A Potentially Fast Primality Test

Tsz-Wo Sze

February 20, 2007

1 Introduction

In 2002, Agrawal, Kayal and Saxena [3] gave the first deterministic, polynomial-time primality testing algorithm. The main step was the following.

Theorem 1.1. (AKS) *Given an integer $n > 1$, let r be an integer such that $\mathrm{ord}_r(n) > \log^2 n$. Suppose*

$$(x+a)^n \equiv x^n + a \pmod{n, x^r - 1} \qquad \text{for } a = 1, \cdots, \lfloor \sqrt{\phi(r)} \log n \rfloor. \quad (1.1)$$

Then, n has a prime factor $\leq r$ or n is a prime power.

The running time is $O(r^{1.5} \log^3 n)$. It can be shown by elementary means that the required r exists in $O(\log^5 n)$. So the running time is $O(\log^{10.5} n)$. Moreover, by Fouvry's Theorem [8], such r exists in $O(\log^3 n)$, so the running time becomes $O(\log^{7.5} n)$.

In [10], Lenstra and Pomerance showed that the AKS primality test can be improved by replacing the polynomial $x^r - 1$ in equation (1.1) with a specially constructed polynomial $f(x)$, so that the degree of $f(x)$ is $O(\log^2 n)$. The overall running time of their algorithm is $O(\log^6 n)$.

With an extra input integer a, Berrizbeitia [6] has provided a deterministic primality test with time complexity $2^{-\min(k, \lfloor 2 \log\log n \rfloor)} O(\log^6 n)$, where $2^k || n-1$ if $n \equiv 1 \pmod 4$ and $2^k || n+1$ if $n \equiv 3 \pmod 4$. If $k \geq \lfloor 2 \log\log n \rfloor$, this algorithm runs in $O(\log^4 n)$. The algorithm is also a modification of AKS by verifying the congruent equation

$$(1+mx)^n \equiv 1 + mx^n \pmod{n, x^{2^s} - a}$$

for a fixed s and some clever choices of m. The main drawback of this algorithm is that it requires the Jacobi symbol $\left(\frac{a}{n}\right) = -1$ if $n \equiv 1 \pmod 4$ and $\left(\frac{a}{n}\right) = \left(\frac{1-a}{n}\right) = -1$ if $n \equiv 3 \pmod 4$. Since there is no deterministic algorithm to find such a yet, Berrizbeitia's algorithm is considered as a probabilistic test.

There are several efficient probabilistic primality tests, see [11], [12], [13], [9], [5], [1], [2]. By assuming Extended Riemann Hypothesis (see [4]), Miller's primality test [11] is a deterministic algorithm with time complexity $O(\log^4 n)$.

In this paper, we attempt to improve AKS primality test in another direction. We suggest that equation (1.1) may be checked with only the single value $a = -1$. If a certain conjecture (Conjecture 2.7) about cyclotomic polynomials holds, we obtain deterministic a primality testing algorithm with running time $O(r \log^2 n)$. The requirement of r is exactly the same as in AKS. Therefore, the running time would be $O(\log^5 n)$ if r is $O(\log^3 n)$.

1.1 Notation

We use $\mathrm{ord}_a(b)$ to denote the order of b in $(\mathbb{Z}/a\mathbb{Z})^\times$, given $(a, b) = 1$; $\mathbb{F}_q$ to be the finite field with q elements; and $\Phi_k(x)$ to denote the k^{th} cyclotomic polynomial. All logarithms are base 2 unless otherwise specified.

2 The Algorithm

Let $\mathsf{SimplePrimalityTest}(n)$ be an $O(\sqrt{n})$ primality test algorithm.

Algorithm 2.1. $\mathsf{PrimalityTest}(n)$

{
    if $n < n_0 = 8 \times 10^5$, return $\mathsf{SimplePrimalityTest}(n)$;
    if $n = a^e$ for some prime a and some $e > 1$, return COMPOSITE;

    find smallest r such that $\mathrm{ord}_r(n) > \log^2 n$;
    if $1 < (a, n) < n$ for some $a \leq r$, return COMPOSITE;
    if $n \leq r$, return PRIME;

    if $(x-1)^n \not\equiv x^n - 1 \pmod{n, x^r - 1}$, return COMPOSITE;
    return PRIME;
}

Throughout this section, suppose $n > 1$ is an integer and Algorithm 2.1 returns PRIME at the last line. Therefore,

- n is not a non-trivial power of prime (that is, $n \neq p^e$ for some $e > 1$),
- $\mathrm{ord}_r(n) > \log^2 n$,
- all prime divisors of n are greater than r
- $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$.

Let p be a prime dividing n such that $\mathrm{ord}_r(p) > 1$. Since $\mathrm{ord}_r(n) > 1$, such a prime p exists. Let

$$G = \left\{ (\frac{n}{p})^i p^j \pmod{r} \ : \ i, j \in \mathbb{Z} \right\} \subset (\mathbb{Z}/r\mathbb{Z})^\times.$$

Let $t = |G|$. Let $h(x)$ be an irreducible factor of $\Phi_r(x)$ in $\mathbb{F}_p$. Then, $\deg(h) = \mathrm{ord}_r(p) > 1$. Let

$$F = (\mathbb{Z}/p\mathbb{Z})[x]/(h(x)),$$

which is isomorphic to the finite field $\mathbb{F}_{p^{\deg(h)}}$. Let

$$\mathcal{G} = \{f(x) \in F \ : \ f(x) \neq 0 \text{ and } f(x)^n = f(x^n) \text{ in } F\}.$$

In F, it can be shown that $f(x)^n = f(x^n)$ implies $f(x)^{n/p} = f(x^{n/p})$ (see [3] for a proof). Since p is the characteristic of F, we have $f(x)^p = f(x^p)$. Therefore, for all $f \in \mathcal{G}$, we have $f(x)^m = f(x^m)$ for all $m \in G$.

2.1 Upper bounds of $|\mathcal{G}|$

Some upper bounds of the size of $|\mathcal{G}|$ can be shown as follows.

Lemma 2.2. *Suppose n is not a power of p. Then, $|\mathcal{G}| \leq n^{\sqrt{t}}$.*

Proof. The proof is essentially the same as the proof of Lemma 4.8 in [3]. □

Lemma 2.3. *Suppose n is not a power of p. If $\mathrm{ord}_r(n) > \sqrt{t} \geq \sqrt{384}$, then $|\mathcal{G}| \leq n^{\sqrt{t}-2/5}$.*

Proof. Suppose $n^{2/5} \leq p \leq n^{3/5}$. Let

$$\hat{I} = \left\{ (\frac{n}{p})^i p^j \ : \ 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \right\}.$$

The size of $\hat{I}$ satisfies $|\hat{I}| = (\lfloor \sqrt{t} \rfloor + 1)^2 > t$. Since $G = \hat{I} \pmod r$ and $|G| = t$, there exist $m_1, m_2 \in \hat{I}$ with $m_1 < m_2$ such that $m_1 \equiv m_2 \pmod r$. Consider the polynomial $\psi(T) = T^{m_2 - m_1} - 1 \in F[T]$. For all $f(x) \in \mathcal{G}$,

$$\begin{aligned} \psi(f(x)) &= f(x)^{m_2 - m_1} - 1 \\ &= \frac{f(x^{m_2})}{f(x^{m_1})} - 1 \\ &= 0. \end{aligned}$$

Therefore, $\psi(T)$ has at least $|\mathcal{G}|$ roots in F.

Let

$$M = \max \left\{ (\frac{n}{p})^{\lfloor \sqrt{t} \rfloor} p^{\lfloor \sqrt{t} \rfloor - 1}, (\frac{n}{p})^{\lfloor \sqrt{t} \rfloor - 1} p^{\lfloor \sqrt{t} \rfloor} \right\}.$$

Note that $M \leq n^{\lfloor \sqrt{t} \rfloor - 2/5} \leq n^{\sqrt{t} - 2/5}$ since both p, $\frac{n}{p} \geq n^{2/5}$. We claim that m_1, m_2 can be chosen such that $m_2 - m_1 \leq M$. This implies that $|\mathcal{G}| \leq \deg(\psi) = m_2 - m_1 \leq n^{\lfloor \sqrt{t} \rfloor - 2/5}$.

To prove the claim, let $m_1' \equiv m_2' \pmod r$ with $m_1', m_2' \in \hat{I}$ and $m_1' < m_2'$.

If $m_2' < n^{\lfloor \sqrt{t} \rfloor}$, then $m_2' \leq (n/p)^i p^j$ with either $i < \lfloor \sqrt{t} \rfloor$ or $j < \lfloor \sqrt{t} \rfloor$. Then $m_2' \leq M$, so $m_2' - m_1' \leq M$. We can set $m_1 = m_1'$ and $m_2 = m_2'$. The

case $m_1' = 1$ and $m_2' = n^{\lfloor\sqrt{t}\rfloor}$ is not possible; otherwise, $1 \equiv n^{\lfloor\sqrt{t}\rfloor} \pmod{r}$, so $\mathrm{ord}_r(n) \leq \lfloor\sqrt{t}\rfloor$. Finally, assume $1 \neq m_1' < m_2' = n^{\lfloor\sqrt{t}\rfloor}$. The definition of $\hat{I}$ shows that $m_1' | n^{\lfloor\sqrt{t}\rfloor} = m_2'$. Choose $m_1 = 1$ and $m_2 = m_2'/m_1'$. Since $m_1' \geq \min\left\{p, \frac{n}{p}\right\} \geq n^{2/5}$, this completes the proof of the claim.

Now suppose that $p < n^{2/5}$ or $p > n^{3/5}$, Let $n^\delta = \min\left\{p, \frac{n}{p}\right\}$ with $0 < \delta < \frac{2}{5}$. Then $n^{1-\delta} = \max\left\{p, \frac{n}{p}\right\}$. Let

$$\tilde{I} = \left\{ n^{\delta i} n^{(1-\delta)j} \ : \ 0 \leq i \leq A \text{ and } 0 \leq j \leq B \right\},$$

where $A = \left\lfloor \sqrt{\frac{t(1-\delta)}{\delta}} \right\rfloor$ and $B = \left\lfloor \sqrt{\frac{t\delta}{1-\delta}} \right\rfloor$. Then $|\tilde{I}| = (A+1)(B+1) > t$. As before, there exist $m_3, m_4 \in \tilde{I}$, such that $m_3 \equiv m_4 \pmod{r}$ with $m_3 < m_4$. Note that $m_4 \leq n^{A\delta} n^{B(1-\delta)} \leq n^{2\sqrt{t\delta(1-\delta)}} \leq n^{\sqrt{24t/25}} < n^{\sqrt{t}-2/5}$ for $t \geq 384$. All the elements in $\mathcal{G}$ are the roots of the polynomial $T^{m_4} - T^{m_3}$. Therefore, $|\mathcal{G}| \leq m_4 \leq n^{\sqrt{t}-2/5}$. □

2.2 Producing elements of $\mathcal{G}$

One way to find a lower bound on the size of $\mathcal{G}$ is to produce a large number of elements of $\mathcal{G}$. If we have chosen r so that n is a primitive root mod r, then this is easy.

Lemma 2.4. *Assume that n is a primitive root mod r and that $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$. If $(m, r) = 1$, then*

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

for some integer e.

Proof. Write $m \equiv n^f \pmod{r}$. Then

$$x^m - 1 \equiv x^{n^f} - 1 \equiv (x-1)^{n^f}.$$

□

Consider the cyclotomic field of rth roots of unity $\mathbb{Q}(\zeta)$, where ζ is a primitive rth root of unity. The cyclotomic units are generated by the quotients $(\zeta^a - 1)/(\zeta - 1)$ with $(a, r) = 1$. The index of these units in the full group of units of the ring $\mathbb{Z}[\zeta]$ is the class number of the real subfield $\mathbb{Q}(\zeta + \zeta^{-1})$. This class number tends to be rather small, so the cyclotomic units are of small index in the full group of units. Let p be prime and let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta]$ dividing p. The field $\mathbb{Z}[\zeta]/\mathfrak{p}$ is isomorphic to $\mathbb{F}_p[x]/(p, h(x))$, where $h(x)$ is an irreducible factor mod p of $\Phi_r(x)$. Work on Artin's primitive root conjecture (see, for example, [7]) shows that the reduction mod $\mathfrak{p}$ of the group of units of $\mathbb{Z}[\zeta]$ should often be quite large. In fact, it is conjectured to be the full multiplicative group of $\mathbb{Z}[\zeta]/\mathfrak{p}$

for a positive density of primes p. Since the index of the cyclotomic units tends to be small, we expect that the cyclotomic units also generate a large subgroup of the multipicative group. Therefore, the polynomials $x^m - 1$ should generate a large subgroup of $\mathbb{F}_p[x]/(p, h(x))$, so we expect that the group $\mathcal{G}$ should be large for many p.

In the next section, we formulate a conjecture on cyclotomic polynomials (Conjecture 2.7) that can be regarded as a way of producing a large number of introspective polynomials. In the case that n is a primitive root mod r, the following lemma shows that the group obtained is contained in the group generated by $x - 1$.

Lemma 2.5. *If n is a primitive root mod r and $(x-1)^n \equiv x^n - 1 \pmod{n, x^r-1}$, then*

$$\Phi_m(x) \in \{(x-1)^e \ : \ e \in \mathbb{Z}\} \subset F^\times$$

for $(m, r) = 1$.

Proof. Since

$$\Phi_m(x) = \prod_{d|m} (x^{m/d} - 1)^{\mu(d)}$$

where $\mu(d)$ is the Möbius function, the previous lemma yields the result. □

2.3 Cyclotomic polymonials

We conjecture that once equation (1.1) is verified with $a = -1$, the size of $\mathcal{G}$ is larger than the upper bounds in Lemma 2.2 and 2.3. If the conjecture is true, then n must be a prime when Algorithm 2.1 returns PRIME at the last line.

In particular, we have the m^{th} cyclotomic polynomial $\Phi_m(x) \in \mathcal{G}$ for all $m > 0$ with $(m, r) = 1$ as shown in Lemma 2.6. Since there are infinitely distinct $\Phi_m(x)$ in $\mathbb{Z}[x]$, some of them must congruent to each other in F. Note that there exist r distinct $\Phi_q(x)$'s in F for q prime (see Lemma 3.3). By Lemma 3.4, for primes p_1 and q_1, $\Phi_{p_1}(x)$ and $\Phi_{q_1}(x)$ are distinct whenever $p_1 \not\equiv q_1 \pmod{r}$. Conjecture 2.7 suggests a generalized situation that $\Phi_{p_1 \cdots p_k}(x)$ and $\Phi_{q_1 \cdots q_k}(x)$ are distinct unless $p_i \equiv q_{\sigma(i)} \pmod{r}$ for all $1 \le i \le k$ and some permutation σ. Proposition 3.5 proves Conjecture 2.7 with $k = 2$.

Lemma 2.6. *If $(x-1)^n \equiv x^n - 1 \pmod{n, x^r-1}$, then for $k \ge 1$ with $(k, r) = 1$,*

$$\Phi_k(x)^n \equiv \Phi_k(x^n) \pmod{p, \Phi_r(x)}. \tag{2.2}$$

Proof. We use induction. By the hypothesis, $\Phi_1(x) = x - 1$ satisfies the conclusion because $p|n$ and $\Phi_r(x)$ divides $x^r - 1$. Suppose $\Phi_i(x)^n \equiv \Phi_i(x^n) \pmod{p, \Phi_r(x)}$ for $1 \le i < k$ with $(i, r) = 1$.

For $k > 1$ with $(k, r) = 1$, the congruence $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$ implies that

$$(x^k - 1)^n \equiv x^{kn} - 1 \pmod{n, x^{kr} - 1}.$$

Since $p|n$ and $\Phi_r(x)$ divides $x^{kr}-1$,

$$(x^k-1)^n \equiv (x^n)^k - 1 \pmod{p, \Phi_r(x)}.$$

By the identity $T^k - 1 = \prod_{d|k} \Phi_d(T)$,

$$\left(\prod_{d|k} \Phi_d(x)\right)^n \equiv \prod_{d|k} \Phi_d(x^n) \pmod{p, \Phi_r(x)}. \tag{2.3}$$

For any proper divisor d' of k, $(d', r) = 1$ and $\Phi_{d'}(x)^n \equiv \Phi_{d'}(x^n) \pmod{p, \Phi_r(x)}$ by the induction assumption. Let $g(x) = (\Phi_{d'}(x), \Phi_r(x)) \in \mathbb{F}_p[x]$. If $g(x) \neq 1$, let $\alpha \in \overline{\mathbb{F}}_p$ be a root of $g(x)$. Then, $\alpha^{d'} = 1$ and $\alpha^r = 1$. But $(d', r) = 1$ implies that $\alpha = 1$. However, $\Phi_r(1) = \sum_{i=0}^{r-1} 1 = r \neq 0$ in $\mathbb{F}_p$ since r, p are distinct primes. Therefore, $(\Phi_{d'}(x), \Phi_r(x)) = 1$. so equation 2.3 yields

$$\Phi_k(x)^n \equiv \Phi_k(x^n) \pmod{p, \Phi_r(x)}.$$

□

Conjecture 2.7. *Let $p_1, p_2, \cdots, p_k$ be prime numbers that are distinct mod r and none of them are congruent to $-1, 0, 1 \pmod r$. Similarly, let $q_1, q_2, \cdots, q_k$ be primes that are distinct mod r and none of them are congruent to $-1, 0, 1 \pmod r$. Let $h(x)$ be an irreducible factor of $\Phi_r(x)$ mod p. Then,*

$$\Phi_{p_1 p_2 \cdots p_k}(x) \equiv \Phi_{q_1 q_2 \cdots q_k}(x) \pmod{p, h(x)}$$

if and only if there is a permutation σ of $\{1, 2, \ldots, k\}$ such that

$$p_i \equiv q_{\sigma(i)} \pmod r \qquad \text{for } i = 1, 2, \cdots, k.$$

One direction of this conjecture can be proved. In Section 3, we give evidence for the other direction.

Proof of "⇐". We prove a stronger version of the statement:

$$p_i \equiv q_i \pmod r \qquad \text{for } i = 1, 2, \cdots, k,$$

implies

$$\Phi_{p_1 p_2 \cdots p_k}(x) \equiv \Phi_{q_1 q_2 \cdots q_k}(x) \pmod{p, \Phi_r(x)}.$$

We show it by induction. For $k = 1$, the statement is true by Lemma 3.4. For $k > 1$, suppose $p_i \equiv q_i \pmod r$ for $i = 1, 2, \cdots, k$. By the induction assumption,

$$\Phi_{p_1 p_2 \cdots p_{k-1}}(y) \equiv \Phi_{q_1 q_2 \cdots q_{k-1}}(y) \pmod{p, \Phi_r(y)}.$$

Put $y = x^{p_k}$. We have

$$\Phi_{p_1 p_2 \cdots p_{k-1}}(x^{p_k}) \equiv \Phi_{q_1 q_2 \cdots q_{k-1}}(x^{p_k}) \pmod{p, \Phi_r(x^{p_k})}.$$

Since $\Phi_r(x)$ divides $\Phi_r(x^{p_k})$,

$$\Phi_{p_1p_2\cdots p_{k-1}}(x^{p_k}) \equiv \Phi_{q_1q_2\cdots q_{k-1}}(x^{p_k}) \pmod{p, \Phi_r(x)}.$$

We claim that $\Phi_{p_1p_2\cdots p_{k-1}}(x)$ and $\Phi_r(x)$ are relatively prime mod p. To see this, let $\alpha \in \overline{\mathbb{F}_p}$ be a common root mod p of the two polynomials. Then $\alpha^{p_1p_2\cdots p_{k-1}} = 1 = \alpha^r$, so $\alpha = 1$. But $\Phi_r(1) = r \not\equiv 0 \pmod{p}$. Therfore, the two polynomials have no common root mod p, which proves the claim. So $\Phi_{p_1p_2\cdots p_{k-1}}(x)$ is a unit mod $\Phi_r(x)$. Finally,

$$\begin{aligned}
\Phi_{p_1p_2\cdots p_k}(x) &= \frac{\Phi_{p_1p_2\cdots p_{k-1}}(x^{p_k})}{\Phi_{p_1p_2\cdots p_{k-1}}(x)} \\
&\equiv \frac{\Phi_{q_1q_2\cdots q_{k-1}}(x^{p_k})}{\Phi_{q_1q_2\cdots q_{k-1}}(x)} \pmod{p, \Phi_r(x)} \\
&\equiv \frac{\Phi_{q_1q_2\cdots q_{k-1}}(x^{q_k})}{\Phi_{q_1q_2\cdots q_{k-1}}(x)} \pmod{p, \Phi_r(x)} \\
&= \Phi_{q_1q_2\cdots q_k}(x).
\end{aligned}$$

□

In Conjecture 2.7, we require $p_i, q_i \not\equiv -1, 0, 1 \pmod{r}$ for $i = 1, 2, \cdots, k$, otherwise, the conjecture is obviously false. For any prime q, if $q \equiv 0 \pmod{r}$, then $q = r$ and $\Phi_q(x) \equiv 0 \pmod{\Phi_r(x)}$ is not a unit. If $q \equiv 1 \pmod{r}$, we have $\Phi_q(x) \equiv 1 \pmod{\Phi_r(x)}$, which is the multiplicative identity. Then, $\Phi_{qm}(x) \equiv 1 \pmod{\Phi_r(x)}$ for any integer $m > 0$. If $q \equiv -1 \pmod{r}$, then $\Phi_q(x) \equiv -x^{-1} \pmod{\Phi_r(x)}$. The subgroup of $F^\times$ generated by $-x^{-1}$ has only $2r$ elements, where $F = (\mathbb{Z}/p\mathbb{Z})[x]/(h(x))$. We have $\Phi_{qm_1}(x) \equiv \Phi_{qm_2} \pmod{\Phi_r(x)}$ for some $m_1 \equiv m_2 \pmod{2r}$.

2.4 Lower bound for $|\mathcal{G}|$

Assuming Conjecture 2.7 is true, we establish a lower bound for $|\mathcal{G}|$ in Lemma 2.9 that implies the correctness of Algorithm 2.1. See Theorem 2.10.

Recall the following.

Theorem 2.8. (Stirling's approximation) *For $N > 0$,*

$$\sqrt{2\pi N}(\frac{N}{e})^N e^{1/(12N+1)} < N! < \sqrt{2\pi N}(\frac{N}{e})^N e^{1/(12N)}.$$

Lemma 2.9. *If Conjecture 2.7 is true, then $|\mathcal{G}| > \frac{1}{11}\frac{2^r}{\sqrt{r}}$.*

Proof. If $r \leq 5$, then $\frac{1}{11}\frac{2^r}{\sqrt{r}} < 2 \leq |\mathcal{G}|$ since $\mathcal{G}$ has as least two elements, x and $x - 1$.

Suppose $r > 5$, i.e. $r \geq 7$. If Conjecture 2.7 is true, there are $\binom{r-3}{k}$ distinct $\Phi_{p_1p_2\cdots p_k}(x)$ in $\mathcal{G}$ by Lemma 2.6 and Dirichlet's Theorem (Theorem 3.2).

Consider $k = \frac{r-3}{2}$. By Theorem 2.8,

$$\begin{aligned}
\frac{(r-3)!}{(((r-3)/2)!)^2} &> \frac{(\frac{r-3}{e})^{r-3} e^{1/(12r-35)} \sqrt{2\pi(r-3)}}{\left((\frac{r-3}{2e})^{(r-3)/2} e^{1/(6r-18)} \sqrt{2\pi(\frac{r-3}{2})}\right)^2} \\
&= \frac{2^r}{\sqrt{32\pi(r-3)}} e^{\frac{1}{12r-35} - \frac{1}{3r-9}} \\
&> \frac{e^{\frac{1}{49} - \frac{1}{12}}}{\sqrt{32\pi}} \frac{2^r}{\sqrt{r}} \\
&> \frac{1}{11} \frac{2^r}{\sqrt{r}}.
\end{aligned}$$

Therefore, $|\mathcal{G}| \geq \binom{r-3}{(r-3)/2} > \frac{1}{11}\frac{2^r}{\sqrt{r}}$, as required. □

Theorem 2.10. *If Conjecture 2.7 is true, then Algorithm 2.1 returns PRIME at the last line only if n is a prime.*

Proof. If algorithm 2.1 returns PRIME at the last line, then r is an odd prime, n is not a nontrivial power of a prime, $n \geq n_0 = 8 \times 10^5$, and $\mathrm{ord}_r(n) = r - 1 > \log^2 n$. Moreover, all prime divisors of n are greater than r, and $(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$.

Suppose $\mathrm{ord}_r(n) > \sqrt{t} \geq \sqrt{384}$. Let $c = (\log^2 n)/r > 1$ and let

$$f(c,n) = \frac{n^{2/5}}{\log n} \left(\frac{n^{(c-\sqrt{c})\log n}}{\sqrt{c}} \right).$$

Note that $\frac{n^{2/5}}{\log n}$ is increasing for $n > \sqrt{32}$. So $f(c,n)$ is increasing in n for $n > \sqrt{32}$ and $c \geq 1$. The term $\frac{n^{(c-\sqrt{c})\log n}}{\sqrt{c}}$ is increasing in c for $c \geq 1$.

For $n > 392$ and $c \geq c_0 = 1.084$,

$$\frac{n^{2/5}}{\log n} \left(\frac{n^{(c-\sqrt{c})\log n}}{\sqrt{c}} \right) = f(c,n) > f(c_0, 384) > 11,$$

which implies that

$$\frac{1}{11}\frac{2^r}{\sqrt{r}} = \frac{1}{11}\left(\frac{n^{c\log n}}{\sqrt{c}\log n} \right) > n^{\sqrt{c}\log n - \frac{2}{5}} = n^{\sqrt{r} - \frac{2}{5}}.$$

If $1 \leq c < c_0$ and $n \geq n_0$, then $\frac{n^{2/5}}{\log n} > 11\sqrt{c_0}$ for $n \geq n_0$ and

$$\frac{1}{11}\frac{2^r}{\sqrt{r}} > \frac{1}{11}\left(\frac{n^{\sqrt{r}}}{\sqrt{c_0}\log n} \right) > n^{\sqrt{r} - \frac{2}{5}}.$$

If n is not a power of p, then Lemma 2.3 and Lemma 2.9 together imply that

$$n^{\sqrt{n} - \frac{2}{5}} \geq |\mathcal{G}| > n^{\sqrt{n} - \frac{2}{5}},$$

which is a contradiction. Since the algorithm removes nontrivial powers of primes, we must have that n is a prime.

Now suppose that $\mathrm{ord}_r(n) \leq \sqrt{t}$. Then, $r > t \geq (\mathrm{ord}_r\, n)^2 > \log^4 n$. We have

$$\frac{1}{11}\frac{2^r}{\sqrt{r}} \geq \frac{1}{11}\frac{n^{\log n\sqrt{r}}}{\sqrt{r}} > n^{\sqrt{r}}$$

for $n \geq 5$ and $r \geq 3$, which includes all possible values of n and r. By Lemma 2.2 and Lemma 2.9, n is a prime. □

Note that it is possible to minimize the value of n_0 by manipulating the parameters in the proof of Theorem 2.10. However, such minimization is unnecessary for any practical use of Algorithm 2.1 because $n_0 = 8 \times 10^5$ is small enough for running an $O(\sqrt{n})$ algorithm.

3 Evidence for Conjecture 2.7

In this section, we give evidence for Conjecture 2.7. In particular, we prove it for $k = 1, 2$. Recall that p and r are primes as in Conjecture 2.7.

Lemma 3.1. *For any positive integer M,*

$$\sum_{k=0}^{M-1} x^k \equiv 0 \pmod{p, \Phi_r(x)} \qquad \Longleftrightarrow \qquad M \equiv 0 \pmod{r}.$$

Proof. Let $m \equiv M \pmod{r}$ with $0 \leq m < r$. Then,

$$\begin{aligned}
& \sum_{k=0}^{M-1} x^k \equiv 0 && \pmod{p, \Phi_r(x)} \\
\Longleftrightarrow \quad & \sum_{k=0}^{m-1} x^k \equiv 0 && \pmod{p, \Phi_r(x)} \\
\Longleftrightarrow \quad & m = 0 \\
\Longleftrightarrow \quad & M \equiv 0 && \pmod{r}
\end{aligned}$$

□

The following result is well known.

Theorem 3.2. (Dirichlet's theorem) *Let a, d be two positive coprime integers. Then, there are infinitely many primes comgruent to a mod d.*

Lemma 3.3. *For any positive integer N with $(N, r) = 1$, there exist infinitely many primes q such that*

$$\Phi_q(x) \equiv \sum_{k=0}^{N-1} x^k \pmod{p, \Phi_r(x)}.$$

Proof. Given $N > 0$ and $(N, r) = 1$, by Theorem 3.2 there exists a prime q with $q \equiv N \pmod{r}$. By Lemma 3.1,

$$\Phi_q(x) = \sum_{k=0}^{q-1} x^k = x^N \left(\sum_{k=0}^{q-N-1} x^k \right) + \sum_{k=0}^{N-1} x^k \equiv \sum_{k=0}^{N-1} x^k \pmod{p, \Phi_r(x)}.$$

□

Proposition 3.4.

$$\Phi_{p_1}(x) \equiv \Phi_{q_1}(x) \pmod{p, \Phi_r(x)} \qquad \Longleftrightarrow \qquad p_1 \equiv q_1 \pmod{r},$$

where p_1, q_1 are primes.

Proof. If $p_1 = q_1$, the proposition is trivially true.

Without loss of generality, suppose $p_1 < q_1$. Then,

$$\begin{aligned}
& \Phi_{p_1}(x) \equiv \Phi_{q_1}(x) && \pmod{p, \Phi_r(x)} \\
\Longleftrightarrow \quad & \sum_{k=0}^{p_1-1} x^k \equiv \sum_{k=0}^{q_1-1} x^k && \pmod{p, \Phi_r(x)} \\
\Longleftrightarrow \quad & \sum_{k=0}^{q_1-p_1-1} x^k \equiv 0 && \pmod{p, \Phi_r(x)} \\
\Longleftrightarrow \quad & p_1 \equiv q_1 && \pmod{r},
\end{aligned}$$

by Lemma 3.1. □

Proposition 3.5. *Let p_1, p_2, q_1, q_2 be primes p_1, p_2 distinct mod r, and with q_1, q_2 distinct mod r. Moreover, assume that $p_i \not\equiv 1 \pmod{r}$ for $i = 1, 2$. Then,*

$$\Phi_{p_1 p_2}(x) \equiv \Phi_{q_1 q_2}(x) \pmod{p, \Phi_r(x)} \tag{3.4}$$

implies

$$p_1 \equiv q_i \pmod{r} \qquad \text{and} \qquad p_2 \equiv q_j \pmod{r},$$

where $\{i, j\} = \{1, 2\}$.

Proof. **Case 1:** Suppose that all p_1, p_2, q_1, q_2 are distinct mod r. Then, r is at least 7. For primes $p_0 \neq q_0$, $\Phi_{p_0 q_0}(x) = \frac{(x^{p_0 q_0}-1)(x-1)}{(x^{p_0}-1)(x^{q_0}-1)}$. Therefore, $\Phi_{p_1 p_2}(x) \equiv \Phi_{q_1 q_2}(x) \pmod{p, \Phi_r(x)}$ implies

$$\frac{(x^{p_1 p_2}-1)(x-1)}{(x^{p_1}-1)(x^{p_2}-1)} \equiv \frac{(x^{q_1 q_2}-1)(x-1)}{(x^{q_1}-1)(x^{q_2}-1)} \pmod{p, \Phi_r(x)}$$

Multiply both sides by the denominators:

$$(x^{p_1 p_2}-1)(x^{q_1}-1)(x^{q_2}-1) \equiv (x^{q_1 q_2}-1)(x^{p_1}-1)(x^{p_2}-1) \pmod{p, \Phi_r(x)}. \tag{3.5}$$

If $p_1p_2 \equiv q_1q_2 \pmod{r}$, congruence (3.5) becomes

$$\begin{aligned}(x^{q_1}-1)(x^{q_2}-1) &\equiv (x^{p_1}-1)(x^{p_2}-1) \pmod{p, \Phi_r(x)},\\ x^{q_1+q_2}+x^{p_1}+x^{p_2} &\equiv x^{p_1+p_2}+x^{q_1}+x^{q_2} \pmod{p, \Phi_r(x)}.\end{aligned}$$

Note that $p_1+p_2 \not\equiv q_1+q_2 \pmod{r}$. Otherwise, p_1, p_2, q_1, q_2 are distinct roots of $T^2-(p_1+p_2)T+p_1p_2$ in $\mathbb{F}_r$, which is a contradiction. Then, $x^{q_1+q_2}+x^{p_1}+x^{p_2} \pmod{p, x^r-1}$ and $x^{p_1+p_2}+x^{q_1}+x^{q_2} \pmod{p, x^r-1}$ are polynomials with different degrees since the three terms $x^{q_1+q_2}$, x^{p_1}, x^{p_2} are not congruent to any of $x^{p_1+p_2}$, x^{q_1}, x^{q_2}. Therefore, since $\Phi_r(x) = (x^r-1)/(x-1)$,

$$\begin{aligned} & x^{q_1+q_2}+x^{p_1}+x^{p_2} \not\equiv x^{p_1+p_2}+x^{q_1}+x^{q_2} && \pmod{p, x^r-1}\\ \Longrightarrow \quad & \frac{x^{q_1+q_2}-x^{p_1+p_2}}{x-1} \not\equiv \frac{x^{q_1}-x^{p_1}}{x-1}+\frac{x^{q_2}-x^{p_2}}{x-1} && \pmod{p, \Phi_r(x)}\\ \Longrightarrow \quad & x^{q_1+q_2}+x^{p_1}+x^{p_2} \not\equiv x^{p_1+p_2}+x^{q_1}+x^{q_2} && \pmod{p, \Phi_r(x)}\end{aligned}$$

This contradiction implies that $p_1p_2 \not\equiv q_1q_2 \pmod{r}$.

Expanding the terms in congruence (3.5), we have

$$\begin{aligned} & x^{p_1p_2+q_1+q_2}-x^{p_1p_2+q_1}-x^{p_1p_2+q_2}-x^{q_1+q_2}+x^{p_1p_2}+x^{q_1}+x^{q_2}-1\\ \equiv \quad & x^{q_1q_2+p_1+p_2}-x^{q_1q_2+p_1}-x^{q_1q_2+p_2}-x^{p_1+p_2}+x^{q_1q_2}+x^{p_1}+x^{p_2}-1\\ & \pmod{p, \Phi_r(x)}\end{aligned}$$

$$\begin{aligned}\text{Let } f(x) &= x^{p_1p_2+q_1+q_2}+x^{q_1q_2+p_1}+x^{q_1q_2+p_2}+x^{p_1+p_2}+x^{p_1p_2}+x^{q_1}+x^{q_2},\\ g(x) &= x^{q_1q_2+p_1+p_2}+x^{p_1p_2+q_1}+x^{p_1p_2+q_2}+x^{q_1+q_2}+x^{q_1q_2}+x^{p_1}+x^{p_2}.\end{aligned}$$

As before, we first show that $f(x) \not\equiv g(x) \pmod{p, x^r-1}$. Since $x-1$ divides $f(x)-g(x)$, we must have $f(x) \not\equiv g(x) \pmod{p, \Phi_r(x)}$. As a result, congruence (3.5) leads to a contradiction.

The sum of the coefficients in $f(x) \pmod{x^r-1}$ is exactly 7. There are only 7 terms in $f(x)$. Since each power of x is congruent mod x^r-1 to a power x^j with $0 \le j < r$, we see that $f(x)$ is congruent mod x^r-1 to a sum of seven not necessarily distinct such powers x^j. Since $p > r \ge 7$, these cannot cancel each other mod p. A similar result holds for $g(x)$. If $f(x) \equiv g(x) \pmod{p, x^r-1}$, then x^{p_2} is congruent to some term in $f(x)$. The only possibilities are $x^{p_1p_2+q_1+q_2}$ and $x^{q_1q_2+p_1}$. Similarly, x^{p_1} must be congruent to $x^{p_1p_2+q_1+q_2}$ or $x^{q_1q_2+p_2}$.

If

$$p_2 \equiv q_1q_2+p_1 \pmod{r}, \tag{3.6}$$

then $p_1 \not\equiv q_1q_2+p_2 \pmod{r}$; otherwise, $p_2-p_1 \equiv q_1q_2 \equiv p_1-p_2 \pmod{r}$, which is impossible. Therefore, $p_1 \equiv p_1p_2+q_1+q_2 \pmod{r}$. Then, using these congruences for p_1 and p_2, we obtain

$$\begin{aligned} & x^{q_1q_2+p_2}+x^{p_1+p_2}+x^{p_1p_2}+x^{q_1}+x^{q_2}\\ \equiv \quad & x^{q_1q_2+p_1+p_2}+x^{p_1p_2+q_1}+x^{p_1p_2+q_2}+x^{q_1+q_2}+x^{q_1q_2} \pmod{p, x^r-1}\end{aligned}$$

The only possible term in the left-hand side congruent to $x^{q_1 q_2}$ is $x^{p_1+p_2}$. But congruence (3.6) implies $q_1 q_2 \equiv p_2 - p_1 \pmod{r}$. So $q_1 q_2 \not\equiv p_1 + p_2 \pmod{r}$. Hence, $f(x) \not\equiv g(x) \pmod{p, x^r - 1}$.

If $p_2 \equiv p_1 p_2 + q_1 + q_2 \pmod{r}$, then $p_1 \equiv q_1 q_2 + p_2 \pmod{r}$. The case is the same as before by switching the roles of p_1 and p_2.

Case 2: Suppose that some p_i is congruent to some q_j mod r. we may assume that $p_1 \equiv q_1 \equiv m \pmod{r}$ for some $1 < m < r$. Note that $m \neq 1$ by assumption. By Lemma 3.4, $\Phi_{p_1}(x) \equiv \Phi_{q_1}(x) \equiv \sum_{k=0}^{m-1} x^k \pmod{p, \Phi_r(x)}$. Therefore,

$$\begin{aligned}
& \Phi_{p_1 p_2}(x) \equiv \Phi_{q_1 q_2}(x) && \pmod{p, x^r - 1} \\
\Longrightarrow \quad & \Phi_{p_1}(x)\Phi_{p_1 p_2}(x) \equiv \Phi_{q_1}(x)\Phi_{q_1 q_2}(x) && \pmod{p, x^r - 1} \\
\Longrightarrow \quad & \Phi_{p_1}(x^{p_2}) \equiv \Phi_{q_1}(x^{q_2}) && \pmod{p, x^r - 1} \\
\Longrightarrow \quad & \sum_{k=1}^{m-1} x^{kp_2} \equiv \sum_{k=1}^{m-1} x^{kq_2} && \pmod{p, x^r - 1}
\end{aligned}$$

Let $M = \{1, 2, \cdots, m-1\}$. We see that $p_2 M = q_2 M$ as subsets of $\mathbb{Z}/r\mathbb{Z}$. Let $a \equiv p_0 q_0^{-1} \pmod{r}$. Then multiplication by $a \pmod{r}$ is a permutation of M. By Lemma 3.6 below, $a = 1$. Therefore, $p_2 \equiv q_2 \pmod{r}$. □

Lemma 3.6. *Let q be a prime and let $1 < m < q$. Let $M = \{1, 2, \cdots, m-1\}$. Suppose $0 \leq a < q$ and $aM = M$ in $\mathbb{F}_q$. Then, $a = 1$.*

Proof. If $a = 0$, then $aM = \{0\} \neq M$, so we may assume that $a \geq 1$. For any $1 \leq a < q$, multiplication by $a \pmod{q}$ is a permutation of $\{1, 2, \cdots, q-1\}$. If $aM = M$, multiplication by $a \pmod{q}$ is also a permutation of M. As a consequence, multiplication by $a \pmod{q}$ also permutes $\overline{M} \stackrel{\mathsf{def}}{=} \{m, \cdots, q-1\}$. Both M and $\overline{M}$ are not empty since $1 < m < q$.

Suppose $a \neq 1$. Let $q = ua + v$, where the quotient $u = \lfloor q/a \rfloor \geq 1$ and the remainder $v = q - ua < a$. This implies $ua > q/2$. We claim that $\{1, 2, \cdots, ua\} \subseteq M$ and $\{q-1, q-2, \cdots, q-ua\} \subseteq \overline{M}$. Then, $|M| + |\overline{M}| > q$, which leads to a contradiction.

We show by induction that $A_k \stackrel{\mathsf{def}}{=} \{1, 2, \cdots, ak\} \subseteq M$ for $1 \leq k \leq u$. Note that A_k is a set of exactly ak elements in $\mathbb{F}_q$ because $ak \leq au < q$. Since $1 \in M$, we have $a \cdot 1 \in M$. Therefore, $1 \leq a \leq m-1$, so $A_1 \subseteq M$. Assume $A_{k-1} \subseteq M$ for $k > 1$. We have $k \in A_{k-1}$ because $k \leq 2(k-1) \leq a(k-1)$. Then, $ak \in aM = M$, which implies $A_k \subseteq M$.

The statement $\{q-1, q-2, \cdots, q-ak\} \subseteq \overline{M}$ can be shown by a similar argument, beginning with $q - 1 \in \overline{M}$. □

Acknowledgments We thank Lawrence C. Washington for many useful suggestions and discussions.

References

[1] William Adams and Daniel Shanks. Strong primality tests that are not sufficient. *Math. Comp.*, 39(159):255–300, 1982.

[2] Manindra Agrawal and Somenath Biswas. Primality and identity testing via Chinese remaindering. *J. ACM*, 50(4):429–443, 2003.

[3] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2):781–793, 2004.

[4] N. C. Ankeny. The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[5] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[6] Pedro Berrizbeitia. Sharpening "PRIMES is in P" for a large family of numbers. *Math. Comp.*, 74(252):2043–2059 (electronic), 2005.

[7] David A. Clark and M. Ram Murty. The Euclidean algorithm for Galois extensions of $\mathbf{Q}$. *J. Reine Angew. Math.*, 459:151–162, 1995.

[8] Etienne Fouvry. Théorème de Brun-Titchmarsh; application au théorème de Fermat. 79(2):383–407, 1985.

[9] Shafi Goldwasser and Joe Kilian. Primality testing using elliptic curves. *J. ACM*, 46(4):450–472, 1999.

[10] Hendrik W. Lenstra Jr. and Carl Pomerance. Primality testing with gaussian periods. 2005. Preliminary version. Available from `http://www.math.dartmouth.edu/~carlp/PDF/complexity12.pdf`.

[11] Gary L. Miller. Riemann's hypothesis and tests for primality. In *STOC '75: Proceedings of seventh annual ACM symposium on Theory of computing*, pages 234–239, New York, NY, USA, 1975. ACM Press.

[12] Michael O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12(1):128–138, 1980.

[13] Robert Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6(1):84–85, 1977.