PSEUDOPRIMES AND FERMAT NUMBERS

Samuel S. Wagstaff, Jr.[1]
Center for Education and Research in Information Assurance and Security and Department of Computer Sciences, Purdue University, West Lafayette, IN, USA
ssw@cerias.purdue.edu

Received: , Revised: , Accepted: , Published:

Abstract

We prove several theorems about pseudoprimes, some of which deal with composite Fermat numbers. These numbers have more pseudoprime bases than other numbers of similar size and we can exhibit some of their strong pseudoprime bases. The integers for which the set of all strong pseudoprime bases is a subgroup of the group of all pseudoprime bases are identified.

1. Introduction

A *pseudoprime to base* b, or psp(b), is a composite positive integer n that satisfies the conclusion of Fermat's little theorem, that is,

$$b^{n-1} \equiv 1 \pmod{n}\,. \tag{1}$$

Although the converse of Fermat's little theorem is not true, if Congruence (1) holds for a given $b > 1$, then n is likely to be prime. Congruence (1) with $b = 2$ was once considered a test for primality.

Pseudoprimes to base 2 up to $25 \cdot 10^9$ were studied in detail in [9]. The first ten pseudoprimes to base 2 are 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, and 2701. Since [9] appeared in 1980, Feitsma [5] has computed the psp(2) below $2^{64} \approx 1.8 \cdot 10^{19}$. He found 118 968 378 of them.

If one tests Congruence (1) for several different bases b and reports "n is probably prime" only if it holds for every base, the test becomes somewhat more reliable.

A *Carmichael number* is a composite integer n that is a pseudoprime to every base b for which $\gcd(b, n) = 1$. They are sparse compared to primes, although there are infinitely many of them [1]. Thus the probable prime test just mentioned would report that every Carmichael number is prime (unless it found a b with $\gcd(b, n) > 1$).

[1] This work was supported by the CERIAS Center at Purdue University

Rabin [10] and Monier [7] proposed a more reliable test using the fact that 1 has only two square roots modulo a prime number but more than two of them modulo a composite number. If n is odd, then we can write $n - 1 = d \cdot 2^k$, where d is odd. If n is an odd prime and $\gcd(b, n) = 1$, then either

$$b^d \equiv 1 \pmod{n} \quad \text{or} \tag{2}$$

$$b^{d \cdot 2^i} \equiv -1 \pmod{n} \quad \text{for some } i \text{ with } 0 \le i < k. \tag{3}$$

If n is composite and either Congruence (2) or (3) is true, then n is called a *strong pseudoprime to base* b or spsp(b).

The spsp(b) are a proper subset of psp(b), and so are scarcer than psp(b). For example, of the 118 968 378 psp(2) less than 2^{64} found by Feitsma, only 31 894 014 are spsp(2) [5]. The first ten strong pseudoprimes to base 2 are 2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, and 52633.

Rabin and Monier proved that there are no *strong* Carmichael numbers, that is, there is no composite n which is a *strong* pseudoprime to all bases relatively prime to n. In fact they ([10, Theorem 1], [7, Theorem 5]) proved that every composite n is a strong pseudoprime to at most 1/4 of bases b, $1 \le b < n$.

Let us call a base b to which a composite integer n is a pseudoprime but not a strong pseudoprime a *weak pseudoprime base for* n. Beauchemin et al. [3] observed that the weak pseudoprime bases for a composite n are precisely the bases for which the pseudoprime test Congruence (1) missed an opportunity to factor n. Baillie and the author [2, p. 1402] made the same observation. In fact, one has this theorem.

Theorem 1. ([3]) *There is a polynomial-time algorithm to factor a composite integer n, given a weak pseudoprime base b for n.*

See [3, Theorem 1] or [11, Theorem 10.4] for proof. (This algorithm might not factor n completely into prime factors. It simply splits $n = xy$ with $1 < x, y < n$.) As a corollary, Carmichael numbers are easy to factor because they have many weak pseudoprime bases.

Example 1. Let $n = 764636569$. Then n is pseudoprime to base 2 since $2^{n-1} \equiv 1 \pmod{n}$. Let $x = 2^{(n-1)/2} \equiv 254937152 \pmod{n}$. Since $x \not\equiv \pm 1 \pmod{n}$, but $x^2 \equiv 1 \pmod{n}$, we have $p = \gcd(x + 1, n) = 17489$ and $q = \gcd(x - 1, n) = 43721$; these are proper factors of n, and they happen to be primes.

2. Properties of Pseudoprime Bases

Let $\mathbb{F}_n$ be the set of all pseudoprime bases $1 \le b < n$ for n and $\mathbb{R}_n$ be the set of all strong pseudoprime bases $1 \le b < n$ for n.

Monier [7] and Baillie and the author [2, Theorem 1] independently proved this formula.

Theorem 2. ([7],[2]) *The number of bases b (mod n) for which n is a psp(b) is*

$$\#\mathbb{F}_n = \prod_p \gcd(n-1, p-1)\,, \tag{4}$$

where the product is taken over the distinct prime divisors p of n.

Corollary 1. *A product of two distinct primes has a square number of pseudoprime bases.*

Proof. Let $p \neq q$ be the two primes. Then Formula (4) becomes

$$\#\mathbb{F}_{pq} = \gcd(pq-1, p-1)\gcd(pq-1, q-1)\,.$$

We claim these two gcds are equal. Let $g = \gcd(pq-1, p-1)$ and $h = \gcd(pq-1, q-1)$. Then g divides both $pq-1$ and $p-1$, so g divides $pq-1-(p-1) = p(q-1)$. But clearly $\gcd(g, p) = 1$, so g divides $q-1$ and also h. Likewise, h divides g. Therefore, the gcds are equal and the number of pseudoprime bases for pq is the square of one of the gcds. □

Monier [7, Proposition 1] gave a formula for $\#\mathbb{R}_n$. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, $n-1 = 2^k d$, $p_i - 1 = 2^{k_i} d_i$ for $1 \leq i \leq r$, where d and the d_i are odd, and let v be the least k_i.

Theorem 3. ([7]) *With the notation above, we have*

$$\#\mathbb{R}_n = \left(1 + \frac{2^{vr}-1}{2^r-1}\right) \prod_{i=1}^{r} \gcd(d, d_i)\,. \tag{5}$$

Note that $\mathbb{F}_n$ is a group under multiplication modulo n.

Theorem 4. *With the notation above, the following are equivalent:*
(a) The set $\mathbb{R}_n$ is a subgroup of $\mathbb{F}_n$.
(b) The size $\#\mathbb{R}_n$ divides $\#\mathbb{F}_n$.
(c) Either $v = 1$ or $r = 1$.
(d) Either at least one prime congruent to 3 modulo 4 divides n or n is a prime power.

Proof. Statement (a) implies Statement (b): From group theory, the order of a subgroup divides the order of the group.

Statement (b) implies Statement (c): The products in Formulas (4) and (5) both range over the distinct prime factors of n. They differ in that the second product is an odd integer because it omits the powers of 2 (to wit, $\min(2^d, 2^{d_i})$) in the first product. Since $\#\mathbb{R}_n$ divides $\#\mathbb{F}_n$, if we remove the odd parts of the products, we see that $1+\frac{2^{vr}-1}{2^r-1}$ divides a power of 2, say, 2^y where $y \geq r$. If $v=1$, $1+\frac{2^{vr}-1}{2^r-1}=2$, while if $r=1$, then $1+\frac{2^{vr}-1}{2^r-1}=2^v$ where $v=k_1$. However, if $v>1$ and $r>1$, then

$$1+\frac{2^{vr}-1}{2^r-1}=2+2^v+2^{2v}+\cdots,$$

with r terms in this sum. No sum with this form can be a power of 2.

Statement (c) implies Statement (a): It suffices to prove that the product of two strong pseudoprime bases a and b for n is a strong pseudoprime base for n. We consider the two cases in Congruences (2) and (3). If $a^d \equiv b^d \equiv 1 \pmod{n}$, then $(ab)^d \equiv 1 \pmod{n}$. If $a^d \equiv b^d \equiv -1 \pmod{n}$, then $(ab)^d \equiv 1 \pmod{n}$. If $a^d \equiv 1$ and $b^d \equiv -1 \pmod{n}$, then $(ab)^d \equiv -1 \pmod{n}$. If $a^d \equiv -1$ and $b^d \equiv 1 \pmod{n}$, then $(ab)^d \equiv -1 \pmod{n}$.

Now suppose $a^{d\cdot 2^i} \equiv b^{d\cdot 2^j} \equiv -1 \pmod{n}$. If $i<j$, then $(ab)^j \equiv -1 \pmod{n}$, and likewise for $j<i$. Finally, we have the case of $i=j$. If $v=1$, then $i=j=0$, which was handled above. If $r=1$, then n is a prime power and $\mathbb{R}_n=\mathbb{F}_n$ because this is true when n is prime, and all solutions to $x^z \equiv \pm 1 \pmod{n}$ lift to higher powers of the prime. (This last fact was noted in [3].)

Statement (d) is just another way of saying Statement (c). □

Corollary 2. *The set of all odd composite n for which $\mathbb{R}_n$ is not a subgroup of $\mathbb{F}_n$ has asymptotic density 0.*

Proof. If any prime congruent to 3 modulo 4 divides n, then $v=1$. Thus, any odd composite n for which $\mathbb{R}_n$ is not a subgroup of $\mathbb{F}_n$ must have only primes congruent to 1 modulo 4 as its factors, and therefore be the sum of two squares. Landau [6] proved that the set of all $n \leq X$ which are the sum of two squares is $O(X/\sqrt{\log X})$ as $X \to \infty$, so this set has density 0. □

Corollary 3. *The four statements (a), (b), (c), (d) of Theorem 4 are true for almost all odd composite n in the sense of asymptotic density.*

If n is pseudoprime to base b, then b and n are relatively prime and n is pseudoprime to both bases $-b$ and b^{-1} modulo n. The same is true for strong pseudoprime bases. See Theorem 6 below for a proof.

For most composite n the number of pseudoprime bases is small compared to n. The next example is typical for numbers n whose prime factors are all congruent to 1 modulo 4.

Example 2. Let $n=221=13\cdot 17$. Then n is a strong pseudoprime to bases 1, 21, 47, 174, 200, and $220 \equiv -1 \pmod{n}$. It is a weak pseudoprime to bases 18, 38, 64, 86, 103, 118, 135, 157, 183, and 203. These 16 bases form a subgroup of the reduced residue class group modulo 221. The elements of the subgroup have order 1, 2, or 4. The set of strong pseudoprime bases do not form a subgroup. The bases

1 and 220 are a subgroup of order 2. Any combination of strong (s) and weak (w) can occur when bases are multiplied. The examples $21 \cdot 21 \equiv 220$, $21 \cdot 174 \equiv 118$, $21 \cdot 38 \equiv 135$, $47 \cdot 118 \equiv 21$, $18 \cdot 103 \equiv 86$, $64 \cdot 86 \equiv 200$ illustrate the possibilities s · s ≡ s, s · s ≡ w, s · w ≡ w, s · w ≡ s, w · w ≡ w, w · w ≡ s, respectively.

The next theorem is a general result about numbers $b^m \pm 1$. The *cyclotomic polynomial* $\Phi_m(x)$ is the irreducible factor of $x^m - 1$ which does not divide $x^i - 1$ for any $i < m$. The *primitive part* of $b^m - 1$ is $\Phi_m(b)$. The *primitive part* of $b^m + 1$ is $\Phi_{2m}(b)$. An *intrinsic factor* of the primitive part of $b^m \pm 1$ is a factor (always a single prime) of this number which also divides m. For example, the primitive part of $5^6 - 1$ is 21, which has the intrinsic factor 3. See Sections 3.3—3.5 of [11] for more examples of these definitions. The next theorem is Corollary 4.5 of [11].

Theorem 5. ([11]) *For every integer $b > 1$ and integer $m > 2$, every composite divisor of the primitive part of $b^m - 1$ or $b^m + 1$, with any intrinsic factor removed, is a strong pseudoprime to base b.*

Here is a general theorem about strong pseudoprimes.

Theorem 6. *If n is a strong pseudoprime to base b and t is an integer, then n is a strong pseudoprime to base b^t and to base $-b$.*

Proof. If n is a strong pseudoprime to base b, then $\gcd(n, b) = 1$, so it makes sense to allow $t < 0$. The case $t = 0$ is trivial: every composite n is spsp(1). Write $n - 1 = d \cdot 2^k$ with odd d. If $b^d \equiv 1 \pmod{n}$, then $(b^t)^d \equiv 1 \pmod{n}$. Now suppose $b^{d \cdot 2^i} \equiv -1 \pmod{n}$ with $0 \le i < k$. Let 2^u be the highest power of 2 that divides t. If $u \le i$, then $(b^t)^{d \cdot 2^{i-u}} \equiv -1 \pmod{n}$ and $0 \le i - u < s$. But if $u > i$, then $(b^t)^d \equiv 1 \pmod{n}$. In all cases, n is a strong pseudoprime to base b^t. If $b^d \equiv 1 \pmod{n}$, then $(-b)^d \equiv -1 \pmod{n}$. If $b^d \equiv -1 \pmod{n}$, then $(-b)^d \equiv 1 \pmod{n}$. If $b^{d \cdot 2^i} \equiv -1 \pmod{n}$ with $0 < i < k$, then $(-b)^{d \cdot 2^i} \equiv -1 \pmod{n}$. In all cases, n is a strong pseudoprime to base $-b$. □

Corollary 4. *For every integer $b > 1$, integer t, and integer $m > 2$, every composite divisor of the primitive part of $b^m - 1$ or $b^m + 1$, with any intrinsic factor removed, is a strong pseudoprime to base b^t.*

3. Fermat Numbers

It is well known that every prime divisor p of a Fermat number $n = F_k = 2^{2^k} + 1$ satisfies $p \equiv 1 \pmod{2^{k+2}}$. Therefore, composite Fermat numbers have many more pseudoprime bases than typical composite numbers because the value in Formula (4) will be at least $2^{(k+2)r}$ where r is the number of distinct prime factors of F_k.

Since no prime congruent to 3 modulo 4 divides a Fermat number, $\mathbb{R}_{F_k}$ is a subset but not a subgroup of $\mathbb{F}_{F_k}$.

The first five Fermat numbers are prime. The next seven, F_5 through F_{11}, are composite and completely factored. Many factors are known for larger ones, but no larger one is completely factored or proved prime. Here is a corollary to Corollary 4.

Corollary 5. *Every composite Fermat number is a strong pseudoprime to the base 2^t for every integer t.*

Theorem 7. *Every composite Fermat number F_k is a strong pseudoprime to the bases $b = 2^{2^{k-1}+t} \pm 2^t$ for every integer $t \geq 0$.*

Proof. We have $k \geq 5$ because F_0 through F_4 are prime. Since $2^{2^k} \equiv -1 \pmod{F_k}$, we have

$$b^2 = 2^{2^k} \cdot 2^{2t} \pm 2 \cdot 2^{2^{k-1}+2t} + 2^{2t} \equiv -2^{2t} \pm 2 \cdot 2^{2^{k-1}+2t} + 2^{2t} = \pm 2^{2^{k-1}+2t+1} \pmod{F_k}\ .$$

Hence, $b^4 \equiv 2^{2^k+4t+2} \equiv 2^{2^k} 2^{2+4t} \equiv -2^{2(2t+1)} \pmod{F_k}$, so $b^8 \equiv 2^{4(2t+1)} \pmod{F_k}$. By induction, $b^{2^i} \equiv 2^{2^{i-1}(2t+1)} \pmod{F_k}$ for $i \geq 3$. When $i = k+1 (\geq 6)$, we have

$$b^{2^i} \equiv 2^{(2t+1)2^k} \equiv (-1)^{2t+1} \equiv -1 \pmod{F_k}.$$

Thus F_k is a strong pseudoprime to base b. □

Theorem 8. *Let F_k be a composite Fermat number. Let $\mathbb{S}_k$ be the set of all bases mentioned in Corollary 5 and Theorem 7. Then $\mathbb{S}_k$ is a subgroup of $\mathbb{F}_{F_k}$, isomorphic to the direct product of a cyclic group of order 2^{k+1} and a cyclic group of order 2. Every element of $\mathbb{S}_k$ is a strong pseudoprime base for F_k.*

Proof. Let $\mathbb{W}_k$ be the set of all powers of 2 modulo F_k. Since $2^{2^{k+1}}$ is the first power of $2 \equiv 1 \pmod{F_k}$, $\mathbb{W}_k$ is a cyclic group of order 2^{k+1}. Let $x = 2^{2^{k-1}} + 1$ and $y = 2^{2^{k-1}} - 1$. (These x and y are two bases from Theorem 7 with $t = 0$.) As in the proof of Theorem 7 (with $t = 0$), we have $x^2 \equiv 2^{2^{k-1}+1} \pmod{F_k}$. Note that

$$x 2^{2^{k-1}} \equiv (2^{2^{k-1}} + 1) 2^{2^{k-1}} \equiv 2^{2^k} + 2^{2^{k-1}} \equiv -1 + 2^{2^{k-1}} \equiv y \pmod{F_k},$$

so that all bases b in Theorem 7 have the form $x2^t$. For any integers t and s, we have $(x2^t)(x2^s) \equiv x^2 2^{t+s} \equiv 2^{2^{k-1}+1+t+s} \pmod{F_k}$, so $\mathbb{S}_k$ is closed under multiplication modulo F_k and is a subgroup of $\mathbb{F}_{F_k}$.

If $x \in \mathbb{W}_k$, then $x \equiv 2^t \pmod{F_k}$ for some $0 \leq t < 2^{k+1}$ and F_k would have to divide $2^{2^{k-1}-t} + 1$, which is impossible. The coset $x\mathbb{W}_k$ consists of x times all powers of 2. The quotient group $\mathbb{S}_k/\mathbb{W}_k$ is cyclic of order 2.

Finally, the elements of $\mathbb{S}_k$ are strong pseudoprime bases by Corollary 5 and Theorem 7. □

It always happens that F_k is a strong pseudoprime to some bases $b \notin \mathbb{S}_k$. For example, F_5 has 5462 strong bases and 10922 weak bases, while $\mathbb{S}_5$ has 128 elements. One of the strong bases not in $\mathbb{S}_5$ is $b = 448911555$.

Can we find a weak pseudoprime base, and with it a factorization of F_k, by testing random possible bases b modulo F_k? When F_k has r prime factors, there are at least $2^{(k+2)r}$ pseudoprime bases for F_k, some of which are in $\mathbb{S}_k$. But the sample space of b has size 2^{2^k}, so we would have to test about $2^{2^k-(k+2)r}$ to get one pseudoprime base, and it could be strong. This is not practical even for $k = 7$ or 8; we are interested in $k \geq 12$.

Six small prime factors of F_{12} are known. The remaining cofactor is composite with 1133 decimal digits. Can one use the known small factors to construct a weak pseudoprime base b which, when used in Theorem 1, factors F_{12} as ij with $1 < i < j < F_{12}$ and i equals the product of one or more of the small factors? If so, perhaps one could multiply b times an element of $\mathbb{S}_{12}$ to obtain another weak pseudoprime base that factors F_{12} in a way that splits the composite cofactor.

Is there an analogue of Theorem 7 for quasi-Fermat numbers like $6^{2^n} + 1$ or $3 \cdot 2^{2^n} + 1$?

4. Lucas Analogues

Lucas sequences, and their applications to prime testing, were discussed in [2], [4], and [12].

Let D, P, and Q be integers with $P > 0$ and $D = P^2 - 4Q \neq 0$. Define $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, and $V_1 = P$. The Lucas sequences U_k and V_k with parameters P and Q are defined recursively for $k \geq 2$ by $U_k = PU_{k-1} - QU_{k-2}$ and $V_k = PV_{k-1} - QV_{k-2}$. For $k \geq 0$ we also have $U_k = (\alpha^k - \beta^k)/(\alpha - \beta)$ and $V_k = \alpha^k + \beta^k$, where α and β are the distinct roots of $x^2 - Px + Q = 0$. Note that $\alpha\beta = Q$ and $\alpha + \beta = P$.

When $n > 1$ is an odd positive integer, write $\delta(n) = n - (D/n)$ where (D/n) is the Jacobi symbol. Choose D, P, and Q so that the Jacobi symbol $(D/n) = -1$. It is well known [2], [4] that if n is prime and $\gcd(n, Q) = 1$, then

$$U_{n+1} \equiv 0 \pmod{n}\,. \tag{6}$$

Lucas pseudoprimes were defined in [2]. These are analogues of (Fermat) pseudoprimes in which $b^{n-1} - 1$ is replaced by a Lucas sequence. If n is composite and satisfies (6), then we call n a *Lucas pseudoprime*, written lpsp(P, Q). Every n that fails (6) is composite.

The precise set of numbers that are Lucas pseudoprimes depends on the algorithm for choosing D, P, and Q. One algorithm, first proposed by John Selfridge in [9] and mentioned in [2], and which seems to be widely used in primality testing, is this one.

Method 1. Let D be the first element of the sequence 5, −7, 9, −11, 13, −15, ... for which $(D/n) = -1$. Let $P = 1$ and $Q = (1 - D)/4$.

See [2] and [9] for more methods of choosing the parameters. Theorem 9 below is independent of the method.

Strong Lucas pseudoprimes are defined in [2]. If n is odd, then we can write $n + 1 = d \cdot 2^s$ where d is odd. If n is prime and $(D/n) = -1$, then we will have either

$$U_d \equiv 0 \pmod{n} \quad \text{or} \tag{7}$$

$$V_{d\cdot 2^r} \equiv 0 \pmod{n} \quad \text{for some } r \text{ with } 0 \le r < s. \tag{8}$$

If $(D/n) = -1$ and the composite n satisfies either Congruence (7) or (8), then n is called a *strong Lucas pseudoprime* with parameters P and Q, written slpsp(P, Q). If n is an slpsp(P, Q), then n is also an lpsp(P, Q), that is, $U_{n+1} = U_{d\cdot 2^s} \equiv 0 \pmod{n}$.

The following equations show how to use the binary representation of $n + 1$ to efficiently compute the values on the left sides of Congruences (7) and (8).

$$U_{2k} = U_k V_k \tag{9}$$

$$V_{2k} = V_k^2 - 2Q^k \tag{10}$$

$$Q^{2k} = (Q^k)^2 \tag{11}$$

$$U_{k+1} = (PU_k + V_k)/2 \tag{12}$$

$$V_{k+1} = (DU_k + PV_k)/2 \tag{13}$$

$$Q^{k+1} = Q \cdot Q^k \tag{14}$$

Equations (9) and (10) are Equations 4.2.6 and 4.2.7 in Williams [12] while Equations (12) and (13) are Equations 4.2.21 in that book. Equations (9)–(11) are used to double the subscript and exponent; Equations (12)–(14) are used to increment the subscript and exponent by 1. These equations are also given in [4, p. 628].

Here is the Lucas analogue of Theorem 1.

Theorem 9. *There is a polynomial-time algorithm to factor a composite integer n, given integers P, Q such that n is lpsp(P,Q) but not slpsp(P,Q).*

Proof. We prove the theorem for the (more interesting) case of $(D/n) = -1$. The proof for $(D/n) = +1$ is similar. Write $n + 1 = d \cdot 2^s$ with odd d. Consider the numbers

$$U_d, \quad U_{2d}, \quad \ldots, \quad U_{d\cdot 2^s} \bmod n\,. \tag{15}$$

We know that $U_{d\cdot 2^s} = U_{n+1} \equiv 0 \pmod{n}$ since n is lpsp(P,Q). If $U_{d\cdot 2^i} \equiv 0 \pmod{n}$ for all $0 \le i \le s$, then n would be slpsp(P,Q). Since this is not so, at least one of the numbers in List (15) is not 0 modulo n. Let i be the largest integer for which $U_{d\cdot 2^i} \not\equiv 0 \pmod{n}$. Then $0 \equiv U_{d\cdot 2^{i+1}} \equiv U_{d\cdot 2^i}V_{d\cdot 2^i} \pmod{n}$ by Equation (9). If $V_{d\cdot 2^i} \equiv 0 \pmod{n}$, then n would be slpsp(P,Q). Since this is not so, and also $U_{d\cdot 2^i} \not\equiv 0 \pmod{n}$, we see that n divides the product of $U_{d\cdot 2^i}$ and $V_{d\cdot 2^i}$, but neither of them. Therefore, $\gcd(U_{d\cdot 2^i}, n)$ and $\gcd(V_{d\cdot 2^i}, n)$ are proper factors of n. □

Example 3. Let $n = 56279$. Then $n + 1 = d \cdot 2^s$ with $s = 3$, $d = 7035$. Method 1 chooses $D = -7$, $P = 1$, $Q = 2$. We have $U_d \equiv 21281$, $V_d \equiv 25711$, $U_{2d} \equiv 11353$, $V_{2d} \equiv 15865$, $U_{4d} \equiv 22545$, $V_{4d} \equiv 24601$, $U_{n+1} = U_{8d} \equiv 0$, and $V_{8d} \equiv 2020 \pmod{n}$. Then n is a Lucas pseudoprime because $U_{n+1} \equiv 0$. Since neither Congruence (7) nor Congruence (8) hold, n is not a strong Lucas pseudoprime. The first number in List (15) that is $\equiv 0 \pmod{n}$ is U_{8d}. We have $\gcd(U_{4d}, n) = 167$ and $\gcd(V_{4d}, n) = 337$, both proper factors of n.

Let $n = 2018839$. Then $n + 1 = d \cdot 2^s$ with $s = 3$, $d = 252355$. Method 1 chooses $D = -19$, $P = 1$, $Q = 5$. We have $U_d \equiv 119992$, $V_d \equiv 199667$, and $U_{2d} \equiv 0 \pmod{n}$, which leads to $\gcd(U_d, n) = 2459$ and $\gcd(V_d, n) = 821$, two proper factors of n.

Let $n = 10877$. Then $n + 1 = d \cdot 2^s$ with $s = 1$, $d = 5439$. Method 1 chooses $D = 5$, $P = 1$, $Q = -1$. We have $U_d \equiv 0 \pmod{n}$, so Congruence (7) holds, n is a strong Lucas pseudoprime, and no factorization of n is produced.

Let $n = 5459$. Then $n + 1 = d \cdot 2^s$ with $s = 1$, $d = 2729$. Method 1 chooses $D = -7$, $P = 1$, $Q = 2$. We have $U_d \equiv 3550$, $V_d \equiv 3847$, $U_{2d} \equiv 3891$, and $V_{2d} \equiv 0 \pmod{n}$, so Congruence (8) holds with $r = 1$, n is a strong Lucas pseudoprime, and no factorization of n is produced.

Is there an analogue of Fermat numbers for which one can prove Lucas analogues of Corollary 5 or Theorems 7 or 8?

5. Conclusion

In [11] the author listed a dozen suggestions for new ways to factor a large integer n. One of these was to find a weak pseudoprime base for n and use Theorem 1.

The example in Section 2 shows that the product of two strong pseudoprime bases can be a weak pseudoprime base. But Corollary 3 shows that this rarely happens because usually $\mathbb{R}_n$ is a subgroup of $\mathbb{F}_n$. Composite Fermat numbers are exceptions. Moreover, Corollary 5 and Theorem 7 identify explicit strong pseudoprime bases other than the trivial 1 and -1 for all F_k. Suppose we multiply two or more of the bases mentioned in Corollary 5 and Theorem 7. If we could find a weak pseudoprime base for F_k this way, we would have a very fast algorithm for factoring all Fermat numbers. Alas, this hope was dashed by Theorem 8.

It is curious that $2^{11} - 1$ is a strong pseudoprime to base 11. We wondered whether another prime p might be a strong pseudoprime base for $2^p - 1$ when the latter is composite, but found no more examples with $p < 200$.

If a composite n is partially factored, can we easily find a base b, other than those in Theorems 5, 6, 7, and Corollaries 4 and 5, so that n is psp(b) without factoring n completely?

Acknowledgement. The author thanks Robert Baillie, Adam Hammer, Carl Pomerance, and Trevor Wooley for valuable email correspondence that greatly improved this work.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* (2), **139** (1994), 703–722.

[2] R. Baillie and S. S. Wagstaff, Jr., Lucas pseudoprimes, *Math. Comp.*, **35** (1980), 1391–1417.

[3] P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, and C. Pomerance, The generation of random numbers that are probably prime, *J. Cryptology*, **1** (1988), 53–64.

[4] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, *Math. Comp.*, **29** (1975), 620–647.

[5] J. Feitsma, *Pseudoprimes.* Feitsma's web page is `http://www.janfeitsma.nl/math/psp2/index`. Statistics on psp(2) are at `http://www.janfeitsma.nl/math/psp2/statistics`. The database of all psp(2) $< 2^{64}$ is at `http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html`.

[6] E. Landau, Über die Einteilung der positive ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additive Zusammensetzung erforderlichen Quadrate, *Arch. Math. Phys.* (3) **13** (1908), 305–312.

[7] L. Monier, Evaluation and comparison of two efficient primality testing algorithms, *Theoret. Comput. Sci.* **12**, (1980), 97–108.

[8] I. Niven and H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth edition, John Wiley & Sons, Inc., New York, 1991.

[9] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., The pseudoprimes to $25 \cdot 10^9$, *Math. Comp.*, **35**, (1980), 1003–1026.

[10] M. O. Rabin, Probabilistic algorithm for testing primality, *J. Number Theory*, **12**, (1980), 128–138.

[11] S. S. Wagstaff, Jr. *The Joy of Factoring*, Student Mathematical Library, 68. American Mathematical Society, Providence, RI, 2013.

[12] H. C. Williams. *Édouard Lucas and Primality Testing.* Canadian Mathematical Society Series of Monographs and Advanced Texts, 22. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.