Integers that can be written as the sum of two squares

Theorem (Fermat). *Every prime of the form $4k+1$ is the sum of two squares. A positive integer n is the sum of two squares if and only if all prime factors of the form $4k-1$ have an even exponent in the prime-factorization of n.*

Remark. Fermat's proof using *infinite descent* was not complete. Euler completed the proof (almost 100 years later).

Proof steps:

Let $S := \{a^2 + b^2 : a, b \in \mathbb{Z}\}$.

1. If $a \equiv 3 \pmod 4$, then $a \notin S$.

2. If $a, b \in S$, then $ab \in S$.

3. [The crux of the proof] If $gcd(a, b) = 1$ (co-primes), then all positive divisors of $a^2 + b^2$ are in S.

4. [Wilson's Theorem] If p is prime then $(p-1)! \equiv -1 \pmod p$

5. If p is prime and $p = 4k + 1$ for some $k \in \mathbb{Z}$, then
   (a) p divides $[(2k)!]^2 + 1$.
   (b) [Fermat's Theorem] $p \in S$.

6. $n \in \mathbb{Z}^+$ is in S if and only if all prime factors of the form $4k-1$ have an even exponent in the prime-factorization of N.

Proofs

Proof of Part 1: trivial mod 4 arithmetic.

Proof of Part 2: $(a^2 + b^2)(u^2 + v^2) = (au - bv)^2 + (av + bu)^2$.
[Pythagorean theorem for $\alpha\beta$, where $\alpha = a + ib$ and $\beta = u + iv$.]

The proof of Part 3 is long (see the LBB); it uses the Pigeonhole Principle.

Proof of Part 4: see *Wilson's theorem and Fermat's "little theorem"* (and the FROGS HW).

Proof of Part 5a: follows from Wilson's Theorem.

Proof of Part 5b: follows from Parts 5a and 3.

Proof of Part 6: indeed, Part 3 said: If $n = a^2 + b^2$ with co-prime a, b, then n has no divisor (hence no prime factor) of the form $4k-1$. Now, for a general $n = a^2 + b^2$, separate the square and the square-free parts of n.

Homework: Prove that if $n \in S$ and $n = ab$ with a and b relatively prime (coprime), then both a and b are in S too.

Remark. Just as in part 1, mod 8 arithmetic shows that not all positive integers are the sum of three squares. In fact (Gauss), n is *not* the sum of three squares iff $n = 4^k m$ with $m \equiv 7 \pmod 8$ – but the only if part is not easy. However, the following theorem of Lagrange (already conjectured by Fermat) is much easier:

Lagrange's Four Square Theorem (1770): *every positive integer can be written as the sum of four squares* (of integers).

And here are two theorems for the number theory connoisseur:

Jacobi's Two Square Theorem: The number of representations of a positive integer as the sum of two squares is equal to four times the difference of the numbers of divisors congruent to 1 and 3 modulo 4.

Jacobi's Four Square Theorem: The number of representations of a positive integer as the sum of four squares is equal to eight times the sum of all its divisors which are not divisible by 4.