PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 9, September 2008, Pages 3095–3104
S 0002-9939(08)09303-9
Article electronically published on May 7, 2008

A GENERALIZATION OF MILLER'S PRIMALITY THEOREM

PEDRO BERRIZBEITIA AND AURORA OLIVIERI

(Communicated by Ken Ono)

ABSTRACT. For any integer r we show that the notion of ω-prime to base a introduced by Berrizbeitia and Berry, 2000, leads to a primality test for numbers n congruent to 1 modulo r, which runs in polynomial time assuming the Extended Riemann Hypothesis (ERH). For $r = 2$ we obtain Miller's classical result.

1. INTRODUCTION

Let r be a positive integer. Let A_r be the set of integers n such that every divisor d of n is congruent to 1 modulo r. If n is in A_r, it is easy to see (and proved in [5]) that there is an integer $\omega = \omega(n)$ of order r modulo d, for every divisor d of n. Also, the existence of such an ω clearly implies that $n \in A_r$.

In [5] the notion of ω-prime to base a, which for composite n generalizes the notion of a strong pseudoprime, was introduced as follows: Let $n \in A_r$ and let ω be as above. We assume first that $r = q^e$ is a prime power. Write $n - 1 = q^s t$, where $s \geq e$ and $(t, q) = 1$. Let a be an integer. We say that n is ω-prime to base a if either there exists $h \in \mathbb{Z}$ such that $a^t \equiv \omega^{qh} \pmod{n}$ or there exist i, j with $(j, q) = 1$, $0 \leq i \leq s - e$, $1 \leq j \leq r - 1$ such that $a^{q^i t} \equiv \omega^j \pmod{n}$. For a general r, n is said to be an ω-prime to base a if n is $\omega^{r/r'}$-prime to base a for all prime powers r' dividing r.

The main theorem in [5] is the following: Suppose $n \in A_r$ is not a prime, $n \neq (1 + r)^2$, and ω as above; then n is an ω-prime to base a for at most $\frac{\phi(n)}{2r}$ different bases a modulo n.

Since it is easy to verify that if n is prime, then it is an ω-prime to base a for all base a coprime to n, the above theorem leads to a probabilistic primality test with probability of failure at most $\frac{1}{2r}$ for any number $n \in A_r$, for which such an ω is given.

Note that if $r = 2$, then ω can be taken to be -1 for all $n \in A_2$, that is, for all odd n. It follows that the notion of ω-prime to base a coincides in this case with the notion of a strong pseudoprime for composite n, and that the result of [5] above reduces to the Rabin-Monier Theorem [11, 8].

In this paper we show that the notion of ω-prime to base a for numbers $n \in A_r$ described above leads to an ERH Conditional Polynomial Time Deterministic Primality Test for numbers $n \equiv 1 \pmod{r}$, that is, an algorithm that under the assumption of the Extended Riemann Hypothesis (ERH), runs in polynomial time,

Received by the editors April 24, 2007, and, in revised form, August 15, 2007.
2000 *Mathematics Subject Classification.* Primary 11Y11.

and determines whether any given n which is congruent to 1 modulo r is prime or composite. This generalizes Miller's Primality Theorem [8], which is the result for the case $r = 2$. We show that the complexity of our algorithm is at most the complexity of Miller's algorithm, which is $\tilde{O}((\log n)^4)$.

It is now well known that whether a number is prime or composite can be determined in polynomial time. This remarkable fact was proved by Agrawal, Kayal and Saxena, who in 2002 presented their famous algorithm known as the AKS algorithm ([1]). The authors of AKS presented two versions of their result. In the first version (posted on the internet), they proved AKS runs in at most $\tilde{O}((\log n)^{12})$ time. In the second version they improved the upper bound and obtained $\tilde{O}((\log n)^{7.5})$. They conjectured that the complexity was in fact $\tilde{O}((\log n)^6)$ and showed that this is also a lower bound for the complexity. The interest of the AKS test is mainly theoretical, since in practice it cannot be applied to some numbers that are of a size of interest for practical purpose. Even the later improvements on AKS, initiated by the first author in [4], which eventually led to what is known as the practical version of AKS, or as Granville called it in [7], the AKS-Berrizbeitia-Cheng-Bernstein-Mihailescu-Avanzi RP algorithm, is still too slow. Note also that RP stands for Random Polynomial Time, so the test is not completely deterministic. The running time of this algorithm is also $\tilde{O}((\log n)^4)$ (the same order of magnitude as Miller's ERH conditional algorithm). However the algorithm is still much slower than both Miller's algorithm and the generalization presented in this paper. Some discussion of this is given in the final section of the present paper.

Miller proved his result by using a result of Ankeny [2] on the least quadratic nonresidue. Ankeny proved that under ERH the least quadratic nonresidue modulo a prime p is $O((\log p)^2)$. Miller was able to deduce that if n is not prime, the smallest witness for the strong pseudoprime test is $O((\log n)^2)$. In 1985, in his Ph.D. dissertation, Eric Bach [3] gave an explicit bound for the constant implicit in $O((\log n)^2)$. In fact he proved the following result: if G is a proper multiplicative subgroup of the group of units modulo n, then assuming ERH there is an $m \in (\mathbb{Z}_n^* - G)$, $m < 2(\log n)^2$. In particular, Bach made effective Miller's conditional algorithm.

This theorem of Ankeny-Bach leads to an effective version of Miller's theorem as follows. First use the fact, proved independently by Rabin and Monier [11, 8], that if n is a strong pseudoprime to base a, then it is an Euler pseudoprime to base a. Next note that the subset of the multiplicative group of units modulo n consisting in the classes modulo n of the set of bases a for which n is an Euler pseudoprime is in fact a subgroup of the group of units. It was proven by Solovay and Strassen [12] that this subgroup is proper if n is composite. It follows from the above theorem of Bach that assuming ERH there is $m < 2(\log n)^2$ such that n is not an Euler pseudoprime with respect to base m. Such m is called a witness (witness to the fact that n is composite) for the Euler psedoprime test, hence for the strong pseudoprime test.

In this paper we use a strategy which is analogous to the one described above. For an integer $n \in A_r$ for which an rth root of unity ω is given we introduce the notion of Euler ω-prime to base a. We show that the set of bases a for which n is an Euler ω-prime to base a is a subgroup of the multiplicative group of unit modulo n, and we show that this subgroup is proper if n is composite. We also show that

if n is an ω-prime to base a, then it is an Euler ω-prime to base a. Hence we can apply the Ankeny-Bach Theorem to any such n.

To obtain an ERH Conditional Polynomial Time Primality Test for all numbers $n \equiv 1 \pmod{r}$ we will proceed as we did in [5], that is, for any number $n \equiv 1 \pmod{r}$ we apply a polynomial time test due to Pocklington [10] which as a result determines either that n is composite or that $n \in A_r$, and in the latter case it provides an rth root of unity ω, hence the ω-prime to base a test applies.

The paper is organized as follows. Section 2 contains preliminaries and notation borrowed from [5] which provides a comfortable setting for the treatment of the subject. The notion of Euler ω-prime to base a is given in Section 3. There we show that if $n \in A_r$ is an ω-prime to base a, then it is also an Euler ω-prime to base a. In Section 4 we show that set of bases a for which n is an Euler ω-prime to base a is a subgroup of the multiplicative group of units modulo n, and we show that this subgroup is proper if n is composite, hence we can apply the Ankeny-Bach Theorem to any such n. In the last section we present and prove the correctness of an algorithm which is an ERH Conditional Polynomial Time Primality Test for all numbers $n \equiv 1 \pmod{r}$. We also discuss the complexity of this algorithm and compare it to the so-called practical version of AKS.

2. Preliminaries and notation

Let a, n be relative prime integers. The order of a modulo n is denoted by $o_n(a)$. The greatest common divisor of a and n is denoted by (a, n). $[a]$ will denote the class of a modulo n. The cardinality of a set S is denoted by $|S|$.

The following concepts and notation are borrowed from [5].

Definition 2.1 ([5])**.** Let $A \subseteq \mathbb{N}$. An *elementary probabilistic primality test for integers in* A, denoted (T, A), is a collection $T = \{T_n : n \in A\}$ of sets with the properties:

(1) $T_n \subseteq \mathbb{Z}_n^*$ for all $n \in A$.
(2) If $n \in A$ is prime, then $T_n = \mathbb{Z}_n^*$.
(3) If $n \in A$, $a \in \mathbb{Z}_n^*$, then the question of whether $a \in T_n$ can be decided in time polynomial in $\log n$.

Example 2.2. The Fermat test (F, A_2), for $n \in A_2$,

$$F_n = \{[a] \in \mathbb{Z}_n^* | a^{n-1} \equiv 1 \pmod{n}\}.$$

Definition 2.3. Given $0 < \epsilon < 1$, we say that the test (T, A) has *probability of failure less than* ϵ if $\frac{|T_n|}{n} < \epsilon$ for all composite $n \in A$.

Example 2.4. (1) Solovay-Strassen test (S, A_2):

$$S_n = \{[a] \in \mathbb{Z}_n^* | a^{\frac{n-1}{2}} \equiv \left(\tfrac{a}{n}\right) \pmod{n}\},$$

with $n \in A_2$ and where $\left(\frac{a}{n}\right)$ is the Jacobi symbol.

Solovay and Strassen proved in [12] that the probability of failure for this test is less than $\frac{1}{2}$.

(2) The strong pseudoprime test (M, A_2) [8, 11]:

For $n \in A_2$, write $n - 1 = 2^s t$ where t is odd:

$$M_n = \left\{[a] \in \mathbb{Z}_n^* | a^t \equiv 1 \pmod{n} \text{ or } a^{2^i t} \equiv -1 \pmod{n}, 0 \leq i \leq s-1\right\}.$$

Rabin [11] and Monier [9] independently showed that (M, A_2) has probability of failure less than $\frac{1}{4}$.

Example 2.5. Let r be a positive integer, $n \in A_r$ and $\omega = \omega_n$ an integer of order r modulo d, for all d dividing n. Let $\Omega = \{\omega_n\}_{n \in A_r}$.

The rth-order test $(T(\Omega), A_r)$ [5],where

$$T(\Omega)_n = \{[a] \in \mathbb{Z}_n^* | n \text{ is an } \omega_n\text{-prime to base } a\}.$$

It was proved in [5] that $(T(\Omega), A_r)$ has probability of failure less than $\frac{1}{2r}$.

Definition 2.6. The test (T', A') is a *refinement* of (T, A), denoted by $(T, A) \leq (T', A')$, if $A \subseteq A'$ and for all $n \in A$, $T_n \subseteq T'_n$.

Definition 2.7. The test (T, A) is *algebraic* if T_n is a subgroup of $\mathbb{Z}_n^*$ for all $n \in A$.

Definition 2.8. The test (T, A) is *sharp* if $T_n = \mathbb{Z}_n^*$ implies n prime.

Definition 2.9. Let (T, A) be a test and $n \in A$ composite. A *witness* is an element of $\mathbb{Z}_n^* - T_n$.

A probabilistic test becomes deterministic if we can bound the smallest witness for composite n, i.e. for a primality test (T, A) if we can find $\tau = \tau(n)$ such that there is $a < \tau$ satisfying $[a] \in \mathbb{Z}_n^* - T_n$. As mentioned in the Introduction, Miller [8] showed, assuming ERH, that the smallest witness for composite n for the strong pseudoprime test is $O((\log n)^2)$. His result was improved by Bach, [3] who proved:

Theorem 2.10. *Let G a proper subgroup of $\mathbb{Z}_n^*$. Under ERH there is $a \in \mathbb{Z}_n^* - G$ such that $a < 2(\log n)^2$. The smallest such a must be prime.* □

In our language we obtain the following corollary that will be central to this paper. Let (T, A) be an elementary primality test. Let $C(n)$ denote the cost of verifing whether $a \in T_n$.

Corollary 2.11. *Assume $(T, A) \leq (T', A')$ for some sharp algebraic test (T', A'). Then (T, A) is an ERH Conditional Polynomial Time Primality Test with complexity bounded $\tilde{C}(n) = C(n)\pi(2(\log n)^2)$, where $\pi(x)$ denotes the number of primes less than x.*

Proof. By (3) in Definition 2.1, we know that $C(n)$ is bounded by a polynomial. Let n be composite. Then $T_n \subseteq T'_n$ which is a proper subgroup of $\mathbb{Z}_n^*$ (since (T', A') is sharp and algebraic). By Theorem 2.10, there is a prime witness less than $2(\log n)^2$. The statement on the complexity follows trivially. □

3. Euler ω-primes to base a and the generalized Solovay-Strassen test

Throughout this section, let r, n, A_r, ω_n, and Ω be as in Example 2.5.

Definition 3.1. Let p be a prime divisor of n. We define the map $\varphi_p : (\mathbb{Z}_p^*, \cdot) \to (\mathbb{Z}_r, +)$ by defining $\varphi_p([a])$ for $[a] \in \mathbb{Z}_p^*$ as the unique integer modulo r such that it satisfies the congruence

$$a^{\frac{p-1}{r}} \equiv {\omega_n}^{\varphi_p([a])} \pmod{p}.$$

For all $d = p_1 \dots p_k$, with p_i as a prime number divisor of n $(i = 1 \dots k)$, the map $\varphi_d : (\mathbb{Z}_d^*, \cdot) \to (\mathbb{Z}_r, +)$ is defined by

$$\varphi_d([a]) = \sum_i \varphi_{p_i}([a]),$$

where $[a] \in \mathbb{Z}_d^*$.

Note that φ_d, and in particular φ_n, is a group homomorphism.

Definition 3.2. We define the generalized Solovay-Strassen Primality test $(\mathbb{S}(\Omega), A_r)$ by

$$\mathbb{S}(\Omega)_n = \left\{ [a] \in \mathbb{Z}_n^* : a^{\frac{n-1}{r}} \equiv {\omega_n}^{\varphi_n([a])} \pmod{n} \right\}$$

for every $n \in A_r$. If $[a] \in \mathbb{S}(\Omega)_n$, we say n is an *Euler ω_n-prime to base a.*

Remarks 3.3. Since φ_n is a group homomorphism, $\mathbb{S}(\Omega)_n$ is a subgroup of $\mathbb{Z}_n^*$, for all $n \in A_r$. That is, $(\mathbb{S}(\Omega), A_r)$ is algebraic.

The following result is the key for the correctness of the ERH Conditional Polynomial Time Primality test that we will present in Section 5 of this paper.

Theorem 3.4. *$(T(\Omega), A_r)$ is an ERH Conditional Polynomial Time Primality Test.*

The proof of the theorem will consist of two steps: first we prove that $(T(\Omega), A_r) \leq (\mathbb{S}(\Omega), A_r)$, which is the objective of the next theorem. Then, in Section 4 we will prove that $(\mathbb{S}(\Omega), A_r)$ is sharp. The result follows trivially from these two facts, by using Corollary 2.11.

As a corollary of this theorem we will present in Section 5 a polynomial test that under ERH will determine whether a given $n \equiv 1 \pmod{r}$ is prime or composite.

The next lemma is well known.

Lemma 3.5. *Let $a \equiv b \equiv 1 \pmod{m}$. Then*

$$\frac{a-1}{m} + \frac{b-1}{m} \equiv \frac{ab-1}{m} \pmod{m}. \quad \square$$

Theorem 3.6. *For any positive integer r,*

$$(T(\Omega), A_r) \leq (\mathbb{S}(\Omega), A_r).$$

Proof. For reasons that will soon become apparent, we will denote $S(\Omega)_n$ by $\mathbb{S}_n(\omega_n)$. One can easily verify, by using the definition of $\mathbb{S}_n(\omega_n)$ and the Chinese Remainder Theorem, that $\mathbb{S}_n(\omega_n) = \bigcap_{r'} \mathbb{S}_n({\omega_n}^{r/r'})$, where r' runs through the prime powers dividing r. Since by definition, as we pointed out in the Introduction, $T(\Omega)_n = T_n(\omega_n)$ also satisfies the same intersection property, it is sufficient to prove the theorem when r is a prime power.

Let $r = q^e$ be a prime power. Let $n \in A_r$. Write $n = 1 + q^s t$ with $s \geq e$ and $(t, q) = 1$. If $a \in T_n(\omega_n)$, then either $a^t \equiv {\omega_n}^{qh} \pmod{n}$, for some integer h, or $a^{tq^i} \equiv {\omega_n}^j \pmod{n}$, where $0 \leq i \leq s - e$ and $(j, q) = 1$.

Case a). $a^t \equiv {\omega_n}^{qh} \pmod n$, with $h \in \mathbb{Z}$.

Let p be a prime dividing n. Since $n \in A_r$, then $p \equiv 1 \pmod r$ so $\frac{p-1}{r} \in \mathbb{N}$. Therefore $(a^t)^{\frac{p-1}{r}} \equiv {\omega_n}^{qh(\frac{p-1}{r})} \pmod n$, hence $\pmod p$. This gives $\varphi_p([a^t]) = [qh(\frac{p-1}{r})]_r$, where $[\ ]_r$ denotes the class modulo r.

As $\frac{n-1}{r} \equiv \sum_p \frac{p-1}{r} \pmod r$, by Lemma 3.5, the sum is taken over all primes p dividing n (allowing repetition). It follows that

$$\varphi_n([a^t]) = \sum \varphi_p([a^t]) = [qh\Big(\frac{n-1}{r}\Big)]_r.$$

We conclude from this equality and $(a^t)^{\frac{n-1}{r}} \equiv {\omega_n}^{qh(\frac{n-1}{r})} \pmod n$, that $[a^t] \in \mathbb{S}_n(\omega_n)$. But $(t, r) = 1$, thus $[a] \in \mathbb{S}_n(\omega_n)$ because it is easy to verify that $\mathbb{S}_n(\omega_n)$ is an abelian group of index dividing r.

Case b). $a^{tq^i} \equiv {\omega_n}^j \pmod n$, where $0 \leq i \leq s - e$ and $(j, q) = 1$.

Since $o_n(\omega_n^j) = q^e$, we have that $o_n(a^t) = q^{i+e}$. In consequence, $o_p(a^t) = q^{i+e}$ for any p prime dividing n and so $q^{i+e} | (p-1)$. Thus $\frac{p-1}{q^{i+e}} \in \mathbb{N}$. The same reasoning applies to Case a). First, $(a^t)^{\frac{p-1}{q^{i+e}}} \equiv {\omega_n}^{qh(\frac{p-1}{q^{i+e}})} \pmod n$. We thus get $\varphi_p([a^t]) = [qh(\frac{p-1}{q^{i+e}})]_r$.

Again, by Lemma 3.5 $\frac{n-1}{q^{i+e}} \equiv \sum_p \frac{p-1}{q^{i+e}} \pmod r$. Therefore

$$\varphi_n([a^t]) = [qh\Big(\frac{n-1}{q^{i+e}}\Big)]_r.$$

We conclude from this equality and $(a^t)^{\frac{n-1}{q^{i+e}}} \equiv {\omega_n}^{qh(\frac{n-1}{q^{i+e}})} \pmod n$, that $[a^t] \in \mathbb{S}_n(\omega_n)$. As in Case a), since $(t, r) = 1$, then $[a] \in \mathbb{S}_n(\omega_n)$. □

Note that when $r = 2$ and $\Omega = \{-1\}_{n \in A_2}$ then Theorem 3.6 states that if n is a strong pseudoprime to base a, then n is an Euler pseudoprime to base a, which is the Rabin-Monier Theorem.

Corollary 3.7. *If $r = 2$, $(T(-1), A_2) \leq (S, A_2)$.*

4. Probability of failure of the generalized Solovay-Strassen test

We still have to prove that $(\mathbb{S}(\Omega), A_r)$ is sharp. In this section we prove rather more:

Theorem 4.1. *$(\mathbb{S}(\Omega), A_r)$ has probability of failure less than $\frac{1}{r}$.*

Lemma 4.2. *$(\mathbb{S}(\Omega), A_r) \leq (F, A_r)$.*

Proof. Let $n \in A_r$. If $[a] \in S_n(\omega_n)$, then $a^{\frac{n-1}{r}} \equiv {\omega_n}^{\varphi_n([a])} \pmod n$. It is clear that $a^{n-1} \equiv 1 \pmod n$, because ω_n has order r modulo n. Thus $[a] \in F_n$. □

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be the prime factorization of n.

The following lemma is elementary and can be obtained as a trivial consequence of Lemma 2.6 in [5].

Lemma 4.3.

$$[\mathbb{Z}_n^* : F_n] = \prod_{i=1}^{k} p_i^{(\alpha_i - 1)} \frac{(p_i - 1)}{(p_i - 1, n - 1)}. \quad \square$$

Proof of Theorem 4.1. By Lemma 4.2, $(\mathbb{S}(\Omega), A_r)$ is a refinement of $(F, \mathbb{N})$. Hence $\mathbb{S}_n(\omega_n) \subseteq F_n$. If n is not square free, we use Lemma 4.3 to obtain $[\mathbb{Z}_n^* : F_n] \geq p$, for some prime $p|n$. As $n \in A_r$, for all prime divisors p of n, we have $p \equiv 1 \pmod{r}$, whence $p > r$. Thus $[\mathbb{Z}_n^* : F_n] \geq r$; this implies

$$\frac{|\mathbb{S}_n(\omega_n)|}{n} \leq \frac{|F_n|}{n} < \frac{|F_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{r}.$$

Let n be square free. Let p be a prime divisor of n. By the Chinese Remainder Theorem, there exists an integer a satisfying the following congruences:

$$a \equiv \alpha \pmod{p} \quad a \equiv 1 \pmod{(n/p)}$$

where $[\alpha]$ is a generator of $\mathbb{Z}_p^*$. We now show that $[a] \notin \mathbb{S}_n(\omega_n)$.

Since $[\alpha]$ is a generator of $\mathbb{Z}_p^*$, $\alpha^{\frac{p-1}{r}} \equiv {\omega_n}^i \pmod{p}$ for some i coprime with r, so $\varphi_p([a]) = i$. Let $q \neq p$ be any other prime divisor of n. As $a \equiv 1 \pmod{(n/p)}$, we obtain $a^{\frac{q-1}{r}} \equiv 1 \pmod{q}$ whence $\varphi_q([a]) = 0$. It follows that

$$\varphi_n([a]) = \sum_{p|n} \varphi_p([a]) = i.$$

On the other hand, since $a^{\frac{n-1}{r}} \equiv 1 \pmod{(n/p)}$ and ω_n has order r modulo d, for any d dividing n, we conclude that $a^{\frac{n-1}{r}} \not\equiv {\omega_n}^i \pmod{n}$. Thus $[a] \notin \mathbb{S}_n(\omega_n)$.

We will next show that the image of $[a] \in \mathbb{Z}_n^*/\mathbb{S}_n(\omega_n)$ has order divisible by r, from which the conclusion of the theorem follows. Suppose that $[a]^m \in \mathbb{S}_n(\omega_n)$ for some m.

As φ_n is linear, we have $\varphi_n([a^m]) = m\varphi_n([a]) = mi$. So

$$(a^m)^{\frac{n-1}{r}} \equiv {\omega_n}^{mi} \pmod{n}$$

because $a^m \in \mathbb{S}_n(\omega_n)$. Again, since $a^{\frac{n-1}{r}} \equiv 1 \pmod{(n/p)}$, ${\omega_n}^{mi}$ must be congruent to $1 \pmod{(n/p)}$. But ω_n has order r modulo d, for any d dividing n. We obtain that ${\omega_n}^{mi} \equiv 1 \pmod{(n/p)}$ from where we get $r|mi$. Finally $r|m$, since $(r, i) = 1$. □

5. An ERH conditional polynomial time primality test for all numbers $n \equiv 1 \pmod{r}$

It follows from Theorem 3.4 that an ERH Conditional Polynomial Time Primality Test can be given for all numbers $n \in A_r$, for which ω, a primitive rth root of 1 modulo each divisor d of n, is given. In this section we will present such a test for all numbers $n \equiv 1 \pmod{r}$, for a fixed positive integer $r \geq 2$.

We will see in the next proposition, which is obtained by combining Pocklington's Theorem with Bach's Theorem, that assuming ERH a polynomial time algorithm can be given, whose possible inputs are all numbers $n \equiv 1 \pmod{r}$, and whose possible output are:

1) $n \in A_r$, in which case a valid ω is given as part of the output or
2) n is composite.

The ERH Conditional Polynomial Time Test for numbers $n \equiv 1 \pmod{r}$ will be obtained by combining the following proposition with Theorem 3.4.

Proposition 5.1. *Let $r \geq 2$, $n \equiv 1 \pmod{r}$. Assuming ERH, if each of the following conditions are satisfied, then $n \in A_r$. Otherwise, n is composite.*

i) $(a^{\frac{n-1}{q}} - 1, n) = 1$ *or* n, *for all prime* $a < 2(\log n)^2$ *and for all prime* q *dividing* r.
ii) *For each prime divisor* q *of* r *there is a prime* $a < 2(\log n)^2$ *such that* $(a^{\frac{n-1}{q}} - 1, n) = 1$.
iii) $a^{n-1} \equiv 1 \pmod{n}$ *for all prime* $a < 2(\log n)^2$.

Proof. If for some prime divisor q of r, there is an integer a for which i) is not satisfied, then $(a^{\frac{n-1}{q}} - 1, n)$ is a nontrivial factor of n, so n is composite. If for some integer a iii) is not satisfied, then by Fermat's little theorem n must be composite.

Assume now that i) and iii) are satisfied for all prime a in the given range and all prime divisors q of r. Assume ii) is not satisfied. Since we are assuming i) is satisfied then there is a prime divisor q of r such that for all prime a in the given range $a^{\frac{n-1}{q}} \equiv 1 \pmod{n}$. Let $G = \{[a] \in \mathbb{Z}_n^* | a^{\frac{n-1}{q}} \equiv 1 \pmod{n}\}$. If n is prime, then G must be a proper subgroup of $\mathbb{Z}_n^*$ (in fact G has exactly $\frac{n-1}{q}$ elements). It follows from Bach's Theorem that under ERH there would be a positive integer a in the range such that $(a^{\frac{n-1}{q}} - 1, n) \neq n$. Morever, the smallest such a would have to be a prime. Since a satisfies i), it must be $(a^{\frac{n-1}{q}} - 1, n) = 1$. Then a satisfies ii), which contradicts our assumption.

For the converse we assume that i), ii) and iii) are satisfied. For each prime q dividing r let a_q be an integer satisfying ii). Let $\omega_q = a_q^{\frac{n-1}{q^s}}$, where $s = \nu_q(r)$ (the exact power of q dividing r). Let $\omega = \prod_{q|r} \omega_q$. Then ω has order r modulo every prime divisor p of n. In particular, $n \in A_r$. □

We next describe the ERH conditional primality test for all $n \equiv 1 \pmod{r}$. For clarity of exposition we will assume that r is prime. Assume n is large enough so that $n > 2(\log n)^2$.

Let $A = \{a_1 = 2, a_2 = 3, \cdots, a_t\}$ be the set of primes less than $2(\log n)^2$. Thus $|A| = t = \pi(2(\log n)^2)$.

Let $i = 1$.
Trial division with small primes.
While $(i \leq t)$
  If a_i divides n output composite.
Verifying Proposition 5.1.
  Let $\omega_n = (a_i)^{\frac{n-1}{r}} \pmod{n}$.
  If $\omega_n = 1$, $i = i + 1$.
  If $(\omega_n \pmod{n} - 1, n) \neq 1$, output composite.
  If $\omega_n^r \pmod{n} \neq 1$, output composite.
Verifying if small primes are in $T(\Omega)_n$.
  Let $j = 1$
  While $j \leq t$
    If n is not an ω_n-prime to base a_j, output composite
    $j = j + 1$
  Output prime under ERH
Output composite under ERH.

Theorem 5.2. *Assuming ERH we conclude* n *is prime if, and only if, the output is "prime under ERH" and* n *is composite if, and only if, the output is either "composite" or "composite under ERH".*

Using FFT (Fast Fourier Transform), the complexity of the algorithm is $\tilde{O}((\log n)^4)$.

Proof. Suppose the output is "composite". There are four different places in the algorithm where this may occur. If it occurs at the first place it is because a_i divides n. Since $a_i < 2(\log n)^2 < n$ it follows that it is a nontrivial divisor of n, so n is composite. If it occurs at the second place it is because a_i does not satisfy item i) in Proposition 5.1, hence $(a_i{}^{\frac{n-1}{r}} - 1, n)$ is a nontrivial divisor of n. If it occurs at the third place, then Fermat's little theorem implies n is composite. If it occurs at the fourth place, then there is a_j such that n is not an ω_n-prime to base a_j, hence n is composite. If the output is "composite under ERH" it is because items i) and iii) of the previous proposition are satisfied for all $a \in A$, but not item ii). It follows that $a^{\frac{n-1}{r}} \equiv 1 \pmod{n}$ for all prime $a \leq t$. As in the proof of Proposition 5.1, under ERH n must be composite. If the output is "prime under ERH", it is because one has verified that $a_j \in T_n(\omega_n)$ for all $1 \leq j \leq t$. So the result follows from Corollary 2.11.

We next discuss the complexity of the algorithm. It is easy to see that the complexity is bounded by $2C(n)\pi(2(\log n)^2)$, where $C(n)$ is the cost of computing $a^n \pmod{n}$. $C(n)$ involves at most $2\log n$ modular multiplications (multiplication of integers modulo n). Using the Prime Number Theorem ($\pi(x) \approx \frac{x}{\log x}$) we conclude that the complexity of this test is determined by $O(\frac{(\log n)^3}{\log(\log n)})$ modular multiplications, which by using the Fast Fourier Transform is clearly bounded by $\tilde{O}((\log n)^4)$, where $\tilde{O}(f(x)) = O(f(x)(\log f(x))^m)$. □

In the practical version of AKS the complexity is determined by the computation of $(1+x)^n \pmod{n, x^r - a}$, where $r > (\log n)^2$ (hopefully not much bigger) and a is a relatively small integer.

To compute this one must perform about $2\log n$ multiplications of polynomials of degree at most $r-1$, which (using the Fast Fourier Transform) implies around $r \log r$ modular multiplications. Hence one must perform more than $O((\log n)^3 \log(\log n))$ modular multiplications which is quite a bit more than the amount of multiplications required for the test presented in this paper. Moreover, AKS requires a great deal of use of memory space as opposed to our test, which is highly parallelisable. Indeed, to run the algorithm described above, one can partition the set A into k disjoint subsets $A_i, i = 1, \cdots, k$, and run the algorithm separately for each of the A_i's, and then collect the information.

It is reasonable to believe that if r is large, then the smallest witness under ERH for the rth-order test is smaller than the smallest witness for the Miller-Rabin Test. This, however, we leave as a conjecture.

Further research on this topic should include the study of ERH and the Quadratic Frobenius Test [6].

Acknowledgments

We thank Andrew Shallue for his careful revision of our preprint and his various valuable remarks, which helped to improve the overall quality of the paper. We also thank the "Decanato de Investigación y Desarrollo de la Universidad Simón Bolívar" for their financial support of our research group GID-24.

References

[1] Agrawal, M., Kayal, N., and Saxena, N. "Primes in P." Preprint, Aug. 6, 2002. http://www.cse.iitk.ac.in/users/manindra/publications.html.

[2] Ankeny, N. C. The Annals of Mathematicas, 2nd Ser., Vol. 55, No. 1. (Jan., 1952), pp. 65-72. MR0045159 (13:538c)

[3] Bach, E. Analytic methods in the analysis and design of number-theoric algorithms. ACM Distinguished Dissertations. MIT Press, Cambridge, MA, 1985. MR807772 (87i:11185)

[4] Berrizbeitia, P. Sharpening Primes is in P for a large family of numbers. Math. Comp. 74 (2005), no. 252, 2043–2059. MR2164112 (2006e:11191)

[5] Berrizbeitia, P., and Berry, T. G. Generalized Strong Pseudoprime Tests and Applications, J. Symbolic Computation 30 (2000), no. 2, 151–160. MR1777169 (2001f:11201)

[6] Grantham, J. A probable prime test with high confidence. J. Number Theory 72 (1988), no. 1, 32-47. MR1643284 (2000e:11160)

[7] Granville, A. It is easy to determine whether a given integer is prime. Bull. Amer. Math. Soc. (N.S) 42 (2005), no. 1, 3–38. MR2115065 (2005k:11011)

[8] Miller, G. Riemann's hypothesis and tests for primality. J. Comput. System Sci. 13 (1976), no. 3, 300-317. MR0480295 (58:470a)

[9] Monier, L. Evaluation and comparison of two efficient probabilistic primality testing algorithms. Theoret. Comput. Sci. 12 (1980), no. 1, 97–108. MR582244 (82a:68078)

[10] Pocklington, H. C. The Determination of the Prime or Composite Nature of Large Numbers by Fermat's Theorem. Proc. Cambridge Phil. Soc. 18, 29-30, 1914.

[11] Rabin, M. O. Probabilistic algorithm for testing primality. J. Number Theory 12 (1980), no. 1, 128–138. MR566880 (81f:10003)

[12] Solovay, R., and Strassen, V. The fast Monte-Carlo test for primality, SIAM J. Comput. 6 (1977), no. 1, 84–85. MR0429721 (55:2732)

Departamento de Matemáticas P. y A., Universidad Simón Bolívar, Sartenejas, Caracas 1080-A, Venezuela

E-mail address: pedrob@usb.ve

Departamento de Matemáticas P. y A., Universidad Simón Bolívar, Sartenejas, Caracas 1080-A, Venezuela

E-mail address: olivieri@usb.ve