

involve

a journal of mathematics

When is $a^n + 1$ the sum of two squares?

Greg Dresden, Kylie Hess, Saimon Islam, Jeremy Rouse,
Aaron Schmitt, Emily Stamm, Terrin Warren and Pan Yue



When is $a^n + 1$ the sum of two squares?

Greg Dresden, Kylie Hess, Saimon Islam, Jeremy Rouse,
Aaron Schmitt, Emily Stamm, Terrin Warren and Pan Yue

(Communicated by Kenneth S. Berenhaut)

Using Fermat's two squares theorem and properties of cyclotomic polynomials, we prove assertions about when numbers of the form $a^n + 1$ can be expressed as the sum of two integer squares. We prove that $a^n + 1$ is the sum of two squares for all $n \in \mathbb{N}$ if and only if a is a square. We also prove that if $a \equiv 0, 1, 2 \pmod{4}$, n is odd, and $a^n + 1$ is the sum of two squares, then $a^\delta + 1$ is the sum of two squares for all $\delta \mid n$, $\delta > 1$. Using Aurifeuillian factorization, we show that if a is a prime and $a \equiv 1 \pmod{4}$, then there are either zero or infinitely many odd n such that $a^n + 1$ is the sum of two squares. When $a \equiv 3 \pmod{4}$, we define m to be the least positive integer such that $(a + 1)/m$ is the sum of two squares, and prove that if $a^n + 1$ is the sum of two squares for n odd, then $m \mid n$, and both $a^m + 1$ and n/m are sums of two squares.

1. Introduction

Many facets of number theory revolve around investigating terms of a sequence that are *interesting*. For example, if $a_n = 2^n - 1$ is prime (called a Mersenne prime), then n itself must be prime [Hardy and Wright 1979, Theorem 18, p. 15]. In this case, the property that is interesting is primality. Ramanujan was interested in the terms of the sequence $b_n = 2^n - 7$ that are squares. He conjectured that the only such terms are those with $n = 3, 4, 5, 7$ and 15 , and it was later proved by Nagell [1948]; a modern reference is [Stewart and Tall 2002, p. 96]. Finally, if the Fibonacci sequence is defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$, then F_n is prime only if n is prime or $n = 4$ [Hardy and Wright 1979, Theorem 179, p. 148], and the only powers in the Fibonacci sequence are $0, 1, 8$ and 144 , which was proven by Bugeaud, Mignotte, and Siksek [Bugeaud et al. 2006] using similar tools to the proof of Fermat's last theorem.

In this paper, we will consider a number to be *interesting* if it can be expressed as the sum of two squares. The earliest work on this topic relates to Pythagorean

MSC2010: primary 11E25; secondary 11C08, 11R18.

Keywords: cyclotomic polynomials, Fermat's two squares theorem.

Hess, Rouse, Stamm and Warren were supported by the NSF grant DMS-1461189.

triples, which are integer solutions to $a^2 + b^2 = c^2$. Euclid supplied an infinite family of solutions: $a = m^2 - n^2$, $b = 2mn$ and $c = m^2 + n^2$.

Fermat's two squares theorem classifies which numbers can be written as the sum of two squares. Fermat claimed to have proven this theorem in his 1640 letter to Mersenne, but never shared the proof. The first published proof is attributed to Euler and was completed in 1749; see [Cox 1989, p. 11].

Theorem (Fermat's two squares theorem). *A positive integer N can be written as the sum of two squares if and only if in the prime factorization of N ,*

$$N = \prod_{i=1}^k p_i^{e_i},$$

we have $p_i \equiv 3 \pmod{4}$ only if e_i is even.

In light of Fermat's theorem, integers that can be expressed as the sum of two squares become increasingly rare. In particular, if $S(x)$ denotes the number of integers $n \leq x$ that are expressible as a sum of two squares, then Landau [1908] proved

$$\lim_{x \rightarrow \infty} \frac{S(x)}{x/\sqrt{\ln(x)}} = K \approx 0.764.$$

This can be stated more colloquially as "the probability that a number n is the sum of two squares is $K/\sqrt{\ln(n)}$."

A lot of progress has recently been made in understanding the gaps between prime numbers. In particular, [Zhang 2014; Maynard 2015] prove there are bounded gaps between primes infinitely often. The analogous questions for sums of two squares are much easier: problem A2 from the 2000 Putnam competition asked participants to show that there are infinitely many n such that n , $n + 1$ and $n + 2$ are all sums of two squares.

The culmination of several papers on large gaps between primes is [Ford et al. 2018], where it is proven that there are infinitely many n such that

$$p_{n+1} - p_n \gg \frac{\log p_n \log \log p_n \log \log \log p_n}{\log \log \log p_n},$$

where p_n is the n -th prime. This is still quite a ways from the conjectured statement that $p_{n+1} - p_n \gg \log^2 p_n$ holds infinitely often. For sums of two squares, the analogue of this conjecture is that if q_n is the n -th positive integer that is a sum of two squares, one should have $q_{n+1} - q_n \gg \log q_n$ infinitely often. This result was proved in [Richards 1982], and some recent work [Kalmynin 2017] has been done on estimating the moments

$$\sum_{q_{n+1} \leq x} (q_{n+1} - q_n)^\gamma,$$

extending [Hooley 1971].

We are interested in which terms in sequences of the form $a^n + 1$ can be written as a sum of two squares. Curtis [2014] showed that $2^n + 1$ is the sum of two squares if and only if n is even or $n = 3$. Additionally, if n is odd and $3^n + 1$ is the sum of two squares, then n must be the sum of two squares, and $3^p + 1$ is the sum of two squares for all prime numbers $p \mid n$.

The focus of the present paper is to say as much as possible about when $a^n + 1$ is the sum of two squares for a general positive integer a . This paper is the result of two undergraduate research teams working simultaneously and independently over two months in the summer of 2016. The first team, from Wake Forest University, consisted of students Hess, Stamm, and Warren, and was led by Jeremy Rouse; the second team, from Washington and Lee University, consisted of students Islam, Schmitt, and Yue, and was led by Greg Dresden. Remarkably, the two teams ended up covering many of the same topics. Some of the results are unique to the Wake Forest team, while other results were proved by both teams using different methods.

In the case that $n = 2k$ is even, $a^n + 1 = (a^k)^2 + 1^2$ is trivially the sum of two squares. For this reason, we focus on cases when n is odd. Our first result is the following.

Theorem 1.1. *If $a \in \mathbb{Z}$, then $a^n + 1$ is the sum of two squares for every $n \in \mathbb{N}$ if and only if a is a square or $a = -1$.*

This result parallels Artin's conjecture that an integer a is a primitive root modulo every prime if and only if a is not a square and $a \neq -1$.

Example. (1) If $a = 9$, then $9^n + 1 = (3^n)^2 + 1^2$.

(2) If $a = 7$, then there is some odd n such that $7^n + 1$ is not the sum of two squares. For example, $7^3 + 1$ is not the sum of two squares.

For the remainder of the paper, we assume that a is a positive integer. Our next result gives specific criteria that handle the case when a is even.

Theorem 1.2. *Suppose a is even, n is odd, and $a^n + 1$ is the sum of two squares:*

- *If $a + 1$ is the sum of two squares, then $a^\delta + 1$ is the sum of two squares for all $\delta \mid n$.*
- *If $a + 1$ is not the sum of two squares, then there is a unique prime number $p \equiv 3 \pmod{4}$ such that $p^r \parallel a + 1$ for some odd r , and $n = p$.*

Example. (1) If $a \equiv 2 \pmod{4}$, then $a + 1$ is not the sum of two squares and so there is at most one odd exponent n such that $a^n + 1$ is the sum of two squares. For example, with $a = 6$, since $a + 1 = 7$ is divisible by the unique prime $p = 7 \equiv 3 \pmod{4}$, $n = 7$ is the only possible odd n for which $a^n + 1$ is the sum of two squares. Indeed, $6^7 + 1 = 476^2 + 231^2$.

(2) For $a \equiv 0 \pmod{4}$, there are more options. If we let $a = 20$, then since $a + 1 = 3 \cdot 7$ has two prime factors congruent to 3 mod 4 that divide it to an odd power, we conclude that $20^n + 1$ is not the sum of two squares for any odd n . On the other hand, for $a = 24$, since $24^{77} + 1$ is the sum of two squares, we must also have that $24^{11} + 1$, $24^7 + 1$, and $24^1 + 1$ are each the sum of two squares. In general, the most efficient way to test if a positive integer n is a sum of two squares is to compute its prime factorization and use Fermat's two squares theorem.

We consider a special case when a is a multiple of 4.

Theorem 1.3. *Let $a = 4x$, where $x \equiv 3 \pmod{4}$ and x is square-free. If n is odd, then $a^{nx} + 1$ is not the sum of two squares.*

Example. (1) Let $a = 12 = 4 \cdot 3$. Then $12^{3n} + 1$ is not the sum of two squares for any odd n . Note that [Theorem 1.2](#) implies that since $12^3 + 1$ is not the sum of two squares, then $12^{3n} + 1$ is not the sum of two squares for any odd n . However, [Theorem 1.3](#) guarantees, without any computation necessary, that $12^3 + 1$ is not the sum of two squares.

(2) Let $a = 28 = 4 \cdot 7$. Then $28^{7n} + 1$ is not the sum of two squares for any odd n .

The factorization tables for $12^n + 1$ [[Brillhart et al. 2002](#); [Wagstaff](#)] imply that there are sixteen exponents $1 \leq n < 293$ for which $12^n + 1$ is the sum of two squares, which are all prime except for $n = 1$. The two smallest composite exponents n for which $12^n + 1$ could possibly be the sum of two squares are $n = 473 = 11 \cdot 43$ and $n = 545 = 5 \cdot 109$; so far, of those two, we have confirmed only that $12^{545} + 1$ is the sum of two squares.

We now consider the case when a is odd. We split this into three subcases: $a \equiv 1 \pmod{8}$, $a \equiv 5 \pmod{8}$, and $a \equiv 3 \pmod{4}$.

Theorem 1.4. *Let $a \equiv 1 \pmod{8}$. If $a^n + 1$ is the sum of two squares for n odd, then $a^\delta + 1$ is the sum of two squares for all $\delta \mid n$.*

Example. (1) Let $a = 33$. Since $33^{119} + 1$ is the sum of two squares, $33^1 + 1$, $33^7 + 1$, and $33^{17} + 1$ must also be sum of two squares. Since $33^3 + 1$ is not the sum of two squares, we know $33^{3n} + 1$ is not the sum of two squares for any odd n .

(2) Let $a = 41$. Since $42 = 2 \cdot 3 \cdot 7$ is not the sum of two squares, $41^1 + 1$ is not the sum of two squares, and hence $41^n + 1$ is not the sum of two squares for any odd n .

Note that (as seen in the example with $a = 41$) the above theorem implies that if $a \equiv 1 \pmod{8}$ and $a + 1$ is not the sum of two squares, then $a^n + 1$ is not the sum of two squares for any odd n . The next theorem addresses the case that $a \equiv 5 \pmod{8}$.

Theorem 1.5. *Let $a \equiv 5 \pmod{8}$. Then, $a^n + 1$ is never the sum of two squares for n odd.*

Example. Since $13 \equiv 5 \pmod{8}$, we know $13^n + 1$ is not the sum of two squares for any odd n .

It follows that if $a \equiv 0, 1, 2 \pmod{4}$, n is odd, and $a^n + 1$ is the sum of two squares, then $a^\delta + 1$ is the sum of two squares for all $\delta \mid n$. (The case when a is even follows from [Theorem 1.2](#), $a \equiv 1 \pmod{8}$ from [Theorem 1.4](#), and $a \equiv 5 \pmod{8}$ from [Theorem 1.5](#).)

Finally, we consider $a \equiv 3 \pmod{4}$, as covered in three separate results. These first two place considerable restrictions on the values of n for which $a^n + 1$ can be a sum of two squares.

Lemma 1.6. *Let $a \equiv 3 \pmod{4}$, and let m be the smallest integer such that $(a + 1)/m$ is the sum of two squares. If $a^n + 1$ is the sum of two squares, then $n \equiv m \pmod{4}$.*

Theorem 1.7. *Let $a \equiv 3 \pmod{4}$, and let m be the smallest integer such that $(a + 1)/m$ is the sum of two squares. If $a^n + 1$ is a sum of two squares for some odd n , then*

- n/m is a sum of two squares, and
- $a^m + 1$ is the sum of two squares, and
- if $\delta \mid (n/m)$ and δ is the sum of two squares, then $a^{m\delta} + 1$ is the sum of two squares.
- Moreover, if $a^{np^2} + 1$ is the sum of two squares for some $p \equiv 3 \pmod{4}$, then $p \mid (a^n + 1)$.

[Theorem 1.7](#) showcases the advantages of having two teams working independently. When we first shared our results in late July, the Wake Forest group had only the first two parts of the above theorem, and the Washington and Lee group had a weaker version of the third part that was restricted to $m = 1$ and to δ being a prime equivalent to $1 \pmod{4}$. Two weeks later, both teams had improved their results, with Wake Forest coming up with both the fourth part and the stronger version of the third part, as seen here. The proof that resulted from this collaboration is a nice combination of ideas from both teams.

Example. (1) Let $a = 11$. Then $m = 3$, and since $11^3 + 1$ is the sum of two squares, if $11^n + 1$ is the sum of two squares, then $3^j \parallel n$, j odd.

(2) Let $a = 43$. Then $m = 11$, and since $43^{11} + 1$ is not the sum of two squares, we conclude that $43^n + 1$ is not the sum of two squares for any odd n .

(3) If $a = 4713575$, then $m = 21$. It turns out that $a^{21} + 1$ is the sum of two squares, and so if $a^n + 1$ is the sum of two squares, then $21 \mid n$. Sure enough, $a^{105} + 1$ is the sum of two squares (and has 701 decimal digits).

We pause for a moment to remind the reader that [Theorem 1.1](#) states that if a is not a square, then there exists some odd n such that $a^n + 1$ is not the sum of two squares. We can now extend this theorem and demonstrate that in fact there will be infinitely many such exponents:

- If a is even with $a + 1$ not the sum of two squares, or if $a \equiv 5 \pmod{8}$, then [Theorems 1.2](#) and [1.5](#) tell us that $a^n + 1$ fails to be the sum of two squares for infinitely many odd n (in fact, for all but at most one odd exponent n).
- If a is even with $a + 1$ the sum of two squares, or if $a \equiv 1 \pmod{8}$, then we can use [Theorems 1.2](#) and [1.4](#) to state that if $a^\delta + 1$ is not the sum of two squares for some odd exponent δ , then $a^{\delta N} + 1$ fails to be the sum of two squares for all odd integers N .
- Finally, if $a \equiv 3 \pmod{4}$, we call upon [Lemma 1.6](#) to state that $a^n + 1$ can only be a sum of two squares for $n \equiv m \pmod{4}$.

This next result allows one to state that for certain special values of a , there is an infinite collection of odd values of n for which $a^n + 1$ is the sum of two squares.

Theorem 1.8. *Suppose n is odd, $p \equiv 1 \pmod{4}$ is a prime number and $a = px^2$. Then $a^n + 1$ is the sum of two squares if and only if $a^{np} + 1$ is the sum of two squares.*

The above theorem implies that for those specific values of a , there are either no odd n , or an infinite number of odd n , for which $a^n + 1$ is the sum of two squares. In particular, if $a + 1$ is the sum of two squares, then $a^{p^n} + 1$ is the sum of two squares for all $n \geq 0$. If $a + 1$ is not the sum of two squares, one of [Theorems 1.2](#), [1.4](#), or [1.5](#) implies that $a^n + 1$ is not the sum of two squares for any odd n .

Example. (1) Let $a = 17$, where $p = 17$ and $x = 1$. Since 18 is the sum of two squares, $17^{17^n} + 1$ is the sum of two squares for any n .

(2) Let $a = 117$, where $p = 13$ and $x = 3$. Since $a + 1 = 2 \cdot 59$ is not the sum of two squares, $117^{13^n} + 1$ is not the sum of two squares for any n .

Remark. In light of the above theorem, it is natural to ask if there are infinitely many $a \equiv 1 \pmod{8}$ such that $a^n + 1$ is the sum of two squares for infinitely many odd n . This is indeed the case. In particular, the main theorem of [\[Iwaniec 1972\]](#) implies that if x is a real number ≥ 17 , then the number of primes $p \leq x$ with $p \equiv 1 \pmod{8}$ for which $p + 1$ is the sum of two squares is at least $cx/\log(x)^{3/2}$ for some positive constant c .

We can use the ideas from [Theorem 1.8](#) to construct an infinite family of numbers a such that $a^p + 1$ is the sum of two squares. This is our next result.

Theorem 1.9. *If $p \equiv 1 \pmod{4}$ is prime, there is a degree-4 polynomial $f(X)$ with integer coefficients such that $f(X)^p + 1 = g(X)^2 + h(X)^2$ for some $g(X)$ and $h(X)$*

with integer coefficients. Moreover, there is no positive integer n such that $f(n)$ is a square.

Example. If $p = 13$, then $f(X) = 13(13X^2 + 3X)^2$. Then $f(n)^{13} + 1$ is the sum of two squares for every $n \in \mathbb{N}$.

We end with a conjecture about the number of odd n for which $a^n + 1$ is the sum of two squares.

Conjecture 1.10. *Suppose a is a positive integer and $a \neq c^k$ for any positive integer c and $k > 1$. Let m be the smallest positive integer such that $(a + 1)/m$ is the sum of two squares:*

- *If $m = 1$, then there are infinitely many odd n such that $a^n + 1$ is the sum of two squares.*
- *If $a \equiv 3 \pmod{4}$, $a^m + 1$ is the sum of two squares, and m is prime, then there are infinitely many odd n such that $a^n + 1$ is the sum of two squares. (In fact, there should be infinitely many $p \equiv 1 \pmod{4}$ such that $a^{mp} + 1$ is the sum of two squares.)*
- *If $a \equiv 3 \pmod{4}$ and m is composite, then there are only finitely many odd n such that $a^n + 1$ is the sum of two squares.*

The main theoretical tools we use in this paper are the theory of cyclotomic polynomials, and in particular, a classification of which primes divide $\Phi_n(a)$ (see [Theorem 2.1](#)). [Theorems 1.3](#) and [1.8](#) also use the identity $\Phi_n(x) = F(x)^2 - kx^q G(x)^2$ that arises in Aurifeuillian factorization.

The rest of the paper will proceed as follows. In [Section 2](#), we review previous results which we will use. In [Section 3](#), we prove a few facts that will be used in the remainder of the proofs. In [Section 4](#), we prove [Theorem 1.1](#). In [Section 5](#), we prove [Theorems 1.2](#) and [1.3](#). In [Section 6](#), we prove [Theorems 1.4](#), [1.5](#), and [1.7](#), along with [Lemma 1.6](#), and we include a heuristic supporting [Conjecture 1.10](#). In [Section 7](#), we prove [Theorems 1.8](#) and [1.9](#). We conclude with a chart listing all $a \leq 50$ and the first few odd integers n such that $a^n + 1$ is the sum of two squares, as well as a reference to one our theorems.

2. Background

If n is a positive integer and p is a prime number, we write $p^r \parallel n$ if $p^r \mid n$ but $p^{r+1} \nmid n$. If n is a positive integer and we write that n is not a sum of two squares because of the prime p , we mean that $p \equiv 3 \pmod{4}$ and there is an odd r such that $p^r \parallel n$. If a and m are integers with $\gcd(a, m) = 1$, we define $\text{ord}_m(a)$ to be the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. It is well known that $a^r \equiv 1 \pmod{m}$ if and only if $\text{ord}_m(a) \mid r$. Fermat's little theorem states that if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$; it follows that $\text{ord}_p(a) \mid (p - 1)$.

We will make use of the identity (originally due to Diophantus)

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

This applies if $a, b, c, d \in \mathbb{Z}$, and also if a, b, c and d are polynomials.

Let $\Phi_n(x)$ denote the n -th cyclotomic polynomial; recall that $\Phi_n(x)$ is the unique irreducible factor of $x^n - 1$ with integer coefficients that does not divide $x^k - 1$ for any proper divisor k of n . We have $\prod_{d|n} \Phi_d(x) = x^n - 1$ and from this it follows that when n is odd,

$$x^n + 1 = \frac{x^{2n} - 1}{x^n - 1} = \prod_{d|2n, d \nmid n} \Phi_d(x) = \prod_{\delta|n} \Phi_{2\delta}(x).$$

We will make use of the facts that for n odd, $\Phi_{2n}(x) = \Phi_n(-x)$ and that if $n = p^k$ is prime, then

$$\Phi_{p^k}(1) = \lim_{x \rightarrow 1} \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = p.$$

The following theorem classifies prime divisors of $\Phi_n(a)$.

Theorem 2.1. *Assume that $a \geq 2$ and $n \geq 2$:*

- *If p is a prime and $p \nmid n$, then $p \mid \Phi_n(a)$ if and only if $n = \text{ord}_p(a)$.*
- *If p is a prime and $p \mid n$, then $p \mid \Phi_n(a)$ if and only if $n = \text{ord}_p(a) \cdot p^k$. In this case, if $n \geq 3$, then $p^2 \nmid \Phi_n(a)$.*

The authors have not been able to trace the origin of the result above, but it is certainly quite old, and may be contained in the work of A. S. Bang [1886a; 1886b]. This theorem arises in connection with Zsigmondy's work showing that for any a , $n \geq 2$ there is a prime p for which $\text{ord}_p(a) = n$ unless $n = 2$ and $a + 1$ is a power of 2. One can find a proof of the result above in Trygve Nagell's textbook [1964] (see Theorems 94 and 95).

We will also make use of certain identities for cyclotomic polynomials that arise in Aurifeuillian factorization. If k is a square-free positive integer, let $d(k)$ be the discriminant of $\mathbb{Q}(\sqrt{k})$, that is,

$$d(k) = \begin{cases} k & \text{if } k \equiv 1 \pmod{4}, \\ 4k & \text{if } k \equiv 2, 3 \pmod{4}. \end{cases}$$

Suppose that $n \equiv 2 \pmod{4}$, and $d(k) \nmid n$ but $d(k) \mid 2n$. Write the prime factorization of n as $n = 2 \prod_{i=1}^k p_i^{e_i}$ and define $q = \prod_{i=1}^k p_i^{e_i-1}$. Then Theorem 2.1 of [Stevenhagen 1987] states that

$$\Phi_n(x) = F(x)^2 - kx^q G(x)^2$$

for some polynomials $F(x), G(x) \in \mathbb{Z}[x]$. If $x = -kv^2$ for some integer v , we get

$$\Phi_n(-kv^2) = F(-kv^2)^2 + (k^{(q+1)/2} v^q G(-kv^2))^2$$

is the sum of two squares. In the case that $x = kv^2$ for some integer v , we get the factorization

$$\begin{aligned}\Phi_n(kv^2) &= F(kv^2)^2 - k(kv^2)^q G(kv^2)^2 \\ &= (F(kv^2) + k^{(q+1)/2}v^q G(kv^2))(F(kv^2) - k^{(q+1)/2}v^q G(kv^2)).\end{aligned}$$

Theorem 2.7 of [Stevenhagen 1987] states that these two factors are relatively prime.

We will also require some basic facts about quadratic residues. If p is an odd prime, we define $\left(\frac{a}{p}\right)$ to be 1 if $\gcd(a, p) = 1$ and there is some $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$. We define $\left(\frac{a}{p}\right)$ to be -1 if $\gcd(a, p) = 1$ and there is no such x , and we set $\left(\frac{a}{p}\right) = 0$ if $p \mid a$. Euler's criterion gives the congruence $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. The definition of the quadratic residue symbol can be extended. If n is an odd integer with prime factorization $n = \prod_{i=1}^k p_i^{e_i}$, define the Jacobi symbol by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i}.$$

The quadratic reciprocity law for Jacobi symbols states that if a and b are both positive and odd, then

$$\left(\frac{a}{b}\right) = (-1)^{\frac{1}{2}(a-1) \cdot \frac{1}{2}(b-1)} \left(\frac{b}{a}\right).$$

3. General results

The following general lemmas pertain primarily to how the divisors of n affect the divisors of $a^n + 1$, and are used in rest of the sections of the paper. Results of this type are well known and date back to [Lucas 1878; Carmichael 1913/14]. A more modern source is [Stewart 1977]. We provide our own simple and short proofs of these facts to keep the paper self-contained.

Lemma 3.1. *Let $b, n \in \mathbb{Z}$, and n be odd and suppose $b \mid (x + 1)$. Then*

$$b \mid (x^{n-1} - x^{n-2} + x^{n-3} - \dots + 1)$$

if and only if $b \mid n$.

Proof. Let $b \mid (x + 1)$. Then $x + 1 \equiv 0 \pmod{b}$, so $x \equiv -1 \pmod{b}$. Thus,

$$\begin{aligned}x^{n-1} - x^{n-2} + x^{n-3} - \dots - x + 1 &\equiv (-1)^{n-1} - (-1)^{n-2} + (-1)^{n-3} - \dots - (-1) + 1 \pmod{b} \\ &\equiv 1 + 1 + 1 + \dots + 1 + 1 \pmod{b} \\ &\equiv n \pmod{b}.\end{aligned}$$

Therefore $b \mid (x^{n-1} - x^{n-2} + x^{n-3} - \dots - x + 1)$ if and only if $n \equiv 0 \pmod{b}$, or equivalently, $b \mid n$. \square

We obtain the following corollary as a result of the above lemma.

Corollary 3.2. *Suppose that n is odd, $\delta \mid n$ and $x^\delta + 1$ is not the sum of two squares because of some prime p . If $p \nmid n$, then $x^n + 1$ is not the sum of two squares.*

Proof. Consider

$$x^n + 1 = (x^\delta + 1)(x^{n-\delta} - x^{n-2\delta} + x^{n-3\delta} - \dots - x^\delta + 1).$$

Since $x^\delta + 1$ is not the sum of two squares because of p , we have $p \equiv 3 \pmod{4}$, r odd and $p^r \parallel (x^\delta + 1)$. Then $p \nmid n$ implies $p \nmid (x^{n-\delta} - x^{n-2\delta} + x^{n-3\delta} - \dots - x^\delta + 1)$ by Lemma 3.1, and thus $p^r \parallel (x^n + 1)$ implying that $x^n + 1$ is not the sum of two squares. □

Lemma 3.3. *Let p be a prime such that $p^e \parallel (a^m + 1)$ for some $e \in \mathbb{N}$, and let $n = mc p^k$ be odd with $\gcd(c, p) = 1$ and $k \geq 0$. Then $p^{e+k} \parallel (a^n + 1)$.*

Proof. Using notation from the statement of the theorem, we can write

$$a^n + 1 = (a^m + 1) \cdot \frac{a^n + 1}{a^m + 1}.$$

Then, recalling how $a^m + 1$ factors into cyclotomics, we let d be the smallest divisor of m such that $p \mid \Phi_{2d}(a)$. Thanks to Theorem 2.1, we know that $p \parallel \Phi_{2dp}(a)$, $p \parallel \Phi_{2dp^2}(a)$, and so on, yet p does not divide into any other cyclotomic expressions not of that form. Now, choose i as large as possible such that $2dp^i \mid m$. Then, by our definition of n , we know that everything in the set $\{dp^{i+1}, dp^{i+2}, \dots, dp^{i+k}\}$ divides into n yet none of them divide into m , and we also know from Theorem 2.1 (as mentioned above) that each of the k expressions $\Phi_{2dp^{i+1}}(a), \Phi_{2dp^{i+2}}(a), \dots, \Phi_{2dp^{i+k}}(a)$ contains exactly one copy of the prime p and that no other cyclotomic divisors of $(a^n + 1)/(a^m + 1)$ contain this prime p . Hence, since $p^e \parallel (a^m + 1)$, we know $p^{e+k} \parallel (a^n + 1)$. □

4. Proof of Theorem 1.1

We begin with a lemma constructing an odd n such that $a^n + 1$ is not the sum of two squares.

Lemma 4.1. *Suppose there exists a prime $p \equiv 3 \pmod{4}$ such that $\left(\frac{a}{p}\right) = -1$. Then either $a^{(p-1)/2} + 1$ or $a^{p(p-1)/2} + 1$ is not a sum of two squares.*

Proof. If $a^{(p-1)/2} + 1$ is not a sum of two squares, then we are done. Suppose $a^{(p-1)/2} + 1$ is a sum of two squares. By Euler’s criterion, we have $a^{(p-1)/2} \equiv -1 \pmod{p}$, and it follows therefore that for some $k \in \mathbb{N}$, $p^{2k} \parallel a^{(p-1)/2} + 1$. By Lemma 3.3, letting $m = (p - 1)/2$ and $n = p(p - 1)/2$, we know that $p^{2k+1} \parallel (a^{p(p-1)/2} + 1)$. Thus, by Fermat’s two squares theorem, $a^{p(p-1)/2} + 1$ is not the sum of two squares. □

As an example, we examine $148^n + 1$. We can conclude from the prime factorization of $148^n + 1$ that $148^n + 1$ is a sum of two squares for all odd $n < 9$. Note that $9 = \frac{19-1}{2}$ and that 19 is the smallest prime $p \equiv 3 \pmod{4}$ for which $\left(\frac{148}{p}\right) = -1$. Calculation and Fermat's two square theorem reveal that $148^{(19-1)/2} + 1 = 148^9 + 1$ is not a sum of two squares.

Proof of Theorem 1.1. Write $a = 2^k a'$, where a' is odd. If $q \equiv 3 \pmod{4}$ is prime, then

$$\left(\frac{a}{q}\right) = \left(\frac{2^k}{q}\right) \left(\frac{a'}{q}\right) = \left(\frac{2^k}{q}\right) \cdot (-1)^{(a'-1)/2} \left(\frac{q}{a'}\right) = \left(\frac{2^k}{q}\right) \left(\frac{-q}{a'}\right).$$

If a' is not a square and $a' \neq -1$, then there is a prime $r \mid a'$ that occurs to an odd power. The system of congruences

$$\begin{aligned} q &\equiv 7 \pmod{8}, \\ -q &\equiv \text{quadratic nonresidue} \pmod{r}, \\ -q &\equiv 1 \pmod{s} \quad \text{for all prime } s \mid a', s \neq r, \end{aligned}$$

has a solution $q \equiv x \pmod{8a'}$ with $\gcd(x, 8a') = 1$. Therefore there is a prime q satisfying these congruences, and we have $\left(\frac{a}{q}\right) = -1$.

In the case that a' is a square but a is not, k is odd. In this case we choose $q \equiv 3 \pmod{8}$ and $-q \equiv 1 \pmod{s}$ for all prime $s \mid a'$. This likewise yields a prime q such that $\left(\frac{a}{q}\right) = -1$.

By Lemma 4.1, either $a^{(p-1)/2} + 1$ or $a^{p(p-1)/2} + 1$ is not a sum of two squares and so there is at least one value of n for which $a^n + 1$ is not a sum of two squares. \square

5. Even

Now we consider the case when a is even. We prove Theorems 1.2 and 1.3.

Proof of Theorem 1.2. Suppose that $a^n + 1$ is the sum of two squares. If $a^\delta + 1$ is also the sum of two squares for every divisor δ of n , then we are done. If not, then let δ be the largest divisor of n such that $a^\delta + 1$ is not the sum of two squares. Thus, $\delta < n$ and so there is a prime p that divides n/δ . By assumption, we have that $a^{\delta p} + 1$ is the sum of two squares and

$$a^{\delta p} + 1 = (a^\delta + 1)(a^{\delta(p-1)} - a^{\delta(p-2)} + \cdots + 1).$$

Lemma 3.1 implies that $\gcd(a^\delta + 1, (a^{\delta p} + 1)/(a^\delta + 1))$ divides p . Since $a^\delta + 1$ is not the sum of two squares, the gcd cannot be 1 and so it must be p . Moreover,

$$\frac{a^{\delta p} + 1}{p^2} = \frac{a^\delta + 1}{p} \cdot \frac{a^{\delta p} + 1}{p(a^\delta + 1)}$$

is a sum of two squares and the product of two relatively prime integers. Thus, $(a^\delta + 1)/p$ is the sum of two squares. It follows that $p \equiv 3 \pmod{4}$ and since $a^\delta + 1$ is odd, we get

$$a^\delta + 1 = p \times \text{sum of two squares} \equiv 3 \pmod{4}.$$

However, since a is even, we must have that $\delta = 1$ and the previous equation implies that p is the unique prime congruent to 3 mod 4 that divides $a + 1$ to an odd power. \square

Now we prove [Theorem 1.3](#) involving a special case when $a \equiv 0 \pmod{4}$.

Proof of Theorem 1.3. First, we show that $a^x + 1$ is not the sum of two squares. We have

$$a^x + 1 = \prod_{d \mid 2x, d \nmid x} \Phi_d(a).$$

We apply [Theorem 2.1](#) of [[Stevenhagen 1987](#)] to $\Phi_{2x}(y) \in \mathbb{Z}[y]$. We set $n = 2x$, $k = x$, $d(k) = 4x$. Then $d(k) \nmid n$ but $d(k) \mid 2n$. We have

$$\Phi_{2x}(y) = F(y)^2 - xyG(y)^2.$$

Assume without loss of generality that the leading coefficient of $F(y)$ is positive. Note that since $\Phi_{2x}(y)$ has even degree, the degree of $F(y)$ is larger than that of $G(y)$.

Replacing y with xy^2 we get

$$\begin{aligned} \Phi_{2x}(xy^2) &= F(xy^2)^2 - x(xy^2)G(xy^2) \\ &= (F(xy^2) + xyG(xy^2))(F(xy^2) - xyG(xy^2)). \end{aligned}$$

Let $f(y)$ and $g(y)$ be the first and second factors above, respectively. We have $\Phi_{2x}(a) = \Phi_{2x}(4x) = f(2)g(2)$. From [Theorem 2.7](#) of [[Stevenhagen 1987](#)] we know $\gcd(f(2), g(2)) = 1$. We claim $f(2) \equiv g(2) \equiv 3 \pmod{4}$. This will follow if we show that the constant coefficients of $f(y)$ and $g(y)$ are both 1, and the linear coefficients of $f(y)$ and $g(y)$ are both odd.

We have $f(y) = a_0 + a_1y + a_2y^2 + \dots$ and $g(y) = a_0 - a_1y + a_2y^2 + \dots$. Since the constant coefficient of $\Phi_{2x}(y)$ is 1, we have $a_0^2 = 1$ and so $a_0 = \pm 1$. If $a_0 = -1$, then since the leading coefficient of $F(y)$ is positive, $f(y)$ and $g(y)$ have positive leading coefficients. However, then $\lim_{y \rightarrow \infty} f(y) = \lim_{y \rightarrow \infty} g(y) = \infty$ but $f(0) = g(0) = -1$. This implies that $f(y)$ and $g(y)$ both have a positive real root, but $f(y)g(y) = \Phi_{2x}(xy^2)$ has no real roots. This is a contradiction and so $a_0 = 1$.

It is well known that if $n > 1$, the coefficient of y in $\Phi_n(y)$ is $-\mu(n)$; see for example, the last equation on page 107 of [[Lehmer 1966](#)]. Multiplying $f(y)$ and $g(y)$, we get

$$\Phi_{2x}(xy^2) = 1 - \mu(2x)xy^2 + \dots = a_0^2 + (2a_0a_2 - a_1^2)y^2 + \dots$$

We have that $\mu(2x) = \pm 1$ is odd and $-\mu(2x) = 2a_0a_2 - a_1^2$. Thus, $a_1^2 \equiv \mu(2x) \pmod{2}$ and so a_1 is odd. Thus, $f(2) \equiv a_0 + 2a_1 \equiv 1 + 2 \equiv 3 \pmod{4}$ and likewise $g(2) \equiv a_0 - 2a_1 \equiv 1 - 2 \equiv 3 \pmod{4}$.

Thus, there is a prime $p \equiv 3 \pmod{4}$ and an odd j such that $p^j \parallel f(2)$ and a prime $q \equiv 3 \pmod{4}$ and an odd k such that $q^k \parallel g(2)$. Since $\gcd(f(2), g(2)) = 1$, we have $p \neq q$.

We claim that at most one of p or q divides x . Suppose to the contrary that $p \mid x$ and $q \mid x$. Since $p \mid \Phi_{2x}(a)$, [Theorem 2.1](#) implies $2x = p \cdot \text{ord}_p(a)$ and since $q \mid \Phi_{2x}(a)$, we get $2x = q \cdot \text{ord}_q(a)$. This implies that $\text{ord}_p(a) = 2x/p$ is a multiple of q and $\text{ord}_q(a) = 2x/q$ is a multiple of p . This is a contradiction, because either $p < q$ (in which case $q \leq \text{ord}_p(a) \leq p - 1$) or $q < p$ (in which case $p \leq \text{ord}_q(a) \leq q - 1$).

Thus, at most one of p or q divides x . Assume without loss of generality that $p \nmid x$. Then we have $p^j \parallel \Phi_{2x}(a)$ and [Theorem 2.1](#) gives $\text{ord}_p(a) = 2x$. This implies $p \nmid \Phi_{2\delta}(a)$ for $\delta \mid x$ with $\delta \neq x$. As a consequence, $p^j \parallel (a^x + 1)$ and so $a^x + 1$ is not the sum of two squares.

Now, let $A = a^x$. Then $A + 1$ is not the sum of two squares, and $A + 1 \equiv 1 \pmod{4}$. Thus, there are at least two primes $\equiv 3 \pmod{4}$ that divide $A + 1$ to an odd power, and [Theorem 1.2](#) implies that $A^n + 1$ is never the sum of two squares for n odd. \square

6. Odd

This section contains proofs of [Theorems 1.4, 1.5, and 1.7](#), along with [Lemma 1.6](#), which pertain to when $a^n + 1$ can be written as a sum of two squares when a is an odd integer. In this section, we define m to be the least positive integer such that $(a + 1)/m$ is the sum of two squares.

We begin with $a \equiv 1 \pmod{4}$. We prove [Theorem 1.4](#) which handles the case $a \equiv 1 \pmod{8}$, and [Theorem 1.5](#) which handles $a \equiv 5 \pmod{8}$.

Proof of [Theorem 1.4](#). Let $a \equiv 1 \pmod{8}$. Then $a^n + 1 \equiv 2 \pmod{8}$ for all n , so $(a^n + 1)/2 \equiv 1 \pmod{4}$. Suppose $a^n + 1$ is the sum of two squares, and assume by contradiction that δ is the largest divisor of n such that $a^\delta + 1$ is not the sum of two squares. Since $(a^\delta + 1)/2 \equiv 1 \pmod{4}$, there exist distinct primes $q_1 \equiv q_2 \equiv 3 \pmod{4}$ such that $q_1^{j_1} \parallel (a^\delta + 1)$ and $q_2^{j_2} \parallel (a^\delta + 1)$, j_1, j_2 odd.

We know from [Lemma 3.3](#) that since $a^n + 1$ is the sum of two squares, $q_1^{l_1} \parallel n$ and $q_2^{l_2} \parallel n$ for some odd l_1 and l_2 . Without loss of generality, suppose $q_1 > q_2$, and consider

$$a^{\delta q_1} + 1 = (a^\delta + 1) \prod_{\delta_x \mid \delta q_1, \delta_x \nmid \delta} \Phi_{2\delta_x}(a).$$

Since $q_1 > q_2$, we know $q_1 \nmid \text{ord}_{q_2}(a)$, and [Theorem 2.1](#) implies $q_2 \nmid (a^{\delta q_1} + 1)/(a^\delta + 1)$. Then $q_2^{j_2} \parallel (a^{\delta q_1} + 1)$, so $a^{\delta q_1} + 1$ is not the sum of two squares. This is a contradiction because $\delta q_1 > \delta$ and $\delta q_1 \mid n$. Thus $a^\delta + 1$ is the sum of two squares for all $\delta \mid n$. \square

Proof of Theorem 1.5. Suppose $a \equiv 5 \pmod{8}$ and n is odd. Then

$$\begin{aligned} a^n + 1 &= a^{2k+1} + 1 \\ &\equiv 5^{2k} \cdot 5 + 1 \pmod{8} \\ &\equiv 6 \pmod{8}. \end{aligned}$$

This implies that $(a^n + 1)/2 \equiv 3 \pmod{4}$, so by Fermat's two squares theorem we know that $a^n + 1$ is never the sum of two squares when n is odd. \square

Next, the following lemmas will be useful in forming contradictions in the proof of Theorem 1.7 because of the restrictions they place on n in order for $a^n + 1$ to be the sum of two squares, where $a \equiv 3 \pmod{4}$ and n odd.

We begin with two lemmas that cover the modulus of permissible exponents n when $a \equiv 3 \pmod{4}$.

Lemma 6.1. *For $a = 4 \cdot 2^i \cdot (4j + 1) - 1$ with $i, j \geq 0$, then $a^n + 1$ can only be written as the sum of two squares (for n odd) if $n \equiv 1 \pmod{4}$.*

Note that this covers values of a such as $a = 3, 7, 15, 19, 31$, and 35 . This explains why $35^9 + 1$ is a sum of two squares but $35^3 + 1$ is not.

Proof. Let us argue by contradiction. Suppose $n \equiv 3 \pmod{4}$. Write $n = 4k + 3$, and note that $a \equiv 4 \cdot 2^i - 1 \pmod{16 \cdot 2^i}$. Then, making liberal use of the binomial theorem on $a^3 \equiv (4 \cdot 2^i - 1)^3$ and $a^4 \equiv (4 \cdot 2^i - 1)^4$, we have:

$$\begin{aligned} a^n + 1 &= a^{4k+3} + 1 \\ &= (a^3) \cdot (a^4)^k + 1 \\ &\equiv (\dots + 3 \cdot (4 \cdot 2^i) - 1) \cdot (\dots - 4 \cdot (4 \cdot 2^i) + 1)^k + 1 \pmod{16 \cdot 2^i} \\ &\equiv (3 \cdot 4 \cdot 2^i - 1) \cdot (1)^k + 1 \pmod{16 \cdot 2^i} \\ &\equiv 12 \cdot 2^i \pmod{16 \cdot 2^i}. \end{aligned}$$

This implies that $(a^n + 1)/(4 \cdot 2^i)$ is equivalent to $3 \pmod{4}$. Then there must be at least one prime equivalent to $3 \pmod{4}$ that appears in the factorization of $(a^n + 1)/(4 \cdot 2^i)$ an odd number of times. This implies the same for $a^n + 1$ and thus by Fermat, $a^n + 1$ is not the sum of two squares. This is a contradiction to our assumption and thus n cannot be equivalent to $3 \pmod{4}$. \square

Lemma 6.2. *For $a = 4 \cdot 2^i \cdot (4j + 3) - 1$ with $i, j \geq 0$, then $a^n + 1$ can only be written as the sum of two squares (for n odd) if $n \equiv 3 \pmod{4}$.*

Note that this covers values of a such as $a = 11, 23, 27, 43$, and so on, including 191 which gives us two values $n = 3$ and $n = 15$ such that $191^n + 1$ is the sum of two squares. Both 3 and 15 , of course, are equivalent to $3 \pmod{4}$.

Proof. Keeping in mind that $a \equiv -1 \pmod{4}$, we have

$$\begin{aligned} a^n + 1 &= (a + 1) \cdot (a^{n-1} - a^{n-2} + \cdots + 1) \\ &= 4 \cdot 2^i \cdot (4j + 3) \cdot (a^{n-1} - a^{n-2} + \cdots + 1). \end{aligned}$$

Since $a \equiv -1 \pmod{4}$, the last expression, $(a^{n-1} - a^{n-2} + \cdots + 1)$, is equivalent to $n \pmod{4}$. The only hope, then, for $a^n + 1$ to be the sum of two squares is for n to be $3 \pmod{4}$, as then $(a^n + 1)/(4 \cdot 2^i)$ will be the product of two expressions both equivalent to $3 \pmod{4}$, resulting in $(a^n + 1)/(4 \cdot 2^i)$ being equivalent to $1 \pmod{4}$. \square

The last two lemmas allow us to now prove one of our earlier lemmas:

Proof of Lemma 1.6. For $a \equiv 3 \pmod{4}$, we can write $a = 4K - 1$, where K can be split into an even part (which we write as 2^i) and an odd part (which we write as either $4j + 1$ or $4j + 3$). In the first case, $a + 1$ equals $4 \cdot 2^i \cdot (4j + 1)$ and since m is the smallest integer such that $(a + 1)/m$ is the sum of two squares, m must be equivalent to $1 \pmod{4}$, and by Lemma 6.1 we have $n \equiv 1 \pmod{4}$ in this case, and so $n \equiv m \pmod{4}$. A similar argument applies to the second case. \square

This lemma places further restrictions on n . Recall that m is the smallest positive integer such that $(a + 1)/m$ is the sum of two squares.

Lemma 6.3. *Let $a \equiv 3 \pmod{4}$. If $a^n + 1$ is the sum of two squares, then for all primes $p \equiv 3 \pmod{4}$ such that $p^e \parallel (a + 1)$, e odd, we have $p^k \parallel n$, k odd. In particular, if $a^n + 1$ is the sum of two squares, then $m \mid n$.*

Proof. Let $a^n + 1$ be the sum of two squares and suppose $p^e \parallel (a + 1)$, e odd, and $p \equiv 3 \pmod{4}$. Select k such that $p^k \parallel n$. Then, Lemma 3.3 implies $p^{e+k} \parallel (a^n + 1)$. Since $a^n + 1$ is the sum of two squares, we know $e + k$ is even, which makes k odd. It follows that since $m = \prod p$ for p such primes of this type, if $a^n + 1$ is the sum of two squares, then $m \mid n$. \square

We will now prove Theorem 1.7, which applies to all $a \equiv 3 \pmod{4}$.

Proof of Theorem 1.7. First we will prove that n/m is the sum of two squares. Suppose that $a^n + 1$ is the sum of two squares and recall that by Lemma 6.3, $m \mid n$. Assume by contradiction that n/m is not the sum of two squares. Then let q be the greatest prime such that $q \equiv 3 \pmod{4}$ and $q^j \parallel n/m$, j odd. If $q \mid m$, then Lemma 3.3 implies that an even power of q divides $a^m + 1$, and so if an odd power of q divides $a^n + 1$, then $q^r \parallel n$, r odd. But m is square-free, so $q \parallel m$. Then $q^{r-1} \parallel n/m$, $r - 1$ even, which is a contradiction. Therefore we can assume $q \nmid m$, so $q^j \parallel n$.

We know that $\Phi_{2q^j}(a)$ divides $a^n + 1$. We have $\Phi_{2q^j}(a) \equiv \Phi_{2q^j}(-1) \equiv \Phi_{q^j}(1) \equiv q \equiv 3 \pmod{4}$. This implies that there exists a prime $p \equiv 3 \pmod{4}$ such that $p^k \parallel \Phi_{2q^j}(a)$, k odd. We can consider two cases: $p \neq q$ and $p = q$.

Suppose $p \neq q$. Then $p \nmid q^j$, so $\text{ord}_p(a) = 2q^j$, which implies $p > q$. Since $a^n + 1$ is the sum of two squares, Lemma 3.3 implies $p^l \parallel n$, l odd. Since $\text{ord}_p(a) > 2$,

$p \nmid a + 1$, so $p \nmid m$. Then p is a prime congruent to 3 (mod 4) that divides n/m to an odd power, and $p > q$, which is a contradiction because we assumed q is the largest such prime.

Now suppose $p = q$. Since $p \mid \Phi_{2p^j}(a)$, it follows that $a^{p^j} + 1 \equiv 0 \pmod{p}$. Repeatedly applying Fermat's little theorem, $a^p \equiv a \pmod{p}$, we find that $p \mid (a+1)$. Since $p \nmid m$, $p^k \parallel (a+1)$, k even. Then [Lemma 3.3](#) implies that $p^{k+j} \parallel a^n + 1$, where $k + j$ is odd, which is a contradiction. Thus if $a^n + 1$ is the sum of two squares, then n/m is also the sum of two squares.

Next we'll prove that $a^m + 1$ is the sum of two squares. Suppose $a^n + 1$ is the sum of two squares, where $n = ms$, and assume by contradiction that $a^m + 1$ is not the sum of two squares. Then there exists some prime $q \equiv 3 \pmod{4}$ such that $q^j \parallel (a^m + 1)$, j odd. Since $s = n/m$ is the sum of two squares, we know $q^k \parallel s$, k even. Then $n = mq^k s'$, where $\gcd(s', q) = 1$, so $q^{k+j} \parallel (a^n + 1)$, $k + j$ odd ([Lemma 3.3](#)). This is a contradiction because we assumed $a^n + 1$ is the sum of two squares. Therefore if $a^n + 1$ is the sum of two squares for some odd n , then $a^m + 1$ is also the sum of two squares.

Let $\delta \mid (n/m)$, where δ is the sum of two squares, and suppose $a^n + 1$ is the sum of two squares. We will show that $a^{m\delta} + 1$ is the sum of two squares. Assume by contradiction that there exists a prime $q \equiv 3 \pmod{4}$ such that $q^j \parallel a^{m\delta} + 1$, j odd.

Since δ is the sum of two squares, we know $q^k \parallel \delta$, k even, $k \geq 0$. Because q must divide $a^n + 1$ to an even power, [Lemma 3.3](#) implies $q^l \parallel n/(m\delta)$, l odd, so $q^{l+k} \parallel n/m$, $l + k$ odd, which is a contradiction because n/m is the sum of two squares. Thus if $a^n + 1$ is the sum of two squares, $a^{m\delta} + 1$ is the sum of two squares for all $\delta \mid n/m$ such that δ is the sum of two squares.

Finally, we will show that if $a^{np^2} + 1$ is the sum of two squares for some $p \equiv 3 \pmod{4}$, then $p \mid (a^n + 1)$. By [Lemma 1.6](#) we know $a^{np} + 1$ is not the sum of two squares, so there exists some $q \equiv 3 \pmod{4}$ with $q^j \parallel (a^{np} + 1)$, j odd. If $q \neq p$, then by [Lemma 3.3](#) we have $q^j \parallel (a^{np^2} + 1)$, j odd, which contradicts $a^{np^2} + 1$ being the sum of two squares. Hence $q = p$, and since $p \mid (a^{np} + 1)$ and $a^{np} \equiv a^n \pmod{p}$, we have $p \mid (a^n + 1)$, as desired. \square

We conclude this section with a heuristic giving evidence for [Conjecture 1.10](#). Suppose first that $a \equiv 0$ or $1 \pmod{4}$. In this case, if $a^n + 1$ is the sum of two squares for any n , then $a + 1$ is the sum of two squares. Let A_p be the event that $\Phi_{2p}(a)$ is the sum of two squares. It seems plausible that the probability that this occurs is approximately

$$\frac{K}{\sqrt{\ln(\Phi_{2p}(a))}} \approx \frac{K}{\sqrt{p}}.$$

Since $\sum_{p \equiv 1 \pmod{4}} 1/\sqrt{p}$ diverges, we should expect an infinite number of the events A_p to occur, and this would yield infinitely many primes p for which $a^p + 1$ is the sum of two squares.

If $a \equiv 2 \pmod{4}$, then [Theorem 1.2](#) implies there is at most one n such that $a^n + 1$ is the sum of two squares.

In the case that $a \equiv 3 \pmod{4}$, let m denote the smallest positive integer such that $(a + 1)/m$ is the sum of two squares. First, consider primes $p \equiv 1 \pmod{4}$ such that $a^{mp} + 1$ is the sum of two squares. We have

$$\frac{a^{mp} + 1}{a^m + 1} = \prod_{d \mid 2mp, d \nmid 2m} \Phi_d(a).$$

[Theorem 2.1](#) implies that if we write $\Phi_d(a) = \gcd(\Phi_d(a), m)c_d$, then the c_d are pairwise coprime and this implies that c_d is the sum of two squares for all d . It seems plausible that the c_d being the sum of two squares are independent, and so the probability that $a^{mp} + 1$ is the sum of two squares is approximately

$$\prod_d \frac{1}{\sqrt{\ln(c_d)}} \approx p^{-\tau(m)/2},$$

where $\tau(m)$ is the number of divisors of m . The sum $\sum_{p \equiv 1 \pmod{4} \text{ prime}} p^{-\tau(m)/2}$ diverges if $m = 1$ or m is prime, and converges if m is composite. In particular, in the case that m is composite, there are only finitely many primes p such that $a^{mp} + 1$ is the sum of two squares.

Then, [Theorem 1.7](#) implies that there are only finitely many primes that can divide some number n such that $a^n + 1$ is the sum of two squares. If there are infinitely many n such that $a^n + 1$ is the sum of two squares, it follows then that there is a prime p such that $a^{p^r} + 1$ is the sum of two squares for infinitely many r . We have $a^{p^r} + 1 = \prod_{i=0}^r \Phi_{2p^i}(a)$. If we write

$$r_i = \frac{\Phi_{2p^i}(a)}{\gcd(\Phi_{2p^i}(a), p)},$$

then [Theorem 2.1](#) implies $\gcd(r_i, r_j) = 1$. It follows from this that r_i is the sum of two squares for all $i \geq 1$. Assuming that these events are independent, the probability this occurs is $\sum_i K/\sqrt{\ln(r_i)}$. But this sum converges. Therefore the “probability is zero” that there are infinitely many n such that $a^n + 1$ is the sum of two squares in the case when $a \equiv 3 \pmod{4}$ and m is composite.

As an example, we consider $a = 4713575$, with a composite m value of $m = 21$. We conjecture that there are finitely many n such that $a^n + 1$ is the sum of two squares. So far, we know only of $n = 21$ and $n = 105$.

7. $p \equiv 1 \pmod{4}$

The previous theorems put constraints on when $a^n + 1$ can be the sum of two squares for different categories of a . The following proof of [Theorem 1.8](#) uses Aurifeuillian

factorization to show that when $a = pv^2$, where $p \equiv 1 \pmod{4}$ is a prime and $p \nmid v$, there are either zero or infinitely many odd integers n such that $a^n + 1$ is the sum of two squares.

Proof of Theorem 1.8. Let $a = pv^2$, where $p \equiv 1 \pmod{4}$ is prime. Suppose $a^n + 1$ is the sum of two squares and consider

$$a^{np} + 1 = \prod_{\delta | n} \Phi_{2\delta}(a) \prod_{\delta | np, \delta \nmid n} \Phi_{2\delta}(a).$$

We know $\prod_{\delta | n} \Phi_{2\delta}(a) = a^n + 1$ is the sum of two squares. Consider the Aurifeuillian factorization of $\Phi_{2\delta}(a)$, where $\delta | np$, $\delta \nmid n$, $x = -kv^2$, $k = -p \equiv 3 \pmod{4}$, and q is odd:

$$\begin{aligned} \Phi_{2\delta}(x) &= (F(x))^2 - kx^q(G(x))^2, \\ \Phi_{2\delta}(-kv^2) &= (F(-kv^2))^2 - k(-kv^2)^q(G(-kv^2))^2 \\ &= (F(-kv^2))^2 + k^{q+1}v^{2q}(G(-kv^2))^2 \\ &= (F(-kv^2))^2 + (k^{(q+1)/2}v^qG(-kv^2))^2 \\ &= \Phi_{2\delta}(a). \end{aligned}$$

Therefore $\Phi_{2\delta}(a)$ is the sum of two squares for any $\delta | np$ with $\delta \nmid n$. Thus $a^{np} + 1$ is the sum of two squares. Conversely, suppose that $a^{np} + 1$ is the sum of two squares. Then we can see again that $\Phi_{2\delta p}(a)$ is the sum of two squares for any factor δ . This implies that $\prod_{\delta | n} \Phi_{2\delta}(a) = a^n + 1$ is the sum of two squares. \square

Now, we will construct an infinite family of numbers $a = f(X)$ such that $a^p + 1$ is the sum of two squares.

Proof of Theorem 1.9. If $p \equiv 1 \pmod{4}$, then there exists an even integer u and an odd integer v such that $p = u^2 + v^2$. Then consider the polynomials

$$\begin{aligned} A(X) &= \frac{1}{2}upX^2 + vX, \\ B(X) &= \frac{1}{2}u^2pX^2 - 1, \\ C(X) &= \frac{1}{2}uvpX^2 + pX. \end{aligned}$$

Let $f(X) = pA(X)^2$; then we have

$$\begin{aligned} f(X)^p + 1 &= (f(X) + 1)\Phi_{2p}(f(X)) \\ &= (pA(X)^2 + 1)\Phi_{2p}(pA(X)^2). \end{aligned}$$

It is straightforward to check that $f(X) + 1$ can be written as the sum of two squares: $pA(X)^2 + 1 = B(X)^2 + C(X)^2$. Then consider the Aurifeuillian

factorization of $\Phi_{2p}(x)$, where we let $k = -p$ and $x = pA(X)^2$. Then we get

$$\begin{aligned}\Phi_{2p}(x) &= F(x)^2 - kxG(x)^2, \\ \Phi_{2p}(pA(X)^2) &= (F(pA(X)^2))^2 - p(-pA(X)^2)(G(pA(X)^2))^2 \\ &= (F(pA(X)^2))^2 + (p^2A(X)^2)(G(pA(X)^2))^2 \\ &= (F(pA(X)^2))^2 + (pA(X)(G(pA(X)^2)))^2.\end{aligned}$$

Therefore, $\Phi_{2p}(f(X))$ can be written as the sum of two squares as well. This implies that $f(X)^p + 1$ is the product of two terms, each of which can be written as the sum of two squares. \square

8. Chart

Here we illustrate the first few odd integers n such that $a^n + 1$ is the sum of two squares for all integers $a \in [1, 50]$.

a	n	Theorem	a	n	Theorem
1	all	1.1	26	—	1.2
2	3	1.2	27	—	1.7
3	1, 5, 13, 65, ...	1.7	28	1, 3, 11, 19, ...	1.2
4	all	1.1	29	—	1.5
5	—	1.5	30	31	1.2
6	7	1.2	31	1, 5, 25, 41, ...	1.7
7	1, 13, 17, 29, ...	1.7	32	—	1.2
8	1	1.2	33	1, 5, 7, 17, ...	1.4
9	all	1.1	34	—	1.2
10	—	1.2	35	1, 9, 13, 29, ...	1.7
11	3, 159, ...	1.7	36	all	1.1
12	1, 5, 11, 23, ...	1.2	37	—	1.5
13	—	1.5	38	—	1.2
14	3	1.2	39	1, 13, 37, 61, ...	1.7
15	1, 29, 89, 97, ...	1.7	40	1, 5, 13, 53, ...	1.2
16	all	1.1	41	—	1.4
17	1, 7, 17, 23, ...	1.8	42	—	1.2
18	19	1.2	43	—	1.7
19	1, 17, 29, 37, ...	1.7	44	1, 5, 7, 17, ...	1.2
20	—	1.2	45	—	1.5
21	—	1.5	46	—	1.2
22	—	1.2	47	—	1.7
23	3, 123, ...	1.7	48	1, 3, 5, 17, ...	1.2
24	1, 7, 11, 19, ...	1.2	49	all	1.1
25	all	1.1	50	—	1.2

Acknowledgements

The authors would like to thank the anonymous referees for helpful comments that improved the exposition.

References

- [Bang 1886a] A. S. Bang, “[Taltheoretiske undersøgelser](#)”, *Tidsskrift Math.* (5) **4** (1886), 70–80.
- [Bang 1886b] A. S. Bang, “[Taltheoretiske undersøgelser \(fortsat, se. s. 80\)](#)”, *Tidsskrift Math.* (5) **4** (1886), 130–137.
- [Brillhart et al. 2002] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$: $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, 3rd ed., Contemporary Mathematics **22**, American Mathematical Society, Providence, RI, 2002.
- [Bugeaud et al. 2006] Y. Bugeaud, M. Mignotte, and S. Siksek, “[Classical and modular approaches to exponential Diophantine equations, I: Fibonacci and Lucas perfect powers](#)”, *Ann. of Math.* (2) **163**:3 (2006), 969–1018. [MR Zbl](#)
- [Carmichael 1913/14] R. D. Carmichael, “[On the numerical factors of the arithmetic forms \$\alpha^n \pm \beta^n\$](#) ”, *Ann. of Math.* (2) **15**:1-4 (1913/14), 49–70. [MR Zbl](#)
- [Cox 1989] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, John Wiley & Sons, New York, 1989. [MR Zbl](#)
- [Curtis 2014] K. Curtis, “Sums of two squares: an analysis of numbers of the form $2^n + 1$ and $3^n + 1$ ”, preprint, 2014.
- [Ford et al. 2018] K. Ford, B. Green, S. Konyagin, J. Maynard, and T. Tao, “[Long gaps between primes](#)”, *J. Amer. Math. Soc.* **31**:1 (2018), 65–105. [MR Zbl](#)
- [Hardy and Wright 1979] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford University Press, New York, 1979. [MR Zbl](#)
- [Hooley 1971] C. Hooley, “[On the intervals between numbers that are sums of two squares](#)”, *Acta Math.* **127** (1971), 279–297. [MR Zbl](#)
- [Iwaniec 1972] H. Iwaniec, “[Primes of the type \$\phi\(x, y\) + A\$ where \$\phi\$ is a quadratic form](#)”, *Acta Arith.* **21** (1972), 203–234. [MR Zbl](#)
- [Kalmynin 2017] A. Kalmynin, “Intervals between numbers that are sums of two squares”, preprint, 2017. [arXiv](#)
- [Landau 1908] E. Landau, “Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen quadrate”, *Arch. Math. Phys.* **13** (1908), 305–312.
- [Lehmer 1966] D. H. Lehmer, “[Some properties of the cyclotomic polynomial](#)”, *J. Math. Anal. Appl.* **15** (1966), 105–117. [MR Zbl](#)
- [Lucas 1878] E. Lucas, “[Théorie des fonctions numériques simplement périodiques](#)”, *Amer. J. Math.* **1**:2 (1878), 184–196. [MR Zbl](#)
- [Maynard 2015] J. Maynard, “[Small gaps between primes](#)”, *Ann. of Math.* (2) **181**:1 (2015), 383–413. [MR Zbl](#)
- [Nagell 1948] T. Nagell, “Løsning till oppgave nr 2”, *Norsk Mat. Tidsskr.* **30** (1948), 62–64.
- [Nagell 1964] T. Nagell, *Introduction to number theory*, 2nd ed., Chelsea, New York, 1964. [MR Zbl](#)
- [Richards 1982] I. Richards, “[On the gaps between numbers which are sums of two squares](#)”, *Adv. in Math.* **46**:1 (1982), 1–2. [MR Zbl](#)

- [Stevenhagen 1987] P. Stevenhagen, “On Aurifeuillian factorizations”, *Nederl. Akad. Wetensch. Indag. Math.* **49**:4 (1987), 451–468. [MR](#) [Zbl](#)
- [Stewart 1977] C. L. Stewart, “On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers”, *Proc. London Math. Soc.* (3) **35**:3 (1977), 425–447. [MR](#) [Zbl](#)
- [Stewart and Tall 2002] I. Stewart and D. Tall, *Algebraic number theory and Fermat’s last theorem*, 3rd ed., A K Peters, Natick, MA, 2002. [MR](#) [Zbl](#)
- [Wagstaff] S. S. Wagstaff, Jr., “The Cunningham Project”, website, <http://homes.cerias.purdue.edu/~ssw/cun/index.html>.
- [Zhang 2014] Y. Zhang, “Bounded gaps between primes”, *Ann. of Math.* (2) **179**:3 (2014), 1121–1174. [MR](#) [Zbl](#)

Received: 2017-10-11

Revised: 2018-06-20

Accepted: 2018-06-24

dresdeng@wlu.edu*Department of Mathematics, Washington and Lee University, Lexington, VA, United States*kylie.hess@emory.edu*Department of Mathematics and Computer Science, Emory University, Atlanta, GA, United States*islams19@wlu.edu*Department of Mathematics, Washington and Lee University, Lexington, VA, United States*rouseja@wfu.edu*Department of Mathematics and Statistics, Wake Forest University, Winston-Salem, NC, United States*aaronschmitt96@gmail.com*Department of Mathematics, Washington and Lee University, Lexington, VA, United States*emily.stamm.12@gmail.com*Department of Mathematics and Statistics, Vassar College, Poughkeepsie, NY, United States*warrentm@uga.edu*Department of Mathematics, University of Georgia, Athens, GA, United States*pany19@wlu.edu*Department of Mathematics, Washington and Lee University, Lexington, VA, United States*

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

MANAGING EDITOR

Kenneth S. Berenhaut Wake Forest University, USA

BOARD OF EDITORS

Colin Adams	Williams College, USA	Chi-Kwong Li	College of William and Mary, USA
Arthur T. Benjamin	Harvey Mudd College, USA	Robert B. Lund	Clemson University, USA
Martin Bohner	Missouri U of Science and Technology, USA	Gaven J. Martin	Massey University, New Zealand
Nigel Boston	University of Wisconsin, USA	Mary Meyer	Colorado State University, USA
Amarjit S. Budhiraja	U of N Carolina, Chapel Hill, USA	Frank Morgan	Williams College, USA
Pietro Cerone	La Trobe University, Australia	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran
Scott Chapman	Sam Houston State University, USA	Zuhair Nashed	University of Central Florida, USA
Joshua N. Cooper	University of South Carolina, USA	Ken Ono	Emory University, USA
Jem N. Corcoran	University of Colorado, USA	Yuval Peres	Microsoft Research, USA
Toka Diagana	Howard University, USA	Y.-F. S. Pétermann	Université de Genève, Switzerland
Michael Dorff	Brigham Young University, USA	Jonathon Peterson	Purdue University, USA
Sever S. Dragomir	Victoria University, Australia	Robert J. Plemmons	Wake Forest University, USA
Joel Foisy	SUNY Potsdam, USA	Carl B. Pomerance	Dartmouth College, USA
Errin W. Fulp	Wake Forest University, USA	Vadim Ponomarenko	San Diego State University, USA
Joseph Gallian	University of Minnesota Duluth, USA	Bjorn Poonen	UC Berkeley, USA
Stephan R. Garcia	Pomona College, USA	József H. Przytycki	George Washington University, USA
Anant Godbole	East Tennessee State University, USA	Richard Rebarber	University of Nebraska, USA
Ron Gould	Emory University, USA	Robert W. Robinson	University of Georgia, USA
Sat Gupta	U of North Carolina, Greensboro, USA	Javier Rojo	Oregon State University, USA
Jim Haglund	University of Pennsylvania, USA	Filip Saidak	U of North Carolina, Greensboro, USA
Johnny Henderson	Baylor University, USA	Hari Mohan Srivastava	University of Victoria, Canada
Glenn H. Hurlbert	Arizona State University, USA	Andrew J. Sterge	Honorary Editor
Charles R. Johnson	College of William and Mary, USA	Ann Trenk	Wellesley College, USA
K. B. Kulasekera	Clemson University, USA	Ravi Vakil	Stanford University, USA
Gerry Ladas	University of Rhode Island, USA	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy
David Larson	Texas A&M University, USA	John C. Wierman	Johns Hopkins University, USA
Suzanne Lenhart	University of Tennessee, USA	Michael E. Zieve	University of Michigan, USA

PRODUCTION

Silvio Levy, Scientific Editor


Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2019 is US \$195/year for the electronic version, and \$260/year (+\$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow[®] from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**

nonprofit scientific publishing

<http://msp.org/>

© 2019 Mathematical Sciences Publishers

involve

2019

vol. 12

no. 4

Euler's formula for the zeta function at the positive even integers	541
SAMYUKTA KRISHNAMURTHY AND MICAH B. MILINOVICH	
Descents and des-Wilf equivalence of permutations avoiding certain nonclassical patterns	549
CADEN BIELAWA, ROBERT DAVIS, DANIEL GREESON AND QINHAN ZHOU	
The classification of involutions and symmetric spaces of modular groups	565
MARC BESSON AND JENNIFER SCHAEFER	
When is $a^n + 1$ the sum of two squares?	585
GREG DRESDEN, KYLIE HESS, SAIMON ISLAM, JEREMY ROUSE, AARON SCHMITT, EMILY STAMM, TERRIN WARREN AND PAN YUE	
Irreducible character restrictions to maximal subgroups of low-rank classical groups of types B and C	607
KEMPTON ALBEE, MIKE BARNES, AARON PARKER, ERIC ROON AND A. A. SCHAEFFER FRY	
Prime labelings of infinite graphs	633
MATTHEW KENIGSBERG AND OSCAR LEVIN	
Positional strategies in games of best choice	647
AARON FOWLKES AND BRANT JONES	
Graphs with at most two trees in a forest-building process	659
STEVE BUTLER, MISA HAMANAKA AND MARIE HARDT	
Log-concavity of Hölder means and an application to geometric inequalities	671
AUREL I. STAN AND SERGIO D. ZAPETA-TZUL	
Applying prospect theory to multiattribute problems with independence assumptions	687
JACK STANLEY AND FRANK P. A. COOLEN	
On weight-one solvable configurations of the Lights Out puzzle	713
YUKI HAYATA AND MASAKAZU YAMAGISHI	