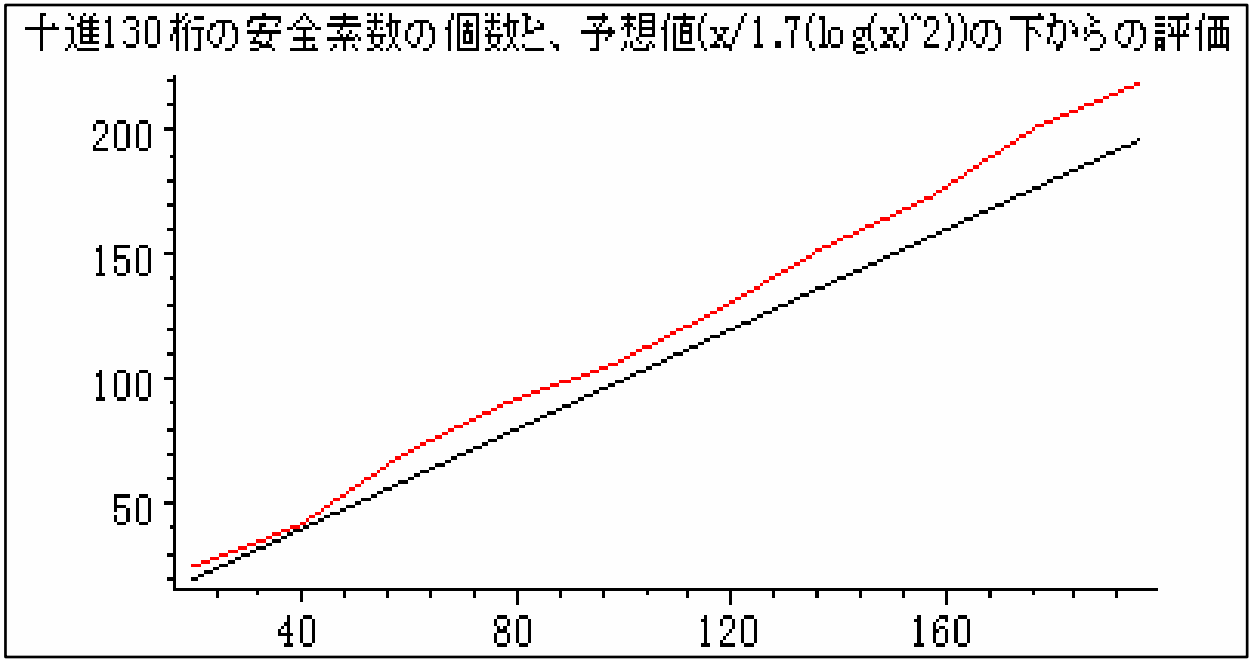




意味:「x 以下の安全素数は x の桁数の**2乗**の定数倍でわった個数だけ十分多く存在する」こと

安全素数の個数を下から評価する(2)

十進130桁

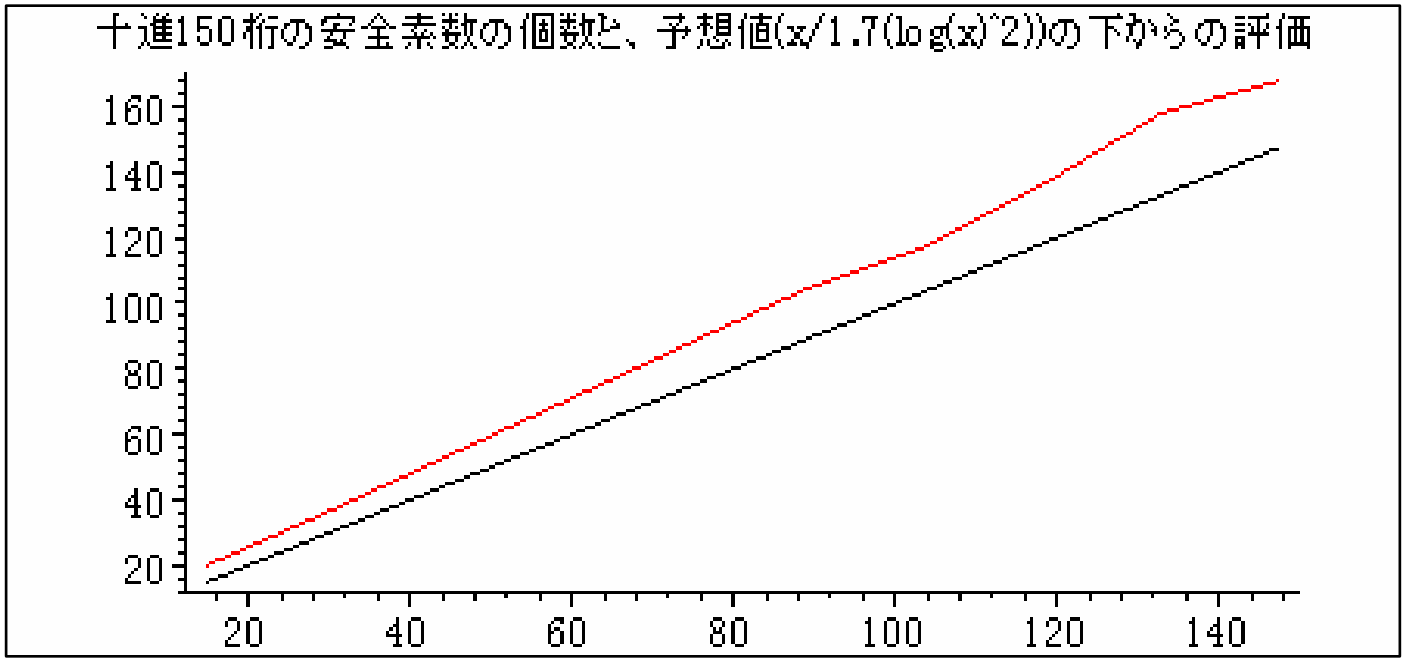


十進130桁の自然数:
57485971628761282736479870151723981987263408526272456345623584523456561423053083796592837695901928374098102983479034750384752345 83

から**3,000,000** の幅で10区間安全素数の個数と予想値を比較したもの.

安全素数の個数を下から評価する(3)

十進150桁



十進150桁の自然数:

502938807938756298761311872298376873436491872364201978326463424619523012364987132649875923918734629130124619874612974918723469187236409872634987123 49

から**3,000,000** の幅で10区間安全素数の個数と予想値を比較したもの