EFFICIENTLY CERTIFYING NON-INTEGER POWERS

Erich Kaltofen and Mark Lavin

Abstract. We describe a randomized algorithm that, given an integer a, produces a certificate that the integer is not a pure power of an integer in expected $(\log a)^{1+o(1)}$ bit operations under the assumption of the Generalized Riemann Hypothesis. The certificate can then be verified in deterministic $(\log a)^{1+o(1)}$ time. The certificate constitutes for each possible prime exponent p a prime number q_p, such that $a \bmod q_p$ is a p-th non-residue. We use an effective version of the Chebotarev density theorem to estimate the density of such prime numbers q_p.

Keywords. Integer roots, integer powers, linear-time algorithm, bit complexity, Chebotarev density theorem.

Subject classification. 11Y16 Number Theory: algorithms; complexity 68W30 Computer Science: symbolic computation and algebraic computation,

1. Introduction

Recent algorithms of Agrawal, Kayal, and Saxena (AKS) and Bernstein have brought primality certificates into deterministic polynomial time (Agrawal *et al.* 2004; Bernstein 2003). A necessary step in all of these new algorithms is to check whether the number being certified is a pure power of a prime. Using Newton iteration to find the roots is one way to check that an integer a is not a pure prime power but it requires $(\log a)^{3+o(1)}$ time (Caviness 1975). Other methods have been proposed using sieving techniques which require $O((\log a)^2)$ time on average (Bach & Sorenson 1993; Balasubramanian & Nagaraj 1996). Daniel Bernstein *et al.* published algorithms running in $(\log a)^{1+o(1)}$ (Bernstein 1998; Bernstein *et al.* 2007). This paper gives a randomized algorithm which can also accomplish this task quickly. Under the assumption of the Generalized Riemann Hypothesis (GRH) our algorithm gives a certificate that a given integer is not a pure power of an integer in $(\log a)^{1+o(1)}$ bit operations, or fails, that with probability no more than 1/2. The certificate can then be verified in deterministic $(\log a)^{1+o(1)}$ time. In all of those complexity bounds, the addition of "$+o(1)$" in the exponent captures additional bit complexities of $C_1(\operatorname{loglog} a)^{C_2}(\operatorname{logloglog} a)^{C_3}$ for real constants C_1, C_2 and C_3. The main distinguishing factor is that we accomplished this task without taking any roots. Our algorithm is a purely modular method without Newton iteration and is highly parallelizable with small memory requirements.

2. Main Idea

Fermat's Little Theorem states that for every prime q and every integer a, $a^q \equiv a \pmod{q}$. If q does not divide a, then we have that $a^{q-1} \equiv 1 \pmod{q}$. Now suppose that $a = b^p$ for some integer b and prime p. If q is another prime that does not divide b and satisfies $q \equiv 1 \pmod{p}$, then $a^{(q-1)/p} \equiv b^{q-1} \equiv 1 \pmod{q}$. The idea of our algorithm is to find a prime q for each prime $p \leq \log_2 a$ such that $q \equiv 1 \pmod{p}$ and $a^{(q-1)/p} \not\equiv 1 \pmod{q}$. Finding such a prime q exposes that a is not a pure p^{th} power. The Chebotarev density theorem provides a way to know the frequency with which these primes occur and is stated below.

Theorem 2.1. *Let L be a Galois extension of $\mathbb{Q}$ and let C be any conjugacy class in $G = Gal(L/\mathbb{Q})$. Then the set $\{q$, an unramified prime in $\mathbb{Z} \mid F_L(q) = C\}$ has density $|C|/|G|$, where $F_L(q)$ is the class of Frobenius elements of all prime ideals in the ring of integers of L that contain q.*

This is not the strongest form of this theorem, however it is strong enough to use in this paper. For a proof of the above theorem see (Narkiewicz 1990). While the Frobenius element depends on the ideal constructed above it, in this case the Frobenius element will always map into the same conjugacy class in the Galois group. The set of automorphisms in the Galois group whose root permutations correspond to a full cycle on the roots of a polynomial is the conjugacy class that is of interest to us. These cycles which do not fix a root correspond to primes, q, which leave $x^p - a$ irreducible modulo q. In the next section we will study the Galois group of the splitting field for $x^p - a$ as well as the conjugacy class of elements that correspond to root permutations which do not fix a root.

3. Notation and Basic Proofs

Let $\mathbb{Q}$ denote the set of rational numbers. The symbol $\mathbb{F}_p$ denotes the finite field with prime number of elements, p. By $a^{1/p}$ we will denote the real p^{th}

root of a and ω_p will denote a primitive p^{th} root of unity. The discriminants of the extensions $\mathbb{Q}(a^{1/p}), \mathbb{Q}(\omega_p)$, and $\mathbb{Q}(a^{1/p}, \omega_p)$ will be denoted by Δ_p , Δ_ω, and $\Delta_{p,\,\omega}$ respectively. Throughout the rest of this paper $\log a$ will be understood to have base 2 unless otherwise noted.

The rest of this section is devoted to basic proofs necessary for the analysis of our algorithm.

Lemma 3.1. *For p a prime, $a \in \mathbb{Q}$ with $a \neq b^p$ for all $b \in \mathbb{Q}$, the p^{th} cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}(a^{1/p})$.*

Proof. A primitive p^{th} root of unity ω_p is a root of Φ_p. Consider the extension $\mathbb{Q}(a^{1/p}, \omega_p)$ over $\mathbb{Q}$. By the Tower Theorem, the degrees of the extensions will satisfy the following equalities:

$$[\mathbb{Q}(a^{1/p}, \omega_p) \colon \mathbb{Q}] = \begin{cases} [\mathbb{Q}(a^{1/p}, \omega_p) \colon \mathbb{Q}(a^{1/p})] \cdot [\mathbb{Q}(a^{1/p}) \colon \mathbb{Q}], \\ [\mathbb{Q}(a^{1/p}, \omega_p) \colon \mathbb{Q}(\omega_p)] \cdot [\mathbb{Q}(\omega_p) \colon \mathbb{Q}]. \end{cases}$$

Since $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and $x^p - a$ are both irreducible over $\mathbb{Q}$, the degrees of the extensions will be $[\mathbb{Q}(\omega_p) \colon \mathbb{Q}] = p - 1$ and $[\mathbb{Q}(a^{1/p}) \colon \mathbb{Q}] = p$. So $[\mathbb{Q}(a^{1/p}, \omega_p) \colon \mathbb{Q}] \geq \operatorname{lcm}(p, p-1) = p(p-1)$ since it is divisible by both p and $p-1$ which are relatively prime. Also $[\mathbb{Q}(a^{1/p}, \omega_p) \colon \mathbb{Q}(a^{1/p})] \leq p - 1$ since ω_p satisfies $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ over $\mathbb{Q}(a^{1/p})[x]$. Therefore $[\mathbb{Q}(a^{1/p}, \omega_p) \colon \mathbb{Q}] = p(p-1)$ which implies $[\mathbb{Q}(a^{1/p}, \omega_p) \colon \mathbb{Q}(a^{1/p})] = p-1$. Hence, the p^{th} cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}(a^{1/p})$. □

It is clear from this lemma that $\mathbb{Q}(a^{1/p}, \omega_p) \cong \mathbb{Q}[y, z]/(y^p - a, \Phi_p(z))$. Therefore, any element in $\mathbb{Q}(a^{1/p}, \omega_p)$ has a canonical representation of the form:

$$\sum_{i=0}^{p-1} \sum_{j=0}^{p-2} \alpha_{i,j}\, a^{i/p}\, \omega_p^j, \text{ with } \alpha_{i,j} \in \mathbb{Q}$$

Theorem 3.2. *Let p be a prime and let $a \in \mathbb{Q}, a \neq b^p$ for all $b \in \mathbb{Q}$. Then the Galois group, $\mathcal{G}$, of the equation $x^p - a$ over $\mathbb{Q}$ is isomorphic to $G = \{\left[\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right] \mid x, y \in \mathbb{F}_p, x \neq 0\}$.*

Proof. The splitting field for $x^p - a$ is $\mathbb{Q}(a^{1/p}, \omega_p)$. The $\mathbb{Q}$-automorphisms of this extension are well defined by simply mapping the generators $a^{1/p}$ and ω_p. Then the set of all $\mathbb{Q}$-automorphisms is

$$\mathcal{G} = \{\phi \colon a^{1/p} \mapsto \omega_p^i a^{1/p}, \omega_p \mapsto \omega_p^j \mid 0 \leq i \leq p-1, 1 \leq j \leq p-1\}$$

Now define $\Psi\colon \mathcal{G} \mapsto G$ by $\Psi(a^{1/p} \mapsto \omega_p^i a^{1/p}, \omega_p \mapsto \omega_p^j) = \left[\begin{smallmatrix} j & i \\ 0 & 1 \end{smallmatrix}\right]$. Next we will show Ψ is an isomorphism.

Suppose that there exist $\sigma, \theta \in \mathcal{G}$ such that $\Psi(\sigma) = \Psi(\theta)$. Then $\Psi(\sigma) = \left[\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right] = \Psi(\theta)$ for some $x, y \in \mathbb{F}_p$, where $x \neq 0$. So $\sigma\colon a^{1/p} \mapsto \omega_p^y a^{1/p}, \omega_p \mapsto \omega_p^x = \theta$. Therefore Ψ is one to one. Now suppose $\left[\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right] \in G$. Then $\sigma \in \mathcal{G}, \sigma\colon a^{1/p} \mapsto \omega_p^y a^{1/p}, \omega_p \mapsto \omega_p^x$ then $\Psi(\sigma) = \left[\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right]$. Thus Ψ is onto. The identity map $id \in \mathcal{G}, id\colon a^{1/p} \mapsto a^{1/p}, \omega_p \mapsto \omega_p$ then $\Psi(id) = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Suppose that $\sigma, \theta \in \mathcal{G}$, let $\sigma = a^{1/p} \mapsto \omega_p^x a^{1/p}, \omega_p \mapsto \omega_p^y$ and $\theta = a^{1/p} \mapsto \omega_p^z a^{1/p}, \omega_p \mapsto \omega_p^w$. We see that $(\sigma\theta)(a^{1/p}) = \omega_p^{x+zy} a^{1/p}$ and $(\sigma\theta)(\omega_p) = \omega_p^{wy}$ by the composition of the maps. So $\Psi(\sigma\theta) = \left[\begin{smallmatrix} wy & x+zy \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} w & z \\ 0 & 1 \end{smallmatrix}\right] = \Psi(\sigma)\Psi(\theta)$. Therefore $\Psi\colon \mathcal{G} \mapsto G$ is isomorphism. □

THEOREM 3.3. *There are exactly $p-1$ automorphisms in the Galois group of $x^p - a$ over $\mathbb{Q}$ that map to full p-cycles on the roots of $x^p - a$.*

PROOF. From the previous theorem, the Galois group is isomorphic to $G = \{\left[\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right] \mid x, y \in \mathbb{F}_p \text{ with } x \neq 0\}$. So $|G| = p(p-1)$. By the Sylow theorems, there exists a p-subgroup of G. Let t denote the number of p-subgroups. Then t divides $p-1$ and $t \equiv 1 \pmod p$. Thus, $t = 1$ meaning there is only one

subgroup of order p. One element in this subgroup is the identity element and the other $p-1$ have order p. These $p-1$ elements of order p correspond to $\mathbb{Q}$-automorphisms of order p. These $\mathbb{Q}$-automorphisms of order p then map to full p-cycles in the set of permutations on the roots of $x^p - a$. □

COROLLARY 3.4. *The set of automorphisms*

$$\{a^{1/p} \mapsto \omega_p^i a^{1/p}, \omega_p \mapsto \omega_p \mid 1 \leq i \leq p-1\}$$

correspond to the full p-cycles and all others fix at least one root.

PROOF. The automorphism $\sigma\colon a^{1/p} \mapsto \omega_p^y a^{1/p}, \omega_p \mapsto \omega_p^z$ maps the root $\omega_p^x a^{1/p}$ to ω_p^{xz+y}. The powers are all taken modulo p, so an automorphism will fix a root if $x \equiv xz + y \pmod p$. If $j = 1$ and $i \neq 0$ then there are no solutions to this congruence, hence no root is fixed. When $j = 1$ and $i = 0$ then σ is the identity automorphism which fixes every root. If $j \neq 1$ then the root $\omega_p^x a^{1/p}$ where $x \equiv y(z-1)^{-1} \pmod p$ will be fixed by the automorphism $\sigma\colon a^{1/p} \mapsto \omega_p^y a^{1/p}, \omega_p \mapsto \omega_p^z$. □

The set of full cycles in the Galois group is the conjugacy class which we need in the Chebotarev Theorem 2.1.

Theorem 3.5. *The discriminant of the field extension $\mathbb{Q}(a^{1/p}, \omega_p)$,denoted by $\Delta_{p,\omega}$, divides $a^{(p-1)^2}\, p^{2p^2-3p}$.*

Proof. The discriminant of the number field $\mathbb{Q}(a^{1/p})$ divides the discriminant of $x^p - a$ which equals $\pm a^{p-1}p^p$. From Lemma 3.1 we see that this number field has dimension p over $\mathbb{Q}$. The discriminant of the number field $\mathbb{Q}(\omega_p)$, of degree $p-1$ over $\mathbb{Q}$, is $\pm p^{p-2}$ by Theorem 2.9 in (Narkiewicz 1990). So from Corollary 2 to Proposition 4.9 in (Narkiewicz 1990), the discriminant of $\mathbb{Q}(a^{1/p}, \omega_p)$ divides $(a^{p-1}p^p)^{p-1}(p^{p-2})^p = a^{(p-1)^2}\, p^{2p^2-3p}$. □

4. Algorithm and Complexity

Our algorithm takes in an integer a and with probability better than 1/2 produces a certificate proving it is not a pure integer power. If a is a pure power, the algorithm always returns FAILURE.

Step 1. Input: Integer $a > 1$

Step 2. Start certificate $S = \{\}$

Step 3. For each prime $p \le \log_2 a$, find 3 primes $q_{p,1}, q_{p,2}, q_{p,3}$ of a magnitude described later such that
$q_{p,i} \equiv 1 \pmod{p}$ for $i = 1, 2, 3$

Step 4. For each p, test if $a^{(q_{p,i}-1)/p} \not\equiv 1$ and $\not\equiv 0 \pmod{q_{p,i}}$ for any of the $q_{p,i}$ and if so then add the pair $(p, q_{p,i})$ to the certificate

Step 5. Repeat Steps 3–4 $\lceil 1 + \log\log a \rceil$ times, but skip primes that have already been added to the certificate.

Step 6. If all the primes have been certified then output the certificate, S. Else return FAILURE.

The highest possible power that a can be is $\log a$. To certify that a is not a pure power we must certify that a is not a p^{th} power for each prime $p \le \log a$. The certificate will then contain $\pi(\lfloor \log a \rfloor)$ pairs, where $\pi(x)$ is the number of primes $\le x$.

Remark: If a is an odd integer that is being tested for primality, then one needs only to check powers up to $\lfloor \log_3 a \rfloor$, since a cannot be a power of 2 in this case.

Before we begin the analysis, we need to have a few bounds concerning the distribution of certifying primes. In (Lagarias *et al.* 1979) Lagarias, Montgomery, and Odlyzko give an effective version of the Chebotarev density and a bound for the least prime in an arithmetic progression. However, the bounds are given with effectively computable constants. Oesterlé (1979) gives many of the same bounds for which he has found the constants. The one that will serve us best is stated below.

THEOREM 4.1. *Assume the Generalized Riemann Hypothesis (GRH). Let $L \supset \mathbb{Q}$ be a Galois extension of degree n_L with Galois group G. Let C denote any conjugacy class in G. Let*

$$\pi_C(x) = |\{q, \text{ an unramified prime in } \mathbb{Z}, q \leq x \mid F_L(q) = C\}|.$$

Then for all $x \geq 2$,

$$\left|\pi_C(x) - \frac{|C|}{|G|}\,\mathrm{Li}(x)\right| \leq \frac{|C|}{|G|}\sqrt{x}\,\Big(2\log_e|\Delta_L| + n_L \log_e x\Big), \tag{4.2}$$

where Δ_L denotes the discriminate of the extension L.

See (Lagarias *et al.* 1979; Oesterlé 1979). Here $\mathrm{Li}(x)$ denotes the offset logarithmic integral of x,

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log_e t}, \text{ where } \mathrm{li}(x) = \int_0^x \frac{dt}{\log_e t} \text{ and } \mathrm{Li}(x) = \mathrm{li}(x) - \mathrm{li}(2)$$

with $\mathrm{li}(2) \approx 1.045163$, and we will make use of the inequalities $\mathrm{Li}(x) > x/\log_e(x)$ for $x > 6.6$ (cf. (Rosser & Schoenfeld 1962), Lemma 4: $\mathrm{li}(x) > x/(\log_e(x) - 1/2) + \mathrm{li}(\sqrt{x})$ for $x \geq e^5$) and

$$\mathrm{li}(x) + \frac{1}{8\pi}\sqrt{x}\log_e(x) > \pi(x) \text{ for } x \geq \frac{3}{2}, \tag{4.3}$$

the latter of which is equivalent to the Riemann hypothesis (Schoenfeld 1976).

Now we want to apply this theorem to our particular extension $\mathbb{Q}(a^{1/p}, \omega_p)$, which is of degree $p(p-1)$ by Lemma 3.1. We saw in Theorem 3.2 and Theorem 3.3 that there were $p-1$ full cycles out of the whole Galois group which had $p(p-1)$ elements. These full cycles form a conjugacy class, C_{cycles}, in the Galois group. The idea is that we factor the polynomial $x^p - a$ over $\mathbb{F}_q$. If a is not a pure p^{th} power, then this polynomial will be irreducible for some q. The density of primes q for which $x^p - a$ is irreducible corresponds to the density of the automorphisms in the Galois group of $x^p - a$ that do not fix any roots. We see from Corollary 3.4 that there are $p-1$ cycles which do not fix a root. Using the Chebotarev Theorem, we see that that the primes we are looking for have density $1/p$ in the set of all primes. Using these facts we are going to estimate how big an interval we need to use to get a density within half of what is predicted by the Chebotarev Theorem.

Theorem 4.4. *Let $a \geq 275$. If $x \geq 10(\log_2 a)^{10}$ then $\pi_{C_{\text{cycles}}}(x) \geq 1/(2p) \cdot \pi(x)$ (assuming the GRH).*

Proof. From Lemma 3.1, Theorem 3.5, and Corollary 3.4, the degree of $\mathbb{Q}(a^{1/p}, \omega_p)$ over $\mathbb{Q}$ is $p(p-1)$ and $|C_{\text{cycles}}|/|G| = 1/p$. From equation (4.2), we have

$$\pi_{C_{\text{cycles}}}(x) - \frac{1}{p}\operatorname{Li}(x) \geq -\frac{\sqrt{x}}{p}\Big(2\log_e|\Delta_{p,\omega}| + p(p-1)\log_e x\Big)$$

Therefore, an x such that

$$\begin{aligned}\pi_{C_{\text{cycles}}}(x) &\geq \frac{1}{p}\operatorname{Li}(x) - \frac{\sqrt{x}}{p}\Big(2\log_e|\Delta_{p,\omega}|) + p(p-1)\log_e x\Big)\\ &\geq \frac{1}{2\,p}\Big(\operatorname{Li}(x) + \operatorname{li}(2) + \frac{1}{2\pi}\sqrt{x}\log_e x\Big) > \frac{1}{2p}\pi(x)\end{aligned}$$

suffices (provided $x \geq 2$), the last inequality by (4.3). For the middle inequality we can estimate, with $2 \leq p \leq \log_2 a$ for $x \geq 7$,

$$\begin{aligned}\frac{1}{2\,p}\operatorname{Li}(x) &\geq \frac{x}{2p\,\log_e x}\\ &\geq \frac{\sqrt{x}}{2p}\Big(4\log_e|\Delta_{p,\omega}| + 2p(p-1)\log_e(x) + \frac{\operatorname{li}(2)}{\sqrt{x}} + \frac{\log_e x}{2\pi}\Big)\end{aligned} \tag{4.5}$$

where (4.5) can be satisfied for $p \leq \log_2(a)$ and $|\Delta_{p,\omega}| \leq a^{(p-1)^2}\, p^{2p^2-3p}$ (Theorem 3.5) by choosing $x \geq 10(\log a)^{10}$ for $a \geq 275$. □

Remark: The estimates in Theorem 4.4 are valid for smaller asymptotic values of x. From the proof if follows that for every $\epsilon > 0$ there is a constant c such that for $x \geq c\log_2(a)^{6+\epsilon}$ we have $\pi_{C_{\text{cycles}}}(x) \geq 1/(2p) \cdot \pi(x)$.

The primes q that are congruent to 1 modulo p have density $1/\phi(p) = 1/(p-1)$ in the set of all primes. These primes are the only ones which could possibly work to expose that a is not a pure power by Fermat's Little Theorem. So if we restrict our search within the set of primes congruent to 1 modulo p then we expect the ones we want to have density $(p-1)/p$.

We see from the above theorem that if we pick a prime, q, below $10\,(\log a)^{10}$ the probability that it will satisfy $q \equiv 1 \pmod{p}$ and $a^{(q-1)/p} \not\equiv 1$ or $0 \pmod{q}$ is at least $(p-1)/(2p)$, which is at least $1/4$. Since the probability that the found prime q will certify our power p is at least $1/4$, the probability that it fails is at worst $3/4$. If we collect i primes, the probability that they all fail is at worst $(3/4)^i$. The probability that at least one prime will certify will then be at least $1-(3/4)^i$. If $i \geq 3$ then the probability that at least one of the i primes will certify a as a non-p^{th} power will be at least $1/2$. In our algorithm, we pick 3 possible certifying primes for each power, so the probability that any given power is certified is at least $1/2$. However, the probability that all $\pi(\lfloor \log a \rfloor)$ powers are certified in one round is very small, approximately $(1/2)^{\log a/\operatorname{loglog} a}$. To fix this problem Steps 3 and 4 are run in a loop up to $1 + \operatorname{loglog} a$ times. The next lemma gives us the probability that a certificate will be produced in $1 + \operatorname{loglog} a$ rounds.

Lemma 4.6. *The above algorithm produces a certificate with probability better than 1/2.*

Proof. If the found primes $q_{p,1}, q_{p,2}, q_{p,3}$ are randomly taken from the interval $[1, 10\,(\log a)^{10}]$, we see from Theorem 4.4 that the probability that $q_{p,i}$ satisfies $q_{p,i} \equiv 1 \pmod{p}$ and $a^{(q_{p,i}-1)/p} \not\equiv 1$ or $0 \pmod{q_{p,i}}$ is at least $(p-1)/(2p) \geq 1/4$. Then the probability that a group of 3 primes will certify a given prime, p, is $1-(3/4)^3 > 1/2$, so the probability that they fail is less than $1/2$. The probability that a given prime, p, fails to be certified in all of the $\lceil 1+\operatorname{loglog} a \rceil$ rounds is less than $(1/2)^{1+\operatorname{loglog} a}$, so the probability that at least one prime certifies the prime, p, is more than $1-(1/2)^{1+\operatorname{loglog} a}$. Then the probability that all $\pi(\lfloor \log a \rfloor)$ primes are certified is more than $(1-(1/2)^{1+\operatorname{loglog} a})^{\pi(\lfloor \log a \rfloor)} \geq (1-(1/2)^{1+\operatorname{loglog} a})^{\log a} = (1-1/(2\log a))^{\log a} = (1-1/(2\log a))^{(2\log a)/2} \geq (1/4)^{1/2} = 1/2$. □

Theorem 4.7. *Under the assumption of the Generalized Riemann Hypothesis with probability better than 1/2, the above algorithm produces a certificate in* $(\log a)^{1+o(1)}$ *time.*

Proof. For each prime p less than $\log a$ we need to find another prime q such that $q \equiv 1 \pmod{p}$ and $a^{(q-1)/p} \not\equiv 1$ or $0 \pmod{q}$. We see from Theorem 4.4 that the primes which will satisfy this congruence have density among the primes at least $(p-1)/(2p)$ on the interval $[0, 10\,(\log a)^{10}]$. So pick a random integer q in this interval and test $q \equiv 1 \pmod{p}$. This will take $O(\log\log a)$ time. If q passes the test for $q \equiv 1 \pmod{p}$, then run the AKS test to ensure the primality of q. It is expected that we will need to test $O(\log\log a)$ integers before finding a prime. Testing each integer for primality will take $O((\log\log a)^{12})$ time (Agrawal *et al.* 2004). Before testing $a^{(q-1)/p} \not\equiv 1$ or $0 \pmod{q}$, we first collect three primes for each power, $q_{p,1}, q_{p,2}, q_{p,3}$. Having collected a number of possible certifying primes, we test $a^{(q_{p,i}-1)/p} \not\equiv 1$ or $0 \pmod{q_{p,i}}$ by first computing $u_{p,i} = (a \bmod q_{p,i})$ for each of the collected $q_{p,i}$'s using multipoint evaluation. These residues $u_{p,i}$ can all be computed in $(\log a)^{1+o(1)}$ (Aho *et al.* 1974). To test $a^{(q_{p,i}-1)/p} \not\equiv 1$ or 0 $\pmod{q_{p,i}}$, we use binary exponentiation on the computed residue $u_{p,i}$. Each can be done in $O((\log q)^3)$ time (Bach & Shallit 1996). There are approximately $3\log a/\log\log a$ of them which need to be computed since there are approximately $\log a/\log\log a$ primes less than $\log a$. Since we have that $q = O((\log a)^{10})$, each congruence is checked in $O((\log q)^3)$ which is $O((\log\log a)^3)$. This gives us that the total time for checking all of the $a^{(q_{p,i}-1)/p} \not\equiv 1$ or $0 \pmod{q_{p,i}}$ will be $O((\log\log a)^3 \log a/(\log\log a)) + (\log a)^{1+o(1)} = (\log a)^{1+o(1)}$. This is Step 4 in our algorithm and it is the most costly. Steps 3 and 4 run in a loop at most $1 + \log\log a$ times. So we have the the running time will be $(1 + \log\log a) \cdot (\log a)^{1+o(1)}$ which is $(\log a)^{1+o(1)}$. □

Remark: One could replace the AKS test with the Miller test which is made deterministic under the GRH. Under the GRH, the Miller test can certify the primality of q in $(\log\log a)^{4+o(1)}$ time, which affects the overall complexity of our algorithm in the exponent of $\log\log a$. However, one should note that this step is not where our algorithm requires the assumption of the GRH.

Though this is formulated as a Monte Carlo algorithm, one could easily turn the algorithm into a Las Vegas algorithm by running it over and over again until a certificate is produced. The expected running time of such an algorithm would be $(1/2)(\log a)^{1+o(1)} + (1/4)(\log a)^{1+o(1)} + (1/8)(\log a)^{1+o(1)} + \cdots + (1/2^k)(\log a)^{1+o(1)} + \cdots = (\log a)^{1+o(1)} \sum_{i=1}^{\infty}(1/2)^i = (\log a)^{1+o(1)}$.

Theorem 4.8. *A certificate produced by our algorithm can be verified in* $(\log a)^{1+o(1)}$ *time.*

Proof. For each prime power p less than $\log a$, the congruence $q \equiv 1$ $\pmod{p}$ and $a^{(q-1)/p} \not\equiv 1$ or $0 \pmod{q}$ needs to be checked with its paired prime, q. We can compute $u_q = (a \bmod q)$ for all the q's at once using multipoint evaluation in $(\log a)^{1+o(1)}$ time (Aho *et al.* 1974). Then by using binary exponentiation on u_q, checking the congruence $a^{(q-1)/p} \not\equiv 1$ or $0 \pmod{q}$ can be done in $O((\log q)^3)$ time using classic multiplication (Bach & Shallit

1996). From Theorem 4.4 we have that $q = O((\log a)^{10})$, so each congruence is checked in $O((\log q)^3)$ which is $O((\operatorname{loglog} a)^3)$. There are approximately $(\log a)/(\operatorname{loglog} a)$ primes less than $\log a$ for which this congruence needs to be checked. This gives us that the total time will be
$(\log a)^{1+o(1)} + O((\operatorname{loglog} a)^3 \log a/(\operatorname{loglog} a)) = (\log a)^{1+o(1)}$. □

5. Results and Example Certificates

Using $a = 43017772231855, p = 31$ and checking the first 10,000 primes, we found that 338 are congruent to 1 modulo p. Of those 338 primes, 327 of them satisfied $a^{(q-1)/p} \not\equiv 1$ or $0 \pmod{q}$. So we found that $327/338 = .9674556213$ is the actual value using the first 10,000 primes and the value predicted by the cycle structure of the Galois group and the Chebotarev density theorem is $30/31 = .9677419355$. The difference between these two is .0002863141821. In fact the first two primes that are congruent to 1 modulo 31, 311 and 373, certify that 43017772231855 is not a pure 31st power. For $a = 67, p = 5$, 21 of the first 24 primes that are congruent to 1 modulo 5 certify that 67 is not a pure 5th power. There seems to be the general trend that the first or second prime tested that is congruent to 1 modulo p will certify that a is not a pure p^{th} power (the average value is $p/(p-1)$ primes), though as larger p's are checked the gaps between the first and second primes in the progression becomes much larger. Some example certificates illustrate how small the first prime that certifies a as a non-p^{th} power compared to the upper bound used in the proof of Theorem 4.7.

These example certificates were created using this small routine in Maple 7. In this routine we simply look for the first q which exposes a as a non-p^{th} power.

This first one is for Gauss's lifespan 4/30/1777 – 2/23/1855.
$a = 43017772231855 = 5 \cdot 8603554446371$
$S = \{(2,13),(3,19),(5,11),(7,29),(13,53),(17,103),(19,191),(23,47),$
$(29,59),(31,311),(37,223),(41,739)\}$

Here is one for the prime $2^{31}-1$.
$a = 2^{31}-1 = 2147483647$
$S = \{(2,5),(3,13),(5,61),(7,29),(11,23),(13,53),(17,103),(19,191),$
$(23,47),(29,59)\}$

Since these numbers are odd, they cannot be pure powers of 2. So we do not need to check up to the $\log a$ but only up to $\log_3 a$. This will shorten the certificates to be :

$a = 43017772231855$
$S = \{(2, 13), (3, 19), (5, 11), (7, 29), (13, 53), (17, 103), (19, 191), (23, 47), (29, 59)\}$
$a = 2147483647$
$S = \{(2, 5), (3, 13), (5, 61), (7, 29), (11, 23), (13, 53), (17, 103), (19, 191)\}$

6. Future Work/Improvements

It might be advantageous to use trial divisions (cf. (Bach & Sorenson 1993)) to ensure that the number a is not a pure power of a small prime say up to some small prime r. This would allow us to lower the bound on the prime powers we need to certify from $\log a$ to $\log_r a$. Also an assumption in the probabilistic analysis is that each of the trials is independent. This assumption is fair in that for each power we can throw away any primes we find to certify and start all over again. However, it might be useful to analyze the probability that a prime, that is congruent to 1 modulo two different primes, will certify both prime powers. Or that if it does not certify one power does that increase or decrease the chance that it will certify the other. Such an analysis could help save time by allowing the primes found to be saved and used for other prime powers in the certificate.

Acknowledgements

We thank two referees for their helpful comments.

This material is based on work supported in part by the National Science Foundation under Grants Nos. CCR-0113121 and CCR-0305314.

References

Manindra Agrawal, Neerja Kayal & Nitin Saxena (2004). PRIMES is in P. *Annals of Math.* **160**, 781–793.

Alfred Aho, John Hopcroft & Jeffery Ullman (1974). *The Design and Analysis of Computer Algorithms*. Addison-Wesley.

Eric Bach & Jeffrey Shallit (1996). *Algorithmic Number Theory Volume 1: Efficient Algorithms*. MIT Press.

Eric Bach & Jonathan Sorenson (1993). Sieve Algorithms for Perfect Power Testing. *Algorithmica* **9**, 313–328.

R. Balasubramanian & S. V. Nagaraj (1996). Perfect Power Testing. *Inf. Process. Lett.* **58**(2), 59–63.

Daniel Bernstein (1998). Detecting Perfect Powers in Essentially Linear Time. *Mathematics of Computation* **67**, 1253–1283.

Daniel Bernstein (2003). Proving Primality in Essentially Quartic Random Time. http://cr.yp.to/djb.html.

Daniel J. Bernstein, Hendrik W. Lenstra, Jr. & Jonathan Pila (2007). Detecting perfect powers by factoring into coprimes. *Mathematics of Computation* **76**, 385–388.

B. F. Caviness (1975). More on computing roots of integers. *SIGSAM Bull.* **9**(3), 18–20.

J. Lagarias, H. Montgomery & A. Odlyzko (1979). A Bound for the Least Prime Ideal in the Chebotarev Density Theorem. *Inventiones Math.* **54**, 271–296.

Wladyslaw Narkiewicz (1990). *Elementary and Analytic Theory of Algebraic Numbers Second Edition*. Springer-Verlag.

Joseph Oesterlé (1979). Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée. *Société Mathématique de France Astérisque* **61**, 165–167.

J. Barkley Rosser & Lowell Schoenfeld (1962). Approximate formulas of some functions of prime numbers. *Illinois J. Math.* **6**, 64–94.

Lowell Schoenfeld (1976). Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$. II. *Math. Comput.* **30**(134), 337–360.

Manuscript received February 28, 2007

Erich Kaltofen and Mark Lavin
Dept. of Mathematics
North Carolina State University,
Raleigh, North Carolina 27695-8205
USA
kaltofen@math.ncsu.edu
http://www.kaltofen.us