# Primes as sums of squares

Our goal is to prove the following result formulated by Fermat.

**Theorem 1.** *A prime $p$ can be written as the sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

*Proof.* One of the direction is easy. Assume $p = a^2 + b^2$. Since $a^2$ and $b^2$ are each either congruent to 0 or 1 modulo 4, it follows that $p \equiv 0, 1$ or $2 \pmod 4$. But let's not forget that $p$ is a prime, so it cannot possible be divisible by 4, and the only way it can be $\equiv 2 \pmod 4$ is for it to equal 2.

The other direction is much harder. It's clear to do when $p = 2$, but we also have to show that any prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares. For that, we will follow Euler's proof. It might not be the shortest proof one can write down, but it has the advantage that it illustrates the concept of descent (which was the idea Fermat used in his sketch of the proof) and reciprocity that we will encounter again later in the course.

**Reciprocity step:** A prime $p \equiv 1 \pmod 4$, then it divides $N = a^2 + b^2$ with $a$ and $b$ relatively prime integers.

**Descent step:** If a prime $p$ divides a number $N$ of the form $N = a^2+b^2$, where $(a, b) = 1$, then $p$ itself can be written as $p = x^2 + y^2$ for some $(x, y) = 1$.

Clearly the these two claims imply our result. □

We are going to deviate from the historical order and prove first the reciprocity step. (Euler first found the proof for the descent step.)

## 1 Reciprocity step

The reciprocity step follows immediately from the following result.

**Lemma 2.** *The equation*

$$x^2 \equiv -1 \pmod p$$

*has solutions* $\iff$ $p = 2$ *or* $p \equiv 1 \pmod 4$.

*Proof.* **If** $p = 2$, then $x = 1$ is a solution.

**If** $p \equiv 1 \pmod 4$, then $4 \mid p-1 = \phi(p)$ and therefore there exists an integer $a$ with $\operatorname{ord}_p a = 4$. This means that $a^4 \equiv 1 \pmod p$ and $a, a^2, a^3 \not\equiv 1 \pmod 4$. We have

$$a^4 - 1 = (a^2-1)(a^2+1) \equiv 0 \pmod p.$$

But $a^2 - 1 \not\equiv 0 \pmod p$, hence $a^2 \equiv -1 \pmod p$, and $x = a$ is a solution of our equation.

**If** $p \equiv 3 \pmod 4$, assume that $x = a$ is a solution, i.e. $a^2 \equiv -1 \pmod p$. Then $a^4 \equiv 1 \pmod p$, so $\operatorname{ord}_p a \mid 4$. But we also know that $\operatorname{ord}_p a \mid \phi(p) = p-1$. Hence $\operatorname{ord}_p a \mid (p-1, 4) = 2$, which means that $a^2 \equiv 1 \pmod p$. The upshot is that $1 \equiv -1 \pmod p$, so $p \mid 2$. The only way this will happen is for $p = 2$, and we reached a contradiction.

□

# 2 Descent step

Fermat's idea (which he used on a number of other occasions), formalized in this case by Euler in this case, is to show that if we have a solution to a diophantine equation, then we can find a "smaller" (in some sense) solution. Iterating this process means that we can find smaller and smaller positive integers. Hence the process needs to terminate at some point, or we reach a contradiction.

**Lemma 3.** *If $N$ is an integer of the form $N = a^2+b^2$ for some $(a,b) = 1$ and $q = x^2+y^2$ is a* prime *divisor of $N$, then there exist relatively prime integers $c$ and $d$ such that $N/q = c^2+d^2$.*

*Proof.* First note that since $q$ has no trivial divisors, $x$ and $y$ are forced to be relatively prime. We have

$$x^2N - a^2q = x^2(a^2+b^2) - a^2(x^2+y^2) = x^2b^2 - a^2y^2 = (xb-ay)(xb+ay).$$

Since $q \mid N$, it follows that $x^2N - a^2q \equiv 0 \pmod q$, and so

$$(xb-ay)(xb+ay) \equiv 0 \pmod q.$$

Since $q$ is a prime, this can happen only if one of the factors is divisible by $q$. Since we can change the sign of $a$ without affecting our theorem, we can assume that $q \mid xb-ay$, that is $xb - ay = dq$ for some integer $d$.

We would like to show that $x \mid a+dy$. Since $(x,y) = 1$, this is equivalent to showing that $x \mid y(a+dy)$. But

$$y(a+dy) = ay + dy^2 = xb - dq + dy^2 = xb - d(x^2+y^2) + dy^2 = xb - dx^2$$

which is divisible by $x$. Thus $x \mid a+dy$, so there exist an integer $c$ such that $a + dy = cx$. Therefore

$$cxy = (a + dy)y = xb - dx^2 = x(b - dx)$$

and so

$$cy + dx = b.$$

Next we see that

$$N = a^2 + b^2 = (cx - dy)^2 + (cy + dx)^2 = (x^2 + y^2)(c^2 + d^2) = q(c^2 + d^2).$$

Since $(a, b) = 1$ it follows that $(c, d) = 1$ and the proof is complete. □

And now for the actual descent step, assume that we have an odd prime $p$ (and thus $p > 2$) that divides a number $M$ of the form $M = a^2 + b^2$ with $(a, b) = 1$. We want to show that $p \equiv 1 \pmod 4$.

First, note that we can add or subtract any multiple of $p$ from $a$ or $b$ without changing the problem. That is, we can find integers $a_1, b_1$ with $|a_1|, |b_1| < p/2$ such that $p|N_1 = a_1^2 + b_1^2$. In particular, $N_1 < p^2/2$. Denote $d = (a_1, b_1)$ Then $d < p/2$, so $p \nmid d$. We also know that $a_1 = da_2, b_1 = db_2$ and $(a_2, b_2) = 1$. Note that $|a_2| \leq |a_1| < p/2$ and likewise $|b_2| < p/2$. Therefore $N_2 = a_2^2 + b_2^2 < p^2/2$.

We have

$$p \mid a_1^2 + b_1^2 = d^2(a_2^2 + b_2^2).$$

Since $p$ is a prime that does not divide $d$, it follows that $p|N_2 = a_2^2 + b_2^2$.

So we showed that our prime $p$ has to divide a number $M = u^2 + v^2 < p^2/2$ with $(u, v) = 1$ and $|u|, |v| < p/2$. The positive integer $m = M/p$ will have to be $m < p/2$.

Let $q$ be a *prime* divisor of $m$. Clearly $q \neq p$ since $q \leq m < p/2$. In particular $q < p$ and $p \mid \frac{M}{q}$.

Assume that $q$ can be written as the sum of two squares. By Lemma 3, we have $M/q = x^2 + y^2$ for some integers $(x, y) = 1$. But then $p \mid x^2 + y^2 < u^2 + v^2 = M$.

So if all the prime factors of $M$ different from $p$ can be written as sums of two squares, then so can $p$. Since we assumed that this is not the case, it follows that $M$ has some prime divisor $p_1 < p$ that cannot be written as the sum of two squares. By repeating the argument for $p_1$ it follows that there must exist another prime $p_2 < p_1$ that cannot be written as the sum of two squares. This argument cannot continue indefinitely, so at some point we are bound to hit the prime number $5 = 2^2 + 1^2$ which **can** obviously be written as the sum of two squares. The descent step is now proven and this completes the proof of Theorem 1.

Note that we implicitly used the fact that if $(x, y) = 1$ then $3 \nmid x^2 + y^2$. To see this, recall that for any integer $x$ we have $x \equiv 0, 1$ or $-1 \pmod 3$, so $x^2 \equiv 0$ or $1 \pmod 3$. Since $(x, y) = 1$ we cannot have $x^2 \equiv y^2 \equiv 0 \pmod 3$, so $x^2 + y^2 \not\equiv 0 \pmod 3$.