Vol. 34 No. 2　　情　報　処　理　　Feb. 1993

解　説

数論アルゴリズムとその応用

素数判定アルゴリズム†

木田祐司††　牧野潔夫†††

1. はじめに

最も素朴な素数判定（素因数分解）法は小さな数から次々に割り算をしてみることであろう．これでは目的の数 N が素数であると分かるにはおよそ $\sqrt{N}$ 回の割り算が必要である．桁数を基準に考えるとその指数関数の計算量ということになる．これを理論的にも実際的にも少ない計算量で済ませる方法が昔から求められてきた．当然ながらコンピュータ時代になってから盛んに研究されるようになったが，とくに RSA 暗号法の発明とそれに続く Adleman-Rumely の判定法の発見がそれまでの“工夫”とでもいうべきレベルから本当に高度な理論へとこの分野の面目を一新させた．この小文ではもう古典ともいうべき 1980 年以前の方法に簡単に触れてから現在の最新理論を基本となる考え方が分かるように解説する．

2. 1980 年以前

2.1 Fermat テスト

素朴な試し割り算による素数判定は合成数であった場合にはその約数まで求めてしまうという過剰な働きがある．ただ単に素数と合成数を区別するだけならもっと簡単な方法があってもよい．その基本は既約剰類群である．自然数 N に対して

$$(\mathbf{Z}/N\mathbf{Z})^* = \{a+N\mathbf{Z} \mid 0<a<N, \mathrm{GCD}(a,N)=1\}$$

を考え，その元に自然な乗法を定義したものを N を法とする既約剰余類群という．これは N が素数の場合には位数 $N-1$ の巡回群になる．とくに次の三つの定理が成立する．

Fermat の小定理

N が素数で $\mathrm{GCD}(a,N)=1$ ならば

(1)　$a^{N-1}\equiv 1 \bmod N$

である．

Euler の規準

N が素数で $\mathrm{GCD}(a,N)=1$ ならば

(2)　$a^{\frac{N-1}{2}}\equiv\left(\frac{a}{N}\right) \bmod N$

が成り立つ．ただし $\left(\frac{a}{N}\right)$ は平方剰余記号であり，$x^2\equiv a \bmod N$ となる x が存在すれば 1，存在しなければ -1 となる．

定理 (Miller)

素数 N に対し $N-1=2^s d$, $\mathrm{GCD}(d,2)=1$ とおけば $\mathrm{GCD}(a,N)=1$ のとき

(3—1)　$a^d\equiv 1 \bmod N$

または

(3—2)　$a^{2^k d}\equiv -1 \bmod N (0\leq \exists k\leq s-1)$

が成立する．

a を決めて N が(1)または(2)または(3)をみたすかどうか調べることをそれぞれ Fermat テスト，Solovay-Strassen テスト，Miller-Rabin テストという．みたす場合にそのテストをパスしたという．

定理の対偶をとれば「ある a に対してこれらのテストをパスしなければ N は合成数である」ということが結論される．

一方 N がある a に対してこれらのテストをパスしたとしても N が素数であるとはいえない．

確率的には次のことがいえる．

N が合成数のとき N と互いに素な a をランダムにとると N が Solovay-Strassen テスト (Miller-Rabin テスト) をパスする確率は 1/2(1/4) 以下で

† Primality Testing Algorithms by Yûji KIDA (Department of Mathematics, Rikkyô University) and Isao MAKINO (Faculty of Engineering, Kôgakuin University).

†† 立教大学理学部数学科
††† 工学院大学工学部

ある[Ra,SS].

また N が合成数ならば a を $2,3,5,\cdots$ と素数を動かしていけば N 以下のある値で必ず N は Solovay-Strassen テスト (Miller-Rabin テスト) をパスしない．このような a の最小の値の評価は **4.** で行う．

2.2 Pocklington の定理

既約剰余類群の位数にもっと着目して次の定理を得る．

Pocklington の定理

$N-1=F\times G$, $\mathrm{GCD}(F,G)=1$

と分解されているとする．さらに

$F=\prod q_i^{e_i}$ (q_i は異なる素数)

と完全に素因数分解されているものとする．このとき次の条件をみたす a が存在すれば N の任意の素因数 r に対して F は $r-1$ を割り切る．

$$\begin{cases} a^{N-1}\equiv 1 \bmod N \\ \mathrm{GCD}(a^{(N-1)/q_i}-1,N)=1 \text{ for } \forall i \end{cases}$$

とくに $F>\sqrt{N}$ ならば N は素数である．

実際の応用では F には未確定の素因数も含めることができる．とりあえず素数だとして a を求めておきその数の判定を同じようにして行えば良い．これでより小さな数の素数判定に落とすことができ，十分小さくなれば試し割り算などで判定することにより，全体の正当性を確定させることができる．

ここですぐ気がつくのは N が大きいと $N-1$ を十分に素因数分解できる場合はそう多くはないことである．そこで考える群をもっと変化にとんだものにしてこの点を克服しようというのが **3.** 後半に述べる楕円曲線を用いた素数判定法である．

3. 1980年以降

3.1 ガウス和を用いた素数判定法

本格的な素数判定法は Adleman-Rumely 法[APR] から始まる．これを H. W. Lenstra Jr.[Le2] がアレンジしたものを紹介する．

$p_1,p_2,\cdots,p_h$ を素数を小さいものから並べたものとしその積を t とする．さらに素数 $q_1,q_2,\cdots,q_k$ を q_i-1 が t を割り切るものとし，その積を s とする．s は $\sqrt{N}$ より大きくなるように h, k をとる．以下 p,q は今の p_i, q_j で $p_i|(q_j-1)$ となるもの全体を動くとする．χ を q を法とし，p を位数とする指標とする．具体的には g を q を法とする原始根とするとき $\chi(g^x)=\zeta_p{}^x$ で定義される複素関数である．ただし $\zeta_p=\exp(2\pi\sqrt{-1}/p)$ である．このときガウス和 $\tau(\chi)$ は次のように定義される

$$\tau(\chi)=\sum_{a=1}^{q-1}\chi(a)\zeta_q{}^a$$

基本的となる等式は次のものである．

ℓ が素数ならば

$\tau(\chi)^{\ell p-1}-1\equiv\chi(\ell) \bmod \ell$

Fermat の小定理あるいは Euler の規準の類似といえる．

そこでまず $\ell=N$ としてチェックする．パスしたならば $N^{p-1}-1=p^{w_p}u_p$, $p\nmid u_p$ と分解する．ここで N の $\sqrt{N}$ 以下の素因数があったとしてそれを r とおく．r は素数なのだから当然，上の等式をみたしている．これで $\tau(\chi)$ を媒介として $\chi(N)$ と $\chi(r)$ が結びついた．以下アイディアを明確にするためすべての p について $w_p=1$ となる場合だけを扱う．一般に $r^{p-1}-1=pa$ と書けるので，この場合は

$$\chi(r)^{u_p}=\tau(\chi)^{(r^{p-1}-1)u_p}$$
$$=\tau(\chi)^{(N^{p-1}-1)a}=\chi(N)^a$$

となる．u_p の法 p での逆数を両辺にかければ

$\chi(r)=\chi(N)^{b_p}=\chi(N^{b_p})$ for $\exists b_p$

となる．

$b\equiv b_p \bmod p$ for $\forall p$

で b を定めれば

$\chi(r)=\chi(N^b)$ for $\forall\chi$

となる．指標の基本的性質から

$r\equiv N^b \bmod s$

となる．s, r のとり方からこれは N^b を s で割ったあまりが r に等しいことを意味している．そこで N の法 s でのべき乗を次々に計算して (高々 t 乗までで十分)，実際に N を割り切る r が存在しなければ N が素数であることが確定する．なお文献 [Le3] による s は $s>\sqrt[3]{N}$ にとれば十分である．

3.2 ヤコビ和を用いた素数判定法

Cohen-Lenstra[CL] はガウス和を用いた判定法を実際の計算が速くなるように改良した．基本となるのは次の合同式である．

ℓ が素数ならば

$\tau(\chi)^{\phi_\ell-\ell}\equiv\chi(\ell)^\ell \bmod \ell$

ただし ϕ_ℓ は ζ_p をその ℓ 乗にうつし，ζ_q は変えないような体の同形写像である．

詳細は省略する．Bosma-van der Hulst[BH] は円分体テストあるいはガロア理論テストと呼ばれるものと組み合わせることにより理論をすっきりさせ，実際的にも高速化させた．彼らは 1065 桁の数 $(2^{3539}+1)/3$ の実数判定を行っている．

この方法の FORTRAN プログラムが手数料の払い込みで手に入る．問い合わせ先は次のとおり．

M. P. van der Hulst,
University of Amsterdam,
Plantage Muidergracht 24,
1018 TV Amsterdam,
The Netherlands.

3.3 楕円曲線を用いた素数判定法

Pocklington の方法を適用する群を $\bmod N$ の既約剰余類群から $\bmod N$ の楕円曲線に代えたものである．別項の素因数分解の楕円軸曲線法が $p-1$ 法の翻案であることと同様である．

整数 a, b に対して素数 p を法とする楕円曲線 $E(p)$ とは

$$Y^2 \equiv X^3+aX+b \bmod p$$

の解 $(x \bmod p,\ y \bmod p)$ の全体に仮想的な一点 $\mathcal{O}$ を付け加えた集合に次のような演算 $+$ を定義したものである．

2 点 $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$ に対して $P_3=P_1+P_2$ の座標 (x_3, y_3) は

$x_1 \neq x_2$ の場合：

$$\lambda \equiv (y_2-y_1)/(x_2-x_1)$$

$x_1 \equiv x_2, y_1 \equiv y_2 \neq 0$ の場合：

$$\lambda \equiv (3x_1^2+a)/2y_1$$

とおけば

$$\begin{cases} x_3 \equiv \lambda^2-x_1-x_2 \\ y_3 \equiv \lambda(x_1-x_3)-y_1 \end{cases}$$

となる．

$x_1 \equiv x_2, y_1 \equiv -y_2$ の場合：

P_3 は $\mathcal{O}$ になる．

ただし計算はすべて $\bmod p$ で行う．とくに，割算は $\bmod p$ での逆数の積である．$\mathcal{O}$ は (x, y) の型には書けなくて，1 変数増やして射影平面で考えると $[0, 1, 0]$ と書けるものである．

必ずしも素数と限らない一般の整数 N を法とする楕円曲線の定義はかなり面倒になる．ここではそれを避け単に上の定義で p を N に代えたものを扱う．この場合 P_1+P_2 が定義されないことがある．厳密な定義との混同を避けるため $E(N)$ とは書かずに $V(N)$ と書くことにする．N が素数の場合は $E(N)=V(N)$ である．N を素数とみなして Schoof[Sc] の方法で計算した $V(N)$ の位数を $\sharp' V(N)$ としよう．

Pocklington の定理（楕円曲線版）

$m=\sharp' V(N)$ が

$$m=F\times G$$

と分解されているとする．さらに

$$F=\prod q_i^{e_i} \quad (q_i \text{ は異なる素数})$$

と完全に素因数分解されているものとする．このとき $V(N)$ 上に次の条件をみたす点 A が存在すれば N の任意の素因数 p に対して F は $\sharp V(p)$ を割り切る．

$$\begin{cases} mA=\mathcal{O} \\ (m/q_i)A \text{ は定義され } \mathcal{O} \text{ と異なる (for } \forall i). \end{cases}$$

とくに $F>(\sqrt[4]{N}+1)^2$ ならば N は素数である．

ここで a, b を変えると $m=\sharp' V(N)$ も変わる．したがってさまざまの分解の型をもった m が現れるであろう．その中で次の型のものがわれわれの目的に使える．

$m=$小さな素数の積×大きな未確定素数

このときは $F=m$ としても良いが $F=$ “大きな未確定素数”，とするほうがずっと計算を節約できる．

以上から Goldwasser-Kilian[GK] の判定法が得られる．

（1） a, b をランダムに動かす．

（2） $m=\sharp' V(N)$ を計算する．

（3） $m=2\times$ “大きな未確定素数” の型か判定し，なっていなければ（1）からやり直す．

（4） $V(N)$ の点 A で条件をみたすものを捜す．

（5） 再帰的に未確定素数についても同じ方法で素数であることを確定する．

しかしこの方法では Schoof のアルゴリズムが遅くて実用的ではないとされている．もっとも彼らは理論的な実行時間が解析しやすいようにしたのであった．これについては **4.** で述べる．

3.4 虚数乗法テスト

Goldwasser-Kilian が楕円曲線をランダムに動かして都合の良いものを捜したのに対して Atkin

は，先に m を指定し，それから $\sharp' V(N)=m$ となる楕円曲線を構成するというアプローチをとった．これが Atkin-Morain テストである[AM, Mo]．Complex multiplication（虚数乗法）テストとも呼ばれる．アルゴリズムはおおよそ次のとおりである．

（1） 7以上の整数 D を $-D$ が基本判別式になるように動かし，$N=\nu\bar{\nu}$, $\nu\in K$ となる虚二次体 $K=\mathbf{Q}(\sqrt{-D})$ を捜す．これはヤコビ記号 $\left(\frac{-D}{N}\right)$ が1であり，かつ $-D$ に関する Hilbert 多項式が $\bmod N$ で一次式の積に分解されることで判定できる（ここでいう Hilbert 多項式とは判別式が $-D$ の既約な二次形式から作られる j-不変量の最小多項式のことである）．実際には Hilbert 多項式に関する計算が大変なので

(1-1) $-D$ に属するすべての素判別式 d に対してヤコビ記号 $\left(\frac{d}{N}\right)$ が1であることをチェックして適しない候補をかなりふるいおとし，それから

(1-2) Hilbert 多項式を計算する．

(1-3) Hilbert 多項式が $\bmod N$ で一次式の積に分解することを確認する．

ということになる．

（2） ν を求める．

（3） $m=(1\pm\nu)(1\pm\bar{\nu})$（複合同順）を素因数分解してみて必要なだけの分解が得られれば次へ，さもなければ(1)からやり直す．

（4） Hilbert 多項式の $\bmod N$ での根を一つ求め j とおき $k=j/(1728-j) \bmod N$ を計算する．

（5） λ を N の倍数でない任意の整数とし $a=3k\lambda^2$, $b=2k\lambda^3$ に対する楕円曲線 $V(N)$ を考える．$\mathcal{O}$ 以外の一点をとり m 倍したときに $\mathcal{O}$ になるかどうかをテストする．パスしない場合は $\bmod N$ の平方非剰余 c をとって $c\lambda$ を新しい λ とする．

（6） $V(N)$ の点 A で条件をみたすものを捜す．

どの項目も理論的にも実際的にも難しく，プログラムを作るのは容易ではない．幸いに Morain のプログラムが公開されており，ワークステーション上で動かすことができる．また Morain[Mo] には詳細な解説があるので参照されたい．これらは Internet からダウンロードできる．

ftp address :

nuri, inria. fr (128. 93. 1. 26)

thesis :

INRIA/INRIA-publication/TE-090. tar. Z.

program :

INRIA/ecpp. V 3. 4. 1. tar.Z.

ヤコビ和テストで述べた 1065 桁の数 $(2^{3539}+1)/3$ の素数判定はこちらが先に行っていて記録はどんどん更新されている．ヤコビ和テストとどちらが実用的に優れているかは議論の別れるところのようである．

さてこの Atkin-Morain テストの計算量は理論的に厳密な解析が難しくヒューリスティックな議論（証明されていないかなり大胆な仮定を元にした議論）しかできない．それによると $O((\log N)^{6+\varepsilon})$ 以下である．

4. 計算量の評価

この章では N が素数か合成数かを判定するために必要な計算量の評価をする．基本となる演算が N の桁数の多項式時間でできることはとくに断わらずに用いる．

非決定的（non deterministic）な計算量をまず考える．

合成数判定は実際に約数を一つ与えれば一回の割り算で確認できる．つまり桁数の多項式時間で済む．

素数判定のほうはたとえば Pocklington の定理がうまく働く F, a の系列を与えておけば良いからこれも多項式時間でできる (Pratt[Pr])．

決定的（deterministic）な計算量に関してはこの数年顕著な発展がない．以下では主にその中間概念である確率的な計算量を考える．すなわち各操作は明確に規定されていて，終了することがある十分な確率で保証されているような計算である．

4.1 合成数判定の計算量

2. で述べたように N が合成数ならばある a に対し N は Solovay-Strassen (Miller-Rabin) テストをパスしない．さらにこのような a は $1\leq a<N(\mathrm{GCD}(\alpha, N)=1)$ で考えると全体の 1/2(3/4) 以上あるのであった．したがって次のことがいえる．

N が合成数ならば Solovay-Strassen テストを一回行うと 1/2 以上の確率で合成数と判定できる．

テスト一回の計算量は $O(\log^k N)$ であるから

『すべての合成数はその桁数の確率的多項式時間で合成数と判定できる.』

4.2 Miller の理論

N の素数判定は $1\leq a\leq N$, $\mathrm{GCD}(N,a)=1$ なるすべての a に対し Solovay-Strassen テストを行えば良い. しかしこれでは試すべき a の個数が多すぎるのでどの程度の a まで調べたら良いのかを考える. この a の値の上からの評価は大変難しく素数判定を実用時間内に行う程度の良い結果を得るには一般 Riemann 予想を仮定する必要がある.

一般 Riemman 予想

χ を Dirichlet 指標とすると L-関数 $L(s,\chi)$ は $Res>\frac{1}{2}$ で零点をもたない.

この予想を仮定すれば N が合成数のときある $a<2\log^2 N$ があって N は Solovay-Strassen テストをパスしない（詳しくいうと予想をみたす必要のある χ は N のある約数を法とする平方剰余記号だけで十分である）.

『一般 Riemann 予想を仮定すると, すべての数はその桁数の決定的多項式時間で素数か合成数か判定できる.』

実験結果が文献 [Wa] にある.

4.3 Adleman-Rumely の方法

この判定法の計算量は $s>\sqrt{N}$ となる t の大きさによって決まる. これに関しては次の評価が成り立つ.

定理

正の定数 C_1, C_2 があって

$$(\log N)^{C_1 \log\log\log N}\leq t\leq(\log N)^{C_2 \log\log\log N}$$

である.

これから Adleman-Rumely 法の計算量は $O((\log N)^{C\log\log\log N})$ であることが分かる. ただし C は正の定数. しかもこれは決定的計算量である. 限りなく $\log N$ の多項式時間に近づいており, いかに画期的であったかが分かる. ただし上の定理は同時に多項式時間ではないことも示している.

4.4 Goldwasser-Kilian の方法

前章で定義した Goldwasser-Kilian の素数判定法の計算量を解析しよう.

Hasse の定理によると N が素数ならば楕円曲線の位数 $\#V(N)$ は

$$N+1-2\sqrt{N}\leq\#V(N)\leq N+1+2\sqrt{N}$$

をみたす. したがって $\#V(N)$ が $2\times$素数という型になるかはこの範囲にどのくらい $2\times$素数型の数があるかということと密接に関連している. そこで区間 $[(N+1-\sqrt{N})/2,\ (N+1+\sqrt{N})/2]$ に含まれる素数の集合を S とすると次の評価式が成立する.

定理 (Lenstra, Jr.[Le4])

N が素数ならば

$$\frac{\#\{V(N)\mid\#V(N)=2\times q,\ q\in S\}}{\#\{V(N)\}}\geq c\times\frac{\#S}{\sqrt{N}\log N}$$

となる. ただし c は正の定数である.

この式の分子 $\#S$ の評価に関し次の予想がある.

Cramer の予想

正の定数 c_1, c_2 があって十分大きな x に対し

$$\pi(x+\sqrt{x})-\pi(x)\geq c_1\sqrt{x}/\log^{c_2}(x)$$

である.

さらにこの予想の確からしさを支持するものに HeathBrown の定理がある.

定理 (HeathBrown[He]).

$$l(a,b)=\begin{cases}1 & [a,b]\text{ に含まれる素数の個数}\\ & \leq(b-a)/(2\lfloor\log a\rfloor)\\ 0 & \text{その他}\end{cases}$$

とするとある定数 α があって十分大きな x に対し

$$\sum_{x\leq a\leq 2x} l(a,a+\sqrt{a})\leq x^{5/6}\log^{\alpha}x$$

が成立する.

HeathBrown の定理などから N がある例外的な素数の集合に入っていなければ N を法として定義されその位数が $2\times q$ 型になる楕円曲線が $1/\log^k N$ 以上の確率でみつかることが分かる（k はある正の定数）. したがって Goldwasser-Kilian の判定法の条件(3)がみたされる. $q=\#V(N)/2$ が素数かどうかの判定は再帰的にこの方法で行う. 結局

『"ほとんど" すべての素数はその桁数の確率的多項式時間で素数と判定できる.』

4.5 Adleman-Huang の方法

Goldwasser-Kilian 法には判定できない例外的な素数が存在するかもしれず理論的に不完全であった. Adelman-Huang[AH] は超楕円曲線のヤコビ多様体を併用することによりこの例外をなくすことに成功した.

p を素数とし $\mathbf{Z}/p\mathbf{Z}$ 係数の重根をもたない6次

多項式 $f(x)$ により $y^2=f(x)$ で定義される平面曲線 $C=C(f)$ を考える．C は超楕円曲線とよばれる．さらに C に対応するヤコビ多様体を J と表しその $\mathbf{Z}/p\mathbf{Z}$-有理点を $J(p)$ と表す．$J(p)$ はやはり有限アーベル群になりその位数は次の不等式をみたす．

定理

$$p^2-4p^{1.5}+6p-4p^{0.5}+1 \leq \#J(p) \leq p^2+4p^{1.5}+6p+4p^{0.5}+1$$

前章の楕円曲線の場合と同様，素数とは限らない数 N に対しても擬似的な $J(N)$ を考えよう．やはり定義する方程式を単純に mod N で考えた解の集合のことであり，正式のものとは異なる．N を素数とみなして Schoof の方法の類似で計算した $J(N)$ の位数を $\#'J(N)$ としよう．

Pocklington の定理（超楕円曲線のヤコビ多様体版）

ある f に対して $\#'J(N)$ が素数で $J(N)$ の（通常の）点 A があって $\#'J(N)A=\mathcal{O}$ となるならば N は素数である．

一般に Goldwasser-Kilian 法で素数判定可能な素数を *ample* ということにする．ただし Goldwasser-Kilian 法は $\#'V(N)$ の小さな約数を2に限らず小さな素数から何でも良い，と拡張したものとする．また Miller-Rabin 法などで素数であることがほとんど確実な数を *almost prime* ということにする．

以上の準備の下で Adleman-Huang 法は次のように述べられる．

（1） mod N の多項式をいろいろ動かし $N_1=\#'J(N)$ が almost prime となるものをみつける．

（2） mod N_1 の多項式をいろいろ動かし $N_2=\#'J(N_1)$ が almost prime となるものをみつける．

（3） mod N_2 の多項式をいろいろ動かし $N_3=\#'J(N_2)$ が almost prime となるものをみつける．

（4） N_3 が ample ならば終了し，そうでなければ(1)から繰り返す．

ここで N_1, N_2, N_3 はそれぞれおよそ N^2, N^4, N^8 の大きさの数であり，N の素数判定をより大きな数の素数判定に“帰着”するという奇妙なことになっている．それでも良いというのはそれだけ $\#J(N)$ のとりうる値の範囲がひろがり ample になりやすいからである．証明では Cramer の“予想”に対応する命題が“定理”であることが本質的である．

定理 (Iwaniec-Jutila[IJ])

ある正の定数 C があって十分大きな x に対し

$$\pi(x^2+x^{1.5})-\pi(x^2) \geq x^{1.5}/\log^C x$$

である．

Adleman-Huang はどんな素数に対しても，以上の(1)-(4)を1度行ったときに，このテストが終了する確率が $1/\log^k N$ 以上であることを示した（k は正の定数）．つまり

『すべての素数はその桁数の確率的多項式時間で素数と判定できる．』

5. おわりに

素数判定という簡単なものも追及すると深い理論があることがお分かりいただけたであろう．近い将来“確率的”という形容詞が取り除かれることを期待したい．またもともと素数判定法が見直されたのは RSA 暗号に用いるための素数発生にある．しかしこの小文では理論面を重視して実用面の考察は行わなかった．いずれまた別の特集にお任せしたい．

参考文献

[APR] Adleman, L. M., Pomerance, C. and Rumely, R. S.: *On Distinguish Prime Numbers from Composite Numbers*, Ann. of Math. 117, pp. 173-206 (1983).

[AH] Adleman, L. M. and Huang, M. A.: *Primality Testing and Abelian Varieties over Finite Fields*, Springer Lecture Notes in Math. 1512 (1992).

[AM] Atkin, A. O. L. and Morain, F.: *Elliptic Curves and Primality Proving*, to appear.

[An] Ankey, N. C.: *The Least Quadratic Nonredisue*, Annals of Math. 55, pp. 65-72 (1952).

[BH] Bosma, W. and van der Hulst, M.-P.: *Primality Proving with Cyclotomy*, Doctorial Thesis, University of Amsterdam (1990).

[CL] Cohen, H. and Lenstra Jr., H. W.: *Primality Testing and Jacobi Sums*, Math. Comp. 42, pp. 297-330 (1984).

[GK] Goldwasser, S. and Kilian, J.: *Almost All Primes Can Be Quickly Certified*, Proc. 18th annual ACM symp. on Theory of Computing, pp. 316-329 (1986).

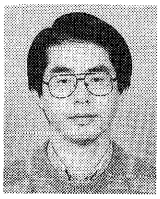
[He] Heath-Brown, D. R.: *The Differences between Consecutive Primes*, J. London, Math. Soc. 18, pp. 7-13 (1978).

[IJ] Iwaniec, H. and Jutila, M.: *Primes in Short Intervals*, Ark. Mat. 17, pp. 167-176 (1979).

[Le1] Lenstra Jr., H. W.: *Miller's Primality Test*,

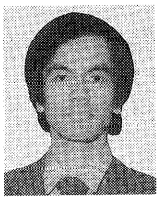
Inform. Process. Lett. 8-2, pp. 86-88 (1979).
[Le2] Lenstra Jr., H. W.: *Primality Testing Algorithms*, Springer Lecture Notes in Math. 901, pp. 243-257 (1981).
[Le3] Lenstra Jr., H. W.: *Divisors in Residue Classes*, Math. Comp. 42, pp. 331-334 (1984).
[Le4] Lenstra Jr., H. W.: *Factoring Integers with Elliptic Curves*, Ann. of Math. 126, pp. 649-673 (1987).
[Mi] Miller, G.L.: *Riemann's Hypothesis and Tests for Primality*, J. Comp. and System Sc. 13, pp. 300-317 (1976).
[Mo] Morain, F.: *Courbes Elliptiques et Tests de Primalité*, Docteure Thèse, L' Universitè Claude Bernard-Lyon I (1990).
[Pr] Pratt, V. R.: *Every Prime Has a Succinct Certificate*, SIAM J. Comp. 4, pp. 214-220 (1975).
[Ra] Rabin, M. O.: *Probabilistic Algorithm for Testing Primality*, J. Number Theory 12, pp. 128-138 (1980).
[Sc] Schoof, R.: *Elliptic Curves over Finite Fields and the Computation of Square Roots Mod p*, Math, Comp. 43, pp. 483-494 (1985).
[SS] Solovay, R. and Strassen, V.: *A Fast Monte-Carlo Test for Primality*, SIAM J. Comput. 6-1, pp. 84-85 (1977), 7-1, p. 118 (1978).
[Wa] Wagon, S.: *Primality Testing*, Math. Intelligencer 8-3, pp. 58-61 (1986).
初等整数論については
[高] 高木貞治，初等整数論講義，共立出版.
代数的整数論については
[石] 石田 信，代数的整数論，森北出版.
を参照されたい.

(平成4年8月14日受付)



木田 祐司（正会員）

1975年東北大学理学部数学科卒業．同大学院修士課程修了．理学博士．1991年より立教大学理学部数学科助教授．整数論と計算機の境界領域を研究中．日本数学会会員.



牧野 潔夫

1972年大阪大学理学部数学科卒業．東京大学大学院博士課程修了．理学博士．1986年より工学院大学工学部助教授．数式処理を利用した整数論の研究に従事．日本数式処理学会理事．日本数学会会員.