

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

Roelof Oosterhuis
University of Groningen

August 21, 2007

Abstract

This document gives a formal proof, verified by the proof assistant 'Isabelle'¹, 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, like in section 1 and 2 of Harold M. Edwards, *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, New York (etc.): Springer Verlag, 1977.

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 $x^2 + 3y^2$.

We remind the reader that the case $n = 4$ of FLT, in contrast to the case $n = 3$, has already been formalised (in the proof assistant 'Coq')². Moreover it should be mentioned that the parametrisation of the Pythagorean Triples can be found as number 23 on the list of 'top 100 mathematical theorems'.³ This research is part of a 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. More information: see <http://www.roelofosterhuis.nl/MScthesis.pdf>

¹See <http://isabelle.in.tum.de/>

²See <http://hal.archives-ouvertes.fr/hal-00009425/en/>

³See <http://www.cs.ru.nl/~freek/100/>

Contents

1	The proof method ‘infinite descent’	3
2	Powers, prime numbers and divisibility	3
2.1	Auxiliary results	4
2.2	Parity of integers	4
2.3	Powers of natural numbers	5
2.4	Powers of integers	5
2.5	Facts about small powers of integers	7
3	Pythagorean triples and Fermat’s last theorem, case $n = 4$	7
3.1	Parametrisation of Pythagorean triples (over \mathbb{N} and \mathbb{Z})	8
3.2	Fermat’s last theorem, case $n = 4$	8
4	The quadratic form $x^2 + Ny^2$	9
4.1	Definitions and auxiliary results	9
4.2	Basic facts if $N \geq 1$	9
4.3	Multiplication and division	10
4.4	Uniqueness ($N > 1$)	10
4.5	The case $N = 3$	11
4.6	Existence ($N = 3$)	12
5	Fermat’s last theorem, case $n = 3$	12

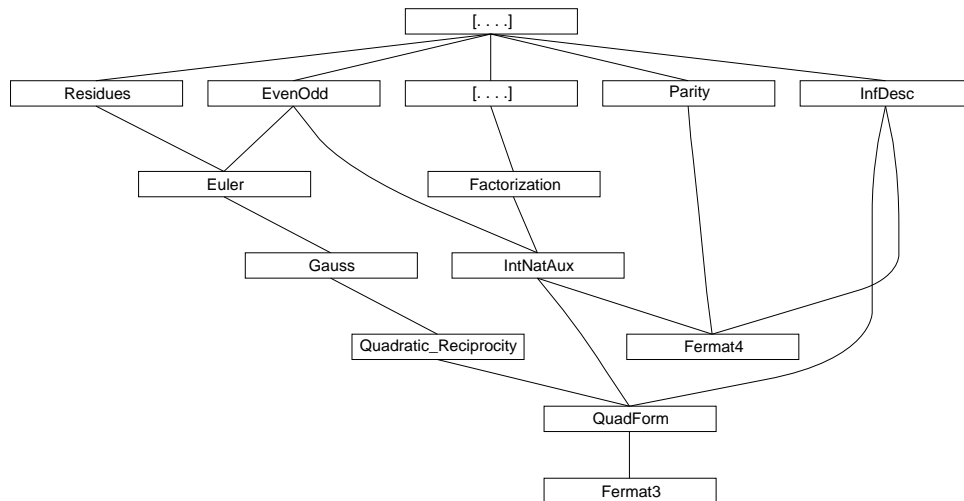


Figure 1: The dependence on existing files in the Isabelle library.

1 The proof method ‘infinite descent’

```
theory InfDesc
  imports Main
begin
```

The method of infinite descent, frequently used in number theory. Based on *less-induct*. $P(n)$ is true for all $n \in \mathbb{N}$ if

- case “0”: given $n = 0$ prove $P(n)$,
- case “smaller”: given $n > 0$ and $\neg P(n)$ prove there exists a smaller integer m such that $\neg P(m)$.

lemma *nat-infinite-descent*:

```
[[ P 0; !!n. n>0 ==> ~ P n ==> (∃ m::nat. m < n ∧ ~P m) ]] ==> P n
⟨proof⟩
```

lemmas *infinite-descent*

```
= nat-infinite-descent [rule-format, case-names 0 smaller]
```

Infinite descent using a mapping to \mathbb{N} : $P(x)$ is true for all $x \in D$ if there exists a $V : D \rightarrow \mathbb{N}$ and

- case “0”: given $V(x) = 0$ prove $P(x)$,
- case “smaller”: given $V(x) > 0$ and $\neg P(x)$ prove there exists a $y \in D$ such that $V(y) < V(x)$ and $\neg P(y)$.

NB: the proof also shows how to use the previous lemma.

corollary *nat-val-infinite-descent*:

```
fixes V:: 'a => nat
assumes ass0: !!x. V x = 0 ==> P x
and assn: !!x. V x > 0 ==> ~P x ==> (∃ y. V y < V x ∧ ~P y)
shows P x
⟨proof⟩
```

lemmas *val-infinite-descent*

```
= nat-val-infinite-descent [rule-format, case-names 0 smaller]
```

end

2 Powers, prime numbers and divisibility

```
theory IntNatAux
```

```
  imports
    ~/src/HOL/NumberTheory/Factorization
    ~/src/HOL/NumberTheory/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.

2.1 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*: $a > (0::\text{int}) \implies a*b > 0 \implies b > 0$
 $\langle \text{proof} \rangle$

2.2 Parity of integers

lemma *power-preserves-even*: $n > 0 \implies (x^n \in \text{zEven}) = (x \in \text{zEven})$
 $\langle \text{proof} \rangle$

lemma *power-preserves-odd*: $n > 0 \implies (x^n \in \text{zOdd}) = (x \in \text{zOdd})$
 $\langle \text{proof} \rangle$

lemma *even-plus-odd*: $a \in \text{zEven} \implies b \in \text{zOdd} \implies a+b \in \text{zOdd}$
 $\langle \text{proof} \rangle$

lemma *odd-plus-odd*: $\llbracket x \in \text{zOdd}; y \in \text{zOdd} \rrbracket \implies x+y \in \text{zEven}$
 $\langle \text{proof} \rangle$

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⟩

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

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

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

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

Theorem: if $n > 0$ and $gcd(a,b) = 1$ 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⟩

2.4 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*:
 $\llbracket zprime\ p; \neg\ p\ dvd\ b; p^n\ dvd\ a*b \rrbracket \implies p^n\ dvd\ a$
 ⟨proof⟩

lemma *zprime-power-zdvd-cancel-left*:
 $\llbracket zprime\ p; \neg\ p\ dvd\ a; p^n\ dvd\ a*b \rrbracket \implies p^n\ dvd\ b$
 ⟨proof⟩

2.5 Facts about small powers of integers

lemma *zadd-power2*: $((a::int)+b)^2 = a^2 + 2*a*b + b^2$
 ⟨proof⟩

lemma *zdiff-power2*: $((a::int)-b)^2 = a^2 - 2*a*b + b^2$
 ⟨proof⟩

lemma *zspecial-product*: $((a::int) + b) * (a - b) = a^2 - b^2$
 ⟨proof⟩

lemma *abs-power2-distrib*: $|a^2| = |a::int|^2$
 ⟨proof⟩

lemma *power2-eq-iff-abs-eq*: $((a::int)^2 = b^2) = (|a| = |b|)$
 ⟨proof⟩

lemma *power2-eq1-iff*: $(a::int)^2 = 1 \implies |a|=1$
 ⟨proof⟩

lemma *zadd-power3*: $((a::int)+b)^3 = a^3 + 3*a^2*b + 3*a*b^2 + b^3$
 ⟨proof⟩

lemma *zdiff-power3*: $((a::int)-b)^3 = a^3 - 3*a^2*b + 3*a*b^2 - b^3$
 ⟨proof⟩

lemma *power3-minus*: $(-a::int)^3 = -(a^3)$
 ⟨proof⟩

lemma *abs-power3-distrib*: $|(x::int)^3| = |x|^3$
 ⟨proof⟩

lemma *cube-square*: $(a::int)*a^2 = a^3$
 ⟨proof⟩

lemma *quartic-square-square*: $(x^2)^2 = (x::int)^4$
 ⟨proof⟩

lemma *power2-ge-self*: $x^2 \geq (x::int)$
 ⟨proof⟩

end

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

```
theory Fermat4
  imports InfDesc 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⟩

3.1 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*: *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⟩

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

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

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

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*:

fixes *c::int*
shows $\neg (a \ b. (a^4 + b^4 = c^2 \wedge a*b*c \neq 0 \wedge a \in \text{zOdd} \wedge \text{zgcd}(a,b)=1))$
(is ?Q c)
 ⟨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

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

theory *QuadForm*

imports

~/src/HOL/NumberTheory/Quadratic-Reciprocity

IntNatAux InfDesc

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 $x^2 + 3y^2$.

4.1 Definitions and auxiliary results

constdefs

is-qn $:: int \Rightarrow int \Rightarrow bool$

is-qn $A N == \exists x y. A = x^2 + N*y^2$

is-cube-form $:: int \Rightarrow int \Rightarrow bool$

is-cube-form $a b == \exists p q. a = p^3 - 9*p*q^2 \wedge b = 3*p^2*q - 3*q^3$

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

<proof>

lemma *zprime-3*: *zprime* 3

<proof>

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

<proof>

4.3 Multiplication and division

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

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

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

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

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 $\exists u v. a^2+N*b^2 = (u^2+N*v^2)*(p^2+N*q^2)$
 $\wedge (\exists e. a = p*u+e*N*q*v \wedge b = p*v - e*q*u \wedge |e|=1)$

⟨proof⟩

corollary *qfN-div-prime-weak*:

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

⟨proof⟩

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

⟨proof⟩

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 $\exists u v. a^2+N*b^2 = (u^2 + N*v^2)*(p^2+N*q^2) \wedge zgcd(u,v)=1$
 $\wedge (\exists e. a = p*u+e*N*q*v \wedge b = p*v-e*q*u \wedge |e|=1)$

⟨proof⟩

lemma *qfN-primedivisor-not*:

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

⟨proof⟩

lemma *qfN-oddprime-cube*:

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

⟨proof⟩

4.4 Uniqueness ($N > 1$)

lemma *qfN-prime-unique*:

$\llbracket zprime (a^2+N*b^2); N > 1; a^2+N*b^2 = c^2+N*d^2 \rrbracket$

$\implies (|a| = |c| \wedge |b| = |d|)$
 $\langle \text{proof} \rangle$

lemma *qfN-square-prime*:

assumes *ass*:

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

$\langle \text{proof} \rangle$

4.5 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*: *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*: *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*: $\text{zgcd}(a,b)=1 \wedge a^2 + 3*b^2 = w^3 \wedge w \in \text{zOdd}$

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

$\langle \text{proof} \rangle$

4.6 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*: $\llbracket p > 2; \text{zprime } p \rrbracket$
 $\implies (\text{Legendre } (a*b) \text{ } p) = (\text{Legendre } a \text{ } p) * (\text{Legendre } b \text{ } p)$
 $\langle \text{proof} \rangle$

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

lemma *Legendre-1mod6*: $\text{zprime } (6*m+1) \implies \text{Legendre } (-3) \text{ } (6*m+1) = 1$
 $\langle \text{proof} \rangle$

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

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

end

5 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*: $(x::\text{int})^3 + y^3 = (x+y)*(x^2 - x*y + y^2)$
 $\langle \text{proof} \rangle$

lemma *two-not-abs-cube*: $|x^3| = (2::\text{int}) \implies \text{False}$
 $\langle \text{proof} \rangle$

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*:
 $\neg (\exists v w. v^3 + w^3 = x^3 \wedge v*w*x \neq 0 \wedge x \in \text{zEven} \wedge \text{zgcd}(v, w) = 1)$ (**is** ?Q x)
 $\langle \text{proof} \rangle$

The theorem. Puts equation in requested shape.

theorem *fermat3*:
assumes *ass*: $(x::\text{int})^3 + y^3 = z^3$
shows $x*y*z=0$
 $\langle \text{proof} \rangle$

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
```