MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 164
OCTOBER 1983, PAGES 699–709

Irreducibility Testing and Factorization of Polynomials

By Leonard M. Adleman and Andrew M. Odlyzko

Abstract. It is shown that under certain hypotheses, irreducibility testing and factorization of polynomials with integer coefficients are polynomial time reducible to primality testing and factorization of integers, respectively. Combined with recently discovered fast primality tests, this yields an almost polynomial time irreducibility algorithm. The assertions of irreducibility produced by this algorithm are always certain and yield short proofs of irreducibility.

1. Introduction. Irreducibility testing and factorization of polynomials with integer coefficients are two of the oldest computational problems in mathematics. Early investigations of these problems were carried out by such prominent mathematicians as Newton, Kronecker, and Eisenstein; see Knuth [16]. In recent years these problems were investigated by Cantor [10], Moenck [20], Musser [22], Risch [25], Weinberger [29], Zassenhaus [30], Zippel [31], and others. In particular, Cantor [10] has shown that the set of irreducible polynomials is in NP; i.e., there are proofs of irreducibility that are of polynomial length in the size of the irreducible polynomial being considered. (The size of a polynomial is defined below.) While this result shows that irreducible polynomials possess succinct certificates of irreducibility, it does not provide any way of finding them. If the Generalized Riemann Hypothesis (GRH) holds, then Weinberger [29] has shown that testing irreducibility can be done in polynomial time. However, if the GRH is false, then Weinberger's algorithm might declare some reducible polynomials to be irreducible, and some irreducible ones reducible.

This paper presents new algorithms which reduce irreducibility testing and factorization of polynomials with integer coefficients to problems of integer primality testing and factorization, respectively. If we assume a certain unproved conjecture, which we call Hypothesis H^+, as well as the GRH, then these reductions are polynomial time, and in particular this leads to an almost polynomial time test for irreducibility. While these hypotheses are much stronger than the GRH assumed by Weinberger, our irreducibility algorithm has the advantage that an assertion of "irreducibility" is "certain" (i.e., provable from Peano's axioms) and does not rely on unproven hypotheses. Hypothesis H^+ and the GRH are used only to prove that the algorithm recognizes all irreducible polynomials rather than just a subset. If Hypothesis H^+ or the GRH is false, then some irreducible polynomials may be asserted to be "reducible", but not the reverse. This situation is the opposite of the

Received January 4, 1982; revised November 1, 1982.
1980 *Mathematics Subject Classification.* Primary 68C05; Secondary 12A20, 10H20.

0025-5718/83 $1.00 + $.25 per page

one associated with Miller's primality test [19], where assertions of "composite" are certain, but if the GRH is false, then conceivably some composite numbers may be asserted to be "prime". In cases when there is a need to establish the irreducibility of polynomials with certainty, our algorithm may be practical. However, to use this algorithm, one would have to carefully analyze the arguments in order to determine explicitly the values of the constants c_i that appear.

Before stating our results precisely, we have to define the size of a polynomial.

Definition. Given $f \in Z[x]$, $f(x) = a_n x^n + \cdots + a_0$, the size of f, denoted by $|f|$, is defined as

$$|f| = 2 + \sum_{k=0}^{n} \|a_k\|,$$

where $\|a_k\|$ is the length of a_k when written in binary, with $\|0\| = 1$.

Note that this definition does not assign a small size to polynomials such as $x^n + 1$. The reason for using the above definition is that it is in many ways the natural one. For example, it can be shown that if $g(x) | f(x)$, then $|g|$ is polynomial in $|f|$. This does not hold if we define the size of a polynomial

$$\sum_{i=0}^{m} a_i x^{k_i},$$

using the sparse encoding $((a_0, k_0), (a_1, k_1), \ldots, (a_m, k_m))$.

THEOREM 1. *Assume Hypothesis H^+ and the GRH, and let $Pr = \{p: p \in Z, p \text{ prime}\}$, $Ir = \{f: f \in Z[x], f \text{ irreducible}\}$. Then*

$$Ir \leqslant_P Pr.$$

THEOREM 2. *Assume Hypothesis H^+ and the GRH, and let FI be the problem of factoring integers, and let FP be the problem of factoring polynomials with integer coefficients. Then*

$$FP \leqslant_P FI.$$

Hypothesis H^+ is discussed at length in Section 2. The polynomial time reductions used are of the Cook (Turing) type.

Given $f \in Z[x]$, this algorithm produces $\leqslant c_1 |f|^{c_2}$ positive integers, each of size (measured by the length of their binary expansion) $\leqslant |f|^{c_3}$, where, as will be the case later on in the paper, the c_i are positive effectively computable constants. If even one of the integers is prime, then $f(x)$ is irreducible. If Hypothesis H^+ and the GRH hold, and $f(x)$ is irreducible, then at least one of these values has to be prime. A recently discovered deterministic algorithm tests the primality of an integer r in time

$$c_4 (\log r)^{c_5 \log\log\log r}$$

(Adleman [1], Adleman, Pomerance, and Rumely [3]). If this algorithm is combined with the basis reduction step, it results in an algorithm that halts in at most

$$c_6 |f|^{c_7 \log\log|f|}$$

steps when dealing with a polynomial $f \in Z[x]$. If the output is "irreducible", then there is a proof from Peano's axioms that f is irreducible. If Hypothesis H^+ and the GRH hold, then, for all $f \in Z[x]$, if f is irreducible, then "irreducible" is output.

The irreducibility testing algorithm is described precisely in Section 3. In Section 4 we sketch the factoring algorithm. It proceeds by factoring the $\leqslant c_1 |f|^{c_2}$ integers produced by our basic reduction and then tries to construct polynomial divisors of f from those factorizations. Because of the slow running times of the best known integer factoring methods [13], [21], [24], this algorithm is probably of little practical significance.

The basic idea behind our algorithm is the same as that of the classical algorithm of von Schubert [15], [16] (which was rediscovered by Kronecker and is usually ascribed to him), namely that the factors of the integer $f(k)$ should provide information about the polynomial factorization of $f(x)$. There are several results in the literature (see [7], [8], [9], and the references in those papers) which say that under appropriate conditions, if $f(k)$ is prime, then $f(x)$ is irreducible. (In [9], $f(k)$ has to be prime for several values of k, actually.) In order to utilize this basic idea to derive an algorithm, we need to discuss some number theoretic results and conjectures, and this is what Section 2 is devoted to.

Since this work was preformed, Lenstra, Lenstra, and Lovász [18] have discovered an algorithm that factors a primitive univariate polynomial in polynomial time. Their method uses lattice basic reduction and does not depend on any unproved hypotheses. Because of the completely different nature of our methods, we feel that they might still be of some interest.

2. Almost-Prime Values of Polynomials. In order to obtain efficient algorithms, we need to assume a very explicit quantitative form of a conjecture about primes representable by polynomials, for which at present there is little hope of finding a proof. The heuristic reasoning behind this conjecture is derived from several well-known unproved conjectures of number theory. In the next few paragraphs we will explain these conjectures and some of the reasoning behind them.

In order to prove the irreducibility of $f \in Z[x]$, we would like to find large values of $k \in Z$ such that $f(k)$ is prime. This does not happen for all irreducible f. For example, $x^2 - x + 2$ is always even, and so is a prime only for $x = 0, 1$. In this case, 2 is the fixed divisor of $x^2 - x + 2$.

Definition. For $f \in Z[x]$, the fixed divisor d_f of f is the largest positive integer d such that $d \mid f(a)$ for all $a \in Z$.

The fixed divisor can be computed very simply by means of the following well-known and easy to prove lemma.

LEMMA 1. *If $f \in Z[x]$, and we express*

$$f(x) = \sum_{j=0}^{n} b_j \binom{x}{j},$$

where

$$\binom{x}{j} = \frac{x(x-1)\cdots(x-j+1)}{j!} \quad \text{for } j \geqslant 1, \binom{x}{0} = 1,$$

then $b_j \in Z$ for $0 \leqslant j \leqslant n$ and $d_f = \mathrm{GCD}(b_0, b_1, \ldots, b_n)$.

Clearly if $d_f > 1$, then $f(k)$ can be prime for only a finite number of k. Remarkably enough, V. Bouniakowsky [6] conjectured in 1857 that if $f(x) \in Z[x]$ is

irreducible, and d_f is the fixed divisor of f, then $d_f^{-1}f(k)$ is a prime for infinitely many k. This conjecture is only known to be true when $\deg f(x) = 1$, in which case it follows from Dirichlet's theorem on primes in arithmetic progressions. However, this conjecture is widely believed to be true, and there is an even more general conjecture, the famous Hypothesis H of Schinzel [26], [27] which deals with sets of prime values taken on simultaneously by several polynomials.

Bateman and Horn [4], [5] went further and conjectured a quantitative form of Hypothesis H which is usually referred to as Hypothesis H^*. In the special case of a single irreducible polynomial $f(x)$ with $d_f = 1$ (the only case covered explictly by Hypothesis H), if for a prime p we let

$$W(p) = |\{k: 0 \leq k \leq p-1,\ f(k) \equiv 0 \pmod{p}\}|$$

and

$$\pi_f(x) = |\{m: 1 \leq m \leq x,\ f(m) \text{ is a prime}\}|,$$

where without loss of generality we may assume that the leading coefficient of $f(x)$ is positive, then Hypotheis H^* asserts that

$$\pi_f(x) \sim \frac{1}{n}\frac{x}{\log x}\prod_p \left\{\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{W(p)}{p}\right)\right\} \tag{2.1}$$

as $x \to \infty$, where $n = \deg f(x)$. This conjecture is supported by the available numerical evidence (see [4], [5] for references and some of the data). Upper bounds for $\pi_f(x)$ of this same general form are also known [14].

Before explaining the reasoning behind the Bateman-Horn conjecture, we will generalize it to cover the case $d_f \neq 1$. Suppose $f(x) \in Z[x]$, $n = \deg f(x)$. It follows from Lemma 1 that we may write

$$f(x) = d_f \sum_{k=0}^{n} a_k \binom{x}{k}, \qquad a_k \in Z,\ (a_0,\ldots,a_n) = 1.$$

For a prime p, we let $r = r_p$ be the least nonnegative integer such that the values of $f(m)d_f^{-1}$, when reduced modulo p, are periodic in m with period p^{r+1}. To see that r exists, note that if we write

$$\frac{a_k}{k!} = \frac{b}{c}, \qquad b, c \in Z,\ (b,c) = 1,$$

and $p^{s_k} \| c$, then the values of $a_k\binom{m}{k}$, when reduced modulo p, are periodic in m with period p^{s_k+1}, and therefore $r \leq \max(s_0,\ldots,s_n)$. Since each $p^{s_k} \mid k!$, $p^r \mid n!$, and so

$$r = r_p \leq \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots \leq \frac{n}{p-1}.$$

Also, note that $r = 0$ for $p > n$.

Given a prime p, and the associated $r = r_p$, let

$$W(p^{r+1}) = \left|\left\{m: 0 \leq m \leq p^{r+1}-1,\ f(m)d_f^{-1} \equiv 0 \pmod{p}\right\}\right|.$$

We now apply the reasoning behind the Bateman-Horn conjecture (2.1). If m is a large integer, we look at the probability that $f(m)d_f^{-1}$ is a prime. Now a random integer around y has probability $(\log y)^{-1}$ of being prime. However, $f(m)d_f^{-1}$ is not

quite random, since it is divisible by a prime p with probability $W(p^{r+1})/p^{r+1}$, whereas a random integer is divisible by p with probability $1/p$. Therefore one is led to conjecture that $f(m)d_f^{-1}$ is prime with probabilty

$$\sim \frac{1}{\log\{d_f^{-1}f(m)\}} \prod_p \left\{\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{W(p^{r+1})}{p^{r+1}}\right)\right\}, \tag{2.2}$$

which suggests that if

$$C(f) = \prod_p \left\{\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{W(p^{r+1})}{p^{r+1}}\right)\right\},$$

then

$$\pi_f(x) = \left|\{m: 0 \leqslant m \leqslant x,\ f(m)d_f^{-1} \text{ is a prime}\}\right|$$

satisfies

$$\pi_f(x) \sim \frac{x}{n\log x} C(f) \tag{2.3}$$

as $x \to \infty$. It is vital to us to know how fast this asymptotic behavior is approached. First of all, the main term should really be a sum of terms like (2.2) for $1 \leqslant m \leqslant x$, with $f(m) \neq 0$. Then, for $x \geqslant \exp(2|f|)$, the sum of these terms will be at least

$$\frac{x}{10n\log x} C(f).$$

In addition, reasoning by analogy with the known results for other arithmetical functions, we might expect the presence of an oscillating term on the order of $x^{1/2+\varepsilon}$. If we let

$$D = \text{absolute value of discriminant of } f(x),$$

then on the Generalized Riemann Hypothesis one can show [17] that sometimes these error terms are

$$O\big(x^{1/2}\log(xD^n)\big).$$

In the present case we might then hope that at least a much weaker bound for the oscillating term holds, namely $D^{c_8}x^{3/4}$ for some positive constant c_8. Let us define $C'(f) = \min(1, C(f))$. (This is done for technical reasons). Then we might hope that for $x \geqslant \exp(2|f|)$,

$$\pi_f(x) \geqslant \frac{x}{10n\log x} C'(f) - D^{c_8}x^{3/4}. \tag{2.4}$$

This bound will give

$$\pi_f(x) \geqslant \frac{x}{20n\log x} C'(f) \tag{2.5}$$

for

$$x \geqslant \max\big(\exp(2|f|),\ D^{c_9}C'(f)^{-5}\big),$$

since $\log D \geqslant c_{10}n$ [23].

Although (2.4) already relies on several currently unprovable assumptions, it is not sufficient for our purposes. We need to know in addition that there are no large gaps

between values of m such that $f(m)d_f^{-1}$ is prime. If p_n denotes the nth prime, then the Prime Number Theorem shows that on average, $p_{n+1} - p_n$ is on the order of $\log p_n$. On the other hand, it is only known that, for every $\varepsilon > 0$,

$$p_{n+1} - p_n = O\left(p_n^{11/20+\varepsilon}\right)$$

as $n \to \infty$. Even on the Riemann Hypothesis, it is only known that

$$p_{n+1} - p_n = O\left(p_n^{1/2+\varepsilon}\right).$$

On the other hand, there is an unproved conjecture of Cramér [11] which asserts that

$$p_{n+1} - p_n = O\left((\log p_n)^2\right). \tag{2.6}$$

The reasoning behind this conjecture is roughly as follows. If the probability that k is in some set S is roughly $\alpha(\log k)^{-1}$, then the probability that none of k, $k+1,\ldots,k+m-1$ is in S is roughly

$$\left(1 - \frac{\alpha}{\log k}\right)^m.$$

If $m \sim \alpha^{-1}(1+\delta)(\log k)^2$ for some $\delta > 0$, then this probability is roughly $k^{-1-\delta}$, and so we expect only a finite number of such gaps. In particular, in the case of prime numbers, $\alpha = 1$, and we obtain conjecture (2.6).

Numerical evidence in favor of a conjecture even stronger than Cramer's (2.6) is presented in [28]. In our case, where we consider values of $a \in Z$ for which $d_f^{-1}f(a)$ is prime, the above reasoning and the conjecture (2.5) lead us to expect that maximal gaps between such values of a, with $a \sim x$, should be no larger than

$$c_{11}C'(f)^{-1}n\log^2 x.$$

Of course we have to allow for exceptions when we consider the set of all polynomials, but since in all known cases strange anomalies occur only for values bounded by powers of the discriminant D of f, we are led to make the following conjecture.

HYPOTHESIS H^+. *There exist positive constants c_{12} and c_{13} such that for any irreducible $f \in Z[x]$, and every x with*

$$x \geqslant C'(f)^{-1}\exp\left\{|f|^{c_{12}} + (\log D)^{c_{12}}\right\},$$

there exists an integer a with

$$x \leqslant a \leqslant x + C'(f)^{-1}(\log D)^{c_{13}}(\log x)^{c_{13}}$$

such that $d_f^{-1}f(a)$ is prime.

3. Irreducibility Testing. In this section we present our algorithm and use it to prove Theorem 1. As we mentioned before, the basic idea is that if a polynomial takes on a prime value, then under appropriate conditions this implies the polynomial is irreducible. In our case we utilize the conditions given by the following very simple lemma.

LEMMA 2. *Given any $a \in N$ and any $b \in Z$, there is a unique polynomial $f \in Z[x]$, $f(x) = a_n x^n + \cdots + a_0$ with $-a/2 < a_i \leqslant a/2$, $0 \leqslant i \leqslant n$, such that $f(a) = b$.*

This is simply the statement that base a expansion is unique. Notice that there is a polynomial time algorithm which on input $a \in N$, $b \in Z$ produces the polynomial f described in Lemma 2. Notice also that if $-a/2 < b \leq a/2$, then $f(x) = b$.

We now state our irreducibility testing algorithm. The constants appearing in it can be computed explicitly, as will be seen from our analysis.

ALGORITHM. On input $f(x) = a_n x^n + \cdots + a_0 \in Z[x]$:

(1) If $GCD(a_n, a_{n-1}, \ldots, a_0) \neq 1$ output "reducible" and halt.

(2) Express

$$f(x) = \sum_{j=0}^{n} b_j \binom{x}{j}, \qquad b_j \in Z,$$

calculate $d = d_f = GCD(b_n, b_{n-1}, \ldots, b_0)$, and write

$$d^{-1} f(x) = \sum_{j=0}^{n} k_j \binom{x}{j}.$$

(3) Let $p_0, p_1, \ldots, p_z$ be the least initial segment of primes such that $p_{z+1} > |f|^{c_{14}}$.

(a) For each $i, 0 \leq i \leq z$, find the least y_i such that $p_i \nmid k_{y_i}$.

(b) Find (using effective versions of the Chinese Remainder Theorem) an integer m such that

(i) $m \equiv y_i \pmod{p_i^{e_i}}$, $0 \leq i \leq z$, where $e_i = [n/(p_i - 1)] + 1$,

(ii) $0 \leq m < M = \prod_{j=0}^{z} p_j^{e_j}$.

(4) For a in the range $\exp(|f|^{c_{15}})$ to $\exp(|f|^{c_{15}}) + |f|^{c_{16}}$ calculate $d^{-1} f(m + Ma)$ and test for primality. If a prime is found output "irreducible", otherwise output "reducible", and halt.

It is clear that the above algorithm runs in time polynomial in the time to test primality. What remains is to show.

(a) If f is irreducible then "ireducible" is output.

(b) If "irreducible" is output then f is irreducible.

We will need to bound certain quantities in terms of $|f|$. There are constants c_{17}, c_{18} independent of f such that

1. For all $h \in Z[x]$, if $h \mid f$, then $|h| < |f|^{c_{17}}$; [16, p. 438].

2. $\log(D) < |f|^{c_{17}}$ where D is the absolute value of the discriminant of f; [12, p. 51].

3. Let $g(x) = f(m + Mx)$, where m and M are as in the algorithm. Then

(i) $|g| < |f|^{c_{18}}$,

(ii) $\log(D') < |f|^{c_{18}}$ where D' is the absolute value of the discriminant of g; [12, p. 51].

(iii) $M < \exp(|f|^{c_{18}})$.

Proof of (a). If f is irreducible, then $g(x) = f(m + Mx)$ is irreducible. Also, because of the construction of m and M, g and f have the same fixed divisor d. We will apply Hypothesis H^+ to g. However, we will first analyze

$$C(g) = \prod_{p} \left\{ \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{W_g(p^{r+1})}{p^{r+1}}\right) \right\}.$$

We have

$$\frac{g(x)}{d} = \frac{f(m + Mx)}{d} = \sum_{j=0}^{n} k_j \binom{m + Mx}{j}.$$

By construction, for $0 \leqslant i \leqslant z$, $M = p_i \cdot n! \cdot r$ for some r, so

$$\sum_{j=0}^{n} k_j \binom{m + Mx}{j} \equiv \sum_{j=0}^{n} k_j \binom{m}{j} \pmod{p_i}.$$

But $m = y_i + p_i^{e_i} w$ for some w, and therefore

$$\sum_{j=0}^{n} k_j \binom{m}{j} \equiv \sum_{j=0}^{n} k_j \binom{y_i}{j} \pmod{p_i}$$

$$\equiv \sum_{j=0}^{y_i} k_j \binom{y_i}{j} \pmod{p_i}.$$

Now by construction $p_i \mid k_j, j = 0, 1, \ldots, y_i - 1$, and therefore

$$\sum_{j=0}^{y_i} k_j \binom{y_i}{j} \equiv k_{y_i} \binom{y_i}{y_i} \equiv k_{y_i} \not\equiv 0 \pmod{p_i}.$$

It follows that $W(p^{r+1}) = 0$ for $p \leqslant |f|^{c_{14}}$ and since for $p > |f|^{c_{14}}$ we have $p^{r+1} = p$ (for c_{14} sufficiently large), we have

$$C(g) \geqslant \prod_{p > |f|^{c_{14}}} \left\{ \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{W(p)}{p}\right) \right\}.$$

We now appeal to the following lemma:

LEMMA 3. *For all irreducible $f \in Z[x]$, if the Generalized Riemann Hypothesis holds for the Dedekind zeta function of the field generated by a root of f as well as for the ordinary Riemann zeta function, and D = absolute value of discriminant of $f(x)$, then for any $Z \geqslant (\log D)^3$,*

$$\prod_{p > Z} \left\{ \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{W(p)}{p}\right) \right\} \geqslant c_{19}$$

for some positive constant c_{19} independent of f.

Proof. We apply Theorem 1.1 of [17]. Since the discriminant of the field generated by a root of $f(x)$ is bounded in absolute value by D, that theorem shows that if

$$S(x) = \sum_{p \leqslant x}{}' (1 - W(p)),$$

where Σ' means that we sum over only those primes p for which $p \nmid D$, then under the assumptions of our lemma,

$$|S(x)| = O\left(x^{1/2} \log(Dx^n)\right).$$

Now there are $\leqslant 2 \log D$ primes p with $p \mid D$, and for $p > Z$,

$$\left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{W(p)}{p}\right) \geqslant 1 - \frac{n}{p} > 1 - \frac{n}{z},$$

so

$$\prod_{\substack{p>Z\\ p|D}} \left\{\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{W(p)}{p}\right)\right\} \geqslant \left(1-\frac{n}{Z}\right)^{2\log D} \geqslant \exp\left(-\frac{4n\log D}{Z}\right)$$

for all $Z \geqslant 2n$, say. Also,

$$\log\left\{\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{W(p)}{p}\right)\right\} = \frac{1-W(p)}{p} + O\left(\frac{W^2(p)}{p^2}\right)$$

$$= \frac{1-W(p)}{p} + O\left(\frac{n^2}{p^2}\right)$$

and, using the Riemann-Stieltjes integral,

$$\sum_{\substack{p>Z\\ p\nmid D}} \frac{1-W(p)}{p} = \int_Z^\infty \frac{1}{x}\,dS(x) = -\frac{S(Z)}{Z} + \int_Z^\infty \frac{S(x)}{x^2}\,dx$$

$$= O(Z^{1/2}\log(DZ^n)),$$

while

$$\sum_{p>Z} \frac{n^2}{p^2} = O\left(\frac{n^2}{Z}\right).$$

The lemma now follows immediately from these estimates.

We cannot apply Lemma 3 directly to g. However, since $(M, p) = 1$ for $p > |f|^{c_{14}}$, it follows that as x takes on the values $0, 1, \ldots, p-1$, $m + Mx$ also takes on the values $0, 1, \ldots, p-1$. Therefore $W_g(p) = W_f(p)$ for $p > |f|^{c_{14}}$. In addition we have $(\log(D))^3 < |f|^{c_{14}}$, and applying Lemma 3 to f we have

$$\prod_{p>|f|^{c_{14}}} \left\{\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{W_g(p)}{p}\right)\right\} = \prod_{p>|f|^{c_{14}}} \left\{\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{W_f(p)}{p}\right)\right\} \geqslant c_{19},$$

and therefore $C(g) \geqslant c_{19}$.

We now apply Hypothesis H^+ and the GRH to g. It follows that there exist constants c_{20}, c_{21} independent of f such that:

(1) $c_{20} > c_{14}$,

(2) $\exp(|f|^{c_{20}}) > 2d$,

(3) $g(a)/d$ is prime for some integer a with

$$\exp(|f|^{c_{20}}) \leqslant a \leqslant \exp(|f|^{c_{20}}) + |f|^{c_{21}}.$$

It follows that $f(m + Ma)/d$ is prime and that the algorithm outputs "irreducible".

Proof of (b). If "irreducible" is output, then $d^{-1}f(m + Ma)$ is prime for some a. Assume f is reducible, then $f = h\hat{h}$ for nonunit polynomials $h, \hat{h}$. It follows that $h(m + Ma)\hat{h}(m + Ma) = dp$ for some prime p. Without loss of generality, $h(m + Ma) \mid d$. For c_{15} large enough, $m + Ma$ exceeds twice the absolute value of the coefficients of h, and twice the absolute value of d. By Lemma 2, h is a constant. By Step I of the algorithm $h = \pm 1$. Notice that the proof of (b) uses neither Hypothesis H^+ nor GRH.

4. Factorization of Polynomials. Theorem 2 is based on the same ideas as Theorem 1, and so we will provide only an outline of its proof.

Assume f is the input. By selecting m, M as in Theorem 1, we can assume that $g(x) = f(m + Mx)$ is such that for an initial segment of primes $p_0, p_1, \ldots, p_z$, $W_g(p_i^{r_i+1}) = 0$. It follows that if $\hat{h}$ is a nontrivial irreducible divisor of f, then $h(x) = \hat{h}(m + Mx)$ is such that $W_h(p_i^{r_i+1}) = 0$ for $p_0, p_1, \ldots, p_z$. If p_z is large enough (greater than $|f|^c$ for an appropriate constant c), then $C(h)$ will be greater than c_{19} (by Lemma 3). By Hypothesis H^+, $h(a)/d_h = q$ for some prime q and some a in a suitable range (as in step 4) of the algorithm above, (but with different constants), where d_h is the fixed divisor of h. Since $d_h | d$ and $d | f(0) = a_0$, it follows that $a_0 h(a)/d_h = a_0 q$ where $a_0 h/d_h$ is a polynomial with integer coefficients. Rewriting, we have $a_0 \hat{h}(m + Ma)/d_h = a_0 q$ where $a_0 \hat{h}/d_h$ is a polynomial with integer coefficients. If Ma is chosen large enough (by forcing $a > \exp(|f|^c)$ for appropriate constant c) then it will exceed twice the absolute value of the coefficients of $a_0 \hat{h}/d_h$ and therefore, by Lemma 2, $a_0 \hat{h}/d_h$ is uniquely determined by $m + Ma$ and $a_0 q$. Further $h = (a_0 \hat{h}/d_h)/G$, where $G = GCD$ of coefficients of $(a_0 \hat{h}/d_h)$.

Therefore the algorithm for factoring polynomials can be as follows:

I. If GCD of coefficients of f is not 1, then output GCD and halt.

II. For each a in the appropriate range: factor $f(m + Ma) = q_1 q_2 \cdots q_t$; for each $q = q_i$, $i = 1, 2, \ldots, t$, find the unique polynomial with "small" coefficients such that $g(m + Ma) = a_0 q$. Find the polynomial $h = g/(\text{GCD of coefficients of } g)$. If $h | f$, output h and halt.

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Department of Computer Science
University of Southern California
Los Angeles, California 90007

Bell Laboratories
Murray Hill, New Jersey 07974

1. L. M. ADLEMAN, *On Distinguishing Prime Numbers from Composite Numbers*, Proc. 21st Annual IEEE Found. Comp. Sci. Conference, IEEE, 1980, pp. 387–406.

2. L. M. ADLEMAN & A. M. ODLYZKO, *Irreducibility Testing and Factorization of Polynomials*, (extended abstract), Proc. 22nd Annual IEEE Found. Comp. Sci. Conference, IEEE, 1981, pp. 409–418.

→ L. M. ADLEMAN, C. POMERANCE & R. RUMELY, "On distinguishing prime numbers from composite numbers," *Ann. of Math.*, v. 117, 1983, pp. 173–206.

4. P. BATEMAN & R. HORN, "A heuristic asymptotic formula concerning the distribution of prime numbers," *Math. Comp.*, v. 16, 1962, pp. 363–367.

5. P. BATEMAN & R. HORN, *Primes Represented by Irreducible Polynomials in One Variable*, Proc. Sympos. Pure Math., vol. 8, 1965, pp. 119–135.

6. V. BOUNIAKOWSKY, "Sur les diviseurs numériques invariables des fonctions rationelles entières," *Mem. Acad. Sci. St. Petersberg*, v. 6, 1857,, pp. 305–329.

7. J. BRILLHART, "Note on irreducibility testing," *Math. Comp.*, v. 35, 1980, pp. 1379–1381.

8. J BRILLHART, M. FILASETA & A. ODLYZKO, "On an irreducibility theorem of A. Cohn," *Canad. J. Math* , v. 33, 1981, pp. 1055–1059.

→ W. S. BROWN & R. L. GRAHAM, "An irreducibility criterion for polynomials over the integers," *Amer. Math. Monthly*, v. 76, 1969, pp. 795–797.

10. D. G. CANTOR, "Irreducible polynomials with integral coefficients have succinct certificates," *J. Algorithms*, v. 2, 1981, pp. 385–392.

11. H. CRAMÉR, "On the order of magnitude of the difference between consecutive prime numbers," *Acta Arith.*, v. 2, 1937, pp. 23–46.

12. E. DEHN, *Algebraic Equations*, Dover reprint, 1960.

13. J. D. DIXON, "Asymptotically fast factorization of integers," *Math. Comp.*, v. 36, 1981, pp. 255–260.

14. H. HALBERTSTAM & H. E. RICHERT, *Sieve Methods*, Academic Press, New York, 1974.

15. B. A. HAUSMANN, "A new simplification of Kronecker's method of factorization of polynomials," *Amer. Math. Monthly*, v. 44, 1937, pp. 574–576.

16. D. E. KNUTH, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981, [Section 4.6.2].

17. J. C. LAGARIAS & A. M. ODLYZKO, "Effective versions of the Chebotarev density theorem," *Algebraic Number Fields* (A. Fröhlich, ed.), (Proc. 1975 Durham Symposium), Academic Press, New York, 1977, pp. 409–464.

18. A. K. LENSTRA, H. W. LENSTRA, JR. & L. LOVÁSZ, "Factoring polynomials with rational coefficients," *Math. Ann.*, v. 261, 1982, pp. 515–534.

19. G. L. MILLER, "Riemann's hypothesis and tests for primality," *J. Comput. System Sci.*, v. 13, 1976, pp. 300–317.

20. R. MOENCK, "On the efficiency of algorithms for polynomial factorization," *Math. Comp.*, v. 31, 1977, pp. 235–250.

21. M. A. MORRISON & J. BRILLHART, "A method of factoring and the factorization of F_7," *Math. Comp.* v. 29, 1975, pp. 183–206.

22. D. MUSSER, "On the efficiency of a polynomial irreducibility test," *J. Assoc. Comput. Mach.*, v. 25, 1978, pp. 271–282.

23. W. NARKIEWICZ, *On the Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw, 1974.

24. C. POMERANCE, "Analysis and comparison of some integer factoring algorithms," pp. 89–139 in *Computational Methods in Number Theory*, Part 1 (H. W. Lenstra, Jr. and r. Tijdeman, eds.), MC Tract #154, Mathematical Center, Amsterdam, 1982.

25. R. RISCH, *Symbolic Integration of Elementary Functions*, Proc. 1968 IBM Summer Inst. on Symbolic and Algebraic Manipulation (R. Tobey, ed.), pp. 133–148.

26. A. SCHINZEL & W. SIERPINSKI, "Sur certaines hypotheses concernant les nombres premiers," *Acta Arith.*, v. 4, 1958, pp. 185–208; erratum, v. 5, 1959, p. 259.

27. A. SCHINZEL, "Remarks on the paper "Sur certaines hypotheses concernant les nombres premiers," " *Acta Arith.*, v. 7, 1961/1962, pp. 1–8.

28. D. SHANKS, "On maximal gaps between consecutive primes," *Math. Comp.*, v. 18, 1964, pp. 646–651.

29. P. J. WEINBERGER, "Finding the number of factors of a polynomial." (To appear.)

30. H. ZASSENHAUS, "On Hensel factorization, Part I," *J. Number Theory*, v. 1, 1969, pp. 291–311.

31. R. ZIPPEL, *Probabilistic Algorithms for Sparse Polynomials*, Ph.D. Thesis, Dept. of Electrical Eng. and Computer Science, MIT, Sept. 1979.