素数判定 PRIMES が決定性多項式時間 P である事の証明について

中村 憲

2002 年 11 月 12 日 — 2003 年 11 月 10 日 版　(DVIed at 19:16 on 12 November, 2003)

自然数 $n > 1$ の自然数の積への分解が $n = 1 \times n = n \times 1$ だけ (即ち n が素数) かどうか判定する問題 (即ち 素数判定 **PRIMES**) が, 入力した n の桁数の多項式の程度の回数の順序立てた加減乗除で可能 (即ち **deterministic polynomial time** 決定性多項式時間 **P**) であるという, 衝撃的論文 [AKS02] がインドの三人の研究者により 2002 年 8 月 6 日付で公表された. 本論説では, その解説を通じて PRIMES と関連する数論アルゴリズムを概観する. 最初に § 1 で PRIMES や P 等の定義をしながら問題の由来や暗号理論との関連を説明し, 次に § 2 で提案されたアルゴリズムを紹介し, その効率や根拠を示す. そして, 更に § 3 で今回の新発見の意義を検討する. 最後に § 4 で以降の発展について述べる. 特に § 2.2 迄は, 高校生でも大要は理解できる様に書いたつもりである. これ迄には, ほとんど数学を使わないで書かれた問答集 [Sti02] や高校数学で理解できる様に試みた解説 [Cox02] があり, また日本語による [Kid03] やドキュメンタリ風の [Bor03] もある. 参考文献の内でネットワークから参照できるものは, その継続的提供が保証されているものばかりではない事に注意しておく.

尚, 最近 'deterministic' を '決定性' や '確定性' でなく '決定的' などと和訳しているものに頻繁に遭遇するが, この日本語は少々違った意味を持つ 'final' や 'definite' と受取られかねないので止めた方が良い. せめて '確定的' とか '決定論的' とすべきであろう. 誤解が迷信となり広がる前に, ここで敢て強調しておきたい.

1. 問題の意味

まず標題の述語を定義しながら, この問題の意味を理解しよう. ここでは厳密性にこだわらないで, 大まかな背景と歴史を述べる. 正確には, これ迄の PRIMES アルゴリズムに関しては [KM95], [CP01, Chapters 3 – 4] 等を, 計算量に関しては [Nis02], [Kob98, Chapter 2] 等を, この問題と公開鍵暗号系との正確な関係については [OO95], [KFM95], [Kob94, Chapter IV] 等を参照して欲しい.

1.1. 素数判定 PRIMES

これは, どんな問題なのだろうか?

ニューヨークタイムズによる [AKS02] の紹介記事の見出しが '2200 年来の数学の問題解

決!' である様に, 自然数 $n > 1$ が素数か, そうでない (即ち合成数) か判定し, 合成数の時には n を素数の積に分解する問題 (即ち素因数分解) は, 数論の出発点となる根本問題である. これは一見簡単そうな問題であり, 実際古代ギリシャ時代にユークリッド原論で, 無限個の素数の存在や, 自然数の一意的素因数分解可能性は知られている. しかし, それを実際に "計算" する視点から見直すとかなり大変である. 例えば 155 桁の

$$n=10941738641570527421809707322040357612003732945449205990913842131476349984288934$$
$$7847179972578912673324976257528997818337970765372440271467435315933543338 97$$

を素因数分解する事を考える. 最も素朴な方法は, 小さい奇数 3, 5, 7, 9, ... で順に n が割切れるかどうか見る方法 (即ち試し割算) であり, 約 5×10^{76} 回の割算が必要である. 地球上に歴史上存在した全コンピュータの, これ迄に実行された総演算回数を, 全部集計すると西暦 2000 年迄で約一モル (6×10^{23}) [CP01, p. 4] で, そろそろ現在は二モルに近付きつつあるそうであるが, これを総動員しても試し割算をしていたのでは, この数は素因数分解できない事になる. 現実には, この数は [Nak99] に解説されている数体篩 **NFS** というアルゴリズムを使う事により, ようやく 1999 年 8 月に 78 桁の二つの自然数 n_1, n_2 の積 $n = n_1 \times n_2$ に分解され, そして n_1, n_2 が素数である事も確認できている [Cab99]. このうち素因数分解は § 1.3 でみる様に, 未だ非常に困難な問題である. 他方 PRIMES はより容易で, これら 78 桁の n_1, n_2 が素数である事については, ちょっと手計算では無理であろうが, 例えば [Nak03, § 1] に紹介されているソフトを使えば誰でも分る.

では, どの程度の手数がかかるのだろう. また, それらソフトはどの様に PRIMES を解いているのだろうか.

素因数分解や PRIMES を考える時に偶数や小さな数は興味がないので, これからは主な考察の対象として

$$n \text{ は大きい奇数}$$

とする. 試し割算により PRIMES を解く方法では, 割算が最大 $\lfloor (n^{1/2} - 1)/2 \rfloor$ 回必要となる, 但し $\lfloor x \rfloor$ は $x > 0$ の小数点以下を切捨てた値を表す. 例えば $n = 200212211123$ なら 223724 回の割算で, ようやく n が素数と分る. この回数は n が大きくなると $n^{1/2}$ に比例して増加する. 自然数 n の正の実数値関数 $f(n)$, $g(n)$ に対して, 或定数 c を用いて全ての n に対して $f(n) \leq cg(n)$ と評価できる時, 即ち $f(n)$ が $g(n)$ に比例して上から抑えられる時, $f(n) = O(g(n))$ と書く. すると最速アルゴリズム [Nak96, § 2.1], [CP01, Chapter 9] による n 以下の整数の加減乗除の計算時間の最大値 (即ち最悪時間計算量, 以下計算量と省略) の評価は

$$O(\lg n \lg\lg n \lg\lg\lg n) \tag{1}$$

程度である, 但し 2 を底とする対数 $\lg = \log_2$ である. これを用いても試し割算では, 計算量は

$$O(n^{1/2} \lg n \lg\lg n \lg\lg\lg n)$$

より改良できない. 事前に $\lfloor n^{1/2} \rfloor$ 以下の素数表があれば, 素数だけの試し割算で済むが, その個数は [CP01, Theorem 1.1.3] により $O(n^{1/2}/\lg n)$ だから, それでも計算量は

$$O(n^{1/2} \lg\lg n \lg\lg\lg n) \tag{2}$$

である.

エラトステネス篩 [CP01, Algorithm 3.2.2] という割算をしないで n 迄の素数表を作成する方法があるが, その場合には計算量は更に大きく

$$O\left(\frac{n \ln n}{\ln \ln n}\right) \tag{3}$$

となる, 但し自然対数 $\ln = \log_e$ である. なお, これ迄に公開されている素数表は [Boo98] が最大であり, その他の各種の素数に関するデータは [Cal02] から参照できる.

これらの方法では高速に PRIMES が解けない事は上の例で見た通りであるが, それを次に少し理論的に説明しよう.

1.2. 決定性多項式時間 P

前節迄の方法では, 計算量が (2) や (3) の様に n のサイズの指数関数の速さで増える指数時間だから高速でない.

ここで n のサイズは n ではないかと不思議に思うかもしれないが, 計算時間を計る時に「n のサイズ」という専門的述語は, 通常の大きさ (絶対値, ここでは n) の意味ではない. 問題なのは, データ n の入力の (最初に与える) 時の形式で考えたサイズであり, それを n のサイズと定義する. つまり一般に n の入力の時のサイズの事を短かく n のサイズと呼ぶのである. これらの問題を考えるときに, 例えば n が最初から素数の積の形で与えられていたのでは無意味である. それは n を十進数等で表した数字の列で与えられているとすべきであり, その時のサイズは十進数なら $\lfloor \log_{10} n \rfloor + 1$ 桁で, 二進数なら $\lfloor \lg n \rfloor + 1$ ビットである. 例えば 十進数 1000 と 9999 は, どちらも入力する場合は同じサイズ 4 桁である. だから, いくら $\varepsilon > 0$ が小さくても $n^\varepsilon = (2^\varepsilon)^{\lg n}$ はサイズ $\lg n$ の指数関数である. これに対して, いくら $K > 0$ が大きくても $\lg^K n = (\lg n)^K$ はサイズ $\lg n$ の多項式である. そこで計算量が入力サイズの多項式, この場合には $O(\lg^K n)$, で評価される確定的な計算方法 (即ち決定性アルゴリズム) がある問題のクラスを多項式 Polynomial の頭文字 P で表し, 実際に計算する上で手の届く範囲の問題として扱われる. 今回紹介する結果は

$$\mathrm{PRIMES} \in \mathrm{P}$$

を具体的にアルゴリズムを与えて証明したものである.

実は, この結論自体は驚くべき事実ではない. 既に PRIMES の計算量は決定性アルゴリズムであるヤコビ和テスト [APS83], [CL84] により, 極めて多項式時間に近い $\ln^{O(\ln \ln \ln n)} n$ である事が知られている. また, 素数判定をする [AH92] にあるアルゴリズムは, 乱数を用いた計算方法 (即ち確率的アルゴリズム) で, もし n は素数という判定を返せば答が必ず正しく, もし n は合成数という判定を返せば答が正しくない確率は $1/2$ よりも小さく, そして計算量は多項式時間である. この様な確率的アルゴリズムがある問題のクラスを RP (Randomized Polynomial-time) で表す. 即ち PRIMES $\in$ RP である. これと対称的に, 直後に紹介する n の合成数判定をする確率的アルゴリズム強擬素数テスト [Mil76], [Rab80], [CP01, § 3.4] は, もし n は素数という判定を返せば答が正しくない確率は $1/2$ よりも小さく, もし n は合成数という判定を返せば答が必ず正しく, そして計算量は多項式時間である. この様な確率的アルゴリズムがある問題のクラスを coRP で表す. 即ち PRIMES $\in$ coRP である. しかも

強擬素数テストは広く成立が確信されている (平方剰余記号に関するディリクレ L 関数に対する) 拡張リーマン仮説 **ERH** の下では, その計算量が多項式時間である決定性 PRIMES アルゴリズムとなる. これとは別の, 合成数判定をするオイラーテストもやはり $\mathrm{PRIMES} \in \mathrm{coRP}$ を保証し, ERH の下で決定性多項式時間 PRIMES アルゴリズムである [BS96, § 9.5]. 従って素数判定には, 必ず正しい答を返す確率的アルゴリズムで, 計算量の期待値が多項式時間のものがある. 即ち $\mathrm{PRIMES} \in \mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$ である. 要するに既に $\mathrm{PRIMES} \in \mathrm{P}$ を期待させる事実は知られていたし, その上それは ERH の下では成立していたのである. 我々を愕然とさせたのは, 今回のアルゴリズムの初等性である. なんとそれはフェルマ小定理のちょっとした一般化しか用いてない!

この結果の実用的価値については, これ迄のところ § 3.2 で述べる様に大勢を覆すものではない. その理由は実用的見地からみれば, より役立つ確率的アルゴリズムが存在するからである. その代表的なものに, すぐ上でも触れた, 簡単で高速なので良く用いられている強擬素数テストがある. ここで $\mathbb{Z}$ を整数全体の集合, $\mathbb{N} = \{m \in \mathbb{Z} \mid m > 0\}$ として, その中で素数全体の部分集合を $\mathbb{P}$ と書く事にする. そして, 与えられた大きな奇数 n に対して, $e,\, m \in \mathbb{N}$ を $n - 1 = 2^e m$ で m が奇数となる様に定める. また更に, もし $b \in \mathbb{Z}$ が n と互いに素で, 即ち b と n の最大公約数 $\gcd(b, n) = 1$ を充し, しかも

$$b^m - 1,\, b^m + 1,\, b^{2m} + 1,\, \ldots,\, b^{2^{e-1}m} + 1$$

の内の何れか一つが n で割切れるなら n は b を底とする強擬素数であるという. もし $n \in \mathbb{P}$ なら, いつも n は b を底とする強擬素数である.

算法 1 (強擬素数テスト). 記号は上の通りとする.

入力 奇数 $n \in 1 + 2\mathbb{N}$, 及び反復回数 $k \in \mathbb{N}$.

出力 $n \notin \mathbb{P}$ という判定, 又は確率 $1 - 4^{-k}$ 以上で $n \in \mathbb{P}$ という判定.

手順 (i) e, m を計算.
(ii) 以下を k 回反復:
(a) ランダムに $b \in \mathbb{Z}$, $2 \leq b \leq n - 2$ を選ぶ.
(b) もし $\gcd(b, n) > 1$ なら $n \notin \mathbb{P}$ と判定して終了.
(c) もし n が b を底とする強擬素数でないなら $n \notin \mathbb{P}$ と判定して終了.
(d) もし k 回未満の実行なら反復継続, さもなくば反復終了.
(iii) 確率 $1 - 4^{-k}$ 以上で $n \in \mathbb{P}$ と判定して終了.

ここで反復回数 $k = \min\{n-2,\, \lfloor 2 \ln^2 n \rfloor\} - 1$ として, 手順 (ii–a) を『順次 $b = 2, \ldots, k+1$ とする.』とすれば, これは ERH の下で決定性アルゴリズムとなる. 一般に, 自然数 n の正の実数値関数 $F(n)$, $G(n)$ に対して $\lim_{n\to\infty} F(n)/G(n) = 0$ の時 $F(n) = o(G(n))$ と書く. すると強擬素数テスト (算法 1) の計算量は正確には ERH の下で

$$O(\lg^4 n \lg\lg n \lg\lg\lg n) = \lg^{4+o(1)} n$$

となる.

1.3. 素因数分解と公開鍵暗号系

まず PRIMES と素因数分解の計算量の比較をした上で, この様な数論アルゴリズムと呼ばれる問題は, 何故そんなに実用上の問題である暗号と結び付くのか, 簡単に説明しよう.

試し割算は素因数分解にも使えるが, 例えば $n = 400849296821720871996 37$ の分解には, 全部で 100106105561 回の試し割算が必要である. そこで様々の工夫がされてきており, それらの計算量は [Nak99, § 1] に簡単に紹介されている. 既知の最速の決定性アルゴリズム類群法の計算量は, ある種の ERH の下で

$$n^{1/5+o(1)}$$

である. 既知の最速の確率的アルゴリズム数体篩 **NFS** の計算量は準指数時間

$$\exp\left(\left(\left(\frac{92+26\sqrt{13}}{27}\right)^{1/3}+o(1)\right)\ \ln^{1/3} n\ \ln^{2/3}\ln n\right)$$

であろうと様々の理論的・実験的考察から予測されている. これらは PRIMES の最速の確率的で ERH の下では決定性のアルゴリズムの計算量 $\lg^{4+o(1)} n$ と比較して圧倒的に遅いのが, 十分に大きい n については明かである. 計算量の増大度を比較する為の説明なので少し正確さを欠くが, もし n が十進 100 桁程度なら, NFS や類群法による素因数分解は, 強擬素数テストによる PRIMES の, それぞれ 100000 倍や 10000000000 倍の計算量で, とても太刀打ちできない. この事実こそ情報セキュリティに重要な役割を果す現代の公開鍵暗号系の数学的基礎である.

例えば RSA 公開鍵暗号系 [Kob94, § IV.2] の真髄は, 受信者が相異る $p, q \in \mathbb{P}$ を選び, それから $n = p \times q$ を計算して, その n を用いた暗号文作成方法を公開する. しかも, その方法で作成された暗号文は p, q を知らなければ解読が殆ど不可能であるという性質を持っている. 送信者達は n だけ知っていれば受信者への暗号文が作成・送信できるが, これは n の素因数分解ができない限り受信者以外には p, q が判らないから, 送信途中で解読されず安全である. 巷に氾濫する情報の中には, 随分いいかげんなものも数多くある. 実際 PRIMES $\in$ P のニュースの直後にも, ネットワークで流れた記事の中に「暗号総崩れ」などというものが見られた. しかし, その安全性の根拠は

素因数分解は加減乗除 (及び素数生成) と比較すると計算が困難である

という事実にあるのだから, 今回の結果が直接に与える影響は理論的には皆無である. ちなみに加減乗除の計算量は (1) の様に多項式時間であり, むしろ PRIMES の計算が容易になれば, 必要な素数の生成が速くなるので好都合なくらいである. しかしながら § 3.2 でみるように, これ迄の所では今回のアルゴリズムは実用上は殆ど注目されていない.

2. アルゴリズム

ここでは提案された決定性 PRIMES アルゴリズムの具体的手順を与え, その計算量が多項式時間である事を説明し, そしてその正当性を証明しよう. この先, 特に § 2.3 以降では, 初等的な数論や代数の知識を仮定して話を進める.

2.1. 計算手順

まず基本的な着想と戦略を説明した後にアルゴリズムを述べる.

通常の様に $x, y \in \mathbb{Z}$ に対して $x - y$ が n で割切れる時に, 即ち $x - y = nz$ となる $z \in \mathbb{Z}$ が存在する時に, 合同式 $x \equiv y \pmod{n}$ を用いて表す. フェルマ小定理 [Kob94, Proposition I.2.3] によると, $b \in \mathbb{Z}$ に対して, $n \in \mathbb{P}$ であれば

$$b^n \equiv b \pmod{n}$$

となる. つまり, これは $n \in \mathbb{P}$ の必要条件を与えている. この必要条件を満足しない b があれば $n \notin \mathbb{P}$ と判定 (即ちフェルマテスト) ができる. これは, 以下の様にして, 変数 X の整数係数多項式の全体 $\mathbb{Z}[X]$ に, 一般化をする事ができる. いま $f, g, F \in \mathbb{Z}[X]$ に対して $f - g$ が (n, F) で割切れる時に, 即ち $f - g = nh_1 + Fh_2$ となる $h_1, h_2 \in \mathbb{Z}[X]$ が存在する時に, 合同式 $f \equiv g \pmod{(n, F)}$ を用いて表し, また特に $F = 0$ の場合は $f \equiv g \pmod{n}$ と書く事にする. この時, 二項係数が n で割切れるかどうか見る事により, 容易に証明できる拡張フェルマ小定理 [AKS02, § 2, Identity] は次の通りである. 一つ $b \in \mathbb{Z}$, $\gcd(b, n) = 1$, を固定する. この時, もし $n \in \mathbb{P}$ であれば

$$(X + b)^n \equiv X^n + b \pmod{n} \tag{4}$$

となり, 更にその時に限り $n \in \mathbb{P}$ である. つまり, これは $n \in \mathbb{P}$ の必要十分条件を与えている! しかし, この必要十分条件では, どうしても確認の為に左辺の多項式の n 個の係数を別々に計算しなくてはならないから, どんなに秀れた工夫をしても計算量は n に比例する以上にかかり, 指数時間とならざるを得ない. そこで, 今回のアルゴリズムで工夫された事のキーポイントは, 各 $b \in \mathbb{Z}$ に加えて, 別に各 $r \in \mathbb{N}$ に対して, もし $n \in \mathbb{P}$ であれば

$$(X + b)^n \equiv X^n + b \pmod{(n,\ X^r - 1)} \tag{5}$$

となる事を利用する点にある. これは必要条件しか与えないが, これを充さない r, b があれば $n \notin \mathbb{P}$ と判定できる. しかも計算に必要な多項式の次数が r より小さく, また係数は n より小さいので, もし r が十分に小さく取れれば, 後に補題 1 で見る様に高速に確認の計算ができる. 鍵となる問題は, どの程度の r, b に対して試せば $n \in \mathbb{P}$ の必要条件 (5) が, 同時に十分条件をも与えるかという点であった.

オリジナルなアルゴリズムの発表後様々な提案がされてきたが, ここでは説明の簡潔さを重視して [Ber03a, § 3] にあるものを, 若干を改良して紹介する. いま

$$\begin{aligned} A &= \{1\} \cup \{a^j \mid a,\ j \in \{2,\ 3,\ 4, \ldots\}\}, \\ \mathbb{P}_x &= \{p \in \mathbb{P} \mid p \le x\} \quad (x > 0), \\ N &= (n-1)(n^2-1)(n^3-1)\cdots\left(n^{4\lceil \lg^2 n \rceil - 1} - 1\right), \\ r &= \min\{p \in \mathbb{P} \mid N \not\equiv 0 \pmod{p}\} \end{aligned}$$

とする, 但し $\lceil x \rceil$ は $x > 0$ の小数点以下を切上げた値を表す.

算法 2 (拡張フェルマテスト XFT). 記号は上の通りとする.

入力 整数 $n \in \mathbb{N}$.

出力 $n \notin \mathbb{P}$ という判定, 又は $n \in \mathbb{P}$ という判定.

手順 (i) $n \in A$ なら $n \notin \mathbb{P}$ と判定して終了.
(ii) $\mathbb{P}_r$ を含む大きさの素数表を計算.
(iii) 以下を昇順に各 $p \in \mathbb{P}$ に対して, 反復:
(a) もし $n = p$ なら $n \in \mathbb{P}$ と判定して終了.
(b) もし $n \equiv 0 \pmod{p}$ なら $n \notin \mathbb{P}$ と判定して終了.
(c) もし $N \equiv 0 \pmod{p}$ なら反復継続, さもなくば $r = p$ として反復終了.
(iv) もし或 $b \in S = \{1, 2, \ldots, r\}$ で (5) が不成立なら $n \notin \mathbb{P}$ と判定して終了.
(v) さもなくば $n \in \mathbb{P}$ と判定して終了.

注意 **1.** これは n が大きい奇数でなくても, どんな自然数に対しても適用できる様になっている. もし $n = 1$ なら $N = 0$ だから $r = \infty$ だが, 実際には手順 (i) で終了するから問題ない. もし n が偶数なら $p = 2$ の場合に, それぞれ $n = 2$ の時は手順 (iii–a) で, また $n > 2$ の時は手順 (iii–b) で終了する. 手順 (iii–c) に実際に到達するのは奇数 $n > 2$ の時であり, しかも $p \leq 4\lceil \lg^2 n \rceil$ の場合はフェルマ小定理により $N \equiv 0 \pmod{p}$ だから, 反復継続される. 従って手順 (iv) が実際に実行されるのは $4\lceil \lg^2 n \rceil < r < n \not\equiv 0 \pmod{2}$ の時に限る.

注意 **2.** 手順 (ii) では $\mathbb{P}_r$ を作成すれば充分であるが, 実際には r の具体的上界があれば, そこ迄で良い. 次節の補題 2 にある評価に基けば, 素数表 $\mathbb{P}_{6.5\lceil \lg^2 n \rceil^{5/2}}$ を作成する事となる. この計算は n の入力毎に必要ではなく, 大きい素数表を一度求めておいて, それを何度も再利用すればよい.

注意 **3.** 手順 (iii–c) では, 実際に N を計算して p で割るのではなく, 合同式 $n^j \equiv 1 \pmod{p}$ $(j = 1, 2, \ldots, 4\lceil \lg^2 n \rceil - 1)$ を順次確認する.

このアルゴリズムの計算量は多項式時間である事を次に示す.

2.2. 計算量評価

拡張フェルマテスト XFT (算法 2) の多項式時間停止性を, 具体的に計算量を評価する事により証明する.

冪乗テスト (i) の部分は, ほぼ線型時間で終る. これ迄の最良の結果 [Ber98] によれば正確には

$$\lg^{1+O\left((\ln\ln\ln n/\ln\ln n)^{1/2}\right)} n$$

である. 以降の計算量は r の大きさに依存するが, その評価は後回しにして, 取り敢えず r と n の式で書く. 注意 2 を考慮すると, 素数表作成 (ii) の計算量は (3) により

$$O\left(\frac{r \ln r}{\ln\ln r}\right)$$

で評価される. 注意 3 によれば, 試し割算 (iii) 一回は, 高々 $O(\lg^2 n)$ 回の合同式 $\bmod q$, $q \leq r$, の演算であり, その計算量は (1) より $O(\lg r \lg\lg r \lg\lg\lg r \lg^2 n)$ だから, 全体としての計

算量は $O(\sharp\mathbb{P}_r \lg r \lg\lg r \lg\lg\lg r \lg^2 n)$ となる, 但し $\sharp\mathbb{P}_r$ は $\mathbb{P}_r$ の要素の個数, 即ち r 以下の素数の個数, を表す. これはまた $\sharp\mathbb{P}_r = O(r/\lg r)$ [CP01, Theorem 1.1.3] により

$$O(r \lg\lg r \lg\lg\lg r \lg^2 n)$$

で評価される. 主要な (iv) の部分については, 各 $b \in S$ に対して (5) のテストにかかる時間評価は, 次の補題 1 で与えられるから, 全体として $\sharp S = r$ 回のテストをする計算量は

$$O(r^2 \lg r \lg^2 n \lg\lg n \lg\lg\lg n) \tag{6}$$

で評価され, これがまた算法 2 の計算量でもある.

補題 1. 一回の (5) のテストに必要な計算量は

$$O(r \lg r \lg^2 n \lg\lg n \lg\lg\lg n)$$

である.

証明. 冪乗に反復平方法 [Kob94, Chapter I, § 3] を用いれば, 高々 $O(\lg n)$ 回の多項式乗算で充分で, 一回の多項式乗算は高速フーリエ変換による算法 [CP01, Chapter 9] 或は [Kam88] によると, 高々 $O(r \lg r)$ 回の合同式 $\bmod n$ の演算で済む. そして一回の合同式 $\bmod n$ の演算は (1) だから補題の評価が得られる. Q.E.D.

最後に r の上界を与える. 注意 1 により $4\lceil\lg^2 n\rceil < r < n \not\equiv 0 \pmod 2$ の時, 従って $n \geq 263$ の時に考えれば良い. ここで

$$M = \operatorname{lcm}\{n-1,\, n^2-1, n^3-1,\, \ldots,\, n^{4\lceil\lg^2 n\rceil - 1} - 1\}$$

とすると $r = \min\{p \in \mathbb{P} \mid M \not\equiv 0 \pmod p\}$ である.

補題 2. 上の仮定と記号の下で

$$r \leq \lceil \lg M \rceil < 6.5 \lceil \lg^2 n \rceil^{5/2}$$

である.

証明. まず k 以下の全ての素数 $p \in \mathbb{P}$ の積の下からの評価

$$\prod_{p \in \mathbb{P}_k} p > 2^k \quad (k \in \mathbb{Z},\, k > 677)$$

が, 例えば [RS62, 式 (3.14)] から直ちに示される事に注意しておこう. そこで $k = \lceil \lg M \rceil$ とすれば, 我々の考えている $n \geq 263$ の範囲では

$$k \geq \left\lceil \lg\left(n^{4\lceil\lg^2 n\rceil - 1} - 1\right)\right\rceil \geq 2083 > 677, \quad \prod_{p \in \mathbb{P}_k} p > 2^k \geq M$$

となり, 全ての $p \in \mathbb{P}_k$ が M を割切る事はないから, 補題の第一の評価が得られる. また $\ell = \lceil \lg^2 n \rceil$, $m = 4\ell - 1$ とすると M の定義の中の $n^{2s-1} - 1\,(1 \leq s \leq \lfloor (m+2)/4 \rfloor = \ell)$ は

不用である. 同様の事は $n^{4s-2}-1\,(1\le s\le \lfloor (m+4)/8\rfloor = \lfloor \ell/2\rfloor)$ 等々に関しても言える. 従って

$$\begin{aligned} M &< \prod_{s=1}^{\ell-1}(n^{4s}-1)\prod_{s=\lfloor \ell/2\rfloor+1}^{\ell}(n^{4s-2}-1)\prod_{s=\ell+1}^{2\ell}(n^{2s-1}-1) \\ &< \prod_{s=1}^{\ell-1} n^{4s}\prod_{s=\lfloor \ell/2\rfloor+1}^{\ell} n^{4s-2}\prod_{s=\ell+1}^{2\ell} n^{2s-1} \\ &= n^{7\ell^2-2\lfloor \ell/2\rfloor^2-2\ell} < n^{13\ell^2/2}. \end{aligned}$$

これから補題の第二の評価が得られる. Q.E.D.

以上により (6) から

定理 1. 拡張フェルマテスト XFT (算法 2) の計算量は

$$O(\lg^{12} n \lg^2 \lg n \lg\lg\lg n) = \lg^{12+o(1)} n$$

である.

が証明された.

注意 4. 証明に見る様に M の定義には無駄な要素が多く含まれているので, それを利用して良い上界が得られれば, 評価は更に改善できる.

2.3. 理論的根拠

ここからは, 初等数論と初等代数は既知として, 拡張フェルマテスト XFT (算法 2) が PRIMES の正しいアルゴリズムである事, 即ち部分正当性, を証明する.

部分正当性の理論的な根拠は次の定理である.

定理 2. *[Ber03a, Theorem 2.3]* 今 $n\in\mathbb{Z}$, $n>1$, に対し, $r\in\mathbb{N}$ と有限集合 $S\subseteq\mathbb{Z}$ が以下の条件を充すとする:

(i) $\gcd(n,r)=1$.
(ii) 全ての $q\in\mathbb{N}$, $\varphi(r)/m\equiv 0 \pmod q$ に対して

$$\binom{\sharp S+\varphi(r)-1}{\sharp S} \ge n^{2q\lfloor(\varphi(r)/q)^{1/2}\rfloor},$$

但し $\varphi(r)=\sharp(\mathbb{Z}/r)^\times$, $m=\sharp\langle n \bmod r\rangle$ である.
(iii) 全ての $a,b\in S$, $a>b$ に対して $\gcd(a-b,n)=1$.
(iv) 全ての $b\in S$ に対して (5) が成立.

この時, ある $p\in\mathbb{P}$ と $w\in\mathbb{N}$ があり $n=p^w$, 即ち n は素数冪である.

この定理を, ひとまず認めて適用し, 先に算法 2 の部分正当性を示す.

定理 3. 拡張フェルマテスト XFT (算法 2) は正しい PRIMES のアルゴリズムである.

証明. まず, 手順 (v) 以外の結論が正しい事は, 自明である. では, 手順 (v) の結論はどうであろうか. 手順 (iii) では p の小さい順に計算しているから, 手順 (iii–c) で求めた r 以下には n の素因数は無く, 定理 2 の条件 (i) は充される. また, 手順 (iv) で定めた S の相異る二要素の差は r より小さいから, 定理 2 の条件 (iii) も同様に充される. 更に, 注意 1 から $r > 2$ で, また

$$q \le m^{-1}\varphi(r), \quad m \ge 4\lceil \lg^2 n \rceil \ge (2\lg n)^2$$

だから

$$n^{2q\lfloor(\varphi(r)/q)^{1/2}\rfloor} \le n^{2m^{-1/2}\varphi(r)} \le n^{\varphi(r)/\lg n} = 2^{\varphi(r)} = 2^{r-1}$$

である. 他方で r に関する数学的帰納法で

$$\binom{\sharp S + \varphi(r) - 1}{\sharp S} = \binom{2r-2}{r} \ge 2^{r-1}$$

である. 従って, これを併せて定理 2 の条件 (ii) も充される. だから手順 (iv) を通過した n に関しては必然的に定理 2 の条件 (iv) も充し n は素数冪となる. 結論として, 手順 (i) により $n \in \mathbb{P}$ である. Q.E.D.

残されたのは定理 2 の証明である.

定理 2 の証明. 一つ $n \equiv 0 \pmod{p}$ となる $p \in \mathbb{P}$ を取る. そして

$$\begin{aligned} I &:= \left\{ p^i n^j \,\middle|\, i,\, j \in \{0\} \cup \mathbb{N} \right\} \subseteq \mathbb{N}, \\ J &:= \left\{ \prod_{b \in S} (X+b)^{k_b} \bmod p \,\middle|\, k_b \in \{0\} \cup \mathbb{N}\ (b \in S) \right\} \subseteq \mathbb{Z}[X], \\ K &:= \left\{ f(X^t) \,\middle|\, f \in J,\, t \in \mathbb{N},\, \gcd(t,\, r) = 1 \right\} \subseteq \mathbb{Z}[X] \end{aligned}$$

を考えると, 拡張フェルマ小定理 (4) と条件 (iv) により, 帰納的に

$$f(X^s) \equiv f(X)^s \pmod{(p,\, X^r - 1)} \quad (s \in I,\, f \in K)$$

が確められる. そこで $h \in \mathbb{Z}[X]$ を $\deg h = \sharp \langle p \bmod r \rangle$ で $h \bmod p \in (\mathbb{Z}/p)[X]$ が 1 の原始 r 乗根の最小多項式である様に一つ固定すると,

$$f(X^s) \equiv f(X)^s \pmod{(p,\, h)} \quad (s \in I,\, f \in K) \tag{7}$$

となる. 条件 (i) により, 乗法群 $(\mathbb{Z}/r)^\times$ の部分群

$$G := I \bmod r = \langle p \bmod r,\, n \bmod r \rangle, \quad q := \left((\mathbb{Z}/r)^\times : G\right),$$

を考え, その完全代表系の一つを

$$T \subseteq \mathbb{N}, \quad \sharp T = q, \quad (\mathbb{Z}/r)^\times / G = \{(t \bmod r)G \mid t \in T\}$$

とする. 更に (7) に注意して, 巡回群 $(\mathbb{Z}[X]/(p,\,h))^{\times}$ の部分群

$$H := K \bmod (p,\,h) = \left\langle X^t + b \bmod (p,\,h) \mid b \in S,\, t \in T \right\rangle$$

を考え, その位数を下から評価する. まず, 条件 (iii) により, 一次既約多項式 $X+b \bmod p\,(b \in S)$ は全て相異るから, J は $(\mathbb{Z}/p)[X]$ に単射で簡約される. 次に,

$$f,\, g \in L := \{0\} \cup \{e \in J \mid \deg e < \varphi(r)\}$$

については, もし $f(X^t) \equiv g(X^t) \pmod{(p,\,h)}$ $(\forall t \in \mathbb{N},\, \gcd(t,\,r) = 1)$ ならば, 次数 $\varphi(r)$ より小さい $f - g \bmod p \in (\mathbb{Z}/p)[X]$ が 1 の原始 r 乗根 $\varphi(r)$ 個全てを零点に持ち, これは $f - g \bmod p$ が $(\mathbb{Z}/p)[X]$ で零多項式である事を意味する. 以上を (7) に注意して纏めると,

$$\begin{aligned} f \neq g \quad &\Longleftrightarrow \quad f \not\equiv g \pmod{p} \\ &\Longleftrightarrow \quad f(X^t) \not\equiv g(X^t) \pmod{(p,\,h)} \quad (\exists t \in \mathbb{N},\, \gcd(t,\,r) = 1) \\ &\Longleftrightarrow \quad f(X^t) \not\equiv g(X^t) \pmod{(p,\,h)} \quad (\exists t \in T) \end{aligned}$$

となる. 即ち, 集合 L から q 組集合 $(\{0\} \cup H)^q$ への写像

$$L \ni f \longmapsto \big(f(X^t) \bmod (p,\,h)\big)_{t \in T} \in (\{0\} \cup H)^q$$

は単射となる. 従って, 条件 (ii) を考慮すると,

$$(1 + {}^{\sharp}H)^q \geq {}^{\sharp}L = 1 + \binom{{}^{\sharp}S + \varphi(r) - 1}{{}^{\sharp}S} > n^{2qc}, \quad c := \lfloor (\varphi(r)/q)^{1/2} \rfloor,$$

である. ここで, ディリクレ部屋割論法により $i,\, j,\, k,\, \ell \in \{0,\, 1, \ldots,\, c\}$ を取り,

$$(i,\, j) \neq (k,\, \ell), \quad u := p^i n^j \equiv v := p^k n^{\ell} \pmod{r}$$

とできる. この時 $1+|u-v| \leq n^{2c} < 1+{}^{\sharp}H$ であり, また (7) より $f^u \equiv f^v \pmod{(p,\,h)}$ $(f \in \{0\} \cup H)$ だから, これは変数 Y の多項式 $Y^u - Y^v$ が体 $\mathbb{Z}[X]/(p,\,h)$ に $1 + |u - v|$ 個より沢山の相異る零点を持つ事になり, 必然的に $u = v$, つまり $p^i n^j = p^k n^{\ell}$ でなくてはならない. もし $j = \ell$ なら $i = k$ なので $j \neq \ell$ となり, これは n が p の冪である事を意味する. Q.E.D.

3. 結果の意義

この節に関しては, かなり著者の私見がある事に注意しておく.

3.1. 理論的貢献

この結果の最大の特徴は, これ迄 $\mathrm{PRIMES} \in \mathrm{P}$ の証明を目指して払われていた努力の様な, リーマン予想, ヤコビ和, 楕円曲線等々の高等数学を用いていない所にある. それは有限体と, その上の多項式環の簡単な性質しか用いておらず, その理解には学部程度の代数学の基

礎知識で充分である事は, 前節迄に於て詳細に見て来た通りである. しかも原論文 [AKS02] も, その改訂版 [AKS03] も僅か 9 頁の長さで, 多くの人々にとり数時間で内容の正しさが確認できるものである. その理由は (5) という $n \in \mathbb{P}$ の必要条件を利用する事の発見にあった. 従って, 新たに高度な数学的手法が提示されてはいないので, その意味での今回の発見による貢献は余り無い. また既に確信されていた $\mathrm{PRIMES} \in \mathrm{P}$ が示されただけなので, それによる数学的理論の新たな展開が期待されるものでも無い. しかしながら長い数学の歴史の当初から存在した最も基本的な問題の一つが, ようやく無条件で厳密に解決された事実そのものの意義はやはり大きく, これにより Agrawal 教授は Clay 数学研究所から表彰されている.

この様に数学に直接理論的影響を与えるとは思われず, また § 3.2 でも見る様に現在迄は応用上の貢献も余り無い様であるが, それでも幾つかの重要な教訓が今回の発見から得られる. その内で, やはりコンピュータの数学研究に与えている効果との関連で二つ挙げておく. 一つは $n \in \mathbb{P}$ の必要十分条件である拡張フェルマ小定理 (4) を, 計算量を少なくするという観点から見直し, 全く当り前の必要条件 (5) に落した事である. これは効率的に計算するという立場で検討して初めて可能な事であり, その目標抜きには条件を悪くする事など思い付き難い. この様に既に考察され尽していると思われている数学的事実でも, コンピュータとの関連で再度研究してみる価値のある事は, まだ他にも多く存在するのではないかと思われる. 必要条件 (5) そのものも何か応用価値があるかもしれないが, それについては今後の課題であろう. もう一つは, 数学の研究スタイルに於るコンピュータネットワークの絶大な効果である. この結果は本原稿を書いている時点では未だ学術雑誌や研究集会報告には, オンラインのものを含めて, どこでも公式に発表されていない. しかしながら, その正しさは公開されて僅か数日で世界中で専門家達により確定され, その内容の改良が総掛りで行われた. これは情報社会の効果だけでなく, この発見の簡潔さにもよるものでもあろうが, それにしても十年前には考えられなかった. この様なスタイルは, これからの一つの中心的な共同研究のありかたとなるであろう.

3.2. 実用的価値

現在迄は, 実用上で生成する必要がある素数は, せいぜい数百桁である. これに関しては, 強擬素数テスト (算法 1) 等の従来の各種の素数判定アルゴリズムで充分である. 特に強擬素数テストの計算量は $\lg^{4+o(1)} n$ であり, 工業的には ERH は通常は正しいとして扱われているから問題はない. しかしながら拡張フェルマテスト XFT (算法 2) の計算量は定理 3 の $\lg^{12+o(1)} n$ であり, 遥かに及ばない. その後 § 4.1 に見る様に, アルゴリズムの改良がされて計算量は $\lg^{7.5+o(1)} n$ 迄下げられており, また予想としては $\lg^{6+o(1)} n$ 迄下げられると考えられているが, それでも強擬素数テストには及ばない. 理論的な評価だけではなく, その後に幾つかの計算機実験 [Mor02], [Ber03a] や実装 [CP03], [BP03] 等の報告がされているが, それらの報告も現状では今回の拡張フェルマテスト XFT の実用性に軍配を挙げていない.

暗号理論等の産業界の要請に応える点だけで考えなければ, 確率的なものであれ決定性のものであれ, より巨大な十進で数千桁の n に通用する, どんな未証明の仮説にも基かない, しかも実用的なアルゴリズムが求められる. その一つの代表は, 先に § 1.2 で触れたヤコビ和テスト [CL84] で, これは十進 2000 桁の n の素数判定を約 10^{14} クロックサイクルで実行している [Ber03a], [Mih98], [Mih99]. もう一つの代表は, やはり § 1.2 で触れた $\mathrm{PRIMES} \in \mathrm{ZPP}$ を

保証する方法の改良である 楕円曲線素数判定 **ECPP** [AM93] で, これは十進 2000 桁の n の素数判定を約 10^{15} クロックサイクルで実行している [Ber03a], [Mor02], [Mor03a], [Mor03b]. 残念ながら, ここでもやはり今回の拡張フェルマテスト XFT の実用性に, これ迄の所では, 軍配を挙げてはいない. しかしながら, この意味での高度な非産業的実用性の分野では, まだまだ理論的にも実用的にも検討すべき課題が山積していると思われる.

拡張フェルマテストの実装は, 実用的かどうかは別として, 比較的簡単に誰でもできるであろうが, その実際の例が [Gal], [Lus] 等にある.

4. 発展

余りにも進展が急速なので, この論説が印刷される頃には更なる展開があると思われる. ネットワーク等で充分に情報収集して欲しい.

4.1. アルゴリズムの改良

まず, 論文 [AKS02] の原著者達自身による, 最新の改訂版 [AKS03] の計算手順を証明抜きで書く.

集合 A は算法 2 の通りとして

$$\begin{aligned} N &= (n-1)(n^2-1)(n^3-1)\cdots\left(n^{4\lfloor \lg n \rfloor^2}-1\right), \\ r &= \min\{s \in \mathbb{N} \mid N \not\equiv 0 \pmod{s}\} \end{aligned}$$

とする.

算法 3 (拡張フェルマテスト XFT 改良版). 記号は上の通りとする.

入力 整数 $n \in \mathbb{N}$.

出力 $n \notin \mathbb{P}$ という判定, 又は $n \in \mathbb{P}$ という判定.

手順 (i) $n \in A$ なら $n \notin \mathbb{P}$ と判定して終了.
(ii) r を計算する.
(iii) もし或 $s \in \mathbb{N}$, $s \leq r$ で $1 < \gcd(s, n) < n$ なら $n \notin \mathbb{P}$ と判定して終了.
(iv) もし $n \leq r$ なら $n \in \mathbb{P}$ と判定して終了.
(v) もし或 $b \in S = \{1, 2, \ldots, \lfloor 2\varphi(r)^{1/2} \lg n \rfloor\}$ で (5) が不成立なら $n \notin \mathbb{P}$ と判定して終了.
(vi) さもなくば $n \in \mathbb{P}$ と判定して終了.

このアルゴリズムの計算量は

$$\lg^{7.5+o(1)} n$$

であり, 原始根に関するアルティン予想や, 特殊な形の素数 (Sophie Germain 素数) の集合 $\{p \in \mathbb{P} \mid 2p+1 \in \mathbb{P}\}$ の密度に関する予想に基いて

$$\lg^{6+o(1)} n$$

であろうと期待されている.

4.2. その他の展開

今回のアルゴリズムの発見者達以外による変種は幾つかあるが, ここではそれには触れないで他の二つの関連する展開を述べる.

一つは, 有限体上の多項式環の剰余環の単数群の部分群の大きさの下からの評価の改良である. 具体的には定理 2 の証明に現れた $\sharp H$ の評価を良くする事により (5) をテストする回数 $\sharp S$ を少くする事である. これを定式化して [Vol02a], [Vol02b], [Ber03c] では次の問題を考えて, 拡張フェルマテスト XFT を改良している.

> 要素の個数が q 個の有限体 $\mathbb{F}_q$ の部分集合 S に零点を持たない変数 X の二次以上の多項式 $h \in \mathbb{F}_q[X]$ に対して, 単数群 $(\mathbb{F}_q[X]/h)^\times$ の部分群 $H = \langle X - s \bmod h \mid s \in S \rangle$ を考え, その位数 $\sharp H$ を下から評価せよ.

この問題は, 別にグラフ理論や, 有限体上の射影直線の可換被覆の有理点の個数評価にも応用を持つ.

もう一つは, 多数の n の族に対して通用する拡張フェルマテスト XFT の改良 [Ber02] である. この方法と楕円曲線素数判定 ECPP を組合せたりする等の手段により, 何の未証明の仮説にも基かないで, 計算量が

$$\lg^{4+o(1)} n$$

となる事が証明できる様な, 確率的アルゴリズム [Che03], [Ber03b] が提案されている.

4.3. 予想と今後の課題

最後に, 本来のアルゴリズムに戻ると, 更に [AKS03] では, 次の予想

$$r \in \mathbb{P},\ \ n \not\equiv 0 \pmod r,\ \ b = -1 \text{ に対して } (5) \text{ が成立} \implies n \in \mathbb{P} \text{ 又は } n^2 \equiv 1 \pmod r$$

を提出して, しかも, もしこれが成立すれば計算量が

$$\lg^{3+o(1)} n$$

となる様な, 決定性アルゴリズムを提案している. これに関しては, すぐにでも実験的な計算に取組めるであろう. ただし, この予想は恐らく成立しないだろうという考察が [LP03] でされている.

いずれにしても, この愛すべき拡張フェルマテスト XFT は, その簡潔性の故に, これからも多くの波及効果を呼ぶ事が予見できる. 実際, 上記の予想に対する考察も今回の発見に動機付けられて開設されたサイト [AIM03] の一部である.

参考文献

[AH92] Leonard M. Adleman and Ming-Deh A. Huang. *Primality testing and abelian varieties over finite fields*, Vol. 1512 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992.

[AIM03] The American Institute of Mathematics. Future directions in algorithmic number theory. http://www.aimath.org/WWN/primesinp/, 2003.

[AKS02] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. http://www.cse. iitk.ac.in/news/primarity.pdf, 6 August 2002. manuscript.

[AKS03] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P (Ver. 3). http://www. cse.iitk.ac.in/news/primarity_v3.pdf, 1 March 2003. preprint.

[AM93] A. Oliver. L. Atkin and François Morain. Elliptic curves and primality proving. *Math. Comp.*, Vol. 61, No. 203, pp. 29–68, 1993.

[APS83] Leonard M. Adleman, Carl Pomerance, and Robert S.Rumely. On distinguishing prime numbers from composite numbers. *Ann. Math.*, Vol. 117, pp. 173–206, 1983.

[Ber98] Daniel J. Bernstein. Detecting perfect powers in essentially linear time. *Math. Comp.*, Vol. 67, No. 223, pp. 1253–1283, 1998.

[Ber02] Pedro Berrizbeitia. Sharpening PRIMES is in P for a large family of numbers. http: //arxiv.org/abs/math.NT/0211334, 20 November 2002. preprint.

[Ber03a] Daniel J. Bernstein. Proving primality after Agrawal-Kayal-Saxena. http://cr.yp.to /papers/aks.pdf, 25 January 2003. manuscript.

[Ber03b] Daniel J. Bernstein. Proving primality in essencially quartic random time. http://cr.yp.to /quartic.pdf, 17 April 2003. preprint.

[Ber03c] Daniel J. Bernstein. Sharper ABC-based bounds for congruent polynomials. http://cr. yp.to/ntheory/abccong-20031001.pdf, 1 October 2003. preprint (to appear in J. Th. Nombre Bordeaux).

[Boo98] Andrew R. Booker. The Nth Prime Page, online calculator. http://www.math.princeton. edu/~arbooker/nthprime.html, 1998.

[Bor03] Folkmar Bornemann. PRIMES is in P: a breakthrough for "Everyman". *Notices Amer. Math. Soc.*, Vol. 50, No. 5, pp. 545–552, 2003.

[BP03] Vibhor Bhatt and G.K. Patra. Analysis on implementation and its future improvements of AKS-class algorithms. http://www.cmmacs.ernet.in/cmmacs/Publications/resch_rep /rrcm0307.pdf, 14 August 2003. research report.

[BS96] Eric Bach and Jeffrey Shallit. *Algorithmic number theory. Vol. 1.* Foundations of Computing Series. MIT Press, Cambridge, MA, 1996. Efficient algorithms.

[Cab99] The Cabal Group. RSA155 announcement, the Proceedings of Eurocrypt 2000. ftp://ftp. cwi.nl/pub/herman/NFSrecords/RSA-155, August 1999.

[Cal02] Chris Caldwell. The Prime Pages (prime number research, records and resources). http: //primes.utm.edu/, 2002.

[Che03] Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS. http: //arxiv.org/abs/math.NT/0301179, 16 January 2003. preprint (to appear in Springer LNCS 2729, CRYPTO 2003).

[CL84] H. Cohen and H. W. Lenstra, Jr. Primality testing and Jacobi sums. *Math. Comp.*, Vol. 42, No. 165, pp. 297–330, 1984.

[Cox02] Paul Cox. PRIMES is in P. http://xocxoc.home.att.net/math/primes.htm, 2002.

[CP01] Richard Crandall and Carl Pomerance. *Prime numbers*. Springer-Verlag, New York, 2001.

[CP03] Richard Crandall and Jason Papadopoulos. On the implementation of AKS-class primality tests. http://developer.apple.com/hardware/ve/pdf/aks3.pdf, 2003. preprint.

[Gal] Yves Gallot. Implementation of the AKS algorithm (C++). http://perso.wanadoo.fr /yves.gallot/src/.

[Kam88] Michael Kaminski. An algorithm for polynomial multiplication that does not depend on the ring constants. *J. Algorithms*, Vol. 9, No. 1, pp. 137–147, 1988.

[KFM95] 黒澤馨, 藤岡淳, 宮地充子. 暗号理論への応用. 岡本龍明, 太田和夫 (編) , 暗号・ゼロ知識証明・数論, 第 III 部, 第 7 章. 共立出版, 1995.

[Kid03] 木田雅成. 素数判定の決定的多項式時間アルゴリズム. 代数的整数論とその周辺, No. 1324 in RIMS Kokyuroku, pp. 22–32, Kyoto, Japan, May 2003. 京都大学数理解析研究所, Kyoto University.

[KM95] 木田祐司, 牧野潔夫. 素数判定アルゴリズム. 岡本龍明, 太田和夫 (編) , 暗号・ゼロ知識証明・数論, 第 III 部, 第 2 章. 共立出版, 1995.

[Kob94] Neal Koblitz. *A course in number theory and cryptography*, Vol. 114 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Kob98] Neal Koblitz. *Algebraic aspects of cryptography*, Vol. 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[LP03] Hendric W. Lenstra and Carl Pomerance. Remarks on Agrawal's conjecture. http://www. aimath.org/WWN/primesinp/articles/html/50a/, 2003.

[Lus] Peter Luschny. AKS deterministic polynomial time primality test (Maple). http://www. luschny.de/math/primes/aks.txt.

[Mih98] Preda Mihăilescu. Cyclotomy primality proving—recent developments. In *Algorithmic number theory (Portland, OR, 1998)*, Vol. 1423 of *Lecture Notes in Comput. Sci.*, pp. 95–110. Springer, Berlin, 1998.

[Mih99] Preda Mihăilescu. Recent developments in primality proving. *Math. Comput. Simulation*, Vol. 49, No. 3, pp. 193–204, 1999.

[Mil76] Gary L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. System Sci.*, Vol. 13, No. 3, pp. 300–317, 1976. Working papers presented at the ACM-SIGACT Symposium on the Theory of Computing (Albuquerque, N.M., 1975).

[Mor02] François Morain. Primalité théorique et primalité pratique ou AKS vs. ECPP. http://www.lix.polytechnique.fr/Labo/Francois.Morain/aks-f.pdf, 4 October 2002. manuscript.

[Mor03a] François Morain. A new record for ECPP. http://www.lix.polytechnique.fr/Labo/Francois.Morain/Primes/x2177y580.annonce, 6 June 2003.

[Mor03b] François Morain. A new record for ECPP. http://www.lix.polytechnique.fr/Labo/Francois.Morain/Primes/0307.annonce, 16 July 2003.

[Nak96] 中村憲. 最近の計算機代数の理論と応用. 数学, Vol. 48, pp. 12–21, 1996. 論説.

[Nak99] Ken Nakamula. *A Survey on the Number Field Sieve*, pp. 263–272. Kluwer Academic Publishers, 1999.

[Nak03] 中村憲. 代数的計算数論の現状. 日本応用数理学会 論文誌, Vol. 13, No. 2, pp. 305 – 320, 2003.

[Nis02] 西野哲朗. P = NP ? 問題. 数学, Vol. 54, No. 1, pp. 86–99, 2002. 論説.

[OO95] 岡本龍明, 太田和夫. 暗号理論. 岡本龍明, 太田和夫 (編), 暗号・ゼロ知識証明・数論, 第 I 部. 共立出版, 1995.

[Rab80] Michael O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, Vol. 12, No. 1, pp. 128–138, 1980.

[RS62] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, Vol. 6, pp. 64–94, 1962.

[Sti02] Anton Stiglic. The PRIMES is in P little FAQ. http://crypto.cs.mgill.ca/~stiglic /PRIMES_P_FAQ.html, 18 October 2002.

[Vol02a] José Felipe Voloch. Improvements to AKS. ftp://ftp.ma.utexas.edu/pub/papers /voloch/aks.pdf, 28 August 2002. manuscript.

[Vol02b] José Felipe Voloch. On some subgroups of the multiplicative group of finite rings. ftp: //ftp.ma.utexas.edu/pub/papers/voloch/gaks2.pdf, 25 September 2002. preprint (to appear in J. Th. Nombre Bordeaux).