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

Roelof Oosterhuis
University of Groningen

May 26, 2024

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:

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

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

$$\mathit{coprime} a b \ \wedge \ ab = c^n \Longrightarrow \exists\, k : |a| = k^n.$$

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

theory *Fermat4*
imports *HOL−Computational-Algebra.Primes*
begin

context
begin

private lemma *nat-relprime-power-divisors*:
  assumes *n0*: *0* < *n* **and** *abc*: (*a*::*nat*)∗*b* = *c*^*n* **and** *relprime*: *coprime a b*
  shows ∃ *k*. *a* = *k*^*n*
⟨*proof*⟩ **lemma** *int-relprime-power-divisors*:
  assumes *0* < *n* **and** *0* ≤ *a* **and** *0* ≤ *b* **and** (*a*::*int*) ∗ *b* = *c* ^ *n* **and** *coprime a b*
  shows ∃ *k*. *a* = *k*^*n*
⟨*proof*⟩

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

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

private lemma *nat-power2-diff*: *a* ≥ (*b*::*nat*) ⟹ (*a*−*b*)^*2* = *a*^*2* + *b*^*2* − *2*∗*a*∗*b*
⟨*proof*⟩ **lemma** *nat-power-le-imp-le-base*: ⟦ *n* ≠ *0*; *a*^*n* ≤ *b*^*n* ⟧ ⟹ (*a*::*nat*) ≤ *b*
  ⟨*proof*⟩ **lemma** *nat-power-inject-base*: ⟦ *n* ≠ *0*; *a*^*n* = *b*^*n* ⟧ ⟹ (*a*::*nat*) = *b*
⟨*proof*⟩

1.1 Parametrisation of Pythagorean triples (over ℕ and ℤ)

private theorem *nat-euclid-pyth-triples*:
  assumes *abc*: (*a*::*nat*)^*2* + *b*^*2* = *c*^*2* **and** *ab-relprime*: *coprime a b* **and** *aodd*: *odd a*
  shows ∃ *p q*. *a* = *p*^*2* − *q*^*2* ∧ *b* = *2*∗*p*∗*q* ∧ *c* = *p*^*2* + *q*^*2* ∧ *coprime p q*
⟨*proof*⟩

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

private corollary *int-euclid-pyth-triples*: ⟦ *coprime* (*a*::*int*) *b*; *odd a*; *a*^*2* + *b*^*2* = *c*^*2*
⟧
  ⟹ ∃ *p q*. *a* = *p*^*2* − *q*^*2* ∧ *b* = *2*∗*p*∗*q* ∧ |*c*| = *p*^*2* + *q*^*2* ∧ *coprime p q*
⟨*proof*⟩

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

Core of the proof. Constructs a smaller solution over ℤ of

$$a^4 + b^4 = c^2 \;\wedge\; \mathit{coprime}\, a\, b \;\wedge\; abc \neq 0 \;\wedge\; a \text{ odd}.$$

private lemma *smaller-fermat4*:
  assumes *abc*: (*a*::*int*)^*4*+*b*^*4*=*c*^*2* **and** *abc0*: *a*∗*b*∗*c* ≠ *0* **and** *aodd*: *odd a*
    and *ab-relprime*: *coprime a b*
  shows

∃ *p q r*. (*p^4+q^4=r^2* ∧ *p∗q∗r* ≠ *0* ∧ *odd p* ∧ *coprime p q* ∧ *r^2* < *c^2*)
⟨*proof*⟩

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

private lemma *no-rewritten-fermat4*:
¬ (∃ (*a*::*int*) *b*. (*a^4* + *b^4* = *c^2* ∧ *a∗b∗c* ≠ *0* ∧ *odd a* ∧ *coprime a b*))
⟨*proof*⟩

The theorem. Puts equation in requested shape.

theorem *fermat-4*:
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 dvd n*
shows *x∗y∗z=0*
⟨*proof*⟩

end

end

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

theory *Quad-Form*
imports
HOL−Number-Theory.Number-Theory
begin

context
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 $x^2 + 3y^2$.

2.1 Definitions and auxiliary results

private lemma *best-division-abs*: (*n*::*int*) > *0* ⟹ ∃ *k*. *2* ∗ |*a* − *k∗n*| ≤ *n*
⟨*proof*⟩

lemma *prime-power-dvd-cancel-right*:
p ^ *n dvd a* **if** *prime* (*p*::′*a*::*semiring-gcd*) ¬ *p dvd b p* ^ *n dvd a* ∗ *b*
⟨*proof*⟩

definition
is-qfN :: *int* ⇒ *int* ⇒ *bool* **where**
is-qfN A N ⟷ (∃ *x y*. *A* = *x^2* + *N∗y^2*)

definition
is-cube-form :: *int* ⇒ *int* ⇒ *bool* **where**
is-cube-form a b ⟷ (∃ *p q. a* = *p^3* − *9∗p∗q^2* ∧ *b* = *3∗p^2∗q* − *3∗q^3*)

private lemma *abs-eq-impl-unitfactor*: |*a::int*| = |*b*| ⟹ ∃ *u. a* = *u∗b* ∧ |*u*|=*1*
⟨*proof*⟩ **lemma** *prime-3-nat*: *prime* (*3::nat*) ⟨*proof*⟩

2.2 Basic facts if $N \geq 1$

lemma *qfN-pos*: ⟦ *N* ≥ *1*; *is-qfN A N* ⟧ ⟹ *A* ≥ *0*
⟨*proof*⟩

lemma *qfN-zero*: ⟦ (*N::int*) ≥ *1*; *a^2* + *N∗b^2* = *0* ⟧ ⟹ (*a* = *0* ∧ *b* = *0*)
⟨*proof*⟩

2.3 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* ⟹ *is-qfN B N* ⟹ *is-qfN* (*A∗B*) *N*
⟨*proof*⟩

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

lemma *qfN-div-prime*:
fixes *p* :: *int*
assumes *ass*: *prime* (*p^2+N∗q^2*) ∧ (*p^2+N∗q^2*) *dvd* (*a^2+N∗b^2*)
shows ∃ *u v. a^2+N∗b^2* = (*u^2+N∗v^2*)∗(*p^2+N∗q^2*)
∧ (∃ *e. a* = *p∗u+e∗N∗q∗v* ∧ *b* = *p∗v* − *e∗q∗u* ∧ |*e*|=*1*)
⟨*proof*⟩

corollary *qfN-div-prime-weak*:
⟦ *prime* (*p^2+N∗q^2::int*); (*p^2+N∗q^2*) *dvd* (*a^2+N∗b^2*) ⟧
⟹ ∃ *u v. a^2+N∗b^2* = (*u^2+N∗v^2*)∗(*p^2+N∗q^2*)
⟨*proof*⟩

corollary *qfN-div-prime-general*: ⟦ *prime P*; *P dvd A*; *is-qfN A N*; *is-qfN P N* ⟧
⟹ ∃ *Q. A* = *Q∗P* ∧ *is-qfN Q N*
⟨*proof*⟩

lemma *qfN-power-div-prime*:
fixes *P* :: *int*
assumes *ass*: *prime P* ∧ *odd P* ∧ *P dvd A* ∧ *P^n* = *p^2+N∗q^2*
∧ *A^n* = *a^2+N∗b^2* ∧ *coprime a b* ∧ *coprime p* (*N∗q*) ∧ *n>0*
shows ∃ *u v. a^2+N∗b^2* = (*u^2* + *N∗v^2*)∗(*p^2+N∗q^2*) ∧ *coprime u v*

∧ (∃ *e*. *a* = *p*∗*u*+*e*∗*N*∗*q*∗*v* ∧ *b* = *p*∗*v*−*e*∗*q*∗*u* ∧ |*e*| = *1*)
⟨*proof*⟩

lemma *qfN-primedivisor-not*:
assumes *ass*: *prime P* ∧ *Q* > *0* ∧ *is-qfN* (*P*∗*Q*) *N* ∧ ¬ *is-qfN P N*
shows ∃ *R*. (*prime R* ∧ *R dvd Q* ∧ ¬ *is-qfN R N*)
⟨*proof*⟩

lemma *prime-factor-int*:
fixes *k* :: *int*
assumes |*k*| ≠ *1*
obtains *p* **where** *prime p p dvd k*
⟨*proof*⟩

lemma *qfN-oddprime-cube*:
⟦ *prime* (*p*^*2*+*N*∗*q*^*2*::*int*); *odd* (*p*^*2*+*N*∗*q*^*2*); *p* ≠ *0*; *N* ≥ *1* ⟧
⟹ ∃ *a b*. (*p*^*2*+*N*∗*q*^*2*)^*3* = *a*^*2* + *N*∗*b*^*2* ∧ *coprime a* (*N*∗*b*)
⟨*proof*⟩

2.4 Uniqueness ($N > 1$)

lemma *qfN-prime-unique*:
⟦ *prime* (*a*^*2*+*N*∗*b*^*2*::*int*); *N* > *1*; *a*^*2*+*N*∗*b*^*2* = *c*^*2*+*N*∗*d*^*2* ⟧
⟹ (|*a*| = |*c*| ∧ |*b*| = |*d*|)
⟨*proof*⟩

lemma *qfN-square-prime*:
assumes *ass*:
prime (*p*^*2*+*N*∗*q*^*2*::*int*) ∧ *N*>*1* ∧ (*p*^*2*+*N*∗*q*^*2*)^*2* = *r*^*2*+*N*∗*s*^*2* ∧ *coprime r s*
shows |*r*| = |*p*^*2*−*N*∗*q*^*2*| ∧ |*s*| = |*2*∗*p*∗*q*|
⟨*proof*⟩

lemma *qfN-cube-prime*:
assumes *ass*: *prime* (*p*^*2* + *N*∗*q*^*2*::*int*) ∧ *N* > *1*
∧ (*p*^*2* + *N*∗*q*^*2*)^*3* = *a*^*2* + *N*∗*b*^*2* ∧ *coprime a b*
shows |*a*| = |*p*^*3*− *3*∗*N*∗*p*∗*q*^*2*| ∧ |*b*| = |*3*∗*p*^*2*∗*q*−*N*∗*q*^*3*|
⟨*proof*⟩

2.5 The case $N = 3$

lemma *qf3-even*: *even* (*a*^*2*+*3*∗*b*^*2*) ⟹ ∃ *B*. *a*^*2*+*3*∗*b*^*2* = *4*∗*B* ∧ *is-qfN B 3*
⟨*proof*⟩

lemma *qf3-even-general*: ⟦ *is-qfN A 3*; *even A* ⟧
⟹ ∃ *B*. *A* = *4*∗*B* ∧ *is-qfN B 3*
⟨*proof*⟩

lemma *qf3-oddprimedivisor-not*:
assumes *ass*: *prime P* ∧ *odd P* ∧ *Q*>*0* ∧ *is-qfN* (*P*∗*Q*) *3* ∧ ¬ *is-qfN P 3*
shows ∃ *R*. *prime R* ∧ *odd R* ∧ *R dvd Q* ∧ ¬ *is-qfN R 3*
⟨*proof*⟩

lemma *qf3-oddprimedivisor*:
⟦ *prime* (*P*::*int*); *odd P*; *coprime a b*; *P dvd* (*a*^*2*+*3*∗*b*^*2*) ⟧
⟹ *is-qfN P 3*
⟨*proof*⟩

lemma *qf3-cube-prime-impl-cube-form*:
assumes *ab-relprime*: *coprime a b* **and** *abP*: *P*^*3* = *a*^*2* + *3*∗*b*^*2*
and *P*: *prime P* ∧ *odd P*
shows *is-cube-form a b*
⟨*proof*⟩

lemma *cube-form-mult*: ⟦ *is-cube-form a b*; *is-cube-form c d*; |*e*| = *1* ⟧
⟹ *is-cube-form* (*a*∗*c*+*e*∗*3*∗*b*∗*d*) (*a*∗*d*−*e*∗*b*∗*c*)
⟨*proof*⟩

lemma *qf3-cube-primelist-impl-cube-form*: ⟦ (∀ *p*∈*set-mset ps*. *prime p*); *odd* (*int* (∏ *i*∈#*ps*. *i*)) ⟧ ⟹
(!! *a b*. *coprime a b* ⟹ *a*^*2* + *3*∗*b*^*2* = (*int*(∏ *i*∈#*ps*. *i*))^*3* ⟹ *is-cube-form a b*)
⟨*proof*⟩

lemma *qf3-cube-impl-cube-form*:
assumes *ass*: *coprime a b* ∧ *a*^*2* + *3*∗*b*^*2* = *w*^*3* ∧ *odd w*
shows *is-cube-form a b*
⟨*proof*⟩

2.6 Existence ($N = 3$)

This part contains the proof that all prime numbers ≡ 1 mod 6 can be written as $x^2 + 3y^2$.

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

lemma *Legendre-zmult*: ⟦ *p* > *2*; *prime p* ⟧
⟹ (*Legendre* (*a*∗*b*) *p*) = (*Legendre a p*)∗(*Legendre b p*)
⟨*proof*⟩

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

lemma *Legendre-1mod6*: *prime* (*6*∗*m*+*1*) ⟹ *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*: *prime* (*6*∗*m*+*1*::*int*) ⟹ ∃ *x y*. *6*∗*m*+*1* = *x*^*2* + *3*∗*y*^*2*
⟨*proof*⟩

end

end

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

theory *Fermat3*
imports *Quad-Form*

begin

context
begin

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

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

private lemma *nat-relprime-power-divisors*:
  assumes *n0*: *0 < n* **and** *abc*: *(a::nat)*b = c^n* **and** *relprime*: *coprime a b*
  shows ∃ *k. a = k^n*
⟨*proof*⟩ **lemma** *int-relprime-odd-power-divisors*:
  assumes *odd n* **and** *(a::int) * b = c ^ n* **and** *coprime a b*
  shows ∃ *k. a = k^n*
⟨*proof*⟩ **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)* ⟹ *False*
⟨*proof*⟩

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

private lemma *no-rewritten-fermat3*:
  ¬ (∃ *v w. v^3+w^3 = x^3* ∧ *v*w*x* ≠ *0* ∧ *even (x::int)* ∧ *coprime v w*)
⟨*proof*⟩

The theorem. Puts equation in requested shape.

theorem *fermat-3*:
  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 dvd n*
  shows *x*y*z=0*
⟨*proof*⟩

end

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.roelofoosterhuis.nl/MScthesis.pdf.

[Wie] Freek Wiedijk. Formalizing 100 theorems. http://www.cs.ru.nl/~freek/100/.