

Exponents 3 and 4 of Fermat's Last Theorem and the Parametrisation of Pythagorean Triples

Roelof Oosterhuis
University of Groningen

December 12, 2009

Abstract

This document gives a formal proof of the cases $n = 3$ and $n = 4$ (and all their multiples) of Fermat's Last Theorem: if $n > 2$ then for all integers x, y, z :

$$x^n + y^n = z^n \implies xyz = 0.$$

Both proofs only use facts about the integers and are developed along the lines of the standard proofs (see, for example, sections 1 and 2 of the book by Edwards [Edw77]).

First, the framework of 'infinite descent' is being formalised and in both proofs there is a central role for the lemma

$$\gcd(a, b) = 1 \wedge ab = c^n \implies \exists k : |a| = k^n.$$

Furthermore, the proof of the case $n = 4$ uses a parametrisation of the Pythagorean triples. The proof of the case $n = 3$ contains a study of the quadratic form $x^2 + 3y^2$. This study is completed with a result on which prime numbers can be written as $x^2 + 3y^2$.

The case $n = 4$ of FLT, in contrast to the case $n = 3$, has already been formalised (in the proof assistant Coq) [DM05]. The parametrisation of the Pythagorean Triples can be found as number 23 on the list of 'top 100 mathematical theorems' [Wie].

This research is part of an M.Sc. thesis under supervision of Jaap Top and Wim H. Hesselink (RU Groningen). The author wants to thank Clemens Ballarin (TU München) and Freek Wiedijk (RU Nijmegen) for their support. For more information see [Oos07].

Contents

1	Powers, prime numbers and divisibility	3
1.1	Auxiliary results	3
1.2	Parity of integers	4
1.3	Powers of natural numbers	4
1.4	Powers of integers	5
1.5	Facts about small powers of integers	6
2	Pythagorean triples and Fermat's last theorem, case $n = 4$	7
2.1	Parametrisation of Pythagorean triples (over \mathbb{N} and \mathbb{Z})	7
2.2	Fermat's last theorem, case $n = 4$	7
3	The quadratic form $x^2 + Ny^2$	8
3.1	Definitions and auxiliary results	8
3.2	Basic facts if $N \geq 1$	8
3.3	Multiplication and division	9
3.4	Uniqueness ($N > 1$)	10
3.5	The case $N = 3$	10
3.6	Existence ($N = 3$)	11
4	Fermat's last theorem, case $n = 3$	11

1 Powers, prime numbers and divisibility

theory *IntNatAux*

imports

~~/src/HOL/Number-Theory/Factorization

~~/src/HOL/Number-Theory/EvenOdd

begin

Contains lemmas about divisibility and coprimality of powers, as well as some results about parities and small powers. Most lemmas are developed for the integers as well as for the natural numbers.

1.1 Auxiliary results

lemma *make-relprime*:

$(a \neq 0 \vee b \neq 0) \implies \exists c d. a = \text{gcd } a b * c \wedge b = \text{gcd } a b * d \wedge \text{gcd } c d = 1$
 $\langle \text{proof} \rangle$

lemma *factor-exists-general*: $(a::\text{nat}) \neq 0 \implies (\exists ps. \text{primel } ps \wedge \text{prod } ps = a)$

$\langle \text{proof} \rangle$

lemma *make-zrelprime*: $(a \neq 0 \vee b \neq 0)$

$\implies \exists c d. a = \text{zgcd } a b * c \wedge b = \text{zgcd } a b * d \wedge \text{zgcd } c d = 1$
 $\langle \text{proof} \rangle$

lemma *int-nat-abs-eq-abs*: $\text{int}(\text{nat}|x::\text{int}|) = |x|$

$\langle \text{proof} \rangle$

lemma *prime-impl-zprime-int*: $\text{prime } (a::\text{nat}) \implies \text{zprime } (\text{int } a)$

$\langle \text{proof} \rangle$

lemma *zprime-factor-exists*: $(a::\text{int}) > 1 \implies \exists p. \text{zprime } p \wedge p \text{ dvd } a$

$\langle \text{proof} \rangle$

lemma *best-division-abs*: $(x::\text{int}) > 0 \implies \exists n. 2 * |y - n*x| \leq x$

$\langle \text{proof} \rangle$

lemma *best-odd-division-abs*: $\llbracket (x::\text{int}) > 0; x \in \text{zOdd} \rrbracket$

$\implies \exists n. 2 * |y - n*x| < x$
 $\langle \text{proof} \rangle$

lemma *zprime-2*: $\text{zprime } 2$

$\langle \text{proof} \rangle$

lemma *zgcd1-iff-no-common-primedivisor*:

$(\text{zgcd } a b = 1) = (\neg(\exists p. \text{zprime } p \wedge p \text{ dvd } a \wedge p \text{ dvd } b))$
 $\langle \text{proof} \rangle$

lemma *pos-zmult-pos*: $a > (0::\text{int}) \implies a*b > 0 \implies b > 0$

$\langle \text{proof} \rangle$

1.2 Parity of integers

lemma *power-preserves-even*: $n > 0 \implies (x^n \in zEven) = (x \in zEven)$
 ⟨proof⟩

lemma *power-preserves-odd*: $n > 0 \implies (x^n \in zOdd) = (x \in zOdd)$
 ⟨proof⟩

lemma *even-plus-odd*: $a \in zEven \implies b \in zOdd \implies a+b \in zOdd$
 ⟨proof⟩

lemma *odd-plus-odd*: $a \in zOdd \implies b \in zOdd \implies a+b \in zEven$
 ⟨proof⟩

lemma *even-plus-odd-prop1*: $a+b \in zOdd \implies a \in zOdd \implies b \in zEven$
 ⟨proof⟩

lemma *even-plus-odd-prop2*: $a+b \in zOdd \implies a \in zEven \implies b \in zOdd$
 ⟨proof⟩

1.3 Powers of natural numbers

lemma *gcd-1-power-left-distrib*: $gcd\ a\ b = 1 \implies gcd\ (a^n)\ b = 1$
 ⟨proof⟩

NB: the next (identical) lemma is just added to illustrate the difference between Isar and Isabelle scripting.

lemma *alternative-gcd-1-power-left-distrib*: $gcd\ a\ b = 1 \implies gcd(a^n)\ b = 1$
 ⟨proof⟩

lemma *gcd-1-power-distrib*: $gcd\ a\ b = 1 \implies gcd(a^n)\ (b^n) = 1$
 ⟨proof⟩

lemma *gcd-power-distrib*: $gcd\ a\ b^n = gcd\ (a^n)\ (b^n)$
 ⟨proof⟩

Useful lemma: if prime $p|a^n$ then $p|a$.

lemma *prime-dvd-power*: $\llbracket \text{prime } p; p\ dvd\ a^n \rrbracket \implies p\ dvd\ a$
 ⟨proof⟩

lemma *prime-power-dvd-cancel-right*:
 $\llbracket \text{prime } p; \neg p\ dvd\ b; p^n\ dvd\ a*b \rrbracket \implies p^n\ dvd\ a$
 ⟨proof⟩

Helping lemma: if $n > 0$ then $a^n|b^n \iff a|b$.

lemma *nat-power-dvd-mono*: $n \neq 0 \implies (a^n\ dvd\ b^n) = (a\ dvd\ (b::nat))$
 ⟨proof⟩

Theorem: if $n > 0$ and $gcd\ ab = 1$ and $ab = c^n$ then $\exists k : a = k^n$. Proof uses induction on the number of prime factors of c .

theorem *nat-relprime-power-divisors*:

assumes *npos*: $n \neq 0$ **and** *abcn*: $a*b = c^n$ **and** *relprime*: $gcd\ a\ b = 1$

shows $\exists k. a = k^n$
 ⟨proof⟩

1.4 Powers of integers

Now turn to the case of integers. This lemma is based on its equivalent for the natural numbers.

corollary *int-relprime-power-divisors*:

assumes $abcn: a*b = c^n$ **and** $n: n > 1$ **and** *relprime*: $zgcd\ a\ b = 1$

shows $\exists k. |a| = k^n$

⟨proof⟩

corollary *int-triple-relprime-power-divisors*:

$\llbracket a*b*c = d^n; n > 1; zgcd\ a\ b = 1; zgcd\ b\ c = 1; zgcd\ c\ a = 1 \rrbracket$

$\implies \exists k\ l\ m. |a| = k^n \wedge |b| = l^n \wedge |c| = m^n$

⟨proof⟩

lemma *neg-odd-power*: $\llbracket x \in zOdd; x \geq 0 \rrbracket \implies (-a::int)^{(nat\ x)} = -(a^{(nat\ x)})$

⟨proof⟩

lemma *neg-even-power*: $\llbracket x \in zEven; x \geq 0 \rrbracket \implies (-a::int)^{(nat\ x)} = a^{(nat\ x)}$

⟨proof⟩

corollary *int-relprime-odd-power-divisors*:

$\llbracket a*b = c^{(nat\ x)}; nat\ x > 1; x \in zOdd; zgcd\ a\ b = 1 \rrbracket \implies \exists k. a = k^{(nat\ x)}$

⟨proof⟩

corollary *int-triple-relprime-odd-power-divisors*:

$\llbracket a*b*c = d^{(nat\ x)}; nat\ x > 1; x \in zOdd; zgcd\ a\ b = 1; zgcd\ b\ c = 1; zgcd\ c\ a = 1 \rrbracket$

$\implies \exists k\ l\ m. a = k^{(nat\ x)} \wedge b = l^{(nat\ x)} \wedge c = m^{(nat\ x)}$

⟨proof⟩

lemma *zgcd-1-power-left-distrib*: $zgcd\ a\ b = 1 \implies zgcd\ (a^n)\ b = 1$

⟨proof⟩

lemma *zgcd-1-power-distrib*: $zgcd\ a\ b = 1 \implies zgcd\ (a^n)\ (b^n) = 1$

⟨proof⟩

lemma *zgcd-power-distrib*: $zgcd\ a\ b^n = zgcd\ (a^n)\ (b^n)$

⟨proof⟩

lemma *zprime-zdvd-zmult-general*: $\llbracket zprime\ p; p\ dvd\ m*n \rrbracket \implies p\ dvd\ m \vee p\ dvd\ n$

⟨proof⟩

lemma *zprime-zdvd-power*: $\llbracket zprime\ p; p\ dvd\ a^n \rrbracket \implies p\ dvd\ a$

⟨proof⟩

lemma *zpower-zdvd-mono*: $n \neq 0 \implies (a^n\ dvd\ b^n) = (a\ dvd\ (b::int))$

⟨proof⟩

lemma *zprime-power-zdvd-cancel-right*:

$\llbracket \text{zprime } p; \neg p \text{ dvd } b; p^{\wedge} n \text{ dvd } a * b \rrbracket \implies p^{\wedge} n \text{ dvd } a$
 $\langle \text{proof} \rangle$

lemma *zprime-power-zdvd-cancel-left*:

$\llbracket \text{zprime } p; \neg p \text{ dvd } a; p^{\wedge} n \text{ dvd } a * b \rrbracket \implies p^{\wedge} n \text{ dvd } b$
 $\langle \text{proof} \rangle$

1.5 Facts about small powers of integers

lemma *zadd-power2*: $((a::\text{int})+b)^{\wedge} 2 = a^{\wedge} 2 + 2*a*b + b^{\wedge} 2$
 $\langle \text{proof} \rangle$

lemma *zdifff-power2*: $((a::\text{int})-b)^{\wedge} 2 = a^{\wedge} 2 - 2*a*b + b^{\wedge} 2$
 $\langle \text{proof} \rangle$

lemma *zspecial-product*: $((a::\text{int}) + b) * (a - b) = a^{\wedge} 2 - b^{\wedge} 2$
 $\langle \text{proof} \rangle$

lemma *abs-power2-distrib*: $|a^{\wedge} 2| = |a::\text{int}|^{\wedge} 2$
 $\langle \text{proof} \rangle$

lemma *power2-eq-iff-abs-eq*: $((a::\text{int})^{\wedge} 2 = b^{\wedge} 2) = (|a| = |b|)$
 $\langle \text{proof} \rangle$

lemma *power2-eq1-iff*: $(a::\text{int})^{\wedge} 2 = 1 \implies |a|=1$
 $\langle \text{proof} \rangle$

lemma *zadd-power3*: $((a::\text{int})+b)^{\wedge} 3 = a^{\wedge} 3 + 3*a^{\wedge} 2*b + 3*a*b^{\wedge} 2 + b^{\wedge} 3$
 $\langle \text{proof} \rangle$

lemma *zdifff-power3*: $((a::\text{int})-b)^{\wedge} 3 = a^{\wedge} 3 - 3*a^{\wedge} 2*b + 3*a*b^{\wedge} 2 - b^{\wedge} 3$
 $\langle \text{proof} \rangle$

lemma *power3-minus*: $(-a::\text{int})^{\wedge} 3 = -(a^{\wedge} 3)$
 $\langle \text{proof} \rangle$

lemma *abs-power3-distrib*: $|(x::\text{int})^{\wedge} 3| = |x|^{\wedge} 3$
 $\langle \text{proof} \rangle$

lemma *cube-square*: $(a::\text{int}) * a^{\wedge} 2 = a^{\wedge} 3$
 $\langle \text{proof} \rangle$

lemma *quartic-square-square*: $(x^{\wedge} 2)^{\wedge} 2 = (x::\text{int})^{\wedge} 4$
 $\langle \text{proof} \rangle$

lemma *power2-ge-self*: $x^{\wedge} 2 \geq (x::\text{int})$
 $\langle \text{proof} \rangle$

end

2 Pythagorean triples and Fermat's last theorem, case $n = 4$

theory *Fermat4*
imports *IntNatAux Parity*
begin

Proof of Fermat's last theorem for the case $n = 4$:

$$\forall x, y, z : x^4 + y^4 = z^4 \implies xyz = 0.$$

lemma *even-eq-two-dvd*: $\text{even } (r::\text{nat}) = (2 \text{ dvd } r)$ *<proof>*

lemma *nat-power2-add*: $((a::\text{nat})+b)^2 = a^2 + b^2 + 2*a*b$ *<proof>*

lemma *nat-power2-diff*: $a \geq (b::\text{nat}) \implies (a-b)^2 = a^2 + b^2 - 2*a*b$
<proof>

lemma *nat-power-le-imp-le-base*: $\llbracket n \neq 0; a^n \leq b^n \rrbracket \implies (a::\text{nat}) \leq b$
<proof>

lemma *nat-power-inject-base*: $\llbracket n \neq 0; a^n = b^n \rrbracket \implies (a::\text{nat}) = b$
<proof>

2.1 Parametrisation of Pythagorean triples (over \mathbb{N} and \mathbb{Z})

theorem *nat-euclid-pyth-triples*:

assumes *abc*: $a^2 + b^2 = c^2$ **and** *ab-relprime*: $\text{gcd } a \ b = 1$ **and** *aodd*: $\text{odd } a$
shows $\exists p \ q. a = p^2 - q^2 \wedge b = 2*p*q \wedge c = p^2 + q^2 \wedge \text{gcd } p \ q = 1$
<proof>

Now for the case of integers. Based on *nat-euclid-pyth-triples*.

corollary *int-euclid-pyth-triples*: $\llbracket \text{zgcd } a \ b = 1; a \in \text{zOdd}; a^2 + b^2 = c^2 \rrbracket$
 $\implies \exists p \ q. a = p^2 - q^2 \wedge b = 2*p*q \wedge |c| = p^2 + q^2 \wedge \text{zgcd } p \ q = 1$
<proof>

2.2 Fermat's last theorem, case $n = 4$

Core of the proof. Constructs a smaller solution over \mathbb{Z} of

$$a^4 + b^4 = c^2 \wedge \text{gcd } ab = 1 \wedge abc \neq 0 \wedge a \text{ odd.}$$

lemma *smaller-fermat4*:

assumes *abc*: $a^4 + b^4 = c^2$ **and** *abc0*: $a*b*c \neq 0$ **and** *aodd*: $a \in \text{zOdd}$
and *ab-relprime*: $\text{zgcd } a \ b = 1$
shows
 $\exists p \ q \ r. (p^4 + q^4 = r^2 \wedge p*q*r \neq 0 \wedge p \in \text{zOdd} \wedge \text{zgcd } p \ q = 1 \wedge r^2 < c^2)$
<proof>

Show that no solution exists, by infinite descent of c^2 .

lemma *no-rewritten-fermat4*:

$\neg (\exists a b. (a^4 + b^4 = c^2 \wedge a*b*c \neq 0 \wedge a \in zOdd \wedge zgcd a b=1))$
 <proof>

The theorem. Puts equation in requested shape.

theorem *fermat4*:
assumes *ass*: $(x::int)^4 + y^4 = z^4$
shows $x*y*z=0$
 <proof>

corollary *fermat-mult4*:
assumes *xyz*: $(x::int)^n + y^n = z^n$ **and** *n*: $4 \text{ dvd } n$
shows $x*y*z=0$
 <proof>

end

3 The quadratic form $x^2 + Ny^2$

theory *QuadForm*
imports
 ~~/src/HOL/Number-Theory/Quadratic-Reciprocity
 IntNatAux
begin

Shows some properties of the quadratic form $x^2 + Ny^2$, such as how to multiply and divide them. The second part focuses on the case $N = 3$ and is used in the proof of the case $n = 3$ of Fermat's last theorem. The last part – not used for FLT3 – shows which primes can be written as $x^2 + 3y^2$.

3.1 Definitions and auxiliary results

definition
is-qn :: $int \Rightarrow int \Rightarrow bool$ **where**
is-qn *A N* $\longleftrightarrow (\exists x y. A = x^2 + N*y^2)$

definition
is-cube-form :: $int \Rightarrow int \Rightarrow bool$ **where**
is-cube-form *a b* $\longleftrightarrow (\exists p q. a = p^3 - 9*p*q^2 \wedge b = 3*p^2*q - 3*q^3)$

lemma *abs-eq-impl-unitfactor*: $|a::int| = |b| \Longrightarrow \exists u. a = u*b \wedge |u|=1$
 <proof>

lemma *zprime-3*: *zprime* 3
 <proof>

3.2 Basic facts if $N \geq 1$

lemma *qn-pos*: $\llbracket N \geq 1; \text{is-qn } A N \rrbracket \Longrightarrow A \geq 0$
 <proof>

lemma *qn-zero*: $\llbracket (N::int) \geq 1; a^2 + N*b^2 = 0 \rrbracket \Longrightarrow (a = 0 \wedge b = 0)$

$\langle proof \rangle$

3.3 Multiplication and division

lemma *qfN-mult1*: $((a::int)^2 + N*b^2)*(c^2 + N*d^2)$
 $= (a*c+N*b*d)^2 + N*(a*d-b*c)^2$
 $\langle proof \rangle$

lemma *qfN-mult2*: $((a::int)^2 + N*b^2)*(c^2 + N*d^2)$
 $= (a*c-N*b*d)^2 + N*(a*d+b*c)^2$
 $\langle proof \rangle$

corollary *is-qfN-mult*: $is-qfN A N \implies is-qfN B N \implies is-qfN (A*B) N$
 $\langle proof \rangle$

corollary *is-qfN-power*: $(n::nat) > 0 \implies is-qfN A N \implies is-qfN (A^n) N$
 $\langle proof \rangle$

lemma *qfN-div-prime*:

assumes *ass*: $zprime (p^2+N*q^2) \wedge (p^2+N*q^2) \text{ dvd } (a^2+N*b^2)$
shows $\exists u v. a^2+N*b^2 = (u^2+N*v^2)*(p^2+N*q^2)$
 $\wedge (\exists e. a = p*u+e*N*q*v \wedge b = p*v - e*q*u \wedge |e|=1)$

$\langle proof \rangle$

corollary *qfN-div-prime-weak*:

$\llbracket zprime (p^2+N*q^2); (p^2+N*q^2) \text{ dvd } (a^2+N*b^2) \rrbracket$
 $\implies \exists u v. a^2+N*b^2 = (u^2+N*v^2)*(p^2+N*q^2)$
 $\langle proof \rangle$

corollary *qfN-div-prime-general*: $\llbracket zprime P; P \text{ dvd } A; is-qfN A N; is-qfN P N \rrbracket$
 $\implies \exists Q. A = Q*P \wedge is-qfN Q N$
 $\langle proof \rangle$

lemma *qfN-power-div-prime*:

assumes *ass*: $zprime P \wedge P \in zOdd \wedge P \text{ dvd } A \wedge P^n = p^2+N*q^2$
 $\wedge A^n = a^2+N*b^2 \wedge zgcd a b=1 \wedge zgcd p (N*q) = 1 \wedge n>0$
shows $\exists u v. a^2+N*b^2 = (u^2 + N*v^2)*(p^2+N*q^2) \wedge zgcd u v=1$
 $\wedge (\exists e. a = p*u+e*N*q*v \wedge b = p*v-e*q*u \wedge |e| = 1)$

$\langle proof \rangle$

lemma *qfN-primedivisor-not*:

assumes *ass*: $zprime P \wedge Q > 0 \wedge is-qfN (P*Q) N \wedge \neg is-qfN P N$
shows $\exists R. (zprime R \wedge R \text{ dvd } Q \wedge \neg is-qfN R N)$

$\langle proof \rangle$

lemma *qfN-oddprime-cube*:

$\llbracket zprime (p^2+N*q^2); (p^2+N*q^2) \in zOdd; p \neq 0; N \geq 1 \rrbracket$
 $\implies \exists a b. (p^2+N*q^2)^3 = a^2 + N*b^2 \wedge zgcd a (N*b)=1$

$\langle proof \rangle$

3.4 Uniqueness ($N > 1$)

lemma *qfN-prime-unique*:

$\llbracket \text{zprime } (a^2 + N*b^2); N > 1; a^2 + N*b^2 = c^2 + N*d^2 \rrbracket$
 $\implies (|a| = |c| \wedge |b| = |d|)$

$\langle \text{proof} \rangle$

lemma *qfN-square-prime*:

assumes *ass*:

$\text{zprime } (p^2 + N*q^2) \wedge N > 1 \wedge (p^2 + N*q^2)^2 = r^2 + N*s^2 \wedge \text{zgcd } r\ s = 1$

shows $|r| = |p^2 - N*q^2| \wedge |s| = |2*p*q|$

$\langle \text{proof} \rangle$

lemma *qfN-cube-prime*:

assumes *ass*: $\text{zprime } (p^2 + N*q^2) \wedge N > 1$

$\wedge (p^2 + N*q^2)^3 = a^2 + N*b^2 \wedge \text{zgcd } a\ b = 1$

shows $|a| = |p^3 - 3*N*p*q^2| \wedge |b| = |3*p^2*q - N*q^3|$

$\langle \text{proof} \rangle$

3.5 The case $N = 3$

lemma *qf3-even*: $a^2 + 3*b^2 \in \text{zEven} \implies \exists B. a^2 + 3*b^2 = 4*B \wedge \text{is-qfN } B\ 3$

$\langle \text{proof} \rangle$

lemma *qf3-even-general*: $\llbracket \text{is-qfN } A\ 3; A \in \text{zEven} \rrbracket$

$\implies \exists B. A = 4*B \wedge \text{is-qfN } B\ 3$

$\langle \text{proof} \rangle$

lemma *qf3-oddprimedivisor-not*:

assumes *ass*: $\text{zprime } P \wedge P \in \text{zOdd} \wedge Q > 0 \wedge \text{is-qfN } (P*Q)\ 3 \wedge \neg \text{is-qfN } P\ 3$

shows $\exists R. \text{zprime } R \wedge R \in \text{zOdd} \wedge R \text{ dvd } Q \wedge \neg \text{is-qfN } R\ 3$

$\langle \text{proof} \rangle$

lemma *qf3-oddprimedivisor*:

$\llbracket \text{zprime } P; P \in \text{zOdd}; \text{zgcd } a\ b = 1; P \text{ dvd } (a^2 + 3*b^2) \rrbracket$

$\implies \text{is-qfN } P\ 3$

$\langle \text{proof} \rangle$

lemma *qf3-cube-prime-impl-cube-form*:

assumes *ab-relprime*: $\text{zgcd } a\ b = 1$ **and** *abP*: $P^3 = a^2 + 3*b^2$

and *P*: $\text{zprime } P \wedge P \in \text{zOdd}$

shows *is-cube-form* $a\ b$

$\langle \text{proof} \rangle$

lemma *cube-form-mult*: $\llbracket \text{is-cube-form } a\ b; \text{is-cube-form } c\ d; |e| = 1 \rrbracket$

$\implies \text{is-cube-form } (a*c + e*3*b*d)\ (a*d - e*b*c)$

$\langle \text{proof} \rangle$

lemma *qf3-cube-primelist-impl-cube-form*: $\llbracket \text{primel } ps; \text{int } (\text{prod } ps) \in \text{zOdd} \rrbracket \implies$

$(\forall a\ b. \text{zgcd } a\ b = 1 \implies a^2 + 3*b^2 = (\text{int } (\text{prod } ps))^3 \implies \text{is-cube-form } a\ b)$

$\langle \text{proof} \rangle$

lemma *qf3-cube-impl-cube-form*:

assumes *ass*: $zgcd\ a\ b=1 \wedge a^2 + 3*b^2 = w^3 \wedge w \in zOdd$

shows *is-cube-form a b*

<proof>

3.6 Existence ($N = 3$)

This part contains the proof that all prime numbers $\equiv 1 \pmod{6}$ can be written as $x^2 + 3y^2$.

First show $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, where p is an odd prime.

lemma *Legendre-zmult*: $\llbracket p > 2; zprime\ p \rrbracket$

$\implies (Legendre\ (a*b)\ p) = (Legendre\ a\ p)*(Legendre\ b\ p)$

<proof>

Now show $\left(\frac{-3}{p}\right) = +1$ for primes $p \equiv 1 \pmod{6}$.

lemma *Legendre-1mod6*: $zprime\ (6*m+1) \implies Legendre\ (-3)\ (6*m+1) = 1$

<proof>

Use this to prove that such primes can be written as $x^2 + 3y^2$.

lemma *qf3-prime-exists*: $zprime\ (6*m+1) \implies \exists\ x\ y.\ 6*m+1 = x^2 + 3*y^2$

<proof>

end

4 Fermat's last theorem, case $n = 3$

theory *Fermat3*

imports *QuadForm*

begin

Proof of Fermat's last theorem for the case $n = 3$:

$$\forall x, y, z : x^3 + y^3 = z^3 \implies xyz = 0.$$

lemma *factor-sum-cubes*: $(x::int)^3 + y^3 = (x+y)*(x^2 - x*y + y^2)$

<proof>

lemma *two-not-abs-cube*: $|x^3| = (2::int) \implies False$

<proof>

Shows there exists no solution $v^3 + w^3 = x^3$ with $vwx \neq 0$ and $\gcd(v, w) = 1$ and x even, by constructing a solution with a smaller $|x^3|$.

lemma *no-rewritten-fermat3*:

$\neg (\exists\ v\ w.\ v^3 + w^3 = x^3 \wedge v*w*x \neq 0 \wedge x \in zEven \wedge zgcd\ v\ w=1)$

<proof>

The theorem. Puts equation in requested shape.

theorem *fermat3*:

assumes *ass*: $(x::int)^3 + y^3 = z^3$

shows $x*y*z=0$
<proof>

corollary *fermat-mult3*:

assumes $xyz: (x::int)^n + y^n = z^n$ **and** $n: 3 \text{ dvd } n$
shows $x*y*z=0$
<proof>

end

References

- [DM05] David Delahaye and Micaela Mayero. Diophantus' 20th problem and fermat's last theorem for $n=4$: Formalization of fermat's proofs in the coq proof assistant. <http://hal.archives-ouvertes.fr/hal-00009425/en/>, 2005.
- [Edw77] Harold M. Edwards. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*. Springer Verlag, 1977.
- [Oos07] Roelof Oosterhuis. Mechanised theorem proving: Exponents 3 and 4 of Fermat's Last Theorem in Isabelle. Master's thesis, University of Groningen, 2007. <http://www.roelfoosterhuis.nl/MScthesis.pdf>.
- [Wie] Freek Wiedijk. Formalizing 100 theorems. <http://www.cs.ru.nl/~freek/100/>.