PROBABILISTIC ALGORITHMS IN INTEGER AND POLYNOMIAL ARITHMETIC

by

Michael Kaminski

Technical Report #419

June 1986
Probabilistic algorithms in integer
and polynomial arithmetic*

Michael Kaminski

Faculty of Computer Science
Technion - Israel Institute of Technology
Haifa 32000
Israel

We present a probabilistic algorithm for testing the result of the product of two
$n$-bit integers (polynomials of degree $n$ over any field) in $4n+o(n)$ bit (algebraic)
operations with the error probability $O(n^{-\varepsilon})$ for any $\varepsilon < 0.5$.

*The first version of this paper was written at the Hebrew University of Jerusalem and presented at 1981 ACM Symposium on Algebraic and Symbolic Computation.
1. Introduction.

For many computational problems it is unknown whether it is possible to check the result faster than to perform the computation itself. For example, it is unknown whether verifying the integer equality \( a \cdot b = c \) can be done in less bit operations than calculating the product \( a \cdot b \). However, it is sometimes much easier to speed up the computation probabilistically if only verifying the result is involved (cf. [13] and [14, p. 17]).

In this paper we present linear-time probabilistic algorithms for verifying integer equalities of the type \( a \cdot b = c \) and polynomial identities of the type \( f(x) \cdot g(x) = h(x) \) for univariate polynomials over any integral domain. (Schwart’s algorithm, cf. Example 1 below, cannot be applied in finite fields if the degree of the polynomials exceeds the number of the field’s elements, and Pippenger’s algorithm for verifying integer equalities, cf. Example 2 below, requires non-linear time.)

The paper is organized as follows: in the next section we sketch Schwart’s and Pippenger’s algorithms for verifying polynomial identities and integer equalities, respectively, and then give an outline of the algorithms presented in this paper. In Section 3 we present a probabilistic algorithm for verifying polynomial identities and in Section 4 we modify the algorithm given in Section 3 so that it can be applied to integer equalities.


Our algorithms are based on an easy generalization of the two examples below.

Example 1 ([13]). Let \( F \) be an infinite integral domain and let \( f(x) \), \( g(x) \) and \( h(x) \) be univariate polynomials of degree \( n \), \( n \) and \( 2n \) respectively. Let \( S \) be an \( m \)-element subset of \( F \) for some \( m > 2n \). The identity \( f(x) \cdot g(x) = h(x) \) can be checked probabilistically as follows:

(i) Choose, randomly, an \( s \in S \).

(ii) Compute \( f(s) \), \( g(s) \) and \( h(s) \).

(iii) If \( f(s) \cdot g(s) \neq h(s) \), then, definitely, \( f(x) \cdot g(x) \neq h(x) \). Otherwise decide that \( f(x) \cdot g(x) = h(x) \).

The error probability does not exceed \( 2n/m \).
Since evaluating a polynomial of degree \( t \) requires \( t \) additions and \( t \) multiplications (tight), stage (ii) of the algorithm involves \( 4n \) additions and \( 4n \) multiplications. One more multiplication is used in stage (iii). Hence the total number of algebraic operations involved is \( 8n + 1 \).

Choosing \( m \) large enough (or repeating (i)-(iii) sufficiently many times) we can make the error probability as small as we wish.

However, the above algorithm fails in finite fields whose number of elements does not exceed \( 2n \).

Since the equality \( f(s)g(s) = h(s) \) is equivalent to \( f(x)g(x) - h(x) = 0 \mod x \cdot s \), the correctness of the algorithm of Example 1 follows from the proposition below.

**Proposition 1.** Let \( F \) be an integral domain and let \( Q \) be an \( m \)-element set of univariate polynomials over \( F \) such that for some \( k, n \) and for any \( k \)-element subset of \( Q, \{q_1(x), \ldots, q_k(x)\} \), the degree of the least common multiple of \( \{q_1(x), \ldots, q_k(x)\} \) (denoted by \( \text{LCM}(q_1(x), \ldots, q_k(x)) \)) exceeds \( n \). If \( 0 \neq p(x) \in F[x] \) and \( \deg p(x) \leq n \), then for a \( q(x) \), randomly chosen from \( Q \), the probability that \( p(x) = 0 \mod q(x) \) does not exceed \((k - 1)m\).

**Proof.** Obviously, it is sufficient to prove that there are at most \( k - 1 \) elements of \( Q \) which divide \( p(x) \). If there were \( k \) such elements \( q_1(x), \ldots, q_k(x) \), say, then \( p(x) \) was divisible by \( \text{LCM}(q_1(x), \ldots, q_k(x)) \). Since \( p(x) \neq 0 \), \( \deg p(x) < n \) and \( \deg(\text{LCM}(q_1(x), \ldots, q_k(x))) > n \), this is impossible. \( \square \)

In Example 1, \( p(x) = f(x)g(x) - h(x) \), \( Q = \{x - s \mid s \in S\} \) and \( k = 2n \).

Now, for a linear-time probabilistic verification of the validity of the polynomial identity \( f(x)g(x) = h(x) \), where \( \deg f(x), \deg g(x) \leq n \) and \( \deg h(x) \leq 2n \), it suffices to establish an \( m \)-element set of monic polynomials \( Q \) satisfying the following conditions.

\( P_1) \) There exists \( k \) such that for any \( k \)-element subset of \( Q, \{q_1(x), \ldots, q_k(x)\} \), \( \deg \text{LCM}(q_1(x), \ldots, q_k(x)) > 2n \).

\( P_2) \) Let \( \text{res}(p(x), q(x)) \) denotes the residue of \( p(x) \) modulo \( q(x) \). For any \( q(x) \in Q \), \( \text{res}(f(x), q(x)), \text{res}(g(x), q(x)), \text{res}(h(x), q(x)) \) and \( \text{res}(\text{res}(f(x), q(x)), \text{res}(g(x), q(x))) = q(x) \) can be computed in \( O(n) \) algebraic operations.
It is possible to choose a \( q(x) \), randomly, from \( Q \) in \( O(n) \) operations. (We assume that a random bit can be generated in one operation.)

Of course, we want the ratio \((k-1)/m\) to be small.

Having such a set \( Q \) we can test probabilistically the validity of the identity \( f(x) \cdot g(x) = h(x) \) in linear time as follows.

(i) Choose a \( q(x) \), randomly, from \( Q \).

(ii) Compute \( h'(x) = \text{res}(h(x), q(x)) \) and \( h''(x) = \text{res}((\text{res}(f(x), q(x))), g(x), q(x)) \).

(iii) If \( h'(x) \neq h''(x) \) then, definitely, \( f(x) \cdot g(x) \neq h(x) \). Otherwise decide that \( f(x) \cdot g(x) = h(x) \).

The error probability does not exceed \((k-1)/m\).

In view of \( P_2 \) and \( P_3 \) stages (i)-(iii) can be performed in \( O(n) \) algebraic operations.

A set \( Q \) satisfying condition \( P_1 \)-\( P_3 \) is given in Section 3.

**Example 2** ([14], p.17). Let \( a, b \) and \( c \) be \( n, n \) and \( 2n \)-bit integers in binary notation, respectively.

The validity of the equality \( a \cdot b = c \) can be checked probabilistically as follows:

(i) Generate a random \( 2\left\lceil \log_2 n \right\rceil \)-bit prime number \( p \).

(ii) Compute \( a' = \text{res}(a, p), b' = \text{res}(b, p) \) and \( c' = \text{res}(c, p) \).

(iii) If \( a' \cdot b' \neq c' \mod p \), then, definitely, \( a \cdot b \neq c \). Otherwise decide that \( a \cdot b = c \). The error probability does not exceed \((2\ln n)/n\), where \( \ln x \) denotes the natural logarithm of \( x \).

Since a random \( O(\log n) \)-bit prime number can be randomly generated in \( O(\log^5 n) \) bit operations (cf. [10]) the total number of operations required to perform stages (i)-(iii) is dominated by the computation of \( a', b' \) and \( c' \) in stage (ii) and is \( O(n \cdot \log n \cdot \log \log n) \) (cf. [1]). The correctness of the above algorithm follows from the proposition below.

**Proposition 2.** Let \( I \) be an \( m \)-element set of positive integers such that for some \( k, n \) and for any \( k \)-element subset of \( I, \{i_1, \ldots, i_k\}, \text{LCM}(i_1, \ldots, i_k) > n \). If \( 0 < d \leq n \), then for an \( i \) randomly chosen from \( I \) the probability that \( d = 0 \mod i \) does not exceed \((k-1)/m\).

The proof of Proposition 2 is similar to that of Proposition 1 and is omitted.
In Example 2, \( d = ab - c, I = \{ p < 2n^2 \mid p \text{ is a prime number} \}, \) \( m = \pi(2n^2), \) where \( \pi(x) \) denotes the number of prime numbers not exceeding \( x, \) and \( k = 2ln2n \) (cf. [6] for the proof of the last equality).

In view of Proposition 2 for a linear-time probabilistic test of the validity of the integer equality \( a\cdot b = c, \) where \( a, b \) and \( c \) are \( n, n \) and \( 2n \)-digit integers (in \( l \)-ary expansion), respectively, it suffices to establish an \( m \)-element set of positive integers \( I \) satisfying the following conditions.

1. There exists a \( k \) such that for any \( k \)-element subset of \( I, \) \( \{i_1, \ldots, i_k\}, LCM(i_1, \ldots, i_k) \geq l^{2n}. \)
2. For all \( i \in I, \) \( \text{res}(a, i), \text{res}(b, i), \text{res}(c, i) \) and \( \text{res}(\text{res}(a, i) \cdot \text{res}(b, i), i) \) can be computed in \( O(n) \) bit operations.
3. It is possible to choose an \( i \) randomly from \( I \) in \( O(n) \) bit operations.

Then we can proceed like in the case of polynomials. Such a set \( I \) is given in Section 4.

In Sections 3 and 4 we assume that \( n \) is large enough so that we can apply appropriate asymptotic estimations.

### 3. Verification of polynomial identities.

A set \( Q \) satisfying conditions \( P_1-P_3 \) of Section 2 is given by the following theorem.

**Theorem 1.** Let \( \delta > \frac{\zeta(2)\zeta(3)}{\zeta(6)} = 1.9435964..., \) where \( \zeta \) is the Riemann Zeta Function and let \( 0 < \varepsilon < 0.5. \) If \( n \) is large enough, then for any integral domain \( F \) the set of polynomials \( Q = \{ x^i - 1 \mid 1 \leq i \leq n^{0.5+\varepsilon} \} \) satisfies the conditions \( P_1-P_3 \) of Section 2 with \( k = 2^{\lfloor \sqrt{\delta n} \rfloor} \) if \( F \) is of characteristic 0 and \( k = 2^{\lfloor \delta p(n)(p-1) \rfloor} \) if \( F \) is of a prime characteristic \( p \neq 0. \)

We prove first a few auxiliary propositions.

**Proposition 3.** Let \( i \) and \( j \) be positive integers such that the ratio \( i/j \) is not a power of a prime number \( p. \) Then cyclotomic polynomials \( \Phi_i(x) \) and \( \Phi_j(x) \) are relatively prime modulo \( p. \)
We remind the reader that $\Phi_l(x)$ is the minimal monic polynomial of the $l$th primitive root of 1, say, $e^{2\pi i / l}$. $\Phi_l(x) = \frac{x^l-1}{\prod_{d|l, d<l} \Phi_d(x)}$ has integer coefficients and $\deg \Phi_l(x) = \phi(l)$, where $\phi$ is the Euler function.

The proof of the following properties of cyclotomic polynomials can be found in [7], pp. 206-207.

1. If $p$ is a prime number, then
   $$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1,$$
   and for an integer $r \geq 1$,
   $$\Phi_{pr}(x) = \Phi_r(x^{p^{r-1}}).$$

2. Let $l = p_1^{r_1} \cdots p_s^{r_s}$ be a positive integer with its prime factorization. Then
   $$\Phi_l(x) = \Phi_{p_1} \cdots \Phi_{p_s} \left( x^{p_1^{r_1}-1} \cdots x^{p_s^{r_s}-1} \right).$$

3. If $p$ is a prime number not dividing $l$, then
   $$\Phi_{pl}(x) = \Phi_l(x^p \Phi_l(x)).$$

Proposition 3 easily follows from the results in [2] (and vice versa), however we give a proof (different from that of [2]) which can be modified to a proof of Proposition 7 (cf. Section 4).

Proof of Proposition 3. It suffices to show that there exists polynomials with integer coefficients $\alpha_{i,j}(x)$ and $\beta_{i,j}(x)$ such that

$$\alpha_{i,j}(x) \Phi_i(x) + \beta_{i,j}(x) \Phi_j(x) \equiv 1 \mod p.$$

We prove the existence of such polynomials by induction on the number of distinct common prime factors of $i$ and $j$.

Basis: $i$ and $j$ are relatively prime. We consider two cases: $i, j > 1$ and $i = 1, j > 1$.

Case of $i, j > 1$. Since $i$ and $j$ are relatively prime, $\frac{x^i-1}{x-1}$ is a unit modulo $\frac{x^j-1}{x-1}$ in the ring of polynomials with integer coefficients (cf. [8], p. 72). Because $\Phi_i(x)$ and $\Phi_j(x)$ divide $\frac{x^i-1}{x-1}$ and $\frac{x^j-1}{x-1}$, respectively, $\Phi_i(x)$ is a unit modulo $\Phi_j(x)$, i.e., there exists polynomials $\alpha_{i,j}(x)$ and $\beta_{i,j}(x)$
such that
\[ \alpha_{i,j}(x)\Phi_i(x) + \beta_{i,j}(x)\Phi_j(x) = 1. \]  
Thus (4) holds for any integer \( p \).

**Case of** \( i = 1, j > 1 \). Let \( j = p_1^{r_1} \cdots p_s^{r_s} \), where \( p_1, \ldots, p_s \) are prime numbers.

If \( s > 1 \), then, by (2) and (3),
\[ \Phi_j(x) = \Phi_{p_1}^{p_1^{r_1-1}} \Phi_{p_2}^{p_2^{r_2-1}} \cdots \Phi_{p_s}^{p_s^{r_s-1}}. \]
Hence \( \Phi_j(1) = \Phi_{p_1}^{p_1^{r_1-1}} \Phi_{p_2}^{p_2^{r_2-1}} \cdots \Phi_{p_s}^{p_s^{r_s-1}} = 1. \) Therefore \( \Phi_j(x) \) is a unit modulo \( x - 1 \).

If \( s = 1 \), then, by (1),
\[ \Phi_j(x) = \Phi_{p_1}^{p_1^{r_1-1}}(x - 1)^{p_1^{r_1-1} - 1} + \cdots + 1. \]
Hence \( \Phi_j(1) = p_1 \). Since \( p \) does not divide \( p_1 \), \( \Phi_j(x) \) is a unit modulo \( x - 1 \) in \( \mathbb{Z}_p[x] \) and (4) follows.

**Inductive Step.** Let \( i = q^u i_1 \) and \( j = q^v j_1 \), where \( q \) is a prime number not dividing neither \( i \), nor \( j \), and \( u, v \geq 1 \). We consider two cases: \( u = v \) and \( v > u \).

**Case of** \( u = v \). Since \( i/j = i_1/j_1, i_1/j_1 \) is not a power of \( p \). Applying (2) and (3) we see that
\[ \Phi_i(x) = \Phi_{i_1}(x^{q^u}) / \Phi_{i_1}(x^{q^{u-1}}) \quad \text{and} \quad \Phi_j(x) = \Phi_{i_1}(x^{q^u}) / \Phi_{j_1}(x^{q^{u-1}}). \]
Since the number of distinct common prime factors of \( i_1 \) and \( j_1 \) is less than the number of distinct common prime factors of \( i \) and \( j \), by the inductive hypothesis, there exist polynomials \( \alpha_{i_1,j_1}(x) \) and \( \beta_{i_1,j_1}(x) \) such that
\[ \alpha_{i_1,j_1}(x)\Phi_{i_1}(x) + \beta_{i_1,j_1}(x)\Phi_{j_1}(x) = 1 \pmod{p}. \]
Then, by (5),
\[ (\alpha_{i,j}(x^{q^u})\Phi_{i_1}(x^{q^{u-1}}))\Phi_{i_1}(x) + (\beta_{i,j}(x^{q^u})\Phi_{j_1}(x^{q^{u-1}}))\Phi_{j_1}(x) \equiv 1 \pmod{p}, \]
i.e., \( \alpha_{i,j}(x) = \alpha_{i_1,j_1}(x^{q^{u-1}})\Phi_{i_1}(x^{q^{u-1}}) \) and \( \beta_{i,j}(x) = \beta_{i_1,j_1}(x^{q^{u-1}})\Phi_{j_1}(x^{q^{u-1}}) \).

**Case of** \( v > u \). Let \( j = q^u j_1 = q^u j_2 \), where \( j_2 = q^{u-v} j_1 \). \( i_1 \) and \( j_2 \) cannot differ by a factor of a power of \( p \): if they do, then \( p = q \) and \( i_1 = j_1 \). But then \( i/j = p^{u-v} \), which contradicts the assumption.
Further, as in (6),

(7) \[ \Phi_j(x) = \Phi_j(x^{q^s}) / \Phi_j(x^{q^{s-1}}) \]
and, by (2) and (3),

(8) \[ \Phi_j(x) = \Phi_j(x^{q^s}) / \Phi_j(x^{q^{s-1}}) = \Phi_j(x^{q^s})\Phi_j(x^{q^{s-1}}) / \Phi_j(x^{q^{s-1}}). \]

We contend that \( \Phi_j(x^{q^{s-1}}) \) divides \( \Phi_j(x^{q^{s-1}}) \), or equivalently, \( \Phi_j(y^{q^s}) \) divides \( \Phi_j(y^{q^s}) \), where \( y \) is a new variable which is substituted for \( x^{q^{s-1}} \). Indeed, since \( q \) does not divide \( j_{1}, e^{2\pi i/q_{1}} \) is a root of \( \Phi_j(y^{q^s}) \).

By the inductive hypothesis, there exist polynomials \( \alpha_{i_{1}j_{2}}(x) \) and \( \beta_{i_{1}j_{2}}(x) \) such that

\[ \alpha_{i_{1}j_{2}}(x)\Phi_1(x) + \beta_{i_{1}j_{2}}(x)\Phi_{j_{2}}(x) = 1 \mod p. \]

Then, by (7), (8) and the above contention,

\[ (\alpha_{i_{1}j_{2}}(x^{q^s})\Phi_1(x^{q^{s-1}}))\Phi_1(x) + (\beta_{i_{1}j_{2}}(x^{q^s})\Phi_j(x^{q^{s-1}}))\Phi_j(x) = 1 \mod p, \]

i.e., \( \alpha_{i_{1}j_{2}}(x) = \alpha_{i_{1}j_{2}}(x^{q^s})\Phi_1(x^{q^{s-1}}) \) and \( \beta_{i_{1}j_{2}}(x) = \beta_{i_{1}j_{2}}(x^{q^s})\Phi_j(x^{q^{s-1}}) / \Phi_j(x^{q^{s-1}}). \)

Proposition 4. Let \( \beta < \frac{\zeta(6)}{\zeta(2)\zeta(3)} = 0.514101... \). If \( k \) is large enough, then for any set \( \{i_1, \ldots, i_k\} \)
of \( k \) positive pairwise distinct integers \( \sum_{i=1}^{k} \phi(i_i) \geq \beta k^2/2. \)

Proof. We may assume that \( \{\phi(i_1), \ldots, \phi(i_k)\} \) are the least \( s \) values of the Euler function i.e., if \( i = \{i_1, \ldots, i_k\} \), then \( \phi(i) \geq \max\{\phi(i_1), \ldots, \phi(i_k)\} \).

Let \( A(x) \) denote the number of positive integers \( i \) with \( \phi(i) \leq x \). Let

(9) \[ M = \max\{\phi(i_1), \ldots, \phi(i_k)\} - 1 \]
and let \( r \) be a positive real number. Then

\[ \sum_{i=1}^{k} \phi(i_i) \geq \sum_{\phi(i) \leq M} \phi(i) \geq \sum_{u=0}^{\lfloor M/r \rfloor - 1} \sum_{ur \leq s(i) < (u+1)r} \phi(i) \geq \sum_{u=0}^{\lfloor M/r \rfloor - 1} ur \sum_{u=0}^{\lfloor M/r \rfloor - 1} 1 \geq \]

\[ r \sum_{u=0}^{\lfloor M/r \rfloor - 1} u [A((u + 1)r) - A(ur)]. \]

It is known from [3] that
\[ A(x) = \alpha x + O \left( \exp \left( \frac{70}{99} (\ln x \cdot \ln \ln x)^{1/2} \right) \right), \]

where \( \alpha = \frac{\zeta(2) \zeta(3)}{\zeta(6)} = 1.9435964... \) and \( \ln x \) denotes the natural logarithm of \( x \). Hence

\[ A(x) = \alpha x + O(\frac{x}{\ln^2 x}), \text{ say}. \]

Since \( x/\ln^2 x \) is a non-decreasing function of \( x \) there exists a positive constant \( C \) such that for all \( x \) and \( y \)

\[ A(x) - A(x-y) \sim \alpha y - Cx/\ln^2 x. \]

Substituting \( \alpha r - CM/\ln^2 M \) for \([A((u+1)r) - A(ur)]\) in (10) we obtain

\[ \sum_{i=r}^{k} \phi(i) \geq r \sum_{u=0}^{\frac{\lfloor M/r \rfloor - 1}{2}} u (\alpha r - CM/\ln^2 M) \]

\[ = \alpha r^2 \left( \frac{\lfloor M/r \rfloor - 1}{2} \right) \frac{M/2}{r} - \frac{CM}{\ln^2 M} \frac{\lfloor M/r \rfloor - 1}{2} \frac{M/2}{r} \]

\[ > \frac{\alpha r^2}{2} (M/r - 2)^2 - \frac{CM}{2\ln^2 M} (M/r)^2 > \frac{\alpha M^2}{2} - (2\alpha M r + \frac{CM^3}{2r^2\ln^2 M}). \]

Substituting \( M/\ln M \) for \( r \) in (13) results

\[ \sum_{i=1}^{k} \phi(i) > \frac{\alpha M^2}{2} - \frac{\alpha M^2}{2} \left( \frac{4+C/\alpha}{\ln M} \right) = \frac{\alpha M^2}{2} + O \left( \frac{\alpha M^2}{2} \right). \]

It follows from (9) that

\[ A(M + 1) \geq k, \]

hence, by (12),

\[ M \geq k/\alpha + o(M) = k/\alpha + o(k). \]

(14) and (16) imply

\[ \sum_{i=1}^{k} \phi(i) > \frac{k^2}{2\alpha} + o(k^2) \geq \beta k^2/2, \]

if \( \beta < 1/\alpha = \frac{\zeta(6)}{\zeta(2)\zeta(3)} \) and \( k \) is large enough. \( \square \)

**Proposition 5.** Let \( R \) be an integral domain of characteristic 0 and let \( \beta \) be as in Proposition 4. If \( k \) is large enough, then for any set \( \{i_1, \ldots, i_k\} \) of \( k \) positive integers the degree of
\[ \text{LCM}(x^i - 1, \ldots, x^k - 1) \text{ exceeds } \beta k^2/2. \]

**Proof.** Since \( \Phi_i(x) \) divides \( x^i - 1 \), \( \text{LCM}(\Phi_i(x), \ldots, \Phi_k(x)) \) divides \( \text{LCM}(x^i - 1, \ldots, x^k - 1) \).

Therefore it suffices to show that

\[ \deg \text{LCM}(\Phi_i(x), \ldots, \Phi_k(x)) > \beta k^2/2. \]

Since cyclotomic polynomials are irreducible over integral domains of characteristic 0,

\[ (18) \quad \text{LCM}(\Phi_i(x), \ldots, \Phi_k(x)) = \prod_{i=1}^{k} \Phi_i(x). \]

Since \( \deg \Phi_i(x) = \phi(i) \), (18) implies

\[ (19) \quad \deg \text{LCM}(\Phi_i(x), \ldots, \Phi_k(x)) = \sum_{i=1}^{k} \phi(i). \]

By Proposition 4, \( \sum_{i=1}^{k} \phi(i) > \beta k^2/2 \), which together with (19) completes the proof.

**Proposition 6.** Let \( R \) be an integral domain of characteristic \( p \neq 0 \) and let \( \beta \) be as in Proposition 4. If \( k \) is large enough, then for any set \( \{i_1, \ldots, i_k\} \) of \( k \) positive integers the degree of \( \text{LCM}(x^{i_1} - 1, \ldots, x^{i_k} - 1) \) exceeds \( \frac{p-1}{p} \frac{\beta k^2}{2} \).

**Proof.** Define a subset \( I \) of \( \{i_1, \ldots, i_k\} \) by

\[ I = \{i \in \{i_1, \ldots, i_k\} \ | \ \text{no } m > 0, \ p^m i \in \{i_1, \ldots, i_k\} \}. \]

Since \( \Phi_i(x) \) divides \( x^i - 1 \) and \( \text{LCM}\{\Phi_i(x) \ | \ i \in I\} \) divides \( \text{LCM}(\Phi_i(x), \ldots, \Phi_k(x)) \), it suffices to show that

\[ \deg \text{LCM}\{\Phi_i(x) \ | \ i \in I\} > \frac{p-1}{p} \frac{\beta k^2}{2}, \]

or, equivalently, since the elements of \( I \) cannot differ by a factor of a power of \( p \), by Proposition 3, it suffices to show that

\[ (20) \quad \sum_{i \in I} \phi(i) > \frac{p-1}{p} \frac{\beta k^2}{2}. \]

In order to prove (20) it suffices to show, by Proposition 4, that

\[ (21) \quad \sum_{i \in I} \phi(i) > \frac{p-1}{p} \sum_{i=1}^{k} \phi(i). \]
Proposition 5, \[ p(x) = \sum_{i \in I} \phi(i) x^i, \] in order to prove (21), it suffices to prove that for all \( i \in I \)

\[ \phi(i) \geq \frac{p^{-1}}{p} \sum_{p^m | i} \phi(i). \] (22)

Since \( \sum_{p^m | i} \phi(i) \leq \sum_{i \in I} \phi(i/p^m) \), for the proof of (22) it suffices to show that

\[ \phi(i) \geq \frac{p^{-1}}{p} \sum_{p^m | i} \phi(i/p^m). \] (23)

Let \( i = p^m i' \), where \((p,i') = 1\).

Then

\[ \sum_{p^m | i} \phi(i/p^m) = \sum_{k=0}^{m} \phi(p^k i') = \phi(i') \sum_{k=0}^{m} \phi(p^k) = \phi(i') \left[ 1 + (p - 1) \sum_{k=0}^{m-1} p^k \right] = p^m \phi(i') = p \phi(i') = \frac{p}{p-1} \phi(i). \] (24)

The equality between the first and the last terms of (24) proves (23) and Proposition 6 follows. □

Proof of Theorem 1. To prove that \( Q \) satisfies condition \( P_1 \), consider two cases: case a): \( F \) is a characteristic 0 and case b): \( F \) is of a prime characteristic \( p \neq 0 \).

Case a.) It suffices to show that if \( n \) is large enough, then for any set of \( k = 2\sqrt{n} \) pairwise distinct integers \( \{i_1, \ldots, i_k\} \) \( \text{deg } LCM(x^{i_1} - 1, \ldots, x^{i_k} - 1) > 2n \). Let \( \beta = \frac{1}{2} \), then \( \beta < \frac{\zeta(6)}{\zeta(2)\zeta(3)} \). By Proposition 5,

\[ \text{deg } LCM(x^{i_1} - 1, \ldots, x^{i_k} - 1) > \frac{\beta k^2}{2} \geq 4\beta n = 2n. \]

Case b). This case can be treated similarly to case a) using Proposition 6. The proof is omitted. □

We pass now to the proof that \( Q \) satisfies condition \( P_2 \). Let \( p(x) = \sum_{j=0}^{m} a_j x^i \). Write \( p(x) \) as

\[ p(x) = \sum_{i=0}^{\lfloor m/i \rfloor} p_i(x) x^{i+1}, \quad \text{where } \deg p_i(x) < i, \quad i = 0, \ldots, \lfloor m/i \rfloor, \quad \text{i.e., } \quad p_0(x) = \sum_{j=0}^{i-1} a_j x^j, \]

\[ p_i(x) = \sum_{j=1}^{2i-1} a_{ij} x^j, \quad \ldots, \quad p_i(x) = \sum_{j=i}^{(i+1)l-1} a_{ij} x^j, \quad \ldots, \quad p_{\lfloor m/i \rfloor}(x) = \sum_{j=i}^{\lfloor m/i \rfloor} a_j x^{j \lfloor m/i \rfloor}. \]
Since \( x^i = 1 \mod x^i - 1 \),

\[
\text{res}(p(x), x^i - 1) = \text{res}(\sum_{t=0}^{[m/i]} p_t(x)x^{it}, x^i - 1) = \sum_{t=0}^{[m/i]} p_t(x)
\]

Since \( \deg p_t(x) < i, t = 0, \ldots, [m/i] \), \( \sum_{t=0}^{[m/i]} p_t(x) \) can be calculated in \( m-i \) additions. Hence the computation of \( \text{res}(f(x), x^i - 1) \), \( \text{res}(g(x), x^i - 1) \) and \( \text{res}(h(x), x^i - 1) \) can be performed in \( n + n + 2n = 4n \) additions.

Using fast multiplication algorithm we can compute \( \text{res}(f(x), x^i - 1) \cdot \text{res}(g(x), x^i - 1) \) in \( O(i \cdot \lg i \cdot \lg gi) \) = \( o(n) \) bit operations, since \( i < n^{0.5+\epsilon} \).

Since \( \deg(\text{res}(f(x), x^i - 1) \cdot \text{res}(g(x), x^i - 1)) < 2i \), its residue modulo \( x^i - 1 \)

can be calculated in \( 2i = o(n) \) operations. Thus \( Q \) satisfies condition \( P_2 \).

Since a random bit can be generated in one operation, \( Q \), obviously satisfies condition \( P_3 \). This completes the proof of Theorem 1. \( \square \)

The error probability when one uses the set \( Q \) is \( k/n^{0.5+\epsilon} \leq 2\sqrt{\ln n/n^{0.5+\epsilon}} \) (or \( 2\sqrt{\ln n/(p-1)/n^{0.5+\epsilon}} = O(n^{-\epsilon}) \).

Remark 1. It follows from the proof of Theorem 1, that the probabilistic test of the identity \( f(x) \cdot g(x) = h(x) \) using the set \( Q \) requires \( 4n + o(n) \) operations, whereas Schwartz's test requires \( 8n + 1 \) operations (cf. Example 1).

4. Verification of integer equalities

A set \( I \) satisfying conditions \( I_1) - I_3 \) of Section 2 is given by the following theorem.

**Theorem 2.** Let \( \delta \) and \( \epsilon \) be as in Theorem 1. If \( n \) is large enough, then the set of integers

\[
I = \left\{ \ell_i - 1 \mid 1 \leq i \leq n^{0.5+\epsilon} \right\}
\]

satisfies the conditions \( I_1) - I_3 \) of Section 2 with \( k = 2\sqrt{\ln n/\phi(I)} \).

For the proof we need a few propositions similar to those of Section 3.

**Proposition 7.** Let \( l \) be an integer greater than 1. If \( l^i \) is not a power of a prime number dividing \( l-1 \), then \( \Phi_i(l) \) and \( \Phi_j(l) \) are relatively prime integers.
The proof of Proposition 7 is similar to that of Proposition 3 and is omitted.

**Proposition 8.** Let \( \beta \) be as in Proposition 4 and let \( l \) be an integer greater than 1. If \( k \) is large enough,

\[
\phi(l) \frac{\beta^2}{2} > l^{\frac{1}{2}}
\]

then for any set \{\( i_1, \ldots, i_k \)\} of \( k \) positive integers \( LCM(l^{i_1} - 1, \ldots, l^{i_k} - 1) > l^{\frac{1}{2}} \).

**Proof.** Let \( l-1 = \prod_{j=1}^{k} p_j^{a_j} \), where \( p_1, \ldots, p_k \) are distinct prime numbers. Define a sequence \( I_0, \ldots, I_g \) of subsets of \( \{i_1, \ldots, i_k\} \) as follows:

\[
I_0 = \{i_1, \ldots, i_k\}, \text{ and for } j = 0, \ldots, g-1
\]

\[
I_{j+1} = \{i \in I_j \mid \text{for no } m > 0 \ p_{j+1}^m i \in I_j\}.
\]

Since \( \Phi(l) \) divides \( l^j - 1 \) and \( I_g \subset \{i_1, \ldots, i_k\} \),

(25) \( LCM(l^{i_1} - 1, \ldots, l^{i_k} - 1) \geq LCM\{\Phi_l(i) \mid i \in I_g\} \).

Since, obviously, no two elements of \( I_g \) differ by a factor of a power of a prime divisor of \( l-1 \), by Proposition 7,

(26) \( LCM\{\Phi_l(i) \mid i \in I_g\} = \prod_{i \in I_g} \Phi_l(i) \).

Since \( \Phi_l(i) > l^{\phi(i)-1} \),

(27) \( \prod_{i \in I_g} \Phi_l(i) > l^{\sum_{i \in I_g} \phi(i) - k} = l^{\sum_{i \in I_g} \phi(i) - k} \).

It follows from the proof of Proposition 6 that

\[
\sum_{i \in I_{j+1}} \phi(i) \geq \frac{P_{j+1} - 1}{P_{j+1}} \sum_{i \in I_j} \phi(i), \ j = 0, \ldots, g-1.
\]

Hence

(28) \( \sum_{i \in I_g} \phi(i) \geq \frac{P_{j+1} - 1}{P_{j+1}} \sum_{i \in I_j} \phi(i) \geq \frac{\phi(l)}{l} \frac{\beta' k^2}{2} > \frac{\phi(l)}{l} \frac{\beta k^2}{2} + k \),

where \( \beta < \beta' \frac{\zeta(6)}{\zeta(2) \zeta(3)} \) satisfies the conditions of Proposition 4. (25)-(28) imply that

\( LCM(l^{i_1} - 1, \ldots, l^{i_k} - 1) \geq l^{\frac{1}{2}} \),

which proves the proposition. \( \square \)
Now, to prove Theorem 2 one can proceed similarly to the proof of Theorem 1. The proof is omitted.

Remark 2. In [4] we used the sets \( \{x^p - 1 \mid p \text{ is a prime number not exceeding } \frac{n}{\log n \cdot \log \log n} \} \) and \( \{p^p - 1 \mid p \text{ is a prime number not exceeding } \frac{n}{\log n \cdot \log \log n} \} \) for probabilistic verification of polynomial identities and integer equalities, respectively. The present approach improves the error probability by a factor of \( \sqrt{\log n} \), which might be used in applications for small values of \( n \).
References


[7]. S. Lang, Algebra, Addison-Wesley, 1965.

[8]. S. Lang, Algebraic number theory, Addison-Wesley, 1970.


