UNIVERSITÀ DEGLI STUDI DI ROMA TRE
FACOLTÀ DI SCIENZE M.F.N.

Sintesi della Tesi di Laurea in Matematica
di

Valeria D'Orazio

L'algoritmo di Agrawal, Kayal e Saxena

Relatore

Prof. Francesco Pappalardi

ANNO ACCADEMICO 2002 - 2003
Ottobre 2003

Classificazione AMS : 11Y5, 94A60
Parole Chiave : Test di primalità - Teoria computazionale dei numeri.

Questa tesi si occupa dell'algoritmo di Agrawal, Kayal e Saxena, con il quale il problema della "primalità" si può risolvere con un algoritmo deterministico polinomiale. Infatti, in un tempo che cresce solo in modo polinomiale rispetto al numero di cifre di n, l'algoritmo AKS dichiara correttamente se un numero intero n è primo o composto.

Nel primo capitolo è stata presentata una panoramica generale sui test di primalità e si è deciso di seguire il testo di Carl Pomerance [CP01].

Si è iniziato con i test più semplici e intuitivi: il metodo delle divisioni per prova e il "crivello di Eratostene". Questi algoritmi, però, si è visto che richiedono un tempo esponenziale nella misura dell'input n.

Sono stati discussi, allora, metodi che riconoscono velocemente numeri composti. Per tali test, però, si sa solo che, se dopo più tentativi un numero non è dichiarato composto, allora, con alta probabilità, è primo. Queste non sono, quindi, dimostrazioni di primalità.

Dal fatto che il Piccolo Teorema di Fermat (Teorema 1.3.1) non si inverte, sono definiti gli pseudoprimi di Fermat:

Definizione 1.3.2. Un numero composto dispari n è uno *pseudoprimo di Fermat* in base a se vale l'equazione $a^n \equiv a \pmod{n}$.

Gli pseudoprimi, nonostante siano rari rispetto ai primi (Teorema 1.3.3), sono infiniti (Teorema 1.3.5) per ogni base $a \geq 2$. Da ciò segue che non è possibile ottenere un test di primalità, nemmeno probabilistico, che utilizzi la nozione di pseudoprimo di Fermat, per determinare correttamente se un numero è primo.

Definizione 1.3.7. Un intero composto dispari n per cui $a^n \equiv a \pmod{n}$ per ogni intero a è un *numero di Carmichael.*

I numeri di Carmichael, come $561 = 3 \cdot 7 \cdot 11$, sono molto rari ma infiniti [AGP94], per cui la condizione $a^n \equiv a \pmod{n}$ è inutile come regola per riconoscere i primi.

A differenza del Piccolo Teorema di Fermat, il Teorema di Wilson dà una condizione sia necessaria che sufficiente per la primalità.

Teorema 1.3.9 (Teorema di Wilson). *Sia n un numero intero positivo. Allora*

$$n \text{ è primo se e solo se } (n-1)! \equiv -1 \pmod{n}.$$

Il problema di verificare la primalità con questo test è che tale verifica richiede un tempo esponenziale $\mathcal{O}(n^2 \log^2 n)$.

E' stata illustrata una nozione più raffinata di quella di pseudoprimo di Fermat, rispetto alla quale non esistono casi eccezionali come i numeri di Carmichael. Per introdurre tale notazione si utilizza il Teorema di Eulero.

Teorema 1.3.12 (Teorema di Eulero). *Siano $p \geq 3$ primo e $a \in \mathbb{Z}$, allora*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Definizione 1.3.13. Sia n un intero composto dispari e sia $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Allora n si dice *pseudoprimo di Eulero* in base a se

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n},$$

dove $\left(\frac{a}{n}\right)$ indica il simbolo di Jacobi.

Dal Teorema di Eulero si deduce il test probabilstico di primalità detto di *Solovay-Strassen*, del 1977. Se si trova una base a per cui la congruenza $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ non è verificata, allora n non è pseudoprimo di Eulero rispetto ad a e quindi non è primo. In totale, il test richiede un tempo $\mathcal{O}(\log^3 n)$.

E' stata data, poi, la definizione di pseudoprimo forte, che è ispirata dalla seguente proprietà dei numeri primi.

Teorema 1.3.16. *Sia p è un primo dispari e $p-1 = 2^s t$, dove t è dispari. Se $p \nmid a$ allora*

$$a^t \equiv 1 \pmod{p} \qquad o \qquad a^{2^i t} \equiv -1 \pmod{p} \qquad 0 \leq i \leq s-1 \tag{1.1}$$

La conclusione del precedente enunciato non vale solo per i primi. infatti, se $n = 91 = 7 \cdot 13$, si vede che (1.1) vale per $a = 10$.

Definizione 1.3.18. Un numero composto e dispari n è uno *pseudoprimo forte* in base a se, scritto $n - 1 = 2^s t$ con t dispari, vale (1.1).

Si è mostrato (Teorema 1.3.22) che, se n è composto, almeno $\frac{3}{4}$ di tutti gli interi a in $[1, n-1]$ sono basi per cui n non è pseudoprimo forte. Da ciò è nato l'algoritmo probabilistico di *Miller-Rabin* del 1980, che verifica la (1.1) e richiede un tempo $\mathcal{O}(\log^3 n)$ per ogni iterazione. La probabilità che il test fallisca per k iterazioni indipendenti è minore o uguale di $\frac{1}{4^k}$. Quindi, a patto di considerare un numero di iterazioni adeguato, è ragionevole concludere che, in caso di successo, n è primo.

E' stato presentato, in seguito, un test di primalità basato sui numeri di Fibonacci (Definizione 1.3.24). Tale test è ispirato alla seguente proprietà dei numeri primi.

Teorema 1.3.25. *Se p è primo, allora*

$$F_{p-\left(\frac{5}{p}\right)} \equiv 0 \pmod{p}. \tag{1.2}$$

Non vale il viceversa, infatti $n = 323 = 17 \cdot 19$ verifica $F_{n-\left(\frac{5}{n}\right)} \equiv 0 \pmod{n}$.

Definizione 1.3.26. Un numero composto n è uno *pseudoprimo di Fibonacci* se vale $F_{n-\left(\frac{5}{n}\right)} \equiv 0 \pmod{n}$.

In generale se $f(x) = x^2 - ax + b \in \mathbb{Z}[x]$, dove a e b sono interi per cui $\Delta = a^2 - 4b$ non è un quadrato, si possono definire le successioni di Lucas

$$U_j = U_j(a,b) = \frac{x^j - (a-x)^j}{x - (a-x)} \pmod{f(x)} \tag{1.3}$$

$$V_j = V_j(a,b) = x^j + (a-x)^j \pmod{f(x)}.$$

Per induzione si ha $U_0 = 0; U_1 = 1; \ldots; U_j = aU_{j-1} - bU_{j-2}$, da cui $U_j \in \mathbb{Z}$. Quindi, se si considera $f(x) = x^2 - x - 1$, gli $U_j(1, -1)$ sono proprio i numeri di Fibonacci F_j.

Teorema 1.3.27. *Siano a, b, Δ interi tali che $\Delta = a^2 - 4b$ non è un quadrato e sia (U_j) una successione definita come in* (1.3). *Se p è un primo e $MCD(p, 2b\Delta) = 1$, allora*

$$U_{p-\left(\frac{\Delta}{p}\right)} \equiv 0 \pmod p. \tag{1.4}$$

Quindi vengono definiti gli pseudoprimi di Lucas e di Frobenius.

Definizione 1.3.28. Un numero composto n con $MCD(n, 2b\Delta) = 1$ è uno *pseudoprimo di Lucas* rispetto a $x^2 - ax + b$ se

$$U_{n-\left(\frac{\Delta}{n}\right)} \equiv 0 \pmod n.$$

Definizione 1.3.29. Siano a, b, Δ interi con $\Delta = a^2 - 4b$ che non è un quadrato. Un numero composto n con $MCD(n, 2b\Delta) = 1$ è uno *pseudoprimo di Frobenius* rispetto a $f(x) = x^2 - ax + b$ se

$$x^n \equiv \begin{cases} a - x \pmod{(f(x), n)} & \text{quando } \left(\frac{\Delta}{n}\right) = -1 \\ x \pmod{(f(x), n)} & \text{quando } \left(\frac{\Delta}{n}\right) = 1 \end{cases} \tag{1.5}$$

E' stato provato da Grantham che per ogni polinomio irriducibile $x^2 - ax + b$ esistono infiniti pseudoprimi di Frobenius [Gra01]. Una delle conseguenze (Teorema 1.3.30) è che esistono, per ogni a,b dati, con Δ che non è un quadrato, infiniti pseudoprimi di Lucas.

In analogia agli pseudoprimi forti, sono stati definiti gli pseudoprimi forti di Lucas (Definizione 1.3.31) e di Frobenius (Definizione 1.3.32). Un test di pseudoprimo forte di Frobenius può fallire, riconoscendo un numero composto come primo, con una probabilità $1/7710$ (Teorema 1.3.33), molto più bassa di $\frac{1}{4}$, ottenuta con il test di Miller-Rabin.

Nel secondo Capitolo è stata presentata la Teoria delle dimostrazioni di primalità, costruendo degli esempi numerici, la cui dimensione è di rilevanza crittografica, per ciascuno dei test illustrati. Lucas, nel 1891, notò che dal Piccolo Teorema di Fermat segue che, se è possibile fattorizzare $p - 1$, allora è facile dimostrare che p è primo.

Teorema 2.1.1 (Lucas). *Se* $n \in \mathbb{N}$ *e* $a \in (\mathbb{Z}/n\mathbb{Z})$ *è tale che*

$$\begin{aligned} &a^{n-1} \equiv 1 \pmod n \\ &ma \quad a^{(n-1)/q} \not\equiv 1 \pmod n \text{ per ogni primo } q \mid n-1, \end{aligned} \tag{2.6}$$

allora n *è primo.*

Questo è un test facile da utilizzare se n è un numero di Fermat $F_n = 2^{2^n} + 1$. Infatti, un corollario del Teorema di Lucas è il Test deterministico di Pepin.

Teorema 2.1.2 (Test di Pepin 1877). *Per* $k \geq 1$*, il numero* $F_k = 2^{2^k} + 1$ *è primo se e solo se* $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.

Si è cercato, poi, un metodo per ottenere "dimostrazioni di primalità" per p fattorizzando solo parzialmente $n - 1$.

Teorema 2.1.3 (Pocklington 1914). *Siano* n *e* a *interi tali che*

$$n - 1 = FR \tag{2.7}$$

$$a^{n-1} \equiv 1 \pmod n \quad e \quad MCD(a^{(n-1)/q} - 1, n) = 1 \text{ per ogni primo } q \mid F, \tag{2.8}$$

allora ogni fattore primo di n *è congruente ad* $1 \pmod F$.

Corollario 2.1.4. *Se valgono* (2.7) *e* (2.8) *e* $F \geq \sqrt{n}$*, allora* n *è primo.*

Il Test di Pocklington è applicabile se è conosciuta la fattorizzazione in primi di F.

Nel Teorema 2.1.5 si è mostrato come il valore di F può essere abbassato.

E' stata, poi, analizzata la nozione di "*certificato succinto* di primalità", basato su un'iterazione del test $p - 1$ di Lucas per provare che ogni $q \mid p - 1$ è, a sua volta, primo (Teorema 2.1.6).

Esiste anche un test "$n + 1$" facilmente verificabile dai numeri di Mersenne $M_n = 2^n - 1$. In analogia con il Teorema 2.1.3 di Pocklington, si ha:

Teorema 2.2.4 (Morrison). *[Mor75] Siano $f = x^2 - ax + b$ e $\Delta = a^2 - 4b$, e sia n un intero positivo con $MCD(n, 2b) = 1$ e $(\frac{\Delta}{n}) = -1$. Se F è un divisore di $n + 1$ e*

$$U_{n+1} \equiv 0 \pmod{n}, \quad MCD(U_{(n+1)/q}, n) = 1 \text{ per ogni primo } q \mid F, \tag{2.9}$$

allora ogni primo $p \mid n$ verifica $p \equiv (\frac{\Delta}{p}) \pmod{F}$. In particolare, se $F > \sqrt{n} + 1$ e valgono le ipotesi (2.9), allora n è primo.

E' possibile, inoltre, descrivere un test di primalità analogo, usando la successione (V_k) (Teorema 2.2.6). Si è dimostrato, inoltre, che si può richiedere anche una fattorizzazione solo parziale di $p + 1$ (Teorema 2.2.8).

Infine, si è visto come, combinando insieme le fattorizzazioni parziali di $p - 1$ e di $p + 1$, si può provare che p è primo (Teorema 2.2.9).

Nel Capitolo tre, è stato presentato l'algoritmo AKS, nella sua forma originaria dell'Agosto 2002 [AKS02].
Il test è basato sulla seguente identità sui numeri primi.

Teorema 3.1.1. *Siano a, n interi con $MCD(a, n) = 1$. Allora n è primo se e solo se*

$$(x - a)^n \equiv (x^n - a) \pmod{n}. \tag{3.10}$$

Controllare quando la (3.10) è verificata, però, richiede un tempo $\mathcal{O}(n)$ esponenziale. L'idea è stata, allora, quella di controllare la (3.10) modulo un polinomio opportuno $x^r - 1$.

Quindi, un'iterazione dell'algoritmo controllerà se vale la congruenza

$$(x - a)^n \equiv (x^n - a) \pmod{x^r - 1, n}. \tag{3.11}$$

Tuttavia, alcuni numeri composti n soddisfano la (3.11) per "pochi" valori di (a, r). Si è mostrato, però, seguendo l'articolo di Agrawal, Kayal e Saxena [AKS02], che, per appropriati valori di r, se l'equazione (3.11) è soddisfatta per alcuni valori di a, allora n deve essere una potenza di un primo (Lemma

3.3.7). La verifica della congruenza (3.11) richiede un tempo $\mathcal{O}(r^2 \log^3 n)$, se si usa l'algoritmo dei quadrati successivi per calcolare le potenze.

In [AKS02] tutte le analisi degli algoritmi sono state calcolate con la matematica veloce della Fast Fourier Transform. Si è scelto di tradurre tutte le analisi utilizzando le stime per la complessità della matematica classica ("naive").

<u>`ALGORITMO AKS`</u>

`Input un intero` $n > 1$.

`se (`n `è della forma` a^b, $b > 1$`) output` $COMPOSTO$;
$r = 2$;
`while (`$r < n$`){`
  `se (`$MCD(n, r) \neq 1$`) output` $COMPOSTO$;
  `se (`r `è primo)`
    `sia` q `il più grande fattore primo di` $r - 1$;
    `se (`$q \geq 4\sqrt{r}\log n$`) e (`$n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$`)`
      `ESCI DAL CICLO while;`
  $r \longleftarrow r + 1$;
`}`
$for \quad a = 1 \quad to \quad 2\sqrt{r}\log n$
  `se (` $(x - a)^n \not\equiv (x^n - a) \pmod{x^r - 1, n}$ `output` $COMPOSTO$;
`output` $PRIMO$.

Nell'algoritmo ci sono due cicli: prima un *while* e poi un for; nel primo si cerca un numero primo r tale che $r - 1$ ha un fattore primo $q \geq 4\sqrt{r}\log n$, e che $q \mid o_r(n)$, dove $o_r(n)$ è l'ordine di r mod n. Tale r esiste sempre come conseguenza del Teorema di Fouvry [Fou85], ed è dell'ordine $\mathcal{O}(\log^6 n)$ (Teorema 3.3.2).

Lemma 3.3.3. *Se n è primo, allora l'algoritmo produce output $PRIMO$.*

Il lemma si verifica facilmente. Per mostrare il "viceversa", cioè che se n è composto l'algoritmo produce output $COMPOSTO$, sono necessari alcuni lemmi supplementari (Lemma 3.3.4, Lemma 3.3.5).

Se l'algoritmo si imbatte in un fattore proprio di n al passo 4, allora l'output $COMPOSTO$. Se non succede niente di quanto detto sopra, l'algoritmo entra nel ciclo for.

Si nota che $(x-a)^n \equiv (x^n - a) \pmod{x^r - 1, n}$ implica che $(x-a)^n \equiv (x^n - a) \pmod{h(x), p}$, dove $h(x)$ è un fattore irriducibile di $\frac{x^r-1}{x-1}$ su $\mathbb{F}_p$. L'insieme degli ℓ binomi $(x + a)$, per $1 \leq a \leq \ell$ genera un gruppo ciclico, generato da $g(x)$, in questo campo di cardinalità maggiore di $n^{2\sqrt{r}}$ (Lemma 3.3.4).
Si definisce un insieme dei numeri, relativo a $g(x)$, chiuso sotto la moltiplicazione (Lemma 3.3.5):

$$I_{g(x)} = \{m \mid g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}.$$

Allora, vale il seguente lemma:

Lemma 3.3.6. *Sia o_g l'ordine di $g(x)$ in $\mathbb{F}_p[x]/(h(x))$. Siano $m_1, m_2 \in I_{g(x)}$. Allora, $m_1 \equiv m_2 \pmod{r}$ implica che $m_1 \equiv m_2 \pmod{o_g}$.*

Infine, la dimostrazione che se n è composto, l'algoritmo produce come output $COMPOSTO$, è una conseguenza del Lemma 3.3.6 (Lemma 3.3.7).

La complessità dell'algoritmo utilizzando l'aritmetica "naive", cioè quella che richiede un tempo quadratico per moltiplicare gli interi, è $\mathcal{O}(\log^{19} n)$ (Teorema 3.4.1).

Tuttavia, l'algoritmo, probabilmente, è molto più veloce, cioè ha una complessità $\mathcal{O}(\log^9 n)$ (Lemma 3.4.4). Infatti, ciò è vero se vale la Congettura 3.4.3 sulla densità dei primi r di *Sophie Germain*, per cui il più grande fattore primo di $r - 1$ è $\frac{r-1}{2}$ ed è primo. Inoltre se vale la congettura seguente

Congettura 3.5.1. *Se $r \nmid n$, e se*

$$(x - 1)^n \equiv (x^n - 1) \pmod{x^r - 1, n},$$

allora o n è primo, o $n^2 \equiv 1 \pmod{r}$, segue un algoritmo di complessità $\mathcal{O}(\log^{6.5} n)$.

Nel Marzo 2003, sulla base di miglioramenti dovuti a Lenstra, l'algoritmo è stato modificato in modo da non dover ricorrere, nella verifica della sua correttezza, al Teorema di Fouvry che è difficile da dimostrare. Lo studio del nuovo lavoro è l'argomento del Capitolo 4.

<u>ALGORITMO AKS CON IL MIGLIORAMENTO DI LENSTRA</u>

Input un intero $n > 1$.

1. se (n è della forma a^b, $b > 1$) output $COMPOSTO$;
2. Cerca il più piccolo r tale che $o_r(n) > 4\log^2 n$;
3. Se $1 < (a, n) < n$ per qualche $a \leq r$, output $COMPOSTO$;
4. Se $n \leq r$, output $PRIMO$;
5. For $a = 1$ to $\left\lfloor 2\sqrt{\varphi(r)}\log n \right\rfloor$
6. se $((x + a)^n \not\equiv x^n + a \pmod{x^r - 1, n})$, output $COMPOSTO$;
7. altrimenti output $PRIMO$.

E' stato dimostato che esiste un $r = \mathcal{O}(\log^5 n)$, tale che $o_r(n) > 4\log^2 n$ (Lemma 4.3.2).

Come nell'algoritmo originario è evidente che se n è primo, allora c'è output $PRIMO$.

Per ottenere l'implicazione inversa, si è fatto uso di più lemmi (Lemma 4.3.4, Lemma 4.3.5, Lemma 4.3.6, Lemma 4.3.7, Lemma 4.3.8). Se l'algoritmo produce output $PRIMO$ al Passo 4, allora n deve essere primo, altrimenti al Passo 3 troverebbe un fattore non banale di n.
Così, l'unico caso che resta da dimostrare è quello in cui l'algoritmo produce output $PRIMO$ al Passo 7.

Ancora utilizzando la nozione di numeri introspettivi (Definizione 4.3.3), è stato mostrato come l'insieme Γ generato dagli ℓ binomi $(x+a)$ nel campo $\mathbb{F} = \mathbb{F}_p[x]/(h(x))$, dove $h(x)$ è un fattore di $\frac{x^r-1}{x-1}$ irriducibile su $\mathbb{F}_p$, ha cardinalità

maggiore o uguale a $\frac{1}{2}n^{2\sqrt{t}}$ (Lemma 4.3.6, Lemma 4.3.8). Infine, si è visto come, nel caso in cui n non è una potenza di p, la cardinalità di Γ è minore di $\frac{1}{2}n^{2\sqrt{t}}$ (Lemma 4.3.7).
Da ciò segue che, avendo un output $PRIMO$, si ha che n è primo (Lemma 4.3.8).

La complessità "naive" del nuovo algoritmo è $\mathcal{O}(\log^{16.5} n)$ (Teorema 4.4.1).

Inoltre, se valgono le congetture di Artin (Congettura 4.4.2) sul numero dei primi $r \leq m$, per cui $o_r(n) = r - 1$, e quella sulla densità dei primi di Sophie-Germain (Congettura 4.4.3) , l'algoritmo richiede un tempo $\mathcal{O}(\log^9 n)$.

Utilizzando il Teorema di Fouvry [Fou85], si dimostra che la complessità dell'algoritmo è $\mathcal{O}(\log^{11.5} n)$ (Teorema 4.4.4).

Il miglior risultato finora ottenuto è dovuto a Lenstra e Pomerance [LP03]. I due matematici, utilizzando i polinomi minimi dei periodi Gaussiani, hanno portato la complessità dell'algoritmo AKS a $\mathcal{O}(\log^9 n)$, non utilizzando né il Teorema di Fouvry né altre congetture.

Il risultato di M. Agrawal, N. Kayal e N. Saxena, ha grande importanza teorica. Tuttavia non sembra, per il momento, avere grande interesse operativo in quanto i tempi di applicazione, anche con le possibili riduzioni dovute ad analisi particolari, sono notevoli.

I test probabilistici di primalità forniscono ancora risultati assolutamente accettabili per le applicazioni in situazioni molto generali; richiedono tempi di elaborazione trascurabili e nelle situazioni reali di applicazione dei numeri primi, sono quelli da prediligere.

Bibliografia

[AGP94] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math. (2)*, 139(3):703–722, 1994.

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

[AKS02] M. Agrawal, N. Kayal, and N. Saxena. Primes is in p. Available from http://www.cse.iitk.ac.in/news/primality.html, 2002.

[AL86] L. M. Adleman and H. W. Lenstra. Finding irreducible polynomials over finite fields. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 350–355. ACM Press, 1986.

[Apo97] T.M. Apostol. *Introduction to Analityc Number Teory*. Springer-Verlag, 1997.

[APR83] Leonard M. Adleman, Carl Pomerance, and Robert S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math. (2)*, 117(1):173–206, 1983.

[Atk86] A. O. L. Atkin. Lecture notes of a conference. August 1986.

[Ber02] P. Berrizbeitia. Sharpening 'primes is in p' for a large family of numbers. Available from ftp://ftp.ma.utexas.edu/pub/papers/voloch/aks.pdf, 2002.

[Ber03] D. Bernstein. Proving primality after agrawal-kayal-saxena. Available from http://cr.yp.to/papers.html # aks, 2003.

[BH96] R. C. Baker and G. Harman. The Brun-Titchmarsh theorem on average. In *Proceedings of a conference in Honor of Heini Halberstam, Vol. 1*, pages 39–103. 1996.

[BLS75] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. 29:620–647, 1975.

[BWJ80] Robert Baillie and Samuel S. Wagstaff Jr. Lucas pseudoprimes. *Math. Comp.*, 35(152):1391–1417, 1980.

[Che03] Q. Cheng. Primality proving via one round of ECPP and one iteration in AKS. Available from http://www.cs.ou.edu/ qcheng/, 2003.

[CL84] H. Choen and A.K. Lenstra. Primality testing and jacobi sums. *Math. Comp.*, 42:297–330, 1984.

[CL87] H. Choen and A.K. Lenstra. Implementation of a new primality test. *Math. Comp.*, 48:103–121, 1987.

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

[CP03] R. Crandall and J. Papadopoulos. On the implementation of aks-class primality tests. Preprint, 15 Mar 2003.

[Fou85] Étienne Fouvry. Théorème de Brun-Titchmarsh: application au théorème de Fermat. *Invent. Math.*, 79(2):383–407, 1985.

[GK86] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *18th Annual Symposium on Foundations of Computer Science*, pages 316–329, Berkeley, California, May 1986. IEEE.

[Gol69] Morris Goldfeld. On the number of primes p for which $p + a$ has a large prime factor. *Mathematika*, 16:23–27, 1969.

[Gra98] Jon Grantham. A probable prime test with high confidence. *J. Number Theory*, 72(1):32–47, 1998.

[Gra01] Jon Grantham. Frobenius pseudoprimes. *Math. Comp.*, 70(234):873–891, 2001.

[HL22] G. H. Hardy and J. E. Littlewood. Some problems of Partitio Numerorum III: On the expression of a number as a sum of primes. *Acta Mathematica*, 44:1–70, 1922.

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

[KS02a] N. Kayal and N. Saxena. Towards a deterministic polynomial time primality test. Available from http://cse.iitk.ac.in/research/bpt2002/primality.html, 2002.

[KS02b] Neeray Kayal and Nitin Saxena. Towards a deterministic polynomial-time test. *Technical report, IIT Kanpur*, 2002.

[Leh30] D. N. Lehmer. An extended theory of Lucas' functions. 31:419–448, 1930. Reprinted in *Selected Papers*, D. McCarthy editor, v. **1**, Ch. Babbage Res. Center, St. Pierre, Manitoba Canada, pp. 11-48 (1981).

[Len02] H. W. Jr. Lenstra. Primality testing with cyclotomic rings. Preprint, 14 Aug 2002.

[Li97] Xian-Jin Li. The positivity of a sequence of numbers and the Riemann hypothesis. *J. Number Theory*, 65(2):325–333, 1997.

[LN86] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, 1986.

[LP03] Jr Lenstra, H. W. and C. Pomerance. Primality testing with gaussian periods. Manuscript, Mar 2003.

[MA03] P. Mihăilescu and R. M. Avanzi. Efficient 'quasi'-deterministic primality test improving aks.draft. Available from www-math.uni-paderborn.de/ preda/papers/myaks1.ps, 23 Apr 2003.

[Mil76] Gary L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. System Sci.*, 13(3):300–317, 1976. Working papers presented at the ACM-SIGACT Symposium on the Theory of Computing (Albuquerque, N.M., 1975).

[Mor75] M. Morrison. A note on primality testing using Lucas sequences. 29:181–182, 1975.

[Nai82a] M. Nair. A new method in elementary prime number theory. *J. London Math. Soc. (2)*, 25(3):385–391, 1982.

[Nai82b] M. Nair. On C hebyshev-type inequalities for primes. *Amer.Math.Monthly*, 89:126–129, 1982.

[Pom02] C. Pomerance. The cyclotomic ring test of agrawal, kayal, and saxena. Preprint, 2002.

[Vol02] J. F. Voloch. Improvements to aks. Available from ftp://ftp.ma.utexas.edu/pub/papers/voloch/aks.pdf, 2002.