

Sums of two and four squares

Roelof Oosterhuis
University of Groningen

August 21, 2007

Abstract

This document gives the formal proofs, verified by the proof assistant ‘Isabelle’¹, of the following results about the sums of two and four squares:

1. Any prime number $p \equiv 1 \pmod{4}$ can be written as the sum of two squares.
2. (Lagrange) Any natural number can be written as the sum of four squares.

The proofs are largely based on chapter II and III of André Weil, *Number theory: an approach through history; From Hammurapi to Legendre*. Boston (etc.): Birkhäuser, 1983.

We remind the reader that the results have been formalised before in the proof assistant HOL-light². A more complete study of the sum of two squares, including the first result, has been formalised in ‘Coq’³. Moreover it should be mentioned that the results can be found as numbers 20 and 19 on the list of ‘top 100 mathematical theorems’.⁴

This research is part of a M.Sc. thesis under supervision of Jaap Top and Wim H. Hesselink (RU Groningen).

More information: <http://www.roelofosterhuis.nl/MScthesis.pdf>

¹See <http://isabelle.in.tum.de/>

²See <http://www.cl.cam.ac.uk/~jrh13/hol-light/>

³See <http://coq.inria.fr/contribs/SumOfTwoSquare.html>

⁴See <http://www.cs.ru.nl/~freek/100/>

Contents

- 1 Sums of two squares 3
- 2 Lagrange's four-square theorem 3

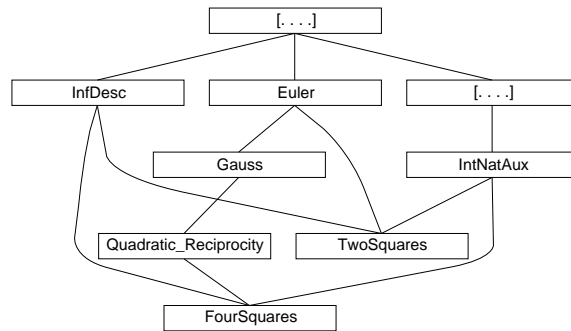


Figure 1: The dependence on existing files in the Isabelle library.

1 Sums of two squares

theory *TwoSquares*

imports *IntNatAux InfDesc*

~/src/HOL/NumberTheory/Euler

begin

Show that $\left(\frac{-1}{p}\right) = +1$ for primes $p \equiv 1 \pmod{4}$.

constdefs

sum2sq :: *int* × *int* ⇒ *int*

sum2sq == $\lambda(a,b). a^2 + b^2$

is-sum2sq :: *int* ⇒ *bool*

is-sum2sq *x* == $\exists a b. \text{sum2sq}(a,b) = x$

lemma *mult-sum2sq*: $\text{sum2sq}(a,b) * \text{sum2sq}(p,q) =$

$\text{sum2sq}(a*p+b*q, a*q-b*p)$

<proof>

lemma *is-mult-sum2sq*: $\text{is-sum2sq } x \implies \text{is-sum2sq } y \implies \text{is-sum2sq } (x*y)$

<proof>

lemma *Legendre-1mod4*: $\text{zprime } (4*m+1) \implies (\text{Legendre } (-1) (4*m+1)) = 1$

<proof>

Use this to prove that such primes can be written as the sum of two squares.

lemma *qf1-prime-exists*: $\text{zprime } (4*m+1) \implies \exists x y. x^2 + y^2 = 4*m+1$

<proof>

end

2 Lagrange's four-square theorem

theory *FourSquares*

imports *IntNatAux InfDesc*

~/src/HOL/NumberTheory/Quadratic-Reciprocity

begin

Shows that all nonnegative integers can be written as the sum of four squares. The proof consists of the following steps:

- For every prime $p = 2n + 1$ the two sets of residue classes

$$\{x^2 \pmod{p} \mid 0 \leq x \leq n\} \text{ and } \{-1 - y^2 \pmod{p} \mid 0 \leq y \leq n\}$$

both contain $n + 1$ different elements and therefore they must have at least one element in common.

- Hence there exist x, y such that $x^2 + y^2 + 1^2 + 0^2$ is a multiple of p .
- The next step is to show, by an infinite descent, that p itself can be written as the sum of four squares.

- Finally, using the multiplicity of this form, the same holds for all positive numbers.

constdefs

$sum4sq :: int \times int \times int \times int \Rightarrow int$
 $sum4sq == \lambda(a,b,c,d). a^2+b^2+c^2+d^2$

$is-sum4sq :: int \Rightarrow bool$
 $is-sum4sq x == \exists a b c d. sum4sq(a,b,c,d) = x$

lemma *mult-sum4sq*: $sum4sq(a,b,c,d) * sum4sq(p,q,r,s) =$
 $sum4sq(a*p+b*q+c*r+d*s, a*q-b*p-c*s+d*r,$
 $a*r+b*s-c*p-d*q, a*s-b*r+c*q-d*p)$
 ⟨proof⟩

lemma *is-mult-sum4sq*: $is-sum4sq x \Longrightarrow is-sum4sq y \Longrightarrow is-sum4sq (x*y)$
 ⟨proof⟩

lemma *mult-oddprime-is-sum4sq*: $\llbracket zprime p; p \in zOdd \rrbracket \Longrightarrow$
 $\exists t. 0 < t \wedge t < p \wedge is-sum4sq (p*t)$
 ⟨proof⟩

lemma *zprime-is-sum4sq*: $zprime p \Longrightarrow is-sum4sq p$
 ⟨proof⟩

theorem *four-squares*: $(n::int) \geq 0 \Longrightarrow \exists a b c d. a^2 + b^2 + c^2 + d^2 = n$
 ⟨proof⟩

end