SUM OF TWO SQUARES

ALEX THOLEN

The final goal is to prove that there exists $a, b \in \mathbb{N}$ such that $a^2 + b^2 = c$ is equivalent to saying that the exponent for every $p \equiv 3 \mod 4$ in the prime factorization of c is even.

Lemma 1. *For primes $p \equiv 1 \mod 4$ the equation $n^2 \equiv -1 \mod p$ has exactly two solutions $n \in \{1, 2, \ldots, p-1\}$, for $p = 2$ there is exactly one solution, and for $p \equiv 3 \mod 4$ there are no solutions.*

Proof. For $p \equiv 1$ we take a primitive root r. From Fermat's Little Theorem, we know that $r^{p-1} \equiv 1$, and as such $r^{\frac{p-1}{2}} \equiv -1$. Now, as $p = 1 + 4 \cdot c$ we can rewrite this as $r^{2c} \equiv -1$. As such r^c, r^{3c} are roots of -1. And these are the only ones - as $(r^a)^2 \implies 2a \equiv 2c \mod 4c$ and there are only those two solutions.

For $p = 2$ we simply have to consider 1.

For $p \equiv 3$ take a primitive root r of modulo p. As such, each number can be written as r^n. From Fermat's Little Theorem, we know that $r^{p-1} \equiv 1$, and as such $r^{\frac{p-1}{2}} \equiv -1$. Now, as $p = 3 + 4 \cdot c$, we can rewrite this to $r^{1+2c} \equiv -1$. Now, consider $a^2 \equiv -1$. Then, we would have $(r^x)^2 \equiv -1 \mod p \to r^{2x} \equiv -1 \mod p \to 2x \equiv 1 + 2c \mod p - 1$. However, as $p - 1$ is even we can reduce this to mod 2 and as such for any number to square to -1 we would need $0 \equiv 1$, which is a contradiction. ■

Lemma 2. *No number that is $3 \mod 4$ is the sum of two squares.*

Proof. Look at the equation $a^2 + b^2 = c$ in mod 4. If we look at what a^2could possibly be, we see that $\{0^2, 1^2, 2^2, 3^2\}$ reduces down to $\{0, 1\}$. As such, $\{0, 1\} + \{0, 1\} = \{0, 1, 2\}$ and could never be $3 \mod 4$. ■

Note that this is also true for primes, which is primarily what this will be used for.

Lemma 3. *If a, b are sums of two squares then $a \cdot b$ is a sum of two squares.*

Proof. We have $m^2 + n^2 = a, x^2 + y^2 = b$. Then,

$$\begin{aligned} a \cdot b &= (m^2 + n^2)(x^2 + y^2) \\ &= m^2x^2 + m^2y^2 + n^2x^2 + n^2y^2 \\ &= m^2x^2 + n^2y^2 + mnxy - mnxy + m^2y^2 + n^2x^2 \\ &= (mx + ny)^2 + (my - nx)^2 \end{aligned}$$

■

Theorem 4. *Every prime $p \equiv 1 \mod 4$ is the sum of two squares.*

Date: March 24, 2022.

Proof. Let's look at things of the form $x+sy$ for $x, y \in \{0, 1, ..., \lfloor\sqrt{p}\rfloor\}$ and s is some constant. The amount of distinct pairs of x, y is $\#\{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}^2 = \{1 + \lfloor\sqrt{p}\rfloor\}^2 > \sqrt{p}^2 = p$ and as such there are more pairs than possible outcomes modulo p. As such, there exists $x', y', x'', y'' \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$ such that $x' + sy' \equiv x'' + sy''$ for any s. Moving things over to one side, we see that there exists for any s some distinct pairs $(x', y'), (x'', y'')$ such that $(x' - x'') + s(y' - y'') \equiv 0$. Now let $x = x' - x''$ and $y = y' - y''$. If we look at the range, we see that $x, y \in \{-\lfloor\sqrt{p}\rfloor, \ldots, \lfloor\sqrt{p}\rfloor\}$ for the equation $x + sy \equiv 0$.

Now, set s to be one of the two square roots of -1 that we proved exist in 1. Move sy over to the right side and square it to get that $x^2 \equiv -y^2$, or $x^2 + y^2 \equiv 0$. Now note that $x^2, y^2 < p$ as $|x, y| \leq \lfloor\sqrt{p}\rfloor < \sqrt{p}$. As such, $x^2 + y^2 < 2p$, and it can't be equal to 0 as that would mean that $x' = x'', y' = y''$ despite them being distinct. And since $p|x^2 + y^2$, we get that $p = x^2 + y^2$ and we have our proof. ■

Theorem 5. *If $x^2 + y^2 \equiv 0 \mod p$ for some $p \equiv 3 \mod 4$, then $p|x, y$.*

Proof. We have $x^2 + y^2 \equiv 0$, and so $x^2 \equiv -y^2$. Since this is mod p, everything has a multiplicative inverse except for 0. So if $x, y \neq 0$ then we can multiply both sides by the multiplicative inverse of y^2 to get $(x \cdot y')^2 \equiv -1$. However 1 showed that there is no square root of -1. And as such, we couldn't multiply by the multiplicative inverse of y^2 and as such $y \equiv 0$ and as such $x \equiv 0$, proving our theorem. ■

Theorem 6. *A natural number n can be represented as a sum of two squares if and only if every prime factor of the form $p \equiv 3 \mod 4$ appears with an even exponent in the prime decomposition of n.*

Proof. Let's begin with the only if. From 5, we see that for a sum of squares to be equal to n any prime of the residue $3 \mod 4$ must divide both x and y and henceforth have $p^2|n$. Dividing the whole thing by p^2 can then further prove that if $p^3|n$ then $p^4|n$, and so on.

Then for the if. Take $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\ldots$ Any prime that isn't $3 \mod 4$ can be written as a sum of squares (4 or $2 = 1^2 + 1^2$) and from 3 we see that also means that $p_i^{a_i}$ is also a sum of squares. Since every prime factor of the form $3 \mod 4$ has an even exponent, we know that they are also a sum of squares, namely $\left(p_i^{\frac{a_i}{2}}\right)^2 + 0^2$. Then again from 3 we can just multiply all these prime factors together and we can see that n is the sum of two squares. ■

And so we've shown which numbers have sum of square representations. But this doesn't help with trying to find any. For that, we need to take a different approach.

To do this, let's begin with defining $[q_1, q_2, q_3, \ldots, q_n]$ for $q_i \in \mathbb{Z}_+$. We define it by the following properties:

(1) $[] = 1$
(2) $[q_1] = q_1$
(3) $[q_1, q_2, q_3, \ldots, q_n] = q_1[q_2, q_3, \ldots, q_n] + [q_3, q_4, \ldots, q_n]$
Note that these three uniquely determine how this function is defined. Then from here let's prove 5 more properties; namely
(4) $[q_1, \ldots, q_n] \in \mathbb{Z}_+$
(5) $[q_2, \ldots, q_n] < [q_1, \ldots, q_n]$
(6) $[q_1, \ldots, q_n] = [q_n, \ldots, q_1]$
(7) $[q_2, \ldots, q_n]$ and $[q_1, \ldots, q_n]$ are relatively prime
(8) $[q_1, q_2, \ldots, q_{s-1}, q_s, q_{s+1}, \ldots, q_n] = [q_1, \ldots, q_s][q_{s+1}, \ldots, q_n] + [q_1, \ldots, q_{s-1}][q_{s+2}, \ldots, q_n]$

Now, to prove 4 we simply note that every operation is either multiplication or addition - as such it can't leave $\mathbb{Z}_+$.

For number 5 we see that from number 3 we get that

$$[q_1, q_2, q_3, \ldots, q_n] = q_1[q_2, q_3, \ldots, q_n] + [q_3, q_4, \ldots, q_n] \geq 1 \cdot [q_2, q_3, \ldots, q_n] + 1 > [q_2, q_3, \ldots, q_n].$$

For number 6 we can prove it by induction - obviously the base case of 1 or 0 elements work fine, and otherwise we can turn $[q_1, \ldots, q_n]$ into $q_1[q_n, \ldots, q_2] + [q_n, \ldots, q_3]$ and into $q_1 q_n[q_2, \ldots, q_{n-1}] + q_1[q_2, \ldots, q_{n-2}] + q_n[q_3, \ldots, q_{n-1}] + [q_3, \ldots, q_{n-2}]$ via two uses of property 3 and the inductive hypothesis, and on the flip side we can do the same thing - turning $[q_n, \ldots, q_1]$ into $q_n[q_1, \ldots, q_{n-1}] + [q_1, \ldots, q_{n-2}]$ into $q_n q_1[q_2, \ldots, q_{n-1}] + q_n[q_3, \ldots, q_{n-1}] + q_1[q_2, \ldots, q_{n-2}] + [q_3, \ldots, q_{n-2}]$.

For number 7 we can prove it by induction - assume that for all $[q_1, \ldots, q_n]$ then $[q_1, \ldots, q_n]$ and $[q_2, \ldots, q_n]$ are relatively prime. Then take an arbitrary $[q_1, \ldots, q_{n+1}]$ - we wish to find the gcd of that and $[q_2, \ldots, q_{n+1}]$. Use property 3 to turn it into $\gcd(q_1[q_2, q_3, \ldots, q_{n+1}] + [q_3, q_4, \ldots, q_{n+1}], [q_2, \ldots, q_{n+1}]$ which from the euclidean algorithm we can reduce down to $\gcd([q_3, q_4, \ldots, q_{n+1}], [q_2, \ldots, q_{n+1}])$. This is assumed by the inductive hypothesis! The base case is simply noting that for 0 elements the gcd of 1 and 1 is ... well ... 1.

Finally for number 8 we can prove it by induction over s - when $s = 1$ we have property 3, and as such we have our base case. Otherwise,

$$[q_1, \ldots, q_s][q_{s+1}, \ldots, q_n] + [q_1, \ldots, q_{s-1}][q_{s+2}, \ldots, q_n]$$

can be turned into

$$[q_1, \ldots, q_s](q_{s+1}[q_{s+2}, \ldots, q_n] + [q_{s+3}, \ldots, q_n]) + [q_1, \ldots, q_{s-1}][q_{s+2}, \ldots, q_n]$$

which when expanded and rearranged becomes

$$(q_{s+1}[q_1, \ldots, q_s] + [q_1, \ldots, q_{s-1}])[q_{s+2}, \ldots, q_n] + [q_1, \ldots, q_s][q_{s+3}, \ldots, q_n]$$

which we can apply property 3 in reverse to obtain

$$[q_1, \ldots, q_{s+1}][q_{s+2}, \ldots, q_n] + [q_1, \ldots, q_s][q_{s+3}, \ldots, q_n]$$

which is precisely the following case.

So now we have the 8 properties (3 defined and 5 proven) that will be needed for the rest of the proof.

Let's use the Euclidean Algorithm to generate the continued fraction of $\frac{r}{s}$ - namely

$$\frac{r}{s} = q_1 + \frac{t}{s}(0 \leq t < s), \frac{s}{t} = q_2 + \frac{u}{t}(0 \leq u < t), \ldots, \frac{v}{w} = q_n + \frac{0}{w}$$

As such we can pair each $\frac{r}{s}$ up with a sequence of numbers $\{q_1, q_2, \ldots, q_n\}$. Each such sequence also has exactly one $\frac{r}{s}$ that produces this sequence - in fact, I claim it is

$$\frac{r}{s} = \frac{[q_1, q_2, \ldots, q_n]}{[q_2, q_3, \ldots, q_n]}.$$

From the first property of $[q_1, \ldots, q_n]$ we see that

$$\left\{\frac{[q_1, \ldots, q_n]}{[q_2, \ldots, q_n]}\right\} = \left\{\frac{q_1[q_2, \ldots, q_n] + [q_3, \ldots, q_n]}{[q_2, \ldots, q_n]}\right\} = \left\{q_1, \frac{[q_2, \ldots, q_n]}{[q_3, \ldots, q_n]}\right\}$$

and as such continues to simplify until we indeed get the desired sequence. The uniqueness is clear - once can simply follow the Euclidean Algorithm backwards to obtain $\frac{r}{s}$ given the $\{q_1, \ldots, q_n\}$.

Now let's get back to our comfy primes that are of the form $p = 4r + 1$. Take some arbitrary integer $u \in \{2, 3, \ldots, 2r\}$. Consider what we get when we do $\{\frac{p}{u}\}$. From the above equation we know that $\frac{p}{u} = \frac{[q_1, q_2, \ldots, q_n]}{[q_2, q_3, \ldots, q_n]}$ and as the numerator and denominator of the right side are relatively prime (property 7 from earlier) we can furthermore conclude that $p = [q_1, q_2, \ldots, q_n]$ and $u = [q_2, q_3, \ldots, q_n]$. Now note that q_1 must be at least 2 (as $\frac{p}{u} \geq \frac{4r+1}{2r} > 2$ and q_1 is in fact the integer part of $\frac{p}{u}$) and that q_n must also be at least 2 (from the fact that in the final step of the Euclidean algorithm were $q_n = 1$ then we would have $\frac{w}{w}$ and that would have been simplified earlier). As such, performing the following sequence of actions can create a mapping between elements u and v:

$$\frac{p}{u} = \frac{[q_1, q_2, \ldots, q_n]}{[q_2, q_3, \ldots, q_n]} \implies$$
$$p = [q_1, q_2, \ldots, q_n] \implies$$
$$p = [q_n, \ldots, q_1] \implies$$
$$\frac{p}{v} = \frac{[q_n, \ldots, q_1]}{[q_{n-1}, \ldots, q_1]}$$

We know that $v \in \{2, 3, \ldots, 2r\}$ as

$$\frac{p}{v} = \frac{[q_n, \ldots, q_1]}{[q_{n-1}, \ldots, q_1]} = \frac{q_n[q_{n-1}, \ldots, q_1] + [q_{n-2}, \ldots, q_1]}{[q_{n-1}, \ldots, q_1]} > q_n \geq 2$$

and $v \neq 1$ because that would mean $[q_{n-1}, \ldots, q_1] = 1$ and yet $[q_{n-1}, \ldots, q_1] \geq q_1 \geq 2$ and so the only possible case in which we would have $v = 1$ is if $p = [q_1]$ but that means that u is also 1 and as such is not relevant. So this is a bijective mapping from $\{2, 3, \ldots, 2r\}$ to $\{2, 3, \ldots, 2r\}$. Now note that there are an odd amount of elements - as such there must be some element which maps to itself (say λ). Now, from the euclidian algorithm there is just one $\{q_1, \ldots, q_n\}$ for $\frac{p}{\lambda}$ and as such $\{q_n, \ldots, q_1\}$ must be exactly the same as $\{q_1, \ldots, q_n\}$ - or in other words it is palindromic. Say we have $n = 2k + 1$. That means that it becomes $[q_1, \ldots, q_k, q_{k+1}, q_k, \ldots, q_1]$. From property 8 of the bracket function we can turn this into

$$p = [q_1, \ldots, q_{k+1}][q_k, \ldots, q_1] + [q_1, \ldots, q_k][q_{k-1}, \ldots, q_1]$$

We can factor out $[q_1, \ldots, q_k]$ though and since p is a prime that means we must either have $[q_1, \ldots, q_k] = 1$ or $[q_1, \ldots, q_k] = p$. It certainly isn't equal to p as it's a subset of $[q_1, \ldots, q_k, q_{k+1}, q_k, \ldots, q_1]$ which p is equal to, and as such we would need $[q_1, \ldots, q_k] = 1$. However $q_1 \geq 2$ and $[q_1, \ldots, q_k] \geq q_1$ and so that also isn't possible. Henceforth we can't have $n = 2k + 1$ as that contradicts p being prime. So instead we have $n = 2k$, and when using property 8 again this time we get

$$p = [q_1, \ldots, q_k][q_k, \ldots, q_1] + [q_1, \ldots, q_{k-1}][q_{k-1}, \ldots, q_1]$$

And from property 6 we can reverse two of those brackets to conclude that we have $p = [q_1, \ldots, q_k]^2 + [q_1, \ldots, q_{k-1}]^2$.

And so all that remains for a constructive proof is to figure out what λ would give this palindromic situation. For that let's use the following identity:

$$[q_1, q_2, \ldots, q_n][q_2, \ldots, q_{n-1}] - [q_1, \ldots, q_{n-1}][q_2, \ldots, q_n] = (-1)^n$$

The base case with $[q_1, q_2]$ is simply $[q_1, q_2][] - [q_1][q_2] = (q_1q_2 + 1)(1) - (q_1)(q_2) = 1 = (-1)^2$. As for the inductive step,

$$[q_1, q_2, \ldots, q_n][q_2, \ldots, q_{n-1}] - [q_1, \ldots, q_{n-1}][q_2, \ldots, q_n] =$$
$$(q_n[q_1, q_2, \ldots, q_{n-1}] + [q_1, \ldots, q_{n-2}])[q_2, \ldots, q_{n-1}] - [q_1, \ldots, q_{n-1}](q_n[q_2, \ldots, q_{n-1}] + [q_2, \ldots, q_{n-2}]) =$$
$$[q_1, \ldots, q_{n-2}][q_2, \ldots, q_{n-1}] - [q_1, \ldots, q_{n-1}][q_2, \ldots, q_{n-2}] = -\text{inductive hypothesis} = (-1)^n$$

As such we have this identity. How is it useful, one may ask? Well, let's go back to the λ that we know must exist. Applying this property to $[q_1, q_2, \ldots, q_k, q_k, \ldots, q_1]$ gets us

$$1 = [q_1, \ldots, q_k, q_k, \ldots, q_1][q_2, \ldots, q_k, q_k, \ldots, q_2] - [q_1, \ldots, q_k, q_k, \ldots, q_2][q_2, \ldots, q_k, q_k, \ldots, q_1]$$

Note that $[q_1, \ldots, q_k, q_k, \ldots, q_1]$ is just p and the second half is simply λ and λ in reverse order, or λ^2. As such we get that

$$1 = p[q_2, \ldots, q_k, q_k, \ldots, q_2] - \lambda^2 \implies -1 \equiv \lambda^2 \mod p$$

As such, if we take the only satisfactory square root of negative 1 (since p is 1 mod 4 we showed that two exist - namely negatives of each other and as such exactly one of them is between 2 and $\frac{p-1}{2}$) we can then apply the above construction to obtain our sum of squares.

Let's finish it off with an example. Take 1009, a random prime thats $1 \mod 4$. Now, use some other technique (the python code I stole used Tanelli-Shanks but there are others) to calculate a square root of -1 - in this case 469. Now time to obtain the $\{q_1, \ldots\}$. Applying the algorithm above we get $[2, 6, 1, 1, 1, 1, 6]$. As such our two squares are $[2, 6, 1, 1]$ and $[2, 6, 1]$ which evaluate to 28 and 15 respectively. As such we have that $1009 = 28^2 + 15^2 = 784 + 225$.

Sources:

Aigner, Martin, and Gunter M Ziegler. Proofs From The Book. 5th ed.

F. W. CLARKE, W. N. EVERITT, L. L. LITTLEJOHN S. J. R. VORSTER: H. J. S. Smith and the Fermat Two Squares Theorem, Amer. Math. Monthly 106 (1999), 652-665.