Euler's proof of the Sums of Two Squares theorem

Theorem: *(Fermat's two squares theorem) Every odd prime p is a sum of two squares if and only if $p \equiv 1$ $(mod\ 4)$.*

For the avoidance of ambiguity, zero will always be a valid possible constituent of "sums of two squares", so for example every square of an integer is trivially expressible as the sum of two squares by setting one of them to be zero.

1. The product of two numbers, each of which is a sum of two squares, is itself a sum of two squares.

This is a well-known property, based on the identity

$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2$$

due to Diophantus.

2. If a number which is a sum of two squares is divisible by a prime which is a sum of two squares, then the quotient is a sum of two squares.

Indeed, suppose for example that $a^2 + b^2$ is divisible by $p^2 + q^2$ and that this latter is a prime. Then $p^2 + q^2$ divides

$$(pb - aq)(pb + aq) = p^2b^2 - a^2q^2 = p^2(a^2 + b^2) - a^2(p^2 + q^2).$$

Since $p^2 + q^2$ is a prime, it divides one of the two factors. Suppose that it divides $pb - aq$. Since

$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2$$

(Diophantus's identity) it follows that $(p^2 + q^2)^2$ must divide $(ap + bq)^2$. So the equation can be divided by $(p^2 + q^2)^2$. Dividing the expression by $(p^2 + q^2)^2$ yields:

$$\frac{a^2 + b^2}{p^2 + q^2} = \left(\frac{ap + bq}{p^2 + q^2}\right)^2 + \left(\frac{aq - bp}{p^2 + q^2}\right)^2$$

and thus expresses the quotient as a sum of two squares, as claimed.

On the other hand if p^2+q^2 divides $pb+aq$, a similar argument holds by using the following variant of Diophantus's identity:

$$(a^2 + b^2)(q^2 + p^2) = (aq + bp)^2 + (ap - bq)^2.$$

3. If a number which can be written as a sum of two squares is divisible by a number which is not a sum of two squares, then the quotient has a factor which is not a sum of two squares.

Suppose q is a number not expressible as a sum of two squares, which divides $a^2 + b^2$. Write the quotient, factored into its (possibly repeated) prime factors, as $p_1 p_2 \cdots p_n$ so that $a^2 + b^2 = qp_1 p_2 \cdots p_n$. If all factors p_i can be written as sums of two squares, then we can divide $a^2 + b^2$ successively by p_1, p_2, etc., and applying step (2.) above we deduce that each successive, smaller, quotient is a sum of two squares. If we get all the way down to q then q itself would have to be equal to the sum of two squares, which is a contradiction. So at least one of the primes p_i is not the sum of two squares.

4. If a and b are relatively prime positive integers then every factor of $a^2 + b^2$ is a sum of two squares.

Let a, b be relatively prime positive integers: without loss of generality $a^2 + b^2$ is not itself prime, otherwise there is nothing to prove. Let q therefore be a proper factor of $a^2 + b^2$, not necessarily prime: we wish to show that q is a sum of two squares. Again, we lose nothing by assuming $q > 2$ since the case $q = 2 = 1^2 + 1^2$ is obvious.

Let m, n, be non-negative integers such that mq, nq are the closest multiples of q (in absolute value) to a, b respectively. The differences $c = a - mq$ and $d = b - nq$ are integers of absolute value strictly less than $q/2$:

To establish this, we begin with the following observation: Let l be the largest integer such that $lq \leq a$, then $lq \leq a < (l + 1)q$. There are three possible cases:

(i) If $a - lq < q/2$ and $|a - (l + 1)q| > q/2$, then m equals l.

(ii) If $|a - (l + 1)q| < q/2$ and $a - lq > q/2$, then m equals $l + 1$.

(iii) That $a - lq = q/2$.

We show that we cannot have $q/2 = c = a - mq$. Obviously, we cannot have $q/2 = c$ if q were odd. We take q to be even and $q > 2$. First note that a and b are coprime only if a^2 and b^2 are coprime. Say $\gcd(a, q/2) > 1$, since $\gcd(a, q/2)|q/2|q|a^2 + b^2$, we would have $\gcd(a, q/2)|b^2$. Therefore, we must have $\gcd(a, q/2) = 1$. As $c = a - mq$, if $c = q/2$ we would have that $q/2|a$, and $\gcd(a, q/2) = q/2 > 1$. As such, we cannot have $c = q/2$. Similarly, we can argue that the difference $d = b - nq$ is an integer of absolute value strictly less than $q/2$.

Multiplying out we obtain

$$a^2 + b^2 = m^2q^2 + 2mqc + c^2 + n^2q^2 + 2nqd + d^2 = Aq + (c^2 + d^2)$$

uniquely defining a non-negative integer A. Since q divides both ends of this equation sequence it follows that $c^2 + d^2$ must also be divisible by q: say $c^2 + d^2 = qr$. Let g be the gcd of c and d. Say $\gcd(g, q) > 1$, then by $c = a - mq$ and $d = b - nq$ we would have $\gcd(a, b) > 1$. Thus, the co-primeness of a, b implies that g and q are coprime. Thus g^2 divides r, so writing $e = c/g$, $f = d/g$ and $s = r/g^2$, we obtain the expression $e^2 + f^2 = qs$ for relatively prime e and f, and with $s < q/2$, since

$$qs = e^2 + f^2 \leq c^2 + d^2 < \left(\frac{q}{2}\right)^2 + \left(\frac{q}{2}\right)^2 = q^2/2.$$

Now finally, the descent step: if q is not the sum of two squares, then by step (3.) there must be a factor q_1 say of s which is not the sum of two squares. But $q_1 \leq s < q/2 < q$ and so repeating these steps (initially with $e, f; q_1$ in place of $a, b; q$, and so on ad infinitum) we shall be able to find a strictly decreasing infinite sequence $q, q_1, q_2, \ldots$ of positive integers which are not themselves the sums of two squares but which divide into a sum of two relatively prime squares. Since such an infinite descent is impossible, we conclude that q must be expressible as a sum of two squares, as claimed.

5. Every prime of the form $4n + 1$ is a sum of two squares.

We will need Fermat's Little Theorem, which we prove in notes below. If $p = 4n + 1$, then by Fermat's Little Theorem each of the numbers $1, 2^{4n}, 3^{4n}, \ldots, (4n)^{4n}$ is congruent to one modulo p. The differences $2^{4n} - 1, 3^{4n} - 2^{4n}, \ldots, (4n)^{4n} - (4n - 1)^{4n}$ are therefore all divisible by p. Each of these differences can be factored as

$$a^{4n} - b^{4n} = \left(a^{2n} + b^{2n}\right)\left(a^{2n} - b^{2n}\right).$$

Since p is prime, it must divide one of the two factors. If in any of the $4n - 1$ cases it divides the first factor, then by the previous step we conclude that p is itself a sum of two squares (since a and b differ by 1, they are relatively prime). So it is enough to show that p cannot always divide the second factor. If it divides all $4n - 1$ differences $2^{2n} - 1, 3^{2n} - 2^{2n}, \ldots, (4n)^{2n} - (4n - 1)^{2n}$, then it would divide all $4n - 2$ differences of successive terms, all $4n - 3$ differences of the differences, and so forth. The kth differences of the sequence $1^k, 2^k, 3^k, \ldots$ can be expressed as

$$\text{performing} \quad [T_1 - I]^k x^k, \quad \text{then setting } x = 1, 2, 3, \ldots$$

where T_h is the shift operator with step h, defined by $T_h f(x) = f(x + h)$, and I is the identity operator. Since the kth differences of the sequence $1^k, 2^k, 3^k, \ldots$ are all equal to $k!$ (see notes below), the $2n$th differences of the sequence $1, 2^{2n}, 3^{2n}, \ldots, (4n)^{2n}$, expressed as

$$\text{performing} \quad [T_1 - I]^{2n} x^{2n}, \qquad \text{then setting } x = 1, 2, 3, \ldots 2n$$

would all be constant and equal to $(2n)!$, which is certainly not divisible by p. Therefore, p cannot divide all the second factors which proves that p is indeed the sum of two squares.

□

Notes:

Integers a and b are coprime only if a^2 and b^2 are coprime

If $d > 1$ is a common divisor of a^2 and b^2 then so is any prime, p, in the prime number decomposition of d. But if $p|a^2$ then $p|a$ and if $p|b^2$ then $p|b$. Therefore, a and b are coprime only if a^2 and b^2 are coprime.

□

Proof of Fermat's little theorem (1st proof)

Fermat's little theorem, which states that

$$a^p \equiv a \pmod{p}$$

for every prime number p and every integer a.

However, the theorem's non-trivial aspect is that if a is not divisible by p then Fermat's little theorem states that

$$a^{p-1} \equiv 1 \pmod{p}$$

for every prime number p. It is this form of the theorem that we use in the proof of the two square theorem.

Proof

This proof, due to Euler, uses induction to prove the theorem for all integers $m \geq 0$.

The base step, that $0^p \equiv 0 \pmod{p}$, is trivial. Next, we must show that if the theorem is true for $m = k$, then it is also true for $m = k + 1$. For this inductive step, we need the following lemma.

Note

$$(x+y)^p = \sum_{i=0}^{p} \binom{n}{i} x^{p-i} y^i = x^p + y^p + \sum_{0<i<p}^{p} \frac{p!}{i!(p-i)!} x^{p-i} y^i.$$

The binomial coefficients are all integers. The numerator contains a factor p by the definition of factorial. When $0 < i < p$, neither of the terms in the denominator includes a factor of p (relying on the primality of p), leaving the coefficient itself to possess a prime factor of p from the numerator, implying that

$$\binom{p}{i} \equiv 0 \pmod{p}, \qquad 0 < i < p.$$

We can now proceed to prove the theorem with the induction.

Assume $k^p \equiv k \pmod{p}$, and consider $(k+1)^p$. We have

$$(k+1)^p \equiv k^p + 1^p \pmod{p}.$$

Using the induction hypothesis, we have that $k^p \equiv k \pmod{p}$; and, trivially, $1^p = 1$. Thus

$$(k+1)^p \equiv k+1 \pmod{p},$$

which is the statement of the theorem for $m = k+1$.

So that

$$a^p \equiv a \pmod{p} \qquad (1),$$

We need the cancellation law now. This states that if u, x, and y are integers, and u is not divisible by a prime number p, and if

$$ux \equiv uy \pmod{p} \qquad (2),$$

then we may "cancel" u to obtain

$$x \equiv y \pmod{p} \qquad (3).$$

We can prove the cancellation law easily using if a prime p divides a product ab (where a and b are integers), then p must divide a or b. Indeed, the assertion (2) simply means that p divides $ux - uy = u(x-y)$. Since p is a prime which does not divide u, it must divide $x - y$ instead; that is, (3) holds.

If a is not divisible by p we can "cancel" an a from both sides of (1), obtaining

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Proof of Fermat's little theorem (2nd proof)

This is a proof of the version of Fermat's little theorem we use in the proof of the two square theorem.

Let us assume that a is positive and not divisible by p. In the sequence of numbers

$$a, 2a, 3a, \dots, (p-1)a$$

none of the terms $a, 2a, ..., (p-1)a$ can be congruent to zero modulo p, since if k is one of the numbers $1, 2, ..., p-1$, then k is relatively prime with p, and so is a, so ka shares no factor with p. Therefore, we know that the numbers $a, 2a, ..., (p-1)a$, when reduced modulo p, must be found among the numbers $1, 2, 3, ..., p-1$.

Furthermore, the numbers $a, 2a, ..., (p-1)a$ must all be distinct after reducing them modulo p, because if

$$ka \equiv ma \pmod{p},$$

where k and m are one of $1, 2, ..., p-1$, then the cancellation law tells us that

$$k \equiv m \pmod{p}.$$

Since both k and m are between 1 and $p-1$, they must be equal. Therefore, the terms $a, 2a, ..., (p-1)a$ when reduced modulo p must be distinct. To summarise: when we reduce the $p-1$ numbers $a, 2a, ..., (p-1)a$ modulo p, we obtain distinct members of the sequence $1, 2, ..., p-1$. Since there are exactly $p-1$ of these, the only possibility is that the former are a rearrangement of the latter.

Therefore, if we multiply together the numbers in each sequence, the results must be identical modulo p:

$$a \times 2a \times 3a \times \cdots \times (p-1)a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \pmod{p}.$$

Collecting together the a terms yields

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Finally, we may "cancel out" the numbers $1, 2, ..., p-1$ from both sides of this equation, obtaining

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

The kth differences of the sequence $1^k, 2^k, 3^k, \ldots$

Denote by $\Delta_h = T_h - I$ where T_h is the shift operator with step h, defined by $T_h f(x) = f(x+h)$, and I is the identity operator.

Applying the Taylor series to $f(x+h)$ with respect to h,

$$[T_h - I]f(x) = h\frac{d}{dx}f(x) + \frac{h^2}{2!}\frac{d^2}{dx^2}f(x) + \cdots .$$

We compute $\Delta_1^k = [T_1 - I]^k$ applied to x^k two ways. First, by employing k successive Taylor expansions, we find:

$$[T_1 - I]^k x^k = \frac{d^k}{dx^k}x^k = k!$$

so it is equal to a constant. Alternatively, we can compute $[T_1 - I]^k x^k$ recursively as follows:

$$[T_1-I]^k x^k = [T_1-I]^{k-1}((x+1)^k-x^k) = [T_1-I]^{k-2}([(x+2)^k-(x+1)^k]-[(x+1)^k-x^k]) = \ldots$$

When we set $x = 1, 2, 3, \ldots$ the above expression represents the kth differences of the sequence $1^k, 2^k, 3^k, \ldots$.

For example, the 4th differences of the sequence $1^4, 2^4, 3^4, 4^4, 5^4, 6^4, 7^4, 8^4$ are obtained by setting x in

$$(x+4)^4 - \binom{4}{1}(x+3)^4 + \binom{4}{2}(x+2)^4 - \binom{4}{3}(x+1)^4 + x^4$$

to $1, 2, 3, 4$ in turn, which reads

$$\begin{gathered}
5^4 - \binom{4}{1}4^4 + \binom{4}{2}3^4 - \binom{4}{3}2^4 + 1^4 \\
6^4 - \binom{4}{1}5^4 + \binom{4}{2}4^4 - \binom{4}{3}3^4 + 2^4 \\
7^4 - \binom{4}{1}6^4 + \binom{4}{2}5^4 - \binom{4}{3}4^4 + 3^4 \\
8^4 - \binom{4}{1}7^4 + \binom{4}{2}6^4 - \binom{4}{3}5^4 + 4^4.
\end{gathered}$$

Each of these us equal to 4!.

□