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

Kylie Hess, Emily Stamm, and Terrin Warren

Wake Forest University

July 28, 2016

Acknowledgements

Thank you to UGA and the organizers of the conference.

Special thank you to Dr. Jeremy Rouse for his guidance and to the National Science Foundation for supporting our research (NSF Grant DMS-1461189).

Fermat's Two Squares Theorem

Question: When is a positive integer a sum of two squares?

Fermat's Two Squares Theorem

Question: When is a positive integer a sum of two squares?

Theorem (Fermat, 1640; Euler, 1749)

A positive integer n can be written as the sum of two squares if and only if, for every prime divisor $p \equiv 3 \pmod 4$, p divides n to an even power.

Fermat's Two Squares Theorem

Question: When is a positive integer a sum of two squares?

Theorem (Fermat, 1640; Euler, 1749)

A positive integer n can be written as the sum of two squares if and only if, for every prime divisor $p \equiv 3 \pmod 4$, p divides n to an even power.

Examples:

- $n = 18 = 2 \cdot 3^2 = 3^2 + 3^2$.

Fermat's Two Squares Theorem

Question: When is a positive integer a sum of two squares?

Theorem (Fermat, 1640; Euler, 1749)

A positive integer n can be written as the sum of two squares if and only if, for every prime divisor $p \equiv 3 \pmod 4$, p divides n to an even power.

Examples:

- $n = 18 = 2 \cdot 3^2 = 3^2 + 3^2$.
- $n = 19 = 0 + 19 = 1 + 18 = 4 + 15 = 9 + 10 = 16 + 3$.

Previous Work

Theorem (Curtis, 2014)

If $2^n + 1$ is a sum of two squares, then n is even or $n = 3$.

Previous Work

Theorem (Curtis, 2014)

If $2^n + 1$ is a sum of two squares, then n is even or $n = 3$.

Theorem (Curtis, 2014)

If n is odd and $3^n + 1$ is the sum of two squares, then $3^p + 1$ is the sum of two squares for all primes $p \mid n$, and n is the sum of two squares.

Previous Work

Theorem (Curtis, 2014)

If $2^n + 1$ is a sum of two squares, then n is even or $n = 3$.

Theorem (Curtis, 2014)

If n is odd and $3^n + 1$ is the sum of two squares, then $3^p + 1$ is the sum of two squares for all primes $p \mid n$, and n is the sum of two squares.

Fact:
If n is even, then $a^n + 1$ can always be written as a sum of two squares.

$$a^{2k} + 1 = a^{k \cdot 2} + 1 = (a^k)^2 + 1^2.$$

Outline

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Theorem (HRSW, 2016)

If $a^n + 1$ can be written as a sum of two squares for all $n \in \mathbb{N}$, then a is a perfect square.

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Definition

If $gcd(a, m) = 1$ *and there is a solution to the congruence* $x^2 \equiv a \pmod{m}$*, then a is called a quadratic residue modulo* m*.*

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Definition

If $gcd(a, m) = 1$ and there is a solution to the congruence $x^2 \equiv a \pmod{m}$, then a is called a quadratic residue modulo m.

Example:

- $x^2 \equiv 4 \pmod{5}$: $x = \pm 2$ so 4 is a quadratic residue modulo 5.

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Definition

If $gcd(a, m) = 1$ and there is a solution to the congruence $x^2 \equiv a \pmod{m}$, then a is called a quadratic residue modulo m.

Example:

- $x^2 \equiv 4 \pmod{5}$: $x = \pm 2$ so 4 is a quadratic residue modulo 5.
- $x^2 \equiv 3 \pmod{5}$: no solution, so 3 is a quadratic non-residue modulo 5.

Definition

The Legendre symbol $\left(\frac{a}{p}\right)$ *is defined to be* 1 *if* a *is a quadratic residue modulo an odd prime* p *and* -1 *if* a *is a quadratic non-residue modulo* p*.*

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Definition

The Legendre symbol $\left(\frac{a}{p}\right)$ *is defined to be* 1 *if* a *is a quadratic residue modulo an odd prime* p *and* -1 *if* a *is a quadratic non-residue modulo* p*.*

- Euler's Criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Lemma

Let p be a prime such that $p^e || a^m + 1$ for some $e \in \mathbb{N}$, and let $n = mcp^k$ with $gcd(c, p) = 1$. Then $p^{e+k} || a^n + 1$.

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Lemma

Let p be a prime such that $p^e || a^m + 1$ for some $e \in \mathbb{N}$, and let $n = mcp^k$ with $gcd(c, p) = 1$. Then $p^{e+k} || a^n + 1$.

There is a prime $p \equiv 3 \pmod 4$ such that $\left(\frac{a}{p}\right) = -1$, and either $a^{\frac{p-1}{2}} + 1$ or $a^{\frac{p(p-1)}{2}} + 1$ is not a sum of two squares.

1. $a^n + 1 = \square + \square \; \forall n \iff a = \square.$

Lemma

Let p be a prime such that $p^e || a^m + 1$ for some $e \in \mathbb{N}$, and let $n = mcp^k$ with $gcd(c, p) = 1$. Then $p^{e+k} || a^n + 1$.

There is a prime $p \equiv 3 \pmod 4$ such that $\left(\frac{a}{p}\right) = -1$, and either $a^{\frac{p-1}{2}} + 1$ or $a^{\frac{p(p-1)}{2}} + 1$ is not a sum of two squares.

Reasoning:

If $\left(\frac{a}{p}\right) = -1$, then $p \mid a^{\frac{p-1}{2}} + 1$. For some $k \in \mathbb{N}$, $p^k \parallel a^{\frac{p-1}{2}} + 1$ and so $p^{k+1} \parallel a^{\frac{p(p-1)}{2}} + 1$. Either k or $k + 1$ must be odd, so either $a^{\frac{p-1}{2}} + 1$ or $a^{\frac{p(p-1)}{2}} + 1$ is not a sum of two squares.

2. Cyclotomic Polynomials

Definition

Let $\Phi_n(x)$ denote the nth cyclotomic polynomial. This polynomial is the unique irreducible factor of $x^n - 1$ that does not divide $x^k - 1$ for any proper divisor k of n.

$$\Phi_n(x) = \prod_{\substack{m \in [1,n] \\ \gcd(m,n)=1}} (x - e^{2\pi i m/n}).$$

2. Cyclotomic Polynomials

Definition

If a and m are integers with $\gcd(a, m) = 1$*, we let* $\mathrm{ord}_m(a)$ *be the smallest positive integer k so that* $a^k \equiv 1 \pmod{m}$.

2. Cyclotomic Polynomials

Definition

If a and m are integers with $\gcd(a, m) = 1$, we let $\mathrm{ord}_m(a)$ be the smallest positive integer k so that $a^k \equiv 1 \pmod{m}$.

Theorem (Lüneburg, 1981)

Assume that $a \geq 2$ and $n \geq 2$.

- *If p is a prime and $p \nmid n$, then $p | \Phi_n(a)$ if and only if $\mathrm{ord}_p(a) = n$.*

2. Cyclotomic Polynomials

Definition

If a and m are integers with $\gcd(a, m) = 1$, we let $\operatorname{ord}_m(a)$ be the smallest positive integer k so that $a^k \equiv 1 \pmod{m}$.

Theorem (Lüneburg, 1981)

Assume that $a \geq 2$ and $n \geq 2$.

- *If p is a prime and $p \nmid n$, then $p | \Phi_n(a)$ if and only if $\operatorname{ord}_p(a) = n$.*
- *If p is a prime and $p | n$, then $p | \Phi_n(a)$ if and only if $n = p^k m$ with $\gcd(m, p) = 1$ and $\operatorname{ord}_p(a) = m$. In this case, when $n \geq 3$, $p^2 \nmid \Phi_n(a)$.*

2. Cyclotomic Polynomials

If $n \geq 1$, is a positive integer, then

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

2. Cyclotomic Polynomials

If $n \geq 1$, is a positive integer, then

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

This leads us to the following fact :

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

3. a is even

Theorem (HRSW, 2016)

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

3. a is even

Consider the case when $a = 6$. Then since $a + 1 = 7$ is not the sum of two squares, when n is odd, $6^n + 1$ is the sum of two squares, then $n = 7$ and in fact, $6^7 + 1 = 476^2 + 231^2$.

3. a is even

Consider the case when $a = 6$. Then since $a + 1 = 7$ is not the sum of two squares, when n is odd, $6^n + 1$ is the sum of two squares, then $n = 7$ and in fact, $6^7 + 1 = 476^2 + 231^2$.

Consider the case when $a = 20$. Then since $a + 1 = 3 \cdot 7$, $a + 1$ is not the sum of two squares because of two distinct primes 3 and 7, so $20^n + 1$ is not the sum of two squares for any odd n.

3. a is even

Consider the case when $a = 6$. Then since $a + 1 = 7$ is not the sum of two squares, when n is odd, $6^n + 1$ is the sum of two squares, then $n = 7$ and in fact, $6^7 + 1 = 476^2 + 231^2$.

Consider the case when $a = 20$. Then since $a + 1 = 3 \cdot 7$, $a + 1$ is not the sum of two squares because of two distinct primes 3 and 7, so $20^n + 1$ is not the sum of two squares for any odd n.

Consider the case when $a = 24$. 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.

3. a is even

Lemma

Let $b, n, \delta \in \mathbb{Z}$, n is odd with $\delta | n$, and suppose $b | a^{\delta} + 1$. Then $b | (a^{n-\delta} - a^{n-2\delta} + a^{n-3\delta} - \cdots - a^{\delta} + 1)$ if and only if $b | n$.

3. a is even

Lemma

Let $b, n, \delta \in \mathbb{Z}$, n is odd with $\delta | n$, and suppose $b | a^{\delta} + 1$. Then $b | (a^{n-\delta} - a^{n-2\delta} + a^{n-3\delta} - \cdots - a^{\delta} + 1)$ if and only if $b | n$.

$$a^n + 1 = (a^{\delta} + 1)(a^{n-\delta} - a^{n-2\delta} + a^{n-3\delta} - \cdots - a^{\delta} + 1)$$

3. a is even

Lemma

Let $b, n, \delta \in \mathbb{Z}$, n is odd with $\delta | n$, and suppose $b | a^\delta + 1$. Then $b | (a^{n-\delta} - a^{n-2\delta} + a^{n-3\delta} - \cdots - a^\delta + 1)$ if and only if $b | n$.

$$a^n + 1 = (a^\delta + 1)(a^{n-\delta} - a^{n-2\delta} + a^{n-3\delta} - \cdots - a^\delta + 1)$$

Note that for the following results, there will be some running assumptions: $\delta | n$ and $a^\delta + 1$ is not the sum of two squares because of the prime number p.

3. a is even

Lemma

Let $b, n, \delta \in \mathbb{Z}$, n is odd with $\delta | n$, and suppose $b | a^\delta + 1$. Then $b | (a^{n-\delta} - a^{n-2\delta} + a^{n-3\delta} - \cdots - a^\delta + 1)$ if and only if $b | n$.

$$a^n + 1 = (a^\delta + 1)(a^{n-\delta} - a^{n-2\delta} + a^{n-3\delta} - \cdots - a^\delta + 1)$$

Note that for the following results, there will be some running assumptions: $\delta | n$ and $a^\delta + 1$ is not the sum of two squares because of the prime number p.

Corollary

If $p \nmid n$, then $a^n + 1$ is not the sum of two squares.

3. a is even

Lemma

If $e > 1$, $a + 1$ is not the sum of two squares because of p, and $n = p^e$, then $a^n + 1$ is not the sum of two squares.

Lemma

Let $e, k \in \mathbb{N}$, where $\delta | k$, $k > 1$, and $\gcd(k, p) = 1$, r is some odd integer such that $p^r || a^\delta + 1$. If $n = kp^e$, then $a^n + 1$ is not the sum of two squares.

3. a is even

Lemma

If $e > 1$, $a + 1$ is not the sum of two squares because of p, and $n = p^e$, then $a^n + 1$ is not the sum of two squares.

Lemma

Let $e, k \in \mathbb{N}$, where $\delta | k$, $k > 1$, and $\gcd(k, p) = 1$, r is some odd integer such that $p^r || a^\delta + 1$. If $n = kp^e$, then $a^n + 1$ is not the sum of two squares.

This leaves only one possible odd multiple of δ, when $n = \delta p$ such that $a^n + 1$ can be the sum of two squares.

3. a is even

Lemma

If $a^{\delta} + 1 \equiv 1 \mod 4$ *is not the sum of two squares, then* $a^{n} + 1$ *is not the sum of two squares for any odd* n *that is a multiple of* δ.

3. a is even

Lemma

If $a^\delta + 1 \equiv 1 \mod 4$ *is not the sum of two squares, then* $a^n + 1$ *is not the sum of two squares for any odd n that is a multiple of* δ.

Proof of Lemma.

Suppose $a^n + 1$ is the sum of two squares for some odd n, then $a^\delta + 1$ is not the sum of two squares implies that there exists at least two distinct prime numbers $p_1, p_2 \equiv 3 \mod 4$ and odd integers r_1, r_2, such that $p_1^{r_1} || a^\delta + 1$ and $p_2^{r_2} || a^\delta + 1$. Then $n = \delta p_1 = \delta p_2$, and thus we have a contradiction. □

3. a is even

Proof of Theorem.

Part 1 of Theorem follows immediately from the previous lemma.

If $a+1$ is not the sum of two squares because of some prime p and for some odd n, a^n+1 is the sum of two squares, then it follows that $p|n$, implying the only possible n such that a^n+1 is the sum of two squares is $p=n$. Then the prime p must be the unique prime where $p \equiv 3 \pmod 4$ so that for some odd integer r, $p^r||a+1$. □

4. $a \equiv 1 \pmod 8$

Theorem (HRSW, 2016)

Let $a \equiv 1 \pmod 8$. If n is an odd integer and $a^n + 1$ is the sum of two squares, then $a^\delta + 1$ is the sum of two squares for all $\delta | n$.

4. $a \equiv 1 \pmod 8$

Theorem (HRSW, 2016)

Let $a \equiv 1 \pmod 8$. If n is an odd integer and $a^n + 1$ is the sum of two squares, then $a^\delta + 1$ is the sum of two squares for all $\delta | n$.

Corollary

If $a + 1$ is not the sum of two squares, then $a^n + 1$ is not the sum of two squares for any odd n.

4. $a \equiv 1 \pmod 8$

Let $a = 33$.

- Since $33^{119} + 1$ is the sum of two squares,
- $33 + 1,\ 33^7 + 1,\ 33^{17} + 1$ are sums of two squares.
- Since $33^3 + 1$ is not the sum of two squares,

  $33^{3n} + 1$ is not the sum of two squares for any odd n.

4. $a \equiv 1 \pmod 8$

Let $a = 33$.

- Since $33^{119} + 1$ is the sum of two squares,
- $33 + 1,\ 33^7 + 1,\ 33^{17} + 1$ are sums of two squares.
- Since $33^3 + 1$ is not the sum of two squares,

  $33^{3n} + 1$ is not the sum of two squares for any odd n.

Let $a = 41$.

- Since $42 = 2 \cdot 3 \cdot 7$ is not the sum of two squares,
- $41^n + 1$ is not the sum of two squares for any odd n.

5. $a \equiv 5 \pmod 8$

Theorem (HRSW, 2016)

When $a \equiv 5 \pmod 8$, $a^n + 1$ can be written as the sum of two squares if and only if n is even.

6. $a \equiv 3 \pmod 4$

Let m be the least positive integer such that $\frac{a+1}{m}$ is the sum of two squares.

Theorem (HRSW, 2016)

Let $a \equiv 3 \pmod 4$. If $a^n + 1$ is a sum of two squares for some odd n, then:

6. $a \equiv 3 \pmod 4$

Let m be the least positive integer such that $\frac{a+1}{m}$ is the sum of two squares.

Theorem (HRSW, 2016)

Let $a \equiv 3 \pmod 4$. If $a^n + 1$ is a sum of two squares for some odd n, then:

- *$\frac{n}{m}$ is a sum of two squares, and*

6. $a \equiv 3 \pmod 4$

Let m be the least positive integer such that $\frac{a+1}{m}$ is the sum of two squares.

Theorem (HRSW, 2016)

Let $a \equiv 3 \pmod 4$. If $a^n + 1$ is a sum of two squares for some odd n, then:

- $\frac{n}{m}$ *is a sum of two squares, and*
- $a^m + 1$ *is the sum of two squares.*

6. $a \equiv 3 \pmod 4$

Let $a = 11$.

- $m = 3$
- Since $11^3 + 1$ is the sum of two squares,
- $11^n + 1$ sum of two squares $\implies$ $\frac{n}{3}$ sum of two squares
- $11^{159} + 1$ is the sum of two squares.

6. $a \equiv 3 \pmod 4$

Let $a = 11$.

- $m = 3$
- Since $11^3 + 1$ is the sum of two squares,
- $11^n + 1$ sum of two squares $\implies$ $\frac{n}{3}$ sum of two squares
- $11^{159} + 1$ is the sum of two squares.

Let $a = 43$.

- $m = 11$
- Since $43^{11} + 1$ is not the sum of two squares,
- $43^n + 1$ is not the sum of two squares for any odd n.

7. Aurifeuillian Factorization

Theorem (HRSW, 2016)

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.

7. Aurifeuillian Factorization

Theorem (HRSW, 2016)

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.

Corollary

It follows that $a^n + 1$ is the sum of two squares for either no odd integer n or for an infinite number of odd n.

7. Aurifeuillian Factorization

Theorem (HRSW, 2016)

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.

Corollary

It follows that $a^n + 1$ is the sum of two squares for either no odd integer n or for an infinite number of odd n.

Let $a = 17$

- $p = 17, x = 1$
- $17 + 1 = 18$ is the sum of two squares, so $17^{17^n} + 1$ is the sum of two squares for any n.

7. Aurifeuillian Factorization

Definition

If k is a squarefree positive integer, define $d(k)$ as:

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

7. Aurifeuillian Factorization

Definition

If k is a squarefree positive integer, define $d(k)$ as:

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

Theorem (Stevenhagen, 1987)

Suppose n even, $d(k) \nmid n$, $d(k) | 2n$. Then:

$$\Phi_n(x) = F(x)^2 - kxG(x)^2$$

for some polynomials $F(x), G(x) \in \mathbb{Z}[x]$.

7. Aurifeuillian Factorization

Let d_i be a divisor of n and $\tau(n)$ be the number of divisors of n.

$$\begin{aligned} a^{np}+1 &= \left(a^n+1\right)\left(a^{np-n}-a^{np-2n}+\cdots+1\right) \\ &= \prod_{i=1}^{\tau(n)} \Phi_{2d_i}(a) \prod_{i=1}^{\tau(n)} \Phi_{2d_i p}(a) \end{aligned}$$

We will show that $\Phi_{2d_i p}(a)$ is the sum of two squares for all d_i.

7. Aurifeuillian Factorization

Consider the Aurifeuillian factorization for $\Phi_{2d_ip}(a)$, where $v = -kx^2,\ k = -p \equiv 3 \pmod 4$:

$$\begin{aligned}
\Phi_{2d_ip}(v) &= \big(F(v)\big)^2 - kv\big(G(v)\big)^2 \\
\Phi_{2d_ip}(-kx^2) &= \big(F(-kx^2)\big)^2 - k(-kx^2)\big(G(-kx^2)\big)^2 \\
&= \big(F(-kx^2)\big)^2 + \big(kxG(-kx^2)\big)^2 \\
&= \Phi_{2d_ip}(a).
\end{aligned}$$

Thank You!

a	n odd
1	all
2	3
3	1, 5, 13, 65,...
4	all
5	-
6	7
7	1, 13, 17, 29,...
8	1
9	all
10	-
11	3, 159,...
12	1, 5, 11, 23...
13	-
14	3
15	1, 29, 89, 97,...

a	n odd
16	all
17	1, 7, 17, 23,...
18	19
19	1, 17, 29, 37,...
20	-
21	-
22	-
23	3, 123,...
24	1, 7, 11, 19,...
25	all
26	-
27	-
28	1, 3, 11, 19,...
29	-
30	31