A note on primality of $ap^k + 1$ numbers

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

7/07/2020

Abstract

In 1876, Edouard Lucas showed that 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. This result was considerably improved by Henry Pocklington in 1914 when he showed that it's not necessary to know all the prime factors of $n-1$ to determine the primality of n. In this paper we optimize Pocklington's primality test for integers of the form $ap^k + 1$ where p is prime, $a < 4(p+1)$, $k \geq 1$. Precisely, this paper shows that if an integer b exists such that $b^{n-1} \equiv 1 \pmod{n}$ and $n \nmid b^{(n-1)/p} - 1$, then n is prime as opposed to Pocklington's primality test that imposes the more stringent hypothesis that n and $b^{(n-1)/p} - 1$ be relatively prime. We also present a conjecture whose proof will significantly reduce the computations required to determine the primality of these integers.

Keywords Primality tests, Lucas' test, Pocklington's test, Prime generation, Pseudoprimes

1. Introduction

The problem of distinguishing primes from composite integers has been of interest to professional and amateur mathematicians alike for many centuries up to date. A number of primality 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 determine whether a number is prime with absolute certainty while others such as Fermat's Primality test, Miller-Rabin test report a 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, more information on these tests can be found in [1], [3], [5], [6]. In this paper we prove a relatively more efficient primality test for integers n of the form $ap^k + 1$, $k \geq 1$, $a < 4(p+1)$, where p is an odd prime. This test does not require computation of some greatest common divisors required in Pocklington's primality test. Much effort is put in determining which positive integers of this form does the divisibility relation $p^k \mid \phi(n)$ hold from which the optimized test is deduced using properties of order of an integer. In section 4, we present a conjecture whose proof will significantly reduce the computations required to determine the primality these integers.

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

Theorem 1.1. Let a and $n > 1$ be relatively prime integers, 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 $\mathrm{ord}_n a \mid \phi(n)$.

For comparison with the optimized test, Pocklington's primality test and one of its variants are stated here. (See [1] pages 622 - 623), [2] pages 29-30, [4] page 381)

Theorem 1.2. Pocklington's Primality Test. Suppose that n is a positive integer with $n-1=FR$ where $(F,R)=1$ and $F>R$. The integer n is prime if there exists an integer b such that $(b^{(n-1)/q}-1,n)=1$ whenever q is a prime with $q \mid F$ and $b^{n-1} \equiv 1 \pmod n$

Theorem 1.3. Let $n-1=ap$, where p is an odd prime such that $2p+1>\sqrt{n}$. If there exists an integer b for which $b^{(n-1)/2} \equiv -1 \pmod n$ and $b^{a/2} \not\equiv -1 \pmod n$, then n is prime.

2. Primes of the form $ap+1$

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

Lemma 2.1. Let $n=ap+1$, where a is a positive integer and p is an odd prime. If $p \mid \phi(n)$ then $a \equiv t \pmod q$ for some prime $q=tp+1$.

Proof. Let $n=p_1^{a_1}p_2^{a_2} \ldots p_k^{a_k}$ be the prime power factorization of n. We have $\phi(n)=p_1^{a_1-1}(p_1-1)\,p_2^{a_2-1}(p_2-1) \ldots p_k^{a_k-1}(p_k-1)$. $p \mid \phi(n)$ implies $p \mid p_i$ or $p \mid p_i-1$ for some $i=1,2,\ldots,k$. If $p \mid p_i$, then $p \mid n-ap=1$, which is not possible hence $p \mid p_i-1$ for some $i=j$, $p_j=q=tp+1$ for some t. $n=mq=m(tp+1)=ap+1$. Factoring out p, we have $p(a-mt)=m-1$, $p \mid m-1$, $m=sp+1$ for some s. $n=mq=(sp+1)(tp+1)=(sq+t)p+1=ap+1$ i.e. $a=sq+t \equiv t \pmod q$. This completes the proof.

Remark. If $a=t$, we have $a \equiv t \pmod q$, $n=q$ is prime. Since p is assumed an odd prime, we have $t \geq 2$. If a is even, $a=t+cq \geq 4(p+1)$. It follows that for all even $a<4(p+1)$, we have $p \mid \phi(n)$ if and only if n is prime. Note that the inequality $a<4(p+1)$ is equivalent to $2p+1>\sqrt{n}$ in Theorem 1.3.

Theorem 2.1. Let $n=ap+1$ where a is even and p is an odd prime with $a<4(p+1)$. If there exists a positive integer b such that $b^{n-1} \equiv 1 \pmod n$ and $b^a \not\equiv 1 \pmod n$ then n is prime.

Proof. We will show that if n is composite and $b^{n-1} \equiv 1 \pmod n$ then $b^a \equiv 1 \pmod n$. Assume n is composite and $b^{n-1} \equiv 1 \pmod n$. 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, $b^a \equiv 1 \pmod n$. Consequently if $b^{n-1} \equiv 1 \pmod n$ and $b^a \not\equiv 1 \pmod n$ then we know n is prime.

Remark. A slightly more efficient primality test is obtained by replacing the hypothesis $b^{n-1} \equiv 1 \pmod n$ with $b^{(n-1)/2} \equiv \pm 1 \pmod n$.

Example 2.1. Suppose we want to test whether $547=42 \cdot 13+1$ is prime. Using fast modular exponentiation techniques, it can be verified that $2^{546} \equiv 1 \pmod{547}$ and $2^{42} \equiv 475 \not\equiv 1 \pmod{547}$ and from Theorem 2.1, 547 is prime.

Using Pocklington's primality test, $547=21 \cdot 26+1$. Taking $b=2$, there's need to further verify that $(2^{42}-1,\ 547)=1$ and $(2^{273}-1, 547)=1$ which takes more steps compared to the previous test.

Alternatively, Theorem 1.3 can be used to show $n=547$ is prime. The advantage of Theorem 2.1 over Theorem 1.3 is if n is prime, any randomly chosen positive integer $b<547$ is guaranteed to satisfy

$b^{(n-1)/2} \equiv \pm 1 \pmod{n}$ unlike $b^{(n-1)/2} \equiv -1 \pmod{n}$ with 50% chance. However, showing that $b^{a/2} \not\equiv -1 \pmod{n}$ is slightly more efficient compared to showing that $b^a \not\equiv -1 \pmod{n}$.

From Theorem 1.2, we note that the largest integer n such that $b^a \equiv 1 \pmod{n}$ is $n = b^a - 1$, $b > 1$. Setting 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 $b^a \not\equiv 1 \pmod{n}$. Furthermore if $b^{n-1} \equiv 1 \pmod{n}$ and $a < 4(p + 1)$, from Theorem 2.1 we know n is prime. We state this result as a corollary.

Corollary 2.1. Let $n = ap + 1$ where a is even and p is an odd prime with $a < 4(p + 1)$. If $b > 1$ is a positive integer relatively prime to n and $p > (b^a - 2)/a$ then $b^{n-1} \equiv 1 \pmod{n}$ if and only if n is prime.

Example 2.2. 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 $2^{n-1} \equiv 1 \pmod{n}$ if and only if n is prime i.e. p is a Sophie Germain prime if and only if $2^{2p} \equiv 1 \pmod{2p + 1}$.
If we take $b = 2$ and $a = 6$, we have $(2^6 - 2)/6 = 31/3 < 11$. Taking $p \geq 11$ and $n = 6p + 1$, we have $2^{n-1} \equiv 1 \pmod{n}$ if and only if n is prime.

On the other hand; To test $n = 6p + 1$, $p \geq 11$ using Pocklington's primality test; In addition to checking the congruence $b^{n-1} \equiv 1 (\text{mod}\ n)$, there's need to verify that $(b^6 - 1, n) = 1$. If $b = 2$, we have to verify that $(63, n) = 1$ unlike Corollary 2.1 for which this step is not necessary.

As noted earlier, using Theorem 1.3 to show $n = 6p + 1$, $p \geq 11$, is prime has 50% chance of working for a randomly chosen base b thus Corollary 2.1 is the most efficient primality test for all $n = ap + 1$, with the prime $p > (b^a - 2)/a$.

Remark. We can make use of the full potential of Lemma 2.1 by noting that if c is a positive integer, $n = ap + 1$, and n is composite for all integers $a < c$ then for all $a < 2cp + c + 2$, we have $p \mid \phi(n)$ if and only if n is prime thus improving the upper bound of a in Theorem 2.1 from $4(p + 1)$ to $2cp + c + 2$. Taking $p = 19$, it can be verified that n is composite for all $a < 10$. It follows that for all $a < 392$, if there exists an integer b such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^a \not\equiv 1 (\text{mod}\ n)$ then n is prime.

In general, Theorem 2.1 can be used to test all integers of the form $ap + 1$ without an upper bound on a. From Lemma 2.1, if $a \neq t + sq$ for all primes $q = tp + 1$ and all integers $s \geq 1$ then $p \mid \phi(n)$ if and only if n is prime. Therefore, if there exists an integer b such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^a \not\equiv 1 (\text{mod}\ n)$ then n is prime. This makes Theorem 2.1 more versatile compared to Theorem 1.3 when generating primes of the form $ap + 1$.

3. Generalization of Theorem 2.1 for higher powers of p

In this section we generalize 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 $a < 4(p + 1)$ then $p^k \mid \phi(n)$ if and only if n is prime. It follows that if n is composite and $b^{n-1} \equiv 1 (\text{mod}\ n)$, the highest power of p in $\text{ord}_n b$ is less than p^k so that $b^{ap^{k-1}} = b^{(n-1)/p} \equiv 1 (\text{mod}\ n)$. We proceed to give a detailed proof.

Lemma 3.1. Let p, v, k_i, s_i, q_i , $1 \le i \le v$ be positive integers, $k_1 \le k_2 \le \cdots \le k_v$, $q_i = s_i p^{k_i} + 1$, $n = \prod_{i=1}^{v} q_i$. Then $n = p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + Mp + 1$ for some integer M. Furthermore if $v \ge 2$, then $n = p^{\sum_{i=1}^{v} ki} \cdot \prod_{i=1}^{v} s_i + Mp^{k_1+k_2} + \sum_{i=1}^{v} s_i\, p^{k_i} + 1$ for some integer M.

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

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

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

For $v + 1$, $1 \le k_1 \le \cdots \le k_{v+1}$;

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

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

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

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

If $v \ge 2$; 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 $v \ge 2$, $1 \le k_1 \le k_2 \le \cdots \le k_v$;

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

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

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

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

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

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

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

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

Lemma 3.2. Let $n = ap^k + 1$, a and k are positive integers, p is an odd prime and $a < p$. If $p^k \mid \phi(n)$ then 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, $v \geq 1$. $\phi(n) = {p_1}^{a_1-1}(p_1-1)\,{p_2}^{a_2-1}(p_2-1) \ldots {p_v}^{a_v-1}(p_v-1)$. $p^k \mid {p_1}^{a_1-1}(p_1-1)\,{p_2}^{a_2-1}(p_2-1) \ldots {p_v}^{a_v-1}(p_v-1)$. A similar argument as in Lemma 2.1 shows that $p^k \mid (p_1-1)(p_2-1) \ldots (p_v-1)$. 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. $A = \{q_1, q_2, \ldots, q_u\}$, $1 \leq u \leq v$. Therefore $n = Q{q_1}^{b_1}{q_2}^{b_2} \ldots {q_u}^{b_u}$ where $Q = 1$ if set B is empty otherwise $Q > 1$. Let the highest power of p that divides $q_i - 1$ be p^{k_i}, $i = 1, 2, \ldots, u$, $1 \leq k_i \leq k$. $q_i = s_i \cdot p^{k_i} + 1$. We must have $s_i > 1$ otherwise $q_i > 2$ is even. 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 $k_1 \leq k_2 \leq \cdots \leq k_u$.

$$n = Q{q_1}^{b_1}{q_2}^{b_2} \ldots {q_u}^{b_u} = Q{q_1}^{b_1-1}{q_2}^{b_2-1} \ldots {q_u}^{b_u-1}q_1q_2 \ldots q_u = Q'q_1q_2 \ldots q_u.\;\; Q' \geq 1.$$

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

for some integer M, the last equality obtained from Lemma 3.1

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

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 3.1;

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

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

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

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

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

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

a contradiction therefore $v = 1$, $n = q_1$. This completes the proof.

Remark. As illustrated in Lemma 2.1, we note that if a is even, we have $p^k \mid \phi(n)$ if and only if n is prime for all $a < 4(p+1)$. From experimental results, if k is large, there's a possibility of strengthening the hypothesis of Lemma 3.2 such that if $n = ap^k + 1$, $a <$, p is an odd prime, then $p^{[k/2]} \mid \phi(n)$ if and only if n is prime. A more rigorous proof should be able to establish this or even stronger results. To motivate further research on this conjecture, we will prove in the next section using the concepts of that section that if $n = ap^2 + 1$, $a < p$ and if an integer b exists such $b^{n-1} \equiv 1 \pmod{n}$ and $b^a \not\equiv 1 (\mathrm{mod}\, n)$ then n is prime. This is a considerable improvement in comparison to Pocklington's primality test that requires that the integer b satisfies $b^{n-1} \equiv 1 \pmod{n}$ and $(b^{ap} - 1, n) = 1$. Much more efficient primality testing is possible assuming this conjecture is true.

Theorem 3.1. Let $n = ap^k + 1$, a and k are positive integers, p is an odd prime, $a < 4(p+1)$. If there exists an integer b such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^{(n-1)/p} \not\equiv 1 (\mathrm{mod}\, n)$ then n is prime.

Proof. Assume n is composite and $b^{n-1} \equiv 1 \pmod{n}$. 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 3.2, we must have $0 \leq t \leq k - 1$ 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 $b^{(n-1)/p} = b^{ap^{k-1}} \equiv 1 \pmod{n}$. Consequently if $b^{n-1} \equiv 1 \pmod{n}$ and $b^{(n-1)/p} \not\equiv 1 (\mathrm{mod}\, n)$ then we know n is prime.

Example 3.1. To test $727 = 6 \cdot 11^2 + 1$ for primality; Using fast modular exponentiation, it can be shown that $2^{6 \cdot 11^2} \equiv 1 \pmod{727}$ and $2^{6 \cdot 11} \equiv 590 \not\equiv 1 \pmod{727}$. Therefore, from Theorem 3.1, 727 is prime.

Alternatively, we can make use of Pocklington's primality test to show that 727 is prime. However, as noted earlier, this test is slightly less efficient compared to the optimized test because the latter requires that $2^{6\cdot 11}-1$ should not be a multiple of 727 whereas the former imposes the more strict condition that $2^{6\cdot 11}-1$ and 727 be relatively prime.

4. Generalization of Lemma 3.2 for $\boldsymbol{am+1}$ integers

Generalization of Lemma 3.2 will provide a relatively more efficient primality test for a broader set of positive integers. Substantial experimental data suggests that if $n=am+1$, $a<4(p+1)$, p is the least prime divisor of m, then $m \mid \phi(n)$ if and only if n is prime

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 $a<4(p+1)$ and $m \mid \phi(n)$ then n is prime.

Remark. 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, 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.

Theorem 4.1. 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 for each prime q_i dividing m, there exists an integer b_i such that ${b_i}^{n-1} \equiv 1 \pmod{n}$ and ${b_i}^{(n-1)/q_i} \not\equiv 1 \pmod{n}$ then n is prime.

Proof. From Theorem 1.1, $\mathrm{ord}_n b_i \mid n-1$. Let $m={q_1}^{a_1}{q_2}^{a_2}\dots{q_k}^{a_k}$ be the prime power factorization of m. The combination of $\mathrm{ord}_n b_i \mid n-1$ and $\mathrm{ord}_n b_i \nmid (n-1)/q_i$ implies ${q_i}^{a_i} \mid \mathrm{ord}_n b_i$. From Theorem 1.1, $\mathrm{ord}_n b_i \mid \phi(n)$ therefore for each i, ${q_i}^{a_i} \mid \phi(n)$ hence $m \mid \phi(n)$. By the hypothesis of Theorem 4.1, n is prime.

Theorem 4.1 has little practical value on its own but becomes powerful when the integer m is known beforehand. Assuming the truth of conjecture 4.1, Theorem 4.1 becomes an optimized primality test for such integers in comparison to Lucas's converse of Fermat's little theorem and occasionally relatively more efficient than Pocklington's primality test, specifically when $(m/p^t)<(n/2)^{(1/3)}$ where p is the least prime divisor of m and p^t is the power of p in the prime power factorization of m.

As remarked earlier, experimental results suggest that if $n=ap^k+1$, $a<4(p+1)$, k is large then n is prime if and only if $p^{[k/2]} \mid \phi(n)$. We state this conjecture formally.

Conjecture 4.2. Let $n=ap^k+1$, $a<p$ where p is an odd prime. If a_i is large, the integer $m=p^{[k/2]}$ divides $\phi(n)$ if and only if n is prime.

Table 1 shows some experimental results supporting the truth of this conjecture. To motivate further research towards its proof, we prove here the case $n=ap^2+1$ and justify its importance by showing that for any positive integer a, there are finitely many pseudoprimes of this form to any base $b>1$.

Lemma 4.1. Let $n=ap^2+1$, $a<p$, p is an odd prime. If $p \mid \phi(n)$, then n is prime.

Proof. Let $n={p_1}^{a_1}{p_2}^{a_2}\dots{p_k}^{a_k}$ be the prime power factorization of n. $\phi(n)={p_1}^{a_1-1}(p_1-1)\,{p_2}^{a_2-1}(p_2-1)\dots{p_k}^{a_k-1}(p_k-1)$. Using a similar argument as in the proof of Lemma 2.1, $p \mid p_i-1$ for some $i=j$. $p_j=tp+1$ for some t. $n=mp_j=m(tp+1)=ap^2+1$. Factoring out p, we have $p(ap-mt)=m-1$, $p \mid m-1$, $m=sp+1$ for some $s\geq 0$. $n=mp_j=(sp+1)(tp+1)=stp^2+(s+t)p+1=ap^2+1$. If $s\geq 1$, we see that $p \mid s+t$, $p\leq s+t\leq st$. $n=stp^2+(s+t)p+1>$

$stp^2 \geq p \cdot p^2 = p^3$, a contradiction because $n = ap^2 < p^3$ therefore $s = 0, n = tp + 1 = p_j$. This completes the proof.

Theorem 4.2. Let $n - 1 = \prod_{i=1}^{k} {p_i}^{s_i}$ where p_i are distinct primes, $s_i \geq 1$. Let $m = \prod_{i=1}^{k} {p_i}^{t_i}$, $0 \leq t_i \leq s_i$ be an integer such that n is prime whenever $m \mid \phi(n)$. If for each prime p_i dividing m, there exists an integer b_i such that ${b_i}^{n-1} \equiv 1 \pmod{n}$ and ${b_i}^{(n-1)/({p_i}^{s_i - t_i + 1})} \not\equiv 1 (\text{mod } n)$ then n is prime.

Proof. Using a similar argument as in the proof of Theorem 4.1, for each i, ${p_i}^{s_i - (s_i - t_i + 1) + 1} = {p_i}^{t_i} \mid \phi(n)$ hence $m \mid \phi(n)$. By the hypotheses of Theorem 4.2, n is prime.

Remark. Theorem 4.2 is a strengthening of Theorem 4.1; It does not require that m and $(n-1)/m$ be relatively prime. Its considerably more efficient than Theorem 4.1 when $t_i < s_i$ for some i.

Theorem 4.3. Let $n = ap^2 + 1$, $p > a$ is prime. If an integer b exists such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^a \not\equiv 1 \pmod{n}$ then n is prime.

Proof. From Lemma 4.1, $p \mid \phi(n)$ if and only if n is prime. Because the integer b satisfies the hypothesis of Theorem 4.2, n is prime.

Remark. From Theorem 4.3, we deduce that for any positive integer a, there are finitely many pseudoprimes to any base $b > 1$. This is true because $b^a \not\equiv 1 \pmod{n}$ for all $n > b^a$.

Table 1 shows the least positive integer k such that n is composite and $p^t \mid \phi(2 \cdot p^k + 1)$, $p = 3, 5$; $t = 1, 2, \ldots, 10$. From this table we see that for all $k < 146$; if $3^{10} \mid \phi(2 \cdot 3^k + 1)$ then n is prime. An appeal to Theorem 4.2 shows that if there exists an integer b such that $b^{n-1} \equiv 1 \pmod{n}$ and $b^{2 \cdot 3^9} \not\equiv 1 (\text{mod } n)$, then n is prime.

Similarly, if $n = 2 \cdot 5^k + 1$, $k < 101$ and if $b^{n-1} \equiv 1 \pmod{n}$ and $b^{2 \cdot 5^5} \not\equiv 1 (\text{mod } n)$, n is prime. This is a considerable time save compared to Lucas's converse of Fermat's little theorem and Pocklington's primality test which require computation of $b^{(n-1)/p}$ mod n.

Table 1: Least values of k such that n is composite and $p^t \mid \phi(n)$, $p = 3, 5$

p^t $t =$	1	2	3	4	5	6	7	8	9	10
$n = 2 \cdot 3^k + 1$, $k =$,	7	19	23	36	37	63	72	77	77	146
$n = 2 \cdot 5^k + 1$, $k =$	6	11	28	28	31	101	101	101		

Similar to Theorem 4.1, Theorem 4.2 requires that the integer m be known for the theorem to be applied. Taking $m = n - 1$, we have Lucas's converse of Fermat's little theorem. Note that from Table 1, the estimate $p^{[k/2]}$ in Conjecture 4.2 is very conservative.

It can be verified that none of the integers in this table is a pseudoprime to base 2. We now turn our attention to investigating pseudoprimes n of the form $ap^k + 1$, $a < p$ for which $p \mid \phi(n)$. From Lemmas 2.1 and 4.1, there are no composites n, $k = 1, 2$ with the property $p \mid \phi(n)$. We will therefore focus on the remaining cases; $k \geq 3$.

Table 2 shows the least positive integer a such that $n = ap^k + 1$ is a pseudoprime to base 2 and $p \mid \phi(n)$, $p = 3, 5, 7, \ldots, 31$; $k = 1, 2, \ldots, 10$.

Table 2: Least values of a such that $n = ap^k + 1$ is a pseudoprime to base 2 and $p \mid \phi(n)$

$p =$	3	5	7	11	13	17	19	23	29	31
$k = 3,\ a =$	64	184	1404	468	74088	170826	658492	216	682908	4263580
$k = 4,\ a =$	110	6408	396	79380	951048	30960	433216	519120	$> 10^7$	$> 10^7$
$k = 5,\ a =$	192	8832	39940	287560	$> 10^7$					
$k = 6,\ a =$	64	13048	1081200	$> 10^7$						
$k = 7,\ a =$	9000	343434	538200	$> 10^7$						
$k = 10,\ a =$	11900	$> 10^7$								

A key observation we make from this table; For all n, we have $a > p$. Moreover, the least values a grow rapidly compared to the primes p and integers k.

Conjecture 4.3. There are no Fermat pseudoprimes to the base 2 of the form $n = ap^k + 1$, $a < p$, where p is an odd prime such that $p \mid \phi(n)$.

This conjecture has been verified for all $p = 3, 5, 7, \ldots, 31$, $k < 10^3$ with no counter-examples. It has also been checked for all odd primes $p < 10^3$, $k \leq 10$. From Table 2, the least values a grow very rapidly in comparison to the primes p and integers k. The probability of obtaining an a with $a < p$ is extremely small. Despite the overwhelming numerical evidence supporting the truth of this conjecture, there may still be some counterexamples.

Theorem 4.4. Let $n = ap^k + 1$ where p is an odd prime with $a < p$. If $2^{n-1} \equiv 1 \pmod{n}$ and $2^a \not\equiv 1 \pmod{n}$ then n is prime.

Proof. From the hypothesis of Theorem 4.4, $2^{n-1} \equiv 1 \pmod{n}$ and assuming the truth of Conjecture 4.3, we have $p \mid \phi(n)$ if and only if n is prime. Because $b = 2$ satisfies the hypothesis of Theorem 4.2, n is prime.

Remark. From Theorem 4.4, we note that for any positive integer a, there are finitely many pseudoprimes n of the form $ap^k + 1$ to the base 2 where p is an odd prime, $a < p$ and $k \geq 1$. Similarly, for any odd prime p, there are finitely many pseudoprimes of the form $ap^k + 1$, $a < p$, $k \geq 1$. This is true because $2^a \not\equiv 1 \pmod{n}$ for all $n > 2^a$.

Conclusion. More research in this direction will produce highly optimized primality tests for integers satisfying the hypotheses of Theorem 4.2.

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

References

[1] Brillhart, John; Lehmer, D.H.; Selfridge, J. L. (April 1975). "New Primality criteria and Factorizations of $2^m \pm 1$". Mathematics of Computation. pp. 622-623

[2] Pocklington, Henry C. (1914-1916) "The determination of the prime or composite nature of large numbers by Fermat's theorem". Proceedings of the Cambridge Philosophical Society. pp. 29-30

[3] Rosen, Kenneth H. Elementary number theory and its applications, 6th edition. Addison-Wesley, 2011. pp. 378-385

[4] Brillhart, John; Selfridge, J. L. (April 1975). "Some factorizations of $2^n \pm 1$ and related results" Mathematics of Computation. pp. 87-96

[5] D.H. Lehmer (1927). "Tests for primality by the converse of Fermat's theorem". Bull. Amer. Math. Soc

[6] Pratt, V. "Every Prime has a Succinct Certificate". SIAM Journal on Computing, vol. 4, 1975.