RIEMANN'S HYPOTHESIS AND TESTS FOR PRIMALITY[†]

Gary L. Miller
Department of Mathematics
University of California, Berkeley, California 94720

Abstract: The purpose of this paper is to present new upper bounds on the complexity of algorithms for testing the primality of a number. The first upper bound is $O(n^{1/7})$; it improves the previously best known bound of $O(n^{1/4})$ due to Pollard [11].

The second upper bound is dependent on the Extended Riemann Hypothesis (ERH): assuming ERH, we produce an algorithm which tests primality and runs in time $O((\log n)^4)$ steps. Thus we show that primality is testable in time a polynomial in the length of the binary representation of a number.

Finally, we give a partial solution to the relationship between the complexity of computing the prime factorization of a number, computing the Euler phi function, and computing other related functions.

Notations. We will assume that n, the number to be factored or tested for primality, is an odd positive integer. We let p, q vary over odd primes, and (a,b) denote the greatest common divisor of a and b. Let $|n|$ denote the length of the binary representation of n, i.e. $|n| = \lceil \log_2 n \rceil$. The number of 2's in n will be denoted by $\#_2(n)$, i.e. $\#_2(n) = \max\{k : 2^k | n\}$. And finally, by a computation step we mean a deterministic Turing machine transition.

Definition. We say an algorithm tests primality in $O(f(n))$ steps if on input a binary number n the algorithm correctly indicates whether n is prime or composite in less than $k \cdot f(n)$ steps, for some constant k.

Theorem 1. There exists an algorithm which tests primality in $O(n^{.134})$ steps.

If we then assume the Extended Riemann's Hypothesis (see appendix), Theorem 1 can be vastly improved:

Theorem 2 (ERH). There exists an algorithm which tests primality in $O(|n|^4 \log\log |n|)$ steps.

Neither of the algorithms produced in Theorems 1 or 2 necessarily finds divisors of composite numbers. They only indicate that the number is composite, in general. The problem of finding a divisor of a composite number or the more general problem of producing the prime factorization of a number seems more difficult. Daniel Shanks in [13] produces $\forall \varepsilon > 0$ an algorithm which factors a number in $O(n^{(1/4)+\varepsilon})$ steps.

Following the definition of set reducibility of Cook [6] and Karp [8] we define functional reducibility:

Definition. Given functions f and g we say that f is polynomial time reducible to g denoted $f \overset{\leq}{p} g$, if there exists a Turing machine which on inputs n and g(n) computes f(n) in $O(|n|^k)$ steps for some constant k. We say f is polynomial time equivalent to g if $f \overset{\leq}{p} g$ and $g \overset{\leq}{p} f$, and denote this relation by $f \overset{\approx}{p} g$.

Definition. Let $n = p_1^{v_1} \ldots p_m^{v_m}$ be the prime factorization of the odd number n. We let "prime factorization" denote the function from the natural numbers to some fixed appropriate coding of the prime factors and their exponents. We also consider the following three functions:

i) $\phi(n) = p_1^{v_1-1}(p_1-1)\ldots p_m^{v_m-1}(p_m-1)$ (Euler's ϕ-function),

ii) $\lambda(n) = \operatorname{lcm}\{p_1^{v_1-1}(p_1-1),\ldots,p_m^{v_m-1}(p_m-1)\}$ (The Carmichael λ-function),

iii) $\lambda'(n) = \operatorname{lcm}\{p_1-1,\ldots,p_m-1\}$.

By the definition of Euler's ϕ-function we see that $\phi \overset{\leq}{p}$ "prime factorization." Since $\operatorname{lcm}(a,b) = a \cdot b/(a,b)$ we see that λ and λ' are both polynomial time reducible to "prime factorization," i.e. λ, $\lambda' \overset{\leq}{p}$ p "prime factorization." As a by-product of our work on Theorem 2 we get:

Theorem 3 (ERH). The functions ϕ, λ, λ' and "prime factorization" are all polynomial time equivalent, i.e. "prime factorization" $\overset{\approx}{p}$ ϕ $\overset{\approx}{p}$ λ $\overset{\approx}{p}$ λ'.

The difficult step in the proof of the above three theorems is demonstrating that there is a "small" quadratic nonresidue. In Theorem 1 we appeal to the work of Burgess who uses Weil's proof of Riemann Hypothesis over finite fields, while in Theorems 2 and 3 we use Ankeny's reduction of the size of the first quadratic nonresidue to the Extended Riemann's Hypothesis.

Motivation of Proofs

Fermat proved that for p prime

$$a^{p-1} \equiv 1 \bmod p \text{ if } (a,p) = 1 .$$

Therefore, if for some a, $1 < a < n$,

$$a^{n-1} \not\equiv 1 \bmod n \qquad (1)$$

then n must be composite. Now, $a^m \bmod n$ can be computed in $O(|m|M(|n|))$ steps (where $M(|n|)$ denotes the cost of multiplying two numbers of length $|n|$) using standard techniques described in [7]. A possible technique for recognizing composite numbers might be to systematically search for an a satisfying (1). This technique could fail for composite n for two reasons:

a) There could be composite n which satisfies Fermat's Congruence. That is,

$$a^{n-1} \equiv 1 \bmod n \text{ for all } (a,n) = 1 .$$

b) The first a satisfying (1) could be very large which would give us an inefficient method.

The rest of the paper will be devoted to handling these two problems. We start by showing that in fact some composite numbers do satisfy Fermat's Congruence.

Theorem 4 (Carmichael) [5]. n satisfies Fermat's Congruence if and only if $\lambda(n)|n-1$.

For example, the composite number $561 = 3 \cdot 11 \cdot 17$ is such that $\lambda(n) = \text{lcm}(2,10,16) = 80$, and 80 divides 560. It follows that $(a,561) = 1$ implies $a^{560} \equiv 1 \bmod 561$ for all natural numbers a. Thus there are composite numbers which satisfy Fermat's Congruence. At first these numbers seem more difficult to recognize as composite. Not only will we recognize them as composite, but we will quickly find a divisor. By what we have done it would seem that the obvious approach would be to use Fermat's test to recognize composite n such that $\lambda(n) \not| n-1$ and some other test for n such that $\lambda(n)|n-1$. Instead we shall separate the composite number into sets according to whether $\lambda'(n) \not| n-1$ or $\lambda'(n)|n-1$.

Since the algorithms used in Theorems 1 and 2 are essentially the same we shall define the following class of algorithms:

Definition of A_f. Let f be a computible function on the natural numbers. We define A_f on input n as follows:

1) Check if n is a perfect power, i.e. $n=m^s$ where $s \geq 2$. If n is a perfect power then output "composite" and halt.

2) Carry out steps i) - iii) for each $a \leq f(n)$. If at any stage i), ii) or iii) holds output "composite" and halt:

i) $a|n$.

ii) $a^{n-1} \not\equiv 1 \bmod n$

iii) $((a^{(n-1)/2^k} \bmod n) - 1, n) \neq 1$ for some k, $1 \leq k \leq \#_2(n-1)$.

3) Output "prime" and halt.

Note. A_f as defined above is a simplified version of the algorithm needed to get Theorem 2. A_f will give an algorithm for testing primality in $O(|n|^5 \log^2 |n|)$ steps.

Before we prove Theorems 1 and 2 we must develop the technical hardware to define f and to show that there is an $a \leq f(n)$ which "works".

We start by considering those composite numbers n which satisfy $\lambda'(n) \not| n-1$. In the following lemma we give a characterization of some of the a's which satisfy $a^{n-1} \not\equiv 1 \bmod n$.

Lemma 1. If $\lambda'(n) \not| n-1$ then there exist primes p and q so that:

1) $p|n, p-1 \not| n-1, q^m | p-1$, and $q^m \not| n-1$ for some integer $m \geq 1$.

2) If a is any q-th nonresidue mod p then $a^{n-1} \not\equiv 1 \bmod n$.

See Appendix for definition of q-th nonresidue mod p and definition of index of a mod p which we will denote by $\text{in}_p a$.

Proof. Let $q_1, \ldots, q_n$ be the distinct prime divisors of n. Thus $\lambda'(n) = \text{lcm}\{q_1-1, \ldots, q_n-1\} \not| n-1$ which implies $q_i - 1 \not| n-1$ for some i. By setting $p = q_i$ we have $p|n$ and $p-1 \not| n-1$. Since $p-1 \not| n-1$, there must exist a prime q and an integer $m \geq 1$ so that $q^m | p-1$ and $q^m \not| n-1$. Thus p and q satisfy condition 1). We next show that p,q satisfy condition 2).

If a and n are not relatively prime then $a^m \not\equiv 1 \bmod n$ for any $m \neq 0$; thus $a^{n-1} \not\equiv 1 \bmod n$. So we can assume $(a,n) = 1$. Suppose the lemma is false, i.e. $a^{n-1} \equiv 1 \bmod n$. Since $p|n$ we have

$$a^{n-1} \equiv 1 \bmod p . \qquad (2)$$

Let b be a generator mod p then by (2) we have $b^{(\text{ind}_p a)(n-1)} \equiv 1 \bmod p$. Since $b^m \equiv 1 \bmod p$ implies $p-1|m$ we have

$$p-1 | (\text{ind}_p a)(n-1) . \qquad (3)$$

Now a is a q-th nonresidue implies $q \not| \text{ind}_p a$. Thus

$$q \not| \text{ind}_p a \text{ and } q^m | p-1 . \qquad (4)$$

Applying (4) to (3) gives $q^m | n-1$ which is a contradiction. ∎

Lemma 1 motivates the definition of the first q-th nonresidue mod p.

Definition. Let N(p,q) be the least a so that a is a q-th nonresidue mod p defined only when $q|p-1$. Using index arguments it is not hard to show that N(p,q) is prime.

Theorem (Ankeny) [1] (ERH). $N(p,q) = O(|p|^2)$

Using Ankeny's Theorem and Lemma 1 we have that if $\lambda'(n) \not| n-1$ then there exists an $a \leq O(|n|^2)$ such that $a^{n-1} \not\equiv 1 \bmod n$.

We now return to a discussion of composite numbers n which have the property that $\lambda'(n)|n-1$. Let $q_1, \ldots, q_m$ be the distinct prime divisors of n; then by the definition of λ' we know that $\#_2(\lambda'(n)) = \max(\#_2(q_1-1), \ldots, \#_2(q_m-1))$. Thus for some $1 \leq i \leq m$, $\#_2(\lambda'(n)) = \#_2(q_i-1)$. We next make a distinction between two types of numbers as

follows:

Definition. Let $q_1,\ldots,q_m$ be the distinct prime divisors of n. We say n is of type A if for some $1 \le j \le m$, $\#_2(\lambda'(n)) > \#_2(q_j-1)$. On the other hand, we say n is of type B if $\#_2(\lambda'(n)) = \#_2(q_1-1) = \#_2(q_m-1)$.

Digressing for a moment to motivate the next three lemmas, suppose we have a composite number $n = pq$. Suppose further that we have a number m so that

$$m \equiv 1 \bmod q \text{ and } m \equiv -1 \bmod p \ . \qquad (5)$$

The first of the restrictions in (5) implies $q \mid m-1$ and the second implies $m \not\equiv 1 \bmod n$. Thus $q = (m-1,n)$. If we could quickly compute some m satisfying (5), we would quickly know a divisor of n. In the following lemmas we develop a method for finding m satisfying (5). We say b has a nontrivial GCD with n if $(b,n) \neq 1$ or n.

Lemma 2A. Let n be a composite number of type A where, say, p and $q \mid n$, and $\#_2(\lambda'(n)) = \#_2(p-1) > \#_2(q-1)$. Assume further that $0 < a < n$ is so that $(\frac{a}{p}) = -1$ where $(\frac{a}{p})$ is the Jacobi symbol (cf. appendix), then either a or $(a^{\lambda'(n)/2} \bmod n) - 1$ has a nontrivial GCD with n.

Proof. Suppose a has a trivial GCD with n. Since $1 < a < n$ it must be that $(a,n) = 1$. Since $q-1 \mid \lambda'(n)$ and $\#_2(q-1) < \#_2(\lambda'(n))$, we have $q-1 \mid \frac{\lambda'(n)}{2}$, thus

$$a^{\lambda'(n)/2} \equiv 1 \bmod q \ . \qquad (1)$$

Since $(a^{\lambda'(n)/2})^2 \equiv 1 \bmod p$ then $a^{\lambda'(n)/2} \equiv \pm 1 \bmod p$. Suppose $a^{\lambda'(n)/2} \equiv 1 \bmod p$ then $p-1 \mid (\mathrm{ind}_p a)(\frac{\lambda'(n)}{2})$ which implies that $\mathrm{ind}_p a$ is even. On the other hand, $(\frac{a}{p}) = -1$ implies $\mathrm{ind}_p a$ is odd (see appendix). So

$$a^{\lambda'(n)/2} \equiv -1 \bmod p \ . \qquad (2)$$

By (1), $q \mid (a^{\lambda'(n)/2} \bmod n) - 1$. By (2), $p \nmid (a^{\lambda'(n)/2} \bmod n) - 1$ since p is an odd prime. Thus $((a^{\lambda'(n)/2} \bmod n) - 1, n) \neq 1, n$. ¤

Lemma 2B. Let n be a composite number with at least two distinct prime divisors, say p and q. Further suppose n is of type B and $1 < a < n$ is so that $(\frac{a}{pq}) = -1$. Then, either a or $(a^{\lambda'(n)/2} \bmod n) - 1$ has a nontrivial divisor with n.

Proof. As in the proof of Lemma 2A we assume that a has a trivial GCD with n, thus $(a,n) = 1$. Without loss of generality we assume that $(\frac{a}{p}) = -1$ and $(\frac{a}{q}) = 1$. Using techniques similar to above we show $a^{\lambda'(n)/2} \equiv -1 \bmod p$ and $a^{\lambda'(n)/2} \equiv 1 \bmod q$. The rest of the argument follows from the above proof. ¤

Lemma 3. If $p \mid n$, $\lambda'(n) \mid m$, and $k = \#_2[\frac{m}{\lambda'(n)}] + 1$ then $a^{\frac{\lambda'(n)}{2}} \equiv a^{\frac{m}{2^k}} \bmod p$.

Proof. Since $a^{\lambda'(n)} \equiv 1 \bmod p$ it follows that $a^{\lambda'(n)/2} \equiv \pm 1 \bmod p$. We consider the two possible values of $a^{\lambda'(n)/2}$ separately:

1) If $a^{\lambda'(n)/2} \equiv 1 \bmod p$ then $a^{m/2^k} \equiv 1 \bmod p$, since by our choice of k and the fact that $\lambda'(n) \mid m$ we have $\frac{\lambda'(n)}{2} \mid \frac{m}{2^k}$.

2) If, on the other hand, $a^{\lambda'(n)/2} \equiv -1 \bmod p$ we note that:

$$a^{\frac{m}{2^k}} \equiv (a^{\frac{\lambda'(n)}{2}})^{\frac{m}{\lambda'(n)2^{k-1}}} \equiv (-1)^{\frac{m}{\lambda'(n)2^{k-1}}}$$

mod p. Since $m/\lambda'(n)2^{k-1}$ is odd, $a^{m/2^k} \equiv -1 \bmod p$.

Using Lemmas 2A and 3 we see that: if n is a type A composite number, $\lambda'(n) \mid n-1$, and $a = N(p,2)$ then either $a \mid n$ or $((a^{(n-1)/2} \bmod n)-1, n) \neq 1, n$. For type B numbers we will need the following definition.

Definition. Let N(pq) be the minimum a so that $(\frac{a}{pq}) \neq 1$ where $(\frac{a}{pq})$ is the Jacobi symbol and N(pq) is defined only when $p \neq q$. Note again that N(pq) is prime.

Theorem (Ankeny) [1] (ERH). $N(pq) = O(|pq|^2)$

Ankeny doesn't actually state the case N(pq) but it follows without any change in his argument. We only need to use the stronger form of Selberg's Theorem 6 [12] referred to as Lemma 2(c) in [1]. Also see [10] for the statement and proof of Ankeny's theorem.

Proof of Theorem 2 (weak form). By Theorems of Ankeny we can pick an integer $c \ge 1$ so that

$$N(p,q) \le c|p|^2 \text{ and } N(pq) \le c|pq|^2 \ .$$

Consider A_f where $f(n) = c|n|^2$.

Analysis of Running Time

1) A_f must first check to see if n is a perfect power which will take $O(|n|^3)$ steps. We leave it to the reader to verify this bound.

2) A_f must check i), ii) and iii) for f(n) different a's.

Check i) takes say $O(|n|^2)$ steps.

Check ii) takes $O(|n|M(|n|))$ steps

Check iii) takes $O((|n|M(|n|)+|n|^2)|n|)$ steps since GCD can be computed in $O(|n|^2)$ steps, see [7], and $1 \le k \le |n|$. Now multiplication takes at least $|n|$ steps thus check iii) takes at most $O(|n|^2 M(|n|))$ steps.

So A_f runs in $O(|n|^4 M(|n|))$ steps. If we use the Schonhage-Strassen algorithm ([14]) for multiplying binary numbers, $M(|n|) = O(|n|\log|n|\log\log|n|)$ and we have $O(|n|^5 \log|n| \log\log|n|)$ steps.

Proof of Correctness of A_f

If n is prime A_f will indicate correctly that n is prime so we need only show that A_f recognizes composite n. If n is composite n it will fall into one of the following three cases.

1) n is a prime power.

2) $\lambda'(n) \nmid n-1$

3) $\lambda'(n) \mid n-1$ and n is not a prime power.

Case 1. If n is a prime power then n is a perfect power and in this case A_f will indicate that A_f is composite.

Case 2. If $\lambda'(n) \nmid n-1$ then by Lemma 1 we have a p and q such that if $a = N(p,q)$ then $a^{n-1} \not\equiv 1 \bmod n$. Thus we need only note that $N(p,q) \leq f(n)$, which follows by our choice of f.

Case 3. If $\lambda'(n) \mid n-1$ and n is not a perfect power:

A) Suppose n is of type A then by Lemmas 2A and 3 we can choose p and k ($k \leq \#_2(n-1)$) such that if $a = N(p,2)$ then either $a \mid n$ or $((a^{(n-1)/2^k} \bmod n) - 1, n) \neq 1, n$. Since $N(p,2) \leq f(n)$, n will be recognized as composite by either step i) or ii).

B) Suppose n is of type B then by Lemmas 2B and 3 and the assumption that n is not a perfect power. We can choose p, q and $k \leq \#_2(n-1)$ so that if $a = N(pq)$ then either $a \mid n$ or $((a^{(n-1)/2^k} \bmod n) - 1, n) \neq 1, n$. Since $N(pq) \leq f(n)$, A_f will indicate that n is composite. ¤

To prove Theorem 1 we need the following results of Burgess.

Theorem (Burgess) [2,3,5]

$$N(p,q) = O(p^{(1/4\sqrt{e})+\varepsilon}) \qquad \text{any } \varepsilon > 0$$

$$N(pq) = O((pq)^{1/4\sqrt{e})+\varepsilon}) \qquad \text{any } \varepsilon > 0$$

Proof of Theorem 1. By the Theorem of Burgess we can pick an integer $c \geq 1$ so that

$$N(p,q) \leq cp^{1/4\sqrt{2.71}} \text{ and } N(pq) \leq c(pq)^{1/4\sqrt{2.71}} .$$

Set $\ell = 4\sqrt{2.71}$. Consider A_f where $f(n) = \lceil cn^{\frac{1}{\ell+1}} \rceil \leq \lceil cn^{.133} \rceil$. Since A_f runs in $O(n^{.134})$ steps we need only show that A_f tests primality. If n is prime then A_f will indicate that n is prime.

Suppose that n is composite. Then n must lie in at least one of the following four cases.

Case 1. n is a prime power.

Case 2. n has a divisor $\leq f(n)$.

Case 3. $\lambda'(n) \nmid n-1$, n has no divisor $\leq f(n)$.

By Lemma 1 there exist primes p, q such that if $a = N(p,q)$ then $a^{n-1} \not\equiv 1 \bmod n$. So we need only show that $a = N(p,q) \leq f(n)$. We have

$$a \leq \lceil cp^{1/\ell} \rceil \tag{5}$$

from above. Since n is composite and for all $a \leq f(n)$ $a \nmid (n)$, we have

$$p \leq \frac{n}{f(n)} \quad \text{i.e.} \quad p \leq \lceil \frac{1}{c} n^{\ell/(\ell+1)} \rceil . \tag{6}$$

Substituting (6) into (5) we have

$$a \leq \lceil n^{1/(\ell+1)} \rceil \leq f(n) \text{ since } c \geq 1 .$$

Case 4. $\lambda'(n) \mid n-1$ and n has no divisor $\leq f(n)$ and n is not a prime power.

A) Suppose n is of type A. Then as in Case 3A of Theorem 1 we need only show $a = N(p,2) \leq f(n)$ where $p \mid n$. Since in this case (5) and (6) hold we get $a \leq f(n)$.

B) Suppose n is of type B. Since n is not a prime power n has at least two distinct prime divisors, say p, q. We need to show that $N(pq) \leq f(n)$ which will follow if we show $pq \not\leq \frac{n}{f(n)}$.

Claim. $n \neq pq$ (see [5]).

Suppose $n = pq$ where $p < q$. Now $q-1 \mid pq-1$, since $\lambda'(n) \mid n-1$. But this implies $q-1 \mid p-1$. Hence $q \leq p$ which contradicts the assumption that $p < q$.

By claim $n = pqr$ where $r \neq 1$. Since $r \mid n$ we have $r \geq f(n)$. Thus $pq \leq \frac{n}{f(n)}$. ¤

Before we prove the stronger form of Theorem 2 as stated in the introduction we prove Theorem 3. To prove Theorem 3 we will need the following lemma:

Lemma 4 (ERH). Let g be any function such that

1) $\lambda'(n) \mid g(n)$

2) $|g(n)| = O(|n|^k)$ for some constant k.

Then "prime factorization" $\overset{p}{\leq} g$.

Proof. Consider the following procedure on n and m.

1) Check if n is a perfect power.

2) Carry out steps i) and ii) for each $a \leq f(n)$ (where f is as in the proof of Theorem 1):

i) $a \mid n$

ii) $((a^{m/2^k} \bmod n) - 1, n) \neq 1$ for some $a \leq k \leq \#_2(m)$.

If $\lambda'(n) \mid m$ then we know by arguments similar to Case 3 of the proof of Theorem 2 that this procedure will produce a divisor of n if n is composite. If we set $m = g(n)$ then in $O(|g(n)| |n|^3 M(|n|))$ steps we will either know that n is prime or that n' is a divisor of n, for some n'. If in the above procedure we replace n by n' then $\lambda'(n') \mid g(n)$ since $n' \mid n$ implies $\lambda'(n') \mid \lambda'(n)$. Thus in $O(|g(n)| |n'|^3 M(n'))$ steps we will either know n' is prime or n'' is a factor of n'. Iterating this procedure at most $|n|$ times we will have all prime factors of n. Thus, we get a prime factorization of n in $O(|g(n)| |n|^4 M(|n|))$ steps. Since $|g(n)| = O(|n|^k)$ it runs in $O(|n|^{k+4} M(|n|))$ steps. ¤

Proof of Theorem 3. By the discussion preceding Theorem 3 we know that ϕ, λ, $\lambda' \overset{p}{\leq}$ "prime factorization". Since ϕ, λ and λ' satisfy Lemma 4 we have "prime factorization" $\overset{p}{\leq} \phi, \lambda, \lambda'$. Thus Theorem 3 follows. ¤

Modification to Algorithm A_f

First note that a in step 2) of A_f need not vary over all numbers $\leq f(n)$ but only prime numbers $\leq f(n)$. Since the number of prime $\leq f(n)$ is $O(\frac{f(n)}{\log f(n)})$, by the prime number theorem, we have

the upper bound for Theorem 2 of $O(|n|^5 \log\log|n|)$ steps.

We amend step 2) in A_f as follows:

2) Compute $p_1,\ldots,p_m$ where p_i is the i-th prime number and m is so that $p_m \leq f(n) < p_{m+1}$. Compute Q, S so that $n-1 = Q2^S$ and Q is odd. Let i = 1 and proceed to ii) (let a denote p_i throughout).

i) If i < m set i to i+1. If i = m then output "prime" and halt.

ii) If a|n then output "composite" and halt.

Compute $a^Q \bmod n$, $a^{Q2} \bmod n,\ldots, a^{Q2^S} \bmod n$.

iii) If $a^{Q2^S} \bmod n \neq 1$ then output "composite" and halt.

iv) If $a^Q \bmod n = 1$ go to i).

Set $J = \max(J : a^{Q2^J} \bmod n \neq 1)$.

v) If $a^{Q2^J} \bmod n = n - 1$ go to i).

vi) Output "composite" and halt.

The running time A_f is $O(|n|^4 \log\log|n|)$. To show that A_f tests primality we need only reconsider Case 3:

Case 3. $\lambda'(n)|n-1$ and n is not a prime power.

A) Suppose n is of type A with $\#_2(\lambda'(n)) = \#_2(p-1) > \#_2(q-1)$ and $p,q|n$. Let $a = N(p,2)$ (thus a is prime). Thus we need only show that either step ii), iii) or vi) outputs "composite" for this a. So suppose $a\nmid n$ and $a^{n-1} \equiv 1 \bmod n$. We show that A_f reaches step vi). If $a^S \equiv 1 \bmod p$ then $2|S$, since $(\frac{a}{p}) = -1$ and p is odd. Since $p|n$ we have $a^Q \not\equiv 1 \bmod n$. Thus A_f will reach step v). By Lemmas 2A and 3, we know there exists a k so that $a^{Q2^k} \equiv 1 \bmod q$ and $a^{Q2^k} \equiv -1 \bmod p$. Suppose $a^{Q2^J} \equiv -1 \bmod n$ then $a^{Q2^J} \equiv -1 \bmod p$ and q. Now $a^{Q2^k} \equiv a^{Q2^J} \equiv -1 \bmod p$ implies k = J. On the other hand, $a^{Q2^k} \equiv 1 \bmod q$ and $a^{Q2^J} \equiv -1 \bmod q$ implies k > J. Thus by contradiction $a^{Q2^J} \not\equiv -1 \bmod n$. Hence A_f reaches step vi).

B) Suppose n is of type B. The proof in this case follows the argument in Case A.

Appendix

Let Z_n denote the ring of integers mod n. Let Z_n^* denote the integers relatively prime to n under multiplication mod n. Z_n^* is a group and if p is a prime then Z_p^* is a cyclic group of order p-1. Thus, the only solutions to the equation $x^2 \equiv 1 \bmod p$ are ± 1. We may pick a generator of the cyclic group Z_p^*, say b, then we define $\text{ind}_p a = \min\{m: b^m \equiv a \bmod p\}$. We note that $\text{ind}_p a$ is dependent on our choice of a generator. We say a is a q-th residue mod p if there exists b $(b^q \equiv a \bmod p)$.

Note. If p, q are primes and $q|p-1$ then a is a q-th residue mod p if and only if $q|\text{ind}_p a$.

Definition. The Legendre symbol $(\frac{a}{p})$ is defined by:

$$(\frac{a}{p}) = \begin{cases} 1 \text{ if a is a quadratic residue mod p and } (a,p) = 1; \\ -1 \text{ if a is a quadratic nonresidue mod p and } (a,p) = 1; \\ 0 \text{ if } (a,p) \neq 1. \end{cases}$$

The Jacobi symbol $(\frac{a}{pq})$ is defined by:

$$(\frac{a}{pq}) = (\frac{a}{p}) \cdot (\frac{a}{q})$$

where $(\frac{a}{p})$ and $(\frac{a}{q})$ are the Legendre symbols.

The above two symbols for fixed denominators define functions which fall into a general class of functions called characters. We define one more character as follows:

$$\chi(a) = \begin{cases} e(2\pi i(\text{ind}_p a)/q) & \text{if } (a,p) = 1 \\ 0 & \text{if } (a,p) \neq 1 \end{cases}$$

where $q|p-1$ and e( ) is the exponential function.

Dirichlet's L functions are defined by:

$$L(S,\chi) = \sum_{n-1}^{\infty} \chi(n)/n^S$$

where χ is a character.

Extended Riemann's Hypothesis (ERH). The zeros of $L(S,\chi)$ in the critical strip, $0 \leq$ (real part of S) ≤ 1 all lie on the line (real part of S) $= \frac{1}{2}$, where χ is any of the three characters above.

References

[1] N.C. Ankeny, "The Least Quadratic Non-Residue," Annals of mathematics 55 (1952) 65-72.

[2] D.A. Burgess, "The Distribution of Quadratic Residues and Non-Residues," Mathematika 4 (1957) 106-112.

[3] _____, "On Character Sums and Primitive Roots," Proc. London Math. Soc. (3) 12 (1962) 179-192.

[4] _____, "On Character Sums and L-series," Proc. London Math. Soc. (3) 12 (1962) 193-206.

[5] R.D. Carmichael, "On Composite Numbers p Which Satisfy the Fermat Congruence $a^{p-1} \equiv p$," American Math. Monthly 19 (1912) 22-27.

[6] S. Cook, "The Complexity of Theorem-proving Procedures," Conference Record of Third ACM Symposium of Theory of Computing (1970) 151-158.

[7] H. Davenport and P. Erdös, "The Distribution of Quadratic and Higher Residues," Publ. Math. Debreien 2 (1952) 252-265.

[8] R. Karp, "Reducibility Among Combinatorial Problems," Complexity of Computer Computations, R.E. Miller and J.W. Thatcher, eds., Plenum Press, New York (1972) 85-103.

[9] D. Knuth, The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, Addison-Wesley, Reading Massachusetts (1969).

[10] H. Montgomery, Topics in Multiplicative Number Theory, Springer-Verlag Lecture Notes #227, 120.

[11] J. Pollard, "An Algorithm for Testing the Primality of Any Integer," Bull. London Math. Soc. 3 (1971) 337-340.

[12] A. Selberg, "Contributions to the Theory of Dirichlet L Functions," Avhandlinger utgett av Det Norske Videnskops, Akademi i Oslo (1934).

[13] D. Shanks, "Class Number, A Theory of Factorization, and Genera," Proceedings of Symposia in Pure Mathematics (20), 1969 Number Theory Institute, AMS (1971) 415-440.

[14] A. Shönhage and V. Strassen, "Schnelle Multiplikation Grosser Zahlen," Computing 7 (1971) 281-292.

†Research sponsored by the National Science Foundation Grant GJ-35604X1 of the Electronics Research Laboratory.