A Deterministic Primality Test for Integers of The Form $ap^k + 1$

Ariko Stephen Philemon
Department of Civil and Environmental Engineering, Makerere University, Uganda.
ariko@cedat.mak.ac.ug , philemonariko@gmail.com

03/05/2020

Abstract

In 1876, Edouard Lucas showed that if n is a positive integer and if an integer b exists such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all prime divisors q of $n-1$, then n is prime, a result known as Lucas's converse of Fermat's little theorem. In this paper we will show that if n is of the form $ap^k + 1$ where p is prime, $a < p$, and $k \geq 1$, then we only need to use a single prime divisor $q = p$ of $n-1$ to determine the primality of n. Precisely, we will show that if an integer b exists such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^{(n-1)/p} \not\equiv 1 \pmod{n}$, then n is prime. We will also use the results of this paper to show that there are no composite integers n of the form $ap + 1$ or ap where p is prime and $a < p$ such that $\phi(n) \mid n-1$. We then prove a conditional deterministic primality test for integers of the form $am + 1$, where a and m are positive integers, $a < p$, p is the least prime divisor of m. Finally, we will generalize Lucas's converse of Fermat's little theorem for all positive integers n of the form $am + 1$, $(a, m) = 1$, with the property that $m \mid \phi(n)$ if and only if n is prime.

Keywords Primality and Compositeness Tests, Pseudoprimes, Carmichael numbers, Lehmer Totient Problem.

1. Introduction

The problem of distinguishing primes from composite integers has been a subject of study for many centuries up to date. A number of tests have been established, some of these tests such as Lucas's converse of Fermat's little theorem, Pocklington primality test, Proth's test, Lucas Lehmer test among others can determine whether a number is prime with absolute certainty while others such as Fermat's Primality test, Miller-Rabin test report an input number is composite or a probable prime. The previous tests depend on the factorization of $n-1$ or $n+1$ to determine the primality of n. In this paper we develop another deterministic test for integers n of the form $ap^k + 1$ with a partially known $n-1$ factorization. We will put in much effort in determining which positive integers n of the form $ap^k + 1$ does the divisibility relation $p^k \mid \phi(n)$ hold from which the primality test will be deduced easily using the properties of order of an integer. We state this basic property we will need in our study.

Definition. Let a and n be relatively prime integers, $n > 1$. The order of a modulo n denoted by $\mathrm{ord}_n a$ is the least positive integer x such that $a^x \equiv 1 \pmod{n}$. **[1]**

Theorem 1.1 Let a and n be relatively prime integers, $n > 1$, then a positive integer x is a solution of the congruence $a^x \equiv 1 \pmod{n}$ if and only if $\mathrm{ord}_n a \mid x$. In particular $\mathrm{ord}_n a \mid \phi(n)$.

2. Primes of the form $\boldsymbol{ap+1}$

In this section we prove the primality of integers of the form ap^k+1 with $k=1$. Later we will generalize the test for higher powers of p.

Lemma 2.1 **Let $\boldsymbol{n=ap+r}$, where $\boldsymbol{a}$ and $\boldsymbol{r}$ are positive integers, $\boldsymbol{r<p}$, $\boldsymbol{p}$ is prime with $\boldsymbol{p>a}$. If $\boldsymbol{p\mid\phi(n)}$ then $\boldsymbol{n=rq}$ for some prime $\boldsymbol{q}$.**

Proof. Let $n=m\,{p_1}^{a_1}$ where p_1 is the largest prime divisor of n , $p_1\nmid m$, $a_1\geq 1$ and $m\geq 1$. We will show that $a_1=1$ and $m=r$. If $m=1$, then $\phi(n)={p_1}^{a_1-1}(p_1-1)$.
If $m>1$, let $m={p_2}^{a_2}\,{p_3}^{a_3}\ldots\,{p_k}^{a_k}$ be the prime power factorization of m.
$\phi(n)={p_1}^{a_1-1}\,(p_1-1)\,{p_2}^{a_2-1}\,(p_2-1)\ldots\,{p_k}^{a_k-1}\,(p_k-1)$. In either case $p\mid\phi(n)$ implies $p\mid p_i$ or $p\mid p_i-1$ for some $i=1,2,\ldots,k$ hence $p\leq p_i\leq p_1$. If $p=p_1$ then $p\mid n-ap=r$ which is not possible because $1\leq r<p$ hence we must have $p<p_1$. From the inequalities $r<p$, $a<p$ and $p<p_1$, we have $n=ap+r<p(a+1)\leq p^2<{p_1}^2$, $n<p^2<{p_1}^2$ hence $a_1=1$, $n=mp_1$. Also, we must have $m<p$, if $m\geq p$ then $n=mp_1>p^2$, a contradiction. $p\mid\phi(n)$ implies $p\mid(p_1-1)$ or $p\mid\phi(m)$. The latter is not possible because $\phi(m)\leq m-1<p$ hence $p\mid(p_1-1)$. $p_1=pt+1$ for some integer t. $n=mp_1=m(pt+1)=ap+r$. Factoring out p, we have $p(a-mt)=m-r$. $p\mid m-r$ and since $1\leq r<p$, and $1\leq m<p$ we conclude that $m=r$. $n=mp_1=rp_1$ completing the proof.

When $r=1$ in lemma 2.1, then $p\mid\phi(n)$ if and only if n is prime. This fact is key in proving our primality test.

Theorem 2.1 **Let $\boldsymbol{n=ap+1}$ where $\boldsymbol{a}$ is a positive integer and $\boldsymbol{p}$ is a prime with $\boldsymbol{p>a}$. If there exists a positive integer $\boldsymbol{b}$ such that $\boldsymbol{b^{n-1}\equiv 1\ (\mathrm{mod}\ n)}$ and $\boldsymbol{b^a\not\equiv 1(\mathrm{mod}\ n)}$ then $\boldsymbol{n}$ is prime.**

Proof. We will show that if n is composite and $b^{n-1}\equiv 1(\mathrm{mod}\ n)$ then $b^a\equiv 1(\mathrm{mod}\ n)$. Assume n is composite and $b^{n-1}\equiv 1(\mathrm{mod}\ n)$. From Theorem 1.1, $\mathrm{ord}_n b\mid\phi(n)$. Therefore if $p\mid\mathrm{ord}_n b$ we have $p\mid\phi(n)$ and from lemma 2.1 we know n is prime, a contradiction because n is assumed composite hence we must have $p\nmid\mathrm{ord}_n b$, equivalently $(\mathrm{ord}_n b,p)=1$. From Theorem 1.1, we also note that $\mathrm{ord}_n b\mid n-1=ap$. $\mathrm{ord}_n b\mid ap$ and $(\mathrm{ord}_n b,p)=1$ imply $\mathrm{ord}_n b\mid a$ and from Theorem 1.1, $b^a\equiv 1\ (\mathrm{mod}\ n)$. Consequently if $b^{n-1}\equiv 1(\mathrm{mod}\ n)$ and $b^a\not\equiv 1(\mathrm{mod}\ n)$ then we know n is prime.

Corollary 2.1 **Let $\boldsymbol{n=2p+1}$, where $\boldsymbol{p}$ is an odd prime. If $\boldsymbol{b}$ is a positive integer relatively prime to $\boldsymbol{n}$ and $\boldsymbol{b\not\equiv\pm1\ (\mathrm{mod}\ n)}$ then $\boldsymbol{n}$ is prime if and only if $\boldsymbol{b^{n-1}\equiv 1\ (\mathrm{mod}\ n)}$ and $\boldsymbol{b^2\not\equiv 1(\mathrm{mod}\ n)}$.**

Proof. Assume $b^{n-1}\equiv 1\ (\mathrm{mod}\ n)$ and $b^2\not\equiv 1(\mathrm{mod}\ n)$, from Theorem 2.1, n is prime.
For the other direction, assume n is prime then $b^2\equiv 1\ (\mathrm{mod}\ n)$ if and only if $b\equiv\pm1\ (\mathrm{mod}\ n)$. Therefore $b\not\equiv\pm1\ (\mathrm{mod}\ n)$ implies $b^2\not\equiv 1(\mathrm{mod}\ n)$. Also, from Fermat's little theorem we have $b^{n-1}\equiv 1\ (\mathrm{mod}\ n)$.

Note that from Theorem 2.1**,** if $b^{n-1}\equiv 1\ (\mathrm{mod}\ n)$ and $b^a\equiv 1(\mathrm{mod}\ n)$ then n may or may not be prime. We can check the two congruences using another base, if we find that $b^{n-1}\not\equiv 1\ (\mathrm{mod}\ n)$ then we know n is composite. If $b^{n-1}\equiv 1\ (\mathrm{mod}\ n)$, we proceed to check the congruence $b^a\equiv 1(\mathrm{mod}\ n)$. If it does not hold then we know n is prime otherwise we repeat the process with another base. We shall show that to determine the primality of n ,we need to use at most $a+1$ incongruent bases modulo n. To prove this, we will need the following result from the theory of power residues.

Theorem 2.2. Let m be a positive integer with a primitive root. If k is a positive integer and a is an integer relatively prime to m, then the congruence $x^k \equiv a(\text{mod}\, n)$ has a solution if and only if $a^{\phi(m)/d} \equiv 1(\text{mod}\, m)$, where $d = (k, \phi(m))$. Furthermore, if there are solutions of $x^k \equiv a(\text{mod}\, n)$, then there are exactly d incongruent solutions modulo m. **[1]**

Theorem 2.3 The primality of $n = ap + 1$ where p is a prime and $p > a$ can be determined using at most $a + 1$ incongruent bases b modulo n with $(b, n) = 1$.

Proof. If n is prime, we note that $\left(a, \phi(n)\right) = (a, ap) = a$ and since n has a primitive root, Theorem 2.2 tells us that $b^a \equiv 1(\text{mod}\, n)$ has a solution if and only if $1^{\phi(n)\,/\,a} = 1^p \equiv 1(\text{mod}\, n)$. This congruence holds trivially. Furthermore, from Theorem 2.2, $b^a \equiv 1(\text{mod}\, n)$ has exactly a incongruent roots modulo n. To determine the primality of n, we pick any $a + 1$ incongruent bases and relatively to n and check the two congruences $b^{n-1} \equiv 1\ (\text{mod}\, n)$ and $b^a \equiv 1(\text{mod}\, n)$. If $b^{n-1} \not\equiv 1\ (\text{mod}\, n)$ for any of the $a + 1$ bases, from Fermat's little theorem n is composite. If $b^{n-1} \equiv 1\ (\text{mod}\, n)$ and $b^a \not\equiv 1(\text{mod}\, n)$ for at least one of the $a + 1$ bases, Theorem 2.1 tells us n is prime. If $b^a \equiv 1(\text{mod}\, n)$ for all the $a + 1$ bases then n is composite because $b^a \equiv 1(\text{mod}\, n)$ has exactly a incongruent solutions modulo n if n is prime. This completes the proof.

We also note that the largest integer n such that $b^a \equiv 1\ (\text{mod}\, n)$ is $n = b^a - 1, b > 1$**.** We can set the integer $n > b^a - 1\ \ i.e\ \ n = ap + 1 > b^a - 1\ , p > (b^a - 2)/a$. It follows that if $p > (b^a - 2)/a$, then $b^a \not\equiv 1\ (\text{mod}\, n)$. Furthermore if $b^{n-1} \equiv 1\ (\text{mod}\, n)$ and $p > a$, then from Theorem 2.1 we know n is prime. We state this result as a corollary.

Corollary 2.2 Let $n = ap + 1$ where a is a positive integer and p is prime with $a < p$. If $b > 1$ is a positive integer relatively prime to n and $p > (b^a - 2)/a$ then $b^{n-1} \equiv 1\ (\text{mod}\, n)$ if and only if n is prime.

Example 2.1 Taking $b = 2$ and $a = 2$, we compute $(b^a - 2)/a = (2^2 - 2)/2 = 1$. Setting the prime $p > 2$, Corollary 2.2 tells us that if $n = 2p + 1$ then $2^{n-1} \equiv 1\ (mod\ n)$ if and only if n is prime.
If we take $b = 2$ and $a = 10$, $(2^{10} - 2)/10 = 102.2$. Taking $p \geq 103$ and $n = 10p + 1$, we have $2^{n-1} \equiv 1\ (\text{mod}\, n)$ if and only if n is prime.

Theorem 2.4 Let a be a fixed positive integer and p be a prime greater than a . There are finitely many Fermat pseudoprimes n of the form $ap + 1$ to any base $b > 1$.

Proof. From corollary 2.2, for a given base b, there are no pseudoprimes of the form $ap + 1$ for all primes $p > (b^a - 2)/a, p > a$ and since there are finitely many primes p with $p \leq (b^a - 2)/a, p \leq a$, it follows that there are finitely many pseudoprimes to the base b.

A direct consequence of Theorem 2.4 is that there are finitely many Carmichael numbers of the form $ap + 1$ where a is a fixed positive integer and p is a prime greater than a. Alternatively, this can be proved using the concept of minimal universal exponent. Note that from Theorem 2.4, if it can be proved that for a given positive integer a, the congruence $b^{n-1} \equiv 1\ (\text{mod}\, n)$ holds for infinitely many n then we have a proof of existence of infinitely many primes of the form $ap + 1$.

Before moving on we will provide another proof (the first proof) to Theorem 2.1 which is dependent on another basic property of congruences proved here. The first attempt of the proof of Theorem 2.1 led to the discovery of lemma 2.1 from which a concise proof of Theorem 2.1 was obtained. The following proof of Theorem 2.1 is not much different from that already given; some readers may wish to skip to the next section.

Theorem 2.5 Let $\boldsymbol{a, b, c \geq 1}$, and $\boldsymbol{m \geq 1}$ be integers such that $\boldsymbol{a \equiv b \ (\mathbf{mod}\ m)}$. Then $\boldsymbol{a \equiv b + mt}$ (mod $\boldsymbol{mc}$) for some integer $\boldsymbol{t, 0 \leq t < c}$.

Proof. $a = b + mk$ for some integer k. From the division algorithm, $k = qc + t$ for some integers q and t, $0 \leq t < c$. $a = b + mk = b + m(qc + t) = b + mt + mcq$. $a - (b + mt) = mcq$. $mc \mid a - (\ b + mt)$. In the language of congruences; $a \equiv b + mt$ (mod mc), $0 \leq t < c$.

Example 2.2 $46 \equiv 1$ (mod 9) $46 \equiv 10 = 1 + 9 \cdot 1 \equiv$ (mod $9 \cdot 2$) $46 \equiv 19 = 1 + 9 \cdot 2 \equiv$ (mod $9 \cdot 3$)

$83 \equiv 6$ (mod 7) $83 \equiv 6 = 6 + 7 \cdot 1 \equiv$ (mod $7 \cdot 2$) $83 \equiv 20 = 6 + 7 \cdot 2 \equiv$ (mod $7 \cdot 3$)

Theorem 2.1 Alternative Proof. Let $\boldsymbol{n = ap + 1}$ where $\boldsymbol{a}$ is a positive integer and $\boldsymbol{p}$ is a prime with $\boldsymbol{p > a}$. If there exists a positive integer $\boldsymbol{b}$ such that $\boldsymbol{b^{n-1} \equiv 1\ (\mathbf{mod}\ n)}$ and $\boldsymbol{b^{a} \not\equiv 1 (\mathbf{mod}\ n)}$ then $\boldsymbol{n}$ is prime.

Proof. Assume n is composite and $b^{n-1} \equiv 1(\text{mod } n)$. The composite integer n has a prime divisor q with $q \leq \sqrt{n} = \sqrt{ap + 1} < \sqrt{p^2 + 1} < p + 1$. $b^{n-1} \equiv 1(\text{mod } q)$. $ord_q b \leq q - 1 < p$ hence $p \nmid \text{ord}_q b$. Equivalently $(\text{ord}_q b, p) = 1$. $\text{ord}_q b \mid n - 1 = ap$. $\text{ord}_q b \mid a$ hence $b^a \equiv 1(mod\ q)$.

From Theorem 2.5, $b^a \equiv 1 + qt$ (mod n) for some integer t. We will show that $qt \equiv 0$ (mod n) from which $b^a \equiv 1$ (mod n) will follow. $b^{ap} \equiv (1 + qt)^p \equiv 1$ (mod n). $\text{ord}_n(1 + qt) \mid p$, $\text{ord}_n(1 + qt) = 1$ or p . If $\text{ord}_n(1 + qt) = p$, then $p \mid \phi(n)$ and from lemma 2.1, we know that n is prime. This is a contradiction because n is assumed to be composite hence we must have $\text{ord}_n(1 + qt) = 1$. $(1 + qt)^1 \equiv 1$ (mod n) , $qt \equiv 0$ (mod n) from which $b^a \equiv 1$ (mod n) follows. Consequently if $b^{n-1} \equiv 1(\text{mod } n)$ and $b^a \not\equiv 1(\text{mod } n)$ then we know n is prime.

3. Some results on Lehmer's totient problem

Lehmer's totient problem asks whether there are any composite integers n such that $\phi(n) \mid n - 1$. Here we show that such composite integers are neither of the form $ap + 1$ nor of the form ap, $a < p$, p is prime.

Theorem 3.1 Let $\boldsymbol{n = ap + 1}$, $\boldsymbol{a}$ is a positive integer, $\boldsymbol{p}$ is a prime and $\boldsymbol{p > a}$. $\boldsymbol{\phi(n) \mid n - 1}$ if and only if $\boldsymbol{n}$ is prime.

Proof. If n is prime, $\phi(n) \mid n - 1$ holds trivially because $\phi(n) = n - 1$. Assume n is composite, from lemma 2.1 we have $p \nmid \phi(n)$, $(\phi(n), p) = 1$. $\phi(n) \mid n - 1 = ap$ and since $(\phi(n), p) = 1$, we must have $\phi(n) \mid a$. $\phi(n) \leq a < \sqrt{a^2 + 1} < \sqrt{ap + 1} = \sqrt{n}$ $i.e\ \phi(n) < \sqrt{n}$. We arrive at a contradiction by using the fact that if n is composite then $\phi(n) \geq \sqrt{n}$ except the case when $n = 6$ for which it is evident that $\phi(n) \nmid n - 1$.

Theorem 3.2 Let $\boldsymbol{n = ap}$, $\boldsymbol{a}$ is a positive integer, $\boldsymbol{p}$ is a prime and $\boldsymbol{p > a}$. $\boldsymbol{\phi(n) \mid n - 1}$ if and only if $\boldsymbol{n}$ is prime.

Proof. The proof is quite straightforward; Since $(a, p) = 1$, $\phi(n) = \phi(a)\phi(p) = \phi(a)(p - 1)$. $\phi(a)(p - 1) \mid ap - 1$. $(p - 1) \mid ap - 1 = a(p - 1) + a - 1$ therefore $p - 1 \mid a - 1$. Since $a < p$, we conclude that $a = 1$, $n = ap = p$.

It can be shown that every positive integer $n > 1$ can be written in the form $ap + r,\ 1 \leq a < p, p$ is prime, $0 \leq r < p$. If n is a composite integer satisfying $\phi(n) \mid n - 1$, Theorems 3.1 and 3.2 tell us n must be of the form $ap + r$, $2 \leq r < p$. Furthermore if n is a composite integer of the form $ap + r$, $a < p, r < p$ and $\phi(n) \mid n - 1$, then $p \nmid \phi(n)$. If $p \mid \phi(n)$ then $p \mid n - 1 = ap + r - 1, p \mid r - 1$, $r = 1$. $n = ap + 1$. From Theorem 3.1, n is prime, a contradiction.

4. Generalization of Theorem 2.1

In this section we develop the primality test presented in Theorem 2.1 for higher powers of p. Using a similar argument presented in the proof of lemma 2.1, it can be shown that if $n = ap^k + 1$, where a and k are positive integers, p is a prime with $p > a$ then $p^k \mid \phi(n)$ if and only if n is prime. It follows that if n is composite and $b^{n-1} \equiv 1 (\mathrm{mod}\, n)$, then the highest power of p in $\mathrm{ord}_n b$ is less than p^k so that $b^{ap^{k-1}} = b^{(n-1)/p} \equiv 1(\mathrm{mod}\, n)$. Therefore if $b^{n-1} \equiv 1(\mathrm{mod}\, n)$ and $b^{(n-1)/p} \not\equiv 1(\mathrm{mod}\, n)$ then n is prime. The details of the proof are given below.

Lemma 4.1 Let $\boldsymbol{p, v, k_i, s_i, q_i}$, $\boldsymbol{1 \leq i \leq v}$ be positive integers, $\boldsymbol{k_1 \leq k_2 \leq \cdots \leq k_v,\ q_i = s_i p^{k_i} + 1}$, $\boldsymbol{n = \prod_{i=1}^{v} q_i}$. Then $\boldsymbol{n = p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + Mp + 1}$ for some integer $\boldsymbol{M}$. Furthermore if $\boldsymbol{v \geq 2}$, then $\boldsymbol{n = p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + Mp^{k_1 + k_2} + \sum_{i=1}^{v} s_i p^{k_i} + 1}$ for some integer $\boldsymbol{M}$.

Proof. We will use proof by induction. First, we prove the general case $v \geq 1$; For the base case, $v = 1$;

$$n = \prod_{i=1}^{1} q_i = s_1 p^{k_1} + 1 = p^{\sum_{i=1}^{1} ki} \cdot \prod_{i=1}^{1} s_i + 0 \cdot p + 1$$

$$\text{Assume } n = \prod_{i=1}^{v} q_i = p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + Mp + 1 \text{ for some integer } v \geq 1,$$

we will show the formula holds for $v + 1$

$$n = \prod_{i=1}^{v+1} q_i = \left(s_{v+1} p^{k_{v+1}} + 1\right) \prod_{i=1}^{v} q_i = \left(s_{v+1} p^{k_{v+1}} + 1\right) \left(p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + Mp + 1\right)$$

$$= \quad p^{\sum_{i=1}^{v+1} ki} \cdot \prod_{i=1}^{v+1} s_i + Mps_{v+1} p^{k_{v+1}} + s_{v+1} p^{k_{v+1}} + p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + Mp + 1$$

$$= \ p^{\sum_{i=1}^{v+1} ki} \cdot \prod_{i=1}^{v+1} s_i + p\left(Ms_{v+1} p^{k_{v+1}} + s_{v+1} p^{k_{v+1} - 1} + p^{\sum_{i=1}^{v} ki - 1} \cdot \prod_{i=1}^{v} s_i + M\right) + 1$$

$$n \ = \ p^{\sum_{i=1}^{v+1} ki} \cdot \prod_{i=1}^{v+1} s_i + M'p + 1$$

If $v \geq 2$; for the base case $v = 2$ we have;

$$n = \prod_{i=1}^{2} q_i = \left(s_1 p^{k_1} + 1\right)\left(s_2 p^{k_2} + 1\right) = s_1 s_2 p^{k_1+k_2} + s_1 p^{k_1} + s_2 p^{k_2} + 1$$

$$= p^{\sum_{i=1}^{2} ki} \cdot \prod_{i=1}^{2} s_i + 0 \cdot p^{k_1+k_2} + \sum_{i=1}^{2} s_i\, p^{k_i} + 1$$

Now assume it holds for some $v \geq 2$, $1 \leq k_1 \leq k_2 \leq \cdots \leq k_v$;

$$n = \prod_{i=1}^{v} q_i \;= p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + M p^{k_1+k_2} + \sum_{i=1}^{v} s_i\, p^{k_i} + 1$$

For $v + 1$, $\;1 \leq k_1 \leq k_2 \leq \cdots \leq k_v \leq k_{v+1}$;

$$n = \prod_{i=1}^{v+1} q_i \;= \left(s_{v+1} p^{k_{v+1}} + 1\right) \prod_{i=1}^{v} q_i \;= \left(s_{v+1} p^{k_{v+1}} + 1\right) \left(p^{\sum_{i=1}^{v} ki} \prod_{i=1}^{v} s_i + M p^{k_1+k_2} + \sum_{i=1}^{v} s_i\, p^{k_i} + 1 \right)$$

$$= \; p^{\sum_{i=1}^{v+1} ki} \cdot \prod_{i=1}^{v+1} s_i + s_{v+1} p^{k_{v+1}} M p^{k_1+k_2} + \sum_{i=1}^{v} s_{v+1} s_i\, p^{k_i+k_{v+1}} + s_{v+1} p^{k_{v+1}} + \; p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i$$

$$+ M p^{k_1+k_2} + \sum_{i=1}^{v} s_i\, p^{k_i} + 1$$

$$= p^{\sum_{i=1}^{v+1} ki} \cdot \prod_{i=1}^{v+1} s_i + p^{k_1+k_2} \left(M s_{v+1} p^{k_{v+1}} + \sum_{i=1}^{v} s_{v+1} s_i\, p^{k_i+k_{v+1}-(k_1+k_2)} + p^{\sum_{i=1}^{v} ki-(k_1+k_2)} \prod_{i=1}^{v} s_i + M \right)$$

$$+ \sum_{i=1}^{v+1} s_i\, p^{k_i} + 1; \qquad k_i + k_{v+1} \geq k_1 + k_2\,, \sum_{i=1}^{v} k_i \geq k_1 + k_2$$

$$n \;=\; p^{\sum_{i=1}^{v+1} ki} \cdot \prod_{i=1}^{v+1} s_i + M' p^{k_1+k_2} + \sum_{i=1}^{v+1} s_i\, p^{k_i} + 1$$

Lemma 4.2. **Let $\boldsymbol{n = ap^k + 1}$, $\boldsymbol{a}$ and $\boldsymbol{k}$ are positive integers, $\boldsymbol{p}$ is an odd prime and $\boldsymbol{a < p}$. If $\boldsymbol{p^k \mid \phi(n)}$ then $\boldsymbol{n}$ is prime.**

Proof. Let $n = {p_1}^{a_1} {p_2}^{a_2} \ldots {p_v}^{a_v}$ be the prime power factorization of n, $v \geq 1$

$\phi(n) = {p_1}^{a_1-1} (p_1 - 1)\, {p_2}^{a_2-1} (p_2 - 1) \ldots {p_v}^{a_v-1} (p_v - 1)$
$p^k \mid {p_1}^{a_1-1} (p_1 - 1)\, {p_2}^{a_2-1} (p_2 - 1) \ldots {p_v}^{a_v-1} (p_v - 1)$. Note that $p \nmid p_i$ for all i. If $p \mid p_i$ then $p \mid n$, $p \mid n - ap^k = 1$, which is not possible. Therefore $p^k \mid (p_1 - 1)(p_2 - 1) \ldots (p_v - 1)$.
For every $i = 1, 2, \ldots, v$, $p \mid p_i - 1$ or $p \nmid p_i - 1$. We can group the primes p_i into two sets A and B where A is the set of all primes p_i for which $p \mid p_i - 1$, B contains all primes p_i for which $p \nmid p_i - 1$. Set A is non empty while set B may or may not be empty. $A = \{q_1, q_2, \ldots, q_u\}$, $1 \leq u \leq v$. If B is non empty, $B = \{q_{u+1},\; q_{u+2},\; \ldots, q_v\}$. Therefore $n = Q {q_1}^{b_1} {q_2}^{b_2} \ldots {q_u}^{b_u}$. If set B is empty, $Q = 1$ otherwise $Q > 1$. Let the highest power of p that divides $q_i - 1$ be p^{k_i}, $i = 1, 2, \ldots, u \qquad 1 \leq k_i \leq k$.
Note that $\phi(n) \leq ap^k < p \cdot p^k = p^{k+1}$ therefore $p^{k+1} \nmid \phi(n)$. It follows that $k_1 + k_2 + \cdots + k_u = k$.
Assume $k_1 \leq k_2 \leq \cdots \leq k_u$. $q_i = s_i \cdot p^{k_i} + 1$. We must have $s_i > 1$ otherwise if $s_i = 1$, $q_i > 2$ is even.

$$n = Qq_1{}^{b_1}q_2{}^{b_2}\dots q_u{}^{b_u} = Qq_1{}^{b_1-1}q_2{}^{b_2-1}\dots q_u{}^{b_u-1}q_1q_2\dots q_u = Q'q_1q_2\dots q_u.\ \ Q' \geq 1.$$

$$n = Q' \cdot \prod_{i=1}^{u} q_i = Q' \cdot \prod_{i=1}^{u}(s_i \cdot p^{k_i} + 1) = Q'\left(p^k \cdot \prod_{i=1}^{u} s_i + Mp + 1\right)$$

for some integer M, the last equality obtained from lemma 4.1

$$n = Q'\left(p^k \cdot \prod_{i=1}^{u} s_i + Mp + 1\right) = ap^k + 1$$

Factoring out p;

$$p\left(ap^{k-1} - Q'p^{k-1} \cdot \prod_{i=1}^{u} s_i - Q'M\right) = Q' - 1$$

$p \mid Q' - 1$. If $Q' > 1$, then $p \leq\ Q' - 1 < Q'$

$$n = Q'\left(p^k \cdot \prod_{i=1}^{u} s_i + Mp + 1\right) > Q'p^k > p \cdot p^k = p^{k+1}\,,$$

a contradiction because $n = ap^k + 1 < p^k(a + 1) \leq p^{k+1}$ hence we must have $Q' = 1$. $Q' = 1$ implies set B is empty and n is square free hence $u = v$.
If $v = 1$, then $n = q_1$ is prime. If $k = 1$, then $k_1 + k_2 + \cdots + k_v = 1$, $v = 1$ and n is prime.
Assume $k \geq 2$ and $v \geq 2$. From lemma 4.1;

$$n = p^k \cdot \prod_{i=1}^{v} s_i + Mp^{k_1+k_2} + \sum_{i=1}^{v} s_i\, p^{k_i} + 1 = ap^k + 1$$

$$ap^k = p^k \cdot \prod_{i=1}^{v} s_i + Mp^{k_1+k_2} + \sum_{i=1}^{v} s_i\, p^{k_i}$$

There's a positive integer h such that $k_1 = k_2 = \cdots = k_h <\ k_{h+1} \leq\ k_{h+2} \leq\ \dots \leq k_v,\quad 1\ \leq\ h \leq\ v.$
Dividing all terms by p^{k_1} we have;

$$ap^{k_2+\cdots+k_v} = p^{k_2+\cdots+k_v} \cdot \prod_{i=1}^{v} s_i + Mp^{k_2} + s_1 + s_2 + \cdots + s_h + s_{h+1}p^{k_{h+1}-k_1} + \cdots + s_v p^{k_v - k_1}$$

$$p \mid s_1 + s_2 + \cdots + s_h \quad p \leq s_1 + s_2 + \cdots + s_h < \prod_{i=1}^{v} s_i$$

$$n = p^k \cdot \prod_{i=1}^{v} s_i + Mp^{k_1+k_2} + \sum_{i=1}^{v} s_i\, p^{k_i} + 1 > p^k \cdot \prod_{i=1}^{v} s_i > p^k \cdot p = p^{k+1}\,,$$

a contradiction therefore $v = 1$, $n = q_1$.

Theorem 4.1 Let $n = ap^k + 1$, a and k are positive integers, p is an odd prime, $a < p$. If there exists a positive integer b such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^{(n-1)/p} \not\equiv 1 (\bmod\ n)$ then n is prime.

Proof. Assume n is composite and $b^{n-1} \equiv 1 \ (\mathrm{mod}\ n)$. From Theorem 1.1, $\mathrm{ord}_n b \mid n-1 = ap^k$. Since $(a, p^k) = 1$, we have $\mathrm{ord}_n b = d_1 d_2$, $d_1 \mid a$, $d_2 \mid p^k$, $d_2 = p^t$. From lemma 4.2, we must have $0 \le t \le k-1$ hence $d_2 \mid p^{k-1}$. $\mathrm{ord}_n b = d_1 d_2 \mid a \cdot p^{k-1}$. It follows from Theorem 1.1 that $b^{(n-1)/p} = b^{ap^{k-1}} \equiv 1 \ (\mathrm{mod}\ n)$. Consequently if $b^{n-1} \equiv 1 \ (\mathrm{mod}\ n)$ and $b^{(n-1)/p} \not\equiv 1 (\mathrm{mod}\ n)$ then we know n is prime.

Example 4.1. Suppose we want to test whether $564899 = 82 \cdot 83^2 + 1$ is prime. Using modular exponentiation, it can be verified that $2^{82 \cdot 83^2} \equiv 1 \ (\mathrm{mod}\ 564899)$ and $2^{82 \cdot 83} \not\equiv 1 \ (\mathrm{mod}\ 564899)$. Therefore, from Theorem 4.1, 564899 is prime.

The Mersenne number M_{21701} is prime, **[2]**. With the help of the Maple engine and Theorem 4.1, it can be shown that the first five prime numbers of the form $(10^{4500} + k) \cdot M_{21701} + 1$, $k \ge 0$, occur at $k = 5318, 48362, 56690, 61206, 71340$. Verifying each of these numbers takes less than 15 seconds on an HP ProBook 640 G1 i5 processor. The test is very efficient, however, testing a number with over a million decimal digits is limited by the memory capacity of the machine.

Experimental Observations

Numerical evidence suggests that there are no composite integers $n = ap^k + 1$, $a < p^{k/2}$, p is prime such that $p^k \mid \phi(n)$. If this is true for all composite integers n, then the upper bound of a in Theorem 4.1 can be significantly improved from p to $p^{k/2}$ for higher values of k. If $a < p^k$, there some composites for which $p^k \mid \phi(n)$ e.g. $4699 = 37 \cdot 127 = 58 \cdot 3^4 + 1$. Are these composites infinitely many for a given prime p? Furthermore if $p^k \mid \phi(n)$ and n is composite, then n has prime factor q of the form $tp + 1$, $q \le \sqrt{n}$. If this is true for all n, then trial division can be combined with the Fermat test to prove the primality of n. If n has no prime divisor of the form $tp + 1 \le \sqrt{n}$ then we know $p^k \nmid \phi(n)$ if n is composite and Theorem 4.1 applies.

Are there any Fermat pseudoprimes $n = ap^k + 1$, $a < p^k$ and $p^k \mid \phi(n)$. Indeed, these pseudoprimes exist, however, they are rare. If $p = 2$, and $k = 20$, we have only one pseudoprime to the base 2, $53282340865 = 50814 \cdot 2^{20} + 1$ compared to 78543 primes. If $p = 3$, and $k = 13$, there are no pseudoprimes to the base 2. Theorem 4.1 can thus be used as a probabilistic primality test for integers of the form $ap^k + 1$, $a < p^k$, p is prime.

The first five Fermat pseudoprimes of the form $ap^k + 1$, $a < p$, to base 2 include; $11305 = 72 \cdot 157 + 1$, $13741 = 60 \cdot 229 + 1$, $13981 = 60 \cdot 233 + 1$, $18705 = 112 \cdot 167 + 1$, $23377 = 48 \cdot 487 + 1$ and to base 3; $286 = 15 \cdot 19 + 1$, $671 = 10 \cdot 67 + 1$, $949 = 12 \cdot 79 + 1$, $11011 = 30 \cdot 367 + 1$, $15203 = 22 \cdot 691 + 1$ and the first four Carmichael numbers; $63973 = 36 \cdot 1777 + 1$, $101101 = 300 \cdot 337 + 1$, $126217 = 72 \cdot 1753 + 1$, $278545 = 336 \cdot 829 + 1$. For all these pseudoprimes $k = 1$.
Are there any Fermat pseudoprimes n of the form $ap^k + 1$ with $a < p$, $k \ge 2$ and p is prime? If they exist, they must be extremely rare. There are no counterexamples to the base 2 for all $n < 10^7$.

For every positive integer n, is there a prime of the form $an + 1$, $a \le n$? When $n = 1, 3, 5$, there's only one value of $a \le n$ for each n so that $an + 1$ is prime. When $n = 31$, there are three values of $a \le n$ that make $an + 1$ prime; $a = 10, 12, 22$. As n grows, numerical evidence shows that the number of solutions a such that $an + 1$ is prime also grows.

Let $n = 4p^t + 1,\ t \geq 1,\ p > 4$ is prime. Define the sequence $r_1 = 4$, $r_{k+1} \equiv {r_k}^2 - 2 (\text{mod}\, n)$, $k \geq 1$, $0 \leq r_k < n$ then n is prime if and only if there exists an integer j, $1 < j < n$, such that $r_j \equiv 4\ (\text{mod}\, n)$.

Generalization of lemma 4.2

Generalization of Lemma 4.2 would provide a primality test for testing a broader set of integers. Lemma 4.2 says that if n is a positive integer of the form $ap^k + 1$, a and k are positive integers, p is an odd prime, $a < p$ and $p^k \mid \phi(n)$ then n is prime. How best can this lemma be generalized for integers of the form $am + 1$ such that for a given positive integer m, a is as large as possible and if $m \mid \phi(n\ )$ then n is prime? Motivated by the upper bound of a in lemma 4.2, the first guess is $a < \text{rad}(m)$. However, this guess is put down with the counterexample $946 = 2 \cdot 11 \cdot 43 = 27 \cdot 35 + 1$, where $a = 27$, $m = 35$, $\text{rad}(m) = 35$. There are many counterexamples to this initial guess. Another guess would be $a < p$, where p is the largest prime divisor of m. This too fails with the counterexamples $34716 = 2^2 \cdot 3 \cdot 11 \cdot 263 = 53 \cdot 5 \cdot 131 + 1$, $a = 53$, $m = 5 \cdot 131$, $p = 131$ and $25272495 = 3^2 \cdot 5 \cdot 79 \cdot 7109 = 1094 \cdot 13 \cdot 1777 + 1$ where $a = 1094$, $m = 13 \cdot 1777$, $p = 1777$. There are many counterexamples to this guess as well. The last guess is $a < p$ where p is the least prime divisor of m. The author has not yet found any counterexamples to this guess. The author is still working on its proof.

Conjecture 4.1 Let $n = am + 1$, where a and m are positive integers and let p be the least prime divisor of m. If $a < p$ and $m \mid \phi(n)$ then n is prime.

In general, if $n = am + 1$, $(\ a, m) = 1$ and we know beforehand that $m \mid \phi(n)$ if and only if n is prime, then the factorization of a is not necessary in determining the primality of n using Lucas's converse of Fermat's little theorem. The following theorem demonstrates this fact.

Theorem 4.2 Let $n = am + 1$, where a and $m > 1$ are relatively prime positive integers such that n is prime whenever $m \mid \phi(n)$. If there exists a positive integer b such that $b^{n-1} \equiv 1\ (\text{mod}\, n)$ and $b^{(n-1)/q} \not\equiv 1 (\text{mod}\, n)$ for all prime divisors q of m then n is prime.

Proof. Assume n is composite and $b^{n-1} \equiv 1\ (\text{mod}\, n)$. From Theorem 1.1, $\text{ord}_n b \mid n - 1 = am$. Since $(a, m) = 1$, $\text{ord}_n b = d_1 d_2$, $d_1 \mid a$ and $d_2 \mid m$. Let $m = {q_1}^{a_1} {q_2}^{a_2} \ldots {q_k}^{a_k}$ be the prime power factorization of m then $d_2 = {q_1}^{b_1} {q_2}^{b_2} \ldots {q_k}^{b_k}$, $0 \leq b_i \leq a_i$. If $b_i = a_i$ for all i, then $d_2 = m$. From Theorem 1.1, $\text{ord}_n b \mid\ \phi(n)$ and since $m = d_2 \mid \text{ord}_n b$, we have $m \mid \phi(n)$, a contradiction. Therefore, there's an integer j, $1 \leq j \leq k$, such that $b_j \leq a_j - 1$. It follows that ${q_j}^{b_j} \mid {q_j}^{a_j - 1}$,

$$d_2 = {q_1}^{b_1} {q_2}^{b_2} \ldots {q_j}^{b_j} \ldots {q_k}^{b_k}\ \mid\ {q_1}^{a_1} {q_2}^{a_2} \ldots {q_j}^{a_j - 1} \ldots {q_k}^{a_k}.$$

$\text{ord}_n b = d_1 d_2 \mid a \cdot\ {q_1}^{a_1} {q_2}^{a_2} \ldots {q_j}^{a_j - 1} \ldots {q_k}^{b_k} = (n-1)/q_j$. From Theorem 1.1,

$$b^{(n-1)/q_j} \equiv 1\ (\text{mod}\, n).$$

Therefore if $b^{n-1} \equiv 1\ (\text{mod}\, n)$ and $b^{(n-1)/q} \not\equiv 1 (\text{mod}\, n)$ for all prime divisors q of m then n is prime.

Note that using the fact that $n - 1 \mid \phi(n)$ if and only if n is prime, Lucas's converse of Fermat's little theorem follows directly from Theorem 4.2. Assuming conjecture 4.1 is true, then Theorem 4.2 can be used to test all integers of the form $am + 1$ with a less than the least prime divisor of m.

From computation results, if $n = a(a + 1) + 1$, $a \equiv 5\ (\text{mod}\ 6)$ and $a \mid \phi(n)$ then n is prime for all $a < 10^8$ except when $a = 9736265$ in which case n is composite. From theorem 4.2, if $a < 10^8$, $a \neq 9736265$, $b^{n-1} \equiv 1\ (\text{mod}\, n)$ and $b^{(n-1)/q} \not\equiv 1 (\text{mod}\, n)$ for all prime divisors q of a, then n is prime.

This result is however not much useful compared to Lemma 4.2 since we had to first test the primality of n. More research on forms of positive integers $n = am + 1$ for which $m \mid \phi(n)$ if and only if n is prime will be very useful for testing their primality using Theorem 4.2. The author is still working on these forms of integers. It can easily be shown that if m is prime then $m \mid \phi(n)$ if and only if $a \equiv b(\text{mod } q)$ for some prime $q = bm + 1$, $a \geq b$. If $a = b$, n is prime otherwise n is composite. If m is an odd prime, we have $b \geq 2$ therefore for all $a \leq 2m$ we have $m \mid \phi(n)$ if and only if n is prime.

For any comments or suggestions on this article, contact the author on **ariko@cedat.mak.ac.ug** or **philemonariko@gmail.com**

Acknowledgement. I thank my former lecturer, Dr. Bamunoba Alex Samuel for the encouragement in Number Theory.

References

[1] Rosen, Kenneth H. Elementary number theory and its applications - 6th edition

[2] A000668 The Online Encyclopedia of Integer Sequences