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

Roelof Oosterhuis
University of Groningen

August 28, 2014

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

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

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 \(x^2 + N y^2\) 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/Old-Number-Theory/Factorization
~/~/src/HOL/Old-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: 
\( (a \neq 0 \lor b \neq 0) \implies \exists \ c \ d . \ a = \text{gcd} \ a \ b \cdot c \land b = \text{gcd} \ a \ b \cdot d \land \text{gcd} \ c \ d = 1 \)
\end{proof}

lemma factor-exists-general: \( (a::nat) \neq 0 \implies (\exists \ ps . \ \text{primel} \ ps \land \text{prod} \ ps = a) \)
\end{proof}

lemma make-zrelprime: \( (a \neq 0 \lor b \neq 0) \)
\( \implies \exists \ c \ d . \ a = \text{zgcd} \ a \ b \cdot c \land b = \text{zgcd} \ a \ b \cdot d \land \text{zgcd} \ c \ d = 1 \)
\end{proof}

lemma int-nat-abs-eq-abs: \( \text{int}(\text{nats}|x::\text{int}|) = |x| \)
\end{proof}

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

lemma zprime-factor-exists: \( (a::\text{int}) > 1 \implies \exists \ p . \ \text{zprime} \ p \land p \ \text{dvd} a \)
\end{proof}

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

lemma best-odd-division-abs: \[ (x::\text{int}) > 0; x \in \text{zOdd} ] \implies \exists \ n . \ 2 \cdot |y - n \cdot x| < x \)
\end{proof}

lemma zprime-2: \( \text{zprime} 2 \)
\end{proof}

lemma zgcd1-iff-no-common-primedivisor: 
\( (\text{zgcd} \ a \ b = 1) = (\neg (\exists \ p . \ \text{zprime} \ p \land p \ \text{dvd} a \land p \ \text{dvd} b)) \)
\end{proof}

lemma pos-zmult-pos: \( a > (0::\text{int}) \implies a \cdot b > 0 \implies b > 0 \)
\end{proof}
1.2 Parity of integers

definition proof

lemma power-preserves-even: \( n > 0 \implies (x^n \in \text{Even}) = (x \in \text{Even}) \)

lemma power-preserves-odd: \( n > 0 \implies (x^n \in \text{Odd}) = (x \in \text{Odd}) \)

lemma even-plus-odd: \( a \in \text{Even} \implies b \in \text{Odd} \implies a + b \in \text{Odd} \)

lemma odd-plus-odd: \( a \in \text{Odd} \implies b \in \text{Odd} \implies a + b \in \text{Even} \)

lemma even-plus-odd-prop1: \( a + b \in \text{Odd} \implies a \in \text{Odd} \implies b \in \text{Even} \)

lemma even-plus-odd-prop2: \( a + b \in \text{Odd} \implies a \in \text{Even} \implies b \in \text{Odd} \)

1.3 Powers of natural numbers

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

lemma alternative-gcd-1-power-left-distrib: \( \gcd a b = 1 \implies \gcd(a^n) b = 1 \)

lemma gcd-1-power-distrib: \( \gcd a b = 1 \implies \gcd(a^n)(b^n) = 1 \)

lemma gcd-power-distrib: \( \gcd a b^n = \gcd(a^n)(b^n) \)

Useful lemma: if prime \( p|a^n \) then \( p|a \).

lemma prime-dvd-power: \([\text{prime } p; p \text{ dvd } a \cdot n] \implies p \text{ dvd } a\)

lemma prime-power-dvd-cancel-right: \([\text{prime } p; \neg p \text{ dvd } b; p \cdot n \text{ dvd } a \cdot b] \implies p \cdot n \text{ dvd } a\)

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

lemma nat-power-dvd-mono: \( n \neq 0 \implies (a^n \text{ dvd } b \cdot n) = (a \text{ dvd } (b :: \text{nat}))\)

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:
\[\text{assumes npos: } n \neq 0 \text{ and abcn: } a \cdot b = c \cdot n \text{ and relprime: } \gcd a b = 1\]
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: \(a \times b = c \times n\) and \(n > 1\) and relprime: \(\gcd a b = 1\)
- **shows** \(\exists k. |a| = k \times n\)

**corollary** int-triple-relprime-power-divisors:
- \(a \times b \times c = d \times n; n > 1; \gcd a b = 1; \gcd b c = 1; \gcd c a = 1\)
- \(\Rightarrow \exists k l m. |a| = k \times n \land |b| = l \times n \land |c| = m \times n\)

**lemma** neg-odd-power: \([ x \in z\text{Odd}; x \geq 0 ] \Rightarrow (\neg a : int) ^ \times (nat x) = -(a \times (nat x))\)

**lemma** neg-even-power: \([ x \in z\text{Even}; x \geq 0 ] \Rightarrow (\neg a : int) ^ \times (nat x) = a \times (nat x)\)

**corollary** int-relprime-odd-power-divisors:
- \(a \times b = c \times (nat x); nat x > 1; x \in z\text{Odd}; \gcd a b = 1\)
- \(\Rightarrow \exists k. a = k \times (nat x)\)

**corollary** int-triple-relprime-odd-power-divisors:
- \(a \times b \times c = d \times (nat x); nat x > 1; x \in z\text{Odd}; \gcd a b = 1; \gcd b c = 1; \gcd c a = 1\)
- \(\Rightarrow \exists k l m. a = k \times (nat x) \land b = l \times (nat x) \land c = m \times (nat x)\)

**lemma** \(\gcd 1\)-power-left-distrib: \(\gcd a b = 1 \Rightarrow \gcd (a \times n) b = 1\)

**lemma** \(\gcd 1\)-power-distrib: \(\gcd a b = 1 \Rightarrow \gcd (a \times n) (b \times n) = 1\)

**lemma** \(\gcd\)\-power-distrib: \(\gcd a b \times n = \gcd (a \times n) (b \times n)\)

**lemma** zprime\-zdvd\-zmult\-general: \([ zprime p; p \vdash d m \times n ] \Rightarrow p \vdash d m \lor p \vdash d n\)

**lemma** zprime\-zdvd\-power: \([ zprime p; p \vdash d a \times n ] \Rightarrow p \vdash d a\)

**lemma** zpower\-zdvd\-mono: \(n \neq 0 \Rightarrow (a \times n \vdash d b \times n) = (a \vdash d (b : \text{int}))\)

**lemma** zprime\-power-zdvd\-cancel-right:
lemma zprime-power-zdvd-cancel-left:
\[ \text{zprime } p; \neg p \text{ dvd } a; p^n \text{ dvd } a \cdot b \implies p^n \text{ dvd } b \]
\langle proof \rangle

1.5 Facts about small powers of integers

lemma zadd-power2: \((a::int) + b)^2 = a^2 + 2 \cdot a \cdot b + b^2\)
\langle proof \rangle

lemma zdiff-power2: \((a::int) - b)^2 = a^2 - 2 \cdot a \cdot b + b^2\)
\langle proof \rangle

lemma zspecial-product: \((a::int) + b) \cdot (a - b) = a^2 - b^2\)
\langle proof \rangle

lemma abs-power2-distrib: \(|a^2| = |a| \cdot |a|\)
\langle proof \rangle

lemma power2-eq-ifff-abs-eq: \((a::int)^2 = b^2) \implies (|a| = |b|)\)
\langle proof \rangle

lemma power2-eq1-iff: \((a::int)^2 = 1 \implies |a| = 1\)
\langle proof \rangle

lemma zdadd-power3: \((a::int) + b)^3 = a^3 + 3 \cdot a^2 \cdot b + 3 \cdot a \cdot b^2 + b^3\)
\langle proof \rangle

lemma zdiff-power3: \((a::int) - b)^3 = a^3 - 3 \cdot a^2 \cdot b + 3 \cdot a \cdot b^2 - b^3\)
\langle proof \rangle

lemma power3-minus: \((-a::int)^3 = -(a^3)\)
\langle proof \rangle

lemma abs-power3-distrib: \(|x::int)^3| = |x|^3\)
\langle proof \rangle

lemma cube-square: \((a::int)^2 = a^3\)
\langle proof \rangle

lemma quartic-square-square: \((x^2)^2 = (x::int)^4\)
\langle proof \rangle

lemma power2-ge-self: \(x^2 \geq (x::int)\)
\langle 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: even \((r :: nat)\) = \(2 \dvd r\) (proof)

lemma nat-power2-add: \((a :: nat) + b \) ^ 2 = \(a^2 + b^2 + 2 * a * b\) (proof)

lemma nat-power2-diff: \(a \geq (b :: nat)\) \(\implies (a - b)^2 = a^2 + b^2 - 2 * a * b\) (proof)

lemma nat-power-le-imp-le-base: \([ n \neq 0; a^\langle n\rangle \leq b \langle n\rangle \] \(\implies (a :: nat) \leq b\) (proof)

lemma nat-power-inject-base: \([ n \neq 0; a^\langle n\rangle = b \langle n\rangle \] \(\implies (a :: nat) = b\) (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: \(\gcd a \ b = 1\) and aodd: \(a \in \mathbb{Z}_{\text{Odd}}\)
shows \(\exists p \ q. \ a = p^2 - q^2 \land b = 2 * p * q \land c = p^2 + q^2 \land \gcd p \ q = 1\) (proof)

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

corollary int-euclid-pyth-triples: \([ \gcd a \ b = 1; a \in \mathbb{Z}_{\text{Odd}}; a^2 + b^2 = c^2 \]\(\implies \exists p \ q. \ a = p^2 - q^2 \land b = 2 * p * q \land |c| = p^2 + q^2 \land \gcd p \ q = 1\) (proof)

2.2 Fermat’s last theorem, case \( n = 4 \)

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

\[
a^4 + b^4 = c^2 \land \gcd a b = 1 \land abc \neq 0 \land a \text{ odd}.
\]

lemma smaller-fermat4:
assumes abc: \(a^4 + b^4 = c^2\) and abc0: \(a \cdot b \cdot c \neq 0\) and aodd: \(a \in \mathbb{Z}_{\text{Odd}}\)
and ab-relprime: \(\gcd a \ b = 1\)
shows \(\exists p \ q \ r. \ (p^4 + q^4 = r^2 \land p \cdot q \cdot r \neq 0 \land p \in \mathbb{Z}_{\text{Odd}} \land \gcd p \ q = 1 \land r^2 < c^2)\) (proof)

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

lemma no-rewritten-fermat4:
The theorem. Puts equation in requested shape.

**Theorem fermat4:**
- **Assumes:** \( (x::int) \cdot 4 + y \cdot 4 = z \cdot 4 \)
- **Shows:** \( x \cdot y \cdot z = 0 \)

**Corollary fermat-mult4:**
- **Assumes:** \( (x::int) \cdot n + y \cdot n = z \cdot n \) and \( n: 4 \text{ dvd } n \)
- **Shows:** \( x \cdot y \cdot z = 0 \)

### 3 The quadratic form \( x^2 + Ny^2 \)

#### 3.1 Definitions and auxiliary results

**Definition**
- \( \text{is-qfN :: int } \Rightarrow \text{ int } \Rightarrow \text{ bool where} \)
  - \( \text{is-qfN A N } \leftrightarrow (\exists x y. A = x^2 + N \cdot y^2) \)

**Definition**
- \( \text{is-cube-form :: int } \Rightarrow \text{ int } \Rightarrow \text{ bool where} \)
  - \( \text{is-cube-form a b } \leftrightarrow (\exists p q. a = p^3 - 9 \cdot p \cdot q^2 \land b = 3 \cdot p^2 \cdot q - 3 \cdot q^3) \)

**Lemma** \( \text{abs-eq-impl-unifactor: } |a::int| = |b| \Rightarrow \exists u. a = u \cdot b \land |u| = 1 \)

**Lemma** \( \text{zprime-3: } \text{zprime 3} \)

### 3.2 Basic facts if \( N \geq 1 \)

**Lemma** \( \text{qfN-pos: } [ N \geq 1; \text{is-qfN A N } ] \Rightarrow A \geq 0 \)

**Lemma** \( \text{qfN-zero: } [ (N::int) \geq 1; a^2 + N \cdot b^2 = 0 ] \Rightarrow (a = 0 \land b = 0) \)
3.3 Multiplication and division

**Lemma** \(\text{gfN-mult1: } ((a::int) \cdot 2 + N \cdot b \cdot 2) \cdot (c \cdot 2 + N \cdot d \cdot 2) = (a+c+N \cdot b \cdot d) \cdot 2 + N \cdot (a \cdot d - b \cdot c) \cdot 2\)

**Proof**

**Lemma** \(\text{gfN-mult2: } ((a::int) \cdot 2 + N \cdot b \cdot 2) \cdot (c \cdot 2 + N \cdot d \cdot 2) = (a \cdot c - N \cdot b \cdot d) \cdot 2 + N \cdot (a \cdot d + b \cdot c) \cdot 2\)

**Proof**

**Corollary** is-gfN-mult: is-gfN \(A\ N\) \(\Rightarrow\) is-gfN \(B\ N\) \(\Rightarrow\) is-gfN \((A \cdot B)\ N\)

**Proof**

**Corollary** is-gfN-power: \((n::nat) > 0 \Rightarrow\) is-gfN \(A\ N\) \(\Rightarrow\) is-gfN \((A \ \hat{\cdot} \ n)\ N\)

**Proof**

**Lemma** \(\text{gfN-div-prime:}\)

- **Assumes** ass: \(\text{zprime } (p \cdot 2 + N \cdot q \cdot 2) \land (p \cdot 2 + N \cdot q \cdot 2) \text{ dvd } (a \cdot 2 + N \cdot b \cdot 2)\)
- **Shows** \(\exists\ u\ v\ a \cdot 2 + N \cdot b \cdot 2 = (u \cdot 2 + N \cdot v \cdot 2) \cdot (p \cdot 2 + N \cdot q \cdot 2)\) \(\land\ (\exists\ e\ a = p \cdot u + e \cdot N \cdot q \cdot v \land b = p \cdot v - e \cdot q \cdot u \land |e| = 1)\)

**Proof**

**Corollary** \(\text{gfN-div-prime-weak:}\)

\(\exists\ u\ v\ a \cdot 2 + N \cdot b \cdot 2 = (u \cdot 2 + N \cdot v \cdot 2) \cdot (p \cdot 2 + N \cdot q \cdot 2)\) \(\land\ \text{gcd } u\ v = 1\)

**Proof**

**Corollary** \(\text{gfN-div-prime-general:}\)

\(\exists\ Q\ A = Q \cdot P \land \text{is-gfN } Q\ N\)

**Proof**

**Lemma** \(\text{gfN-power-div-prime:}\)

- **Assumes** ass: \(\text{zprime } P \land P \in \text{zOdd } \land P \text{ dvd } A \land P \cdot n = p \cdot 2 + N \cdot q \cdot 2\) 
  
  \(\land\ A \cdot n = a \cdot 2 + N \cdot b \cdot 2 \land \text{gcd } a \cdot b = 1 \land \text{gcd } p \cdot (N \cdot q) = 1 \land n > 0\)
- **Shows** \(\exists\ u\ v\ a \cdot 2 + N \cdot b \cdot 2 = (u \cdot 2 + N \cdot v \cdot 2) \cdot (p \cdot 2 + N \cdot q \cdot 2) \land \text{gcd } u\ v = 1\) 
  
  \(\land\ (\exists\ e\ a = p \cdot u + e \cdot N \cdot q \cdot v \land b = p \cdot v - e \cdot q \cdot u \land |e| = 1)\)

**Proof**

**Lemma** \(\text{gfN-primedivisor-not:}\)

- **Assumes** ass: \(\text{zprime } P \land Q > 0 \land \text{is-gfN } (P \cdot Q)\ N\ \land\ \neg\ \text{is-gfN } P\ N\)
- **Shows** \(\exists\ R\ (\text{zprime } R \land R \text{ dvd } Q \land \neg\ \text{is-gfN } R\ N)\)

**Proof**

**Lemma** \(\text{gfN-oddprime-cube:}\)

\(\exists\ a\ b\ (p \cdot 2 + N \cdot q \cdot 2) \cdot 3 = a \cdot 2 + N \cdot b \cdot 2 \land \text{gcd } a \cdot (N \cdot b) = 1\)

**Proof**
3.4 Uniqueness \((N > 1)\)

**lemma qfN-prime-unique:**
\[ [ \text{zprime } (a^2+N*b^2); \ N > 1; \ a^2+N*b^2 = c^2+N*d^2 ] \]
\[ \implies (|a| = |c| \land |b| = |d|) \]

**proof**

**lemma qfN-square-prime:**
\[ \text{assumes } \text{ass}: \]
\[ \text{zprime } (p^2+N*q^2) \land N > 1 \land \ (p^2+N*q^2)^2 = r^2+N*s^2 \land \gcd r s = 1 \]
\[ \text{shows } |r| = |p^2-N*q^2| \land |s| = |2*p*q| \]

**proof**

**lemma qfN-cube-prime:**
\[ \text{assumes } \text{ass}: \]
\[ \text{zprime } (p^2+N*q^2) \land N > 1 \land \ (p^2+N*q^2)^3 = a^2+N*b^2 \land \gcd a b = 1 \]
\[ \text{shows } |a| = |p^3-3*N*p*q^2| \land |b| = |3*p^2*q-N*q^3| \]

**proof**

3.5 The case \(N = 3\)

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

**proof**

**lemma qf3-even-general:**
\[ [ \text{is-qfN A } 3; \ A \in \text{zEven} ] \]
\[ \implies \exists B. \ A = 4*B \land \text{is-qfN B } 3 \]

**proof**

**lemma qf3-oddprimedivisor-not:**
\[ \text{assumes } \text{ass}: \]
\[ \text{zprime } P \land P \in \text{zOdd} \land Q > 0 \land \text{is-qfN } (P*Q) \land \sim \text{is-qfN P } 3 \]
\[ \text{shows } \exists R. \text{zprime } R \land R \in \text{zOdd} \land \text{R dvd Q } \land \sim \text{is-qfN R } 3 \]

**proof**

**lemma qf3-oddprimedivisor:**
\[ [ \text{zprime } P; \ P \in \text{zOdd}; \ \gcd a b = 1; \ P \text{ dvd } (a^2+3*b^2) ] \]
\[ \implies \text{is-qfN P } 3 \]

**proof**

**lemma qf3-cube-prime-impl-cube-form:**
\[ \text{assumes } ab\text{-relprime}: \ \gcd a b = 1 \text{ and } abP: \ P^3 = a^2 + 3*b^2 \]
\[ \text{and } P: \text{zprime } P \land P \in \text{zOdd} \]
\[ \text{shows } \text{is-cube-form a b} \]

**proof**

**lemma cube-form-mult:**
\[ [ \text{is-cube-form a b}; \ \text{is-cube-form c d}; \ |e| = 1 ] \]
\[ \implies \text{is-cube-form } (a*c+e*3*b*d) \ (a*d-e*b*c) \]

**proof**

**lemma qf3-cube-primelist-impl-cube-form:**
\[ [ \text{primel ps}; \ \text{int } (\text{prod ps}) \in \text{zOdd} ] \]
\[ \implies (!! a b. \ \gcd a b = 1 \implies a^2 + 3*b^2 = (\text{int}(\text{prod ps}))^3 \implies \text{is-cube-form a b}) \]

**proof**
3.6 Existence \((N = 3)\)

This part contains the proof that all prime numbers \(\equiv 1 \mod 6\) can be written as \(x^2 + 3y^2\).

First show \((a \cdot b) \cdot p = (a \cdot p) \cdot (b \cdot p)\), where \(p\) is an odd prime.

\textbf{Lemma} \qf3-cube-impl-cube-form:
\begin{align*}
\text{assumes} & \quad \zgcd\ a\ b = 1 \land a^2 + 3\cdot b^2 = w^3 \land w \in z\text{Odd} \\
\text{shows} & \quad \is\text{-cube-form}\ a\ b
\end{align*}

\langle \text{proof} \rangle

4 Fermat’s last theorem, case \(n = 3\)

theory \textit{Fermat3}

\begin{itemize}
  \item Proof of Fermat’s last theorem for the case \(n = 3\):
  \begin{align*}
  \forall x, y, z : \quad x^3 + y^3 = z^3 \implies xyz = 0.
  \end{align*}
  \textbf{lemma} \factor-sum-cubes: \((x::\text{int})^3 + y^3 = (x+y)\cdot(x^2 - x\cdot y + y^2)
  \langle \text{proof} \rangle
  \text{\textbf{lemma} two-not-abs-cube:} \quad |x^3| = (2::\text{int}) \implies \text{False}
  \langle \text{proof} \rangle
  \text{\textit{Sh}ows there exists no solution } v^3 + w^3 = x^3 \text{ with } vwz \neq 0 \text{ and } \gcd(v,w) = 1 \text{ and } x \ even, \text{ by constructing a solution with a smaller } |x^3|.
  \textbf{lemma} \no-rewritten-fermat3:
  \begin{align*}
  \neg (\exists v\ w: v^3 + w^3 = x^3 \land v\cdot w\cdot x \neq 0 \land x \in z\text{Even} \land z\gcd\ v\ w = 1)
  \end{align*}
  \langle \text{proof} \rangle
  \text{The theorem. Puts equation in requested shape.}
  \textbf{theorem} \fermat3:
  \begin{align*}
  \text{assumes} & \quad (x::\text{int})^3 + y^3 = z^3
  \end{align*}
\end{itemize}
shows $x \cdot y \cdot z = 0$
⟨proof⟩
end

corollary fermat-mult3:
  assumes $xyz : (x :: int)^n + y^n = z^n$ and $n : 3$ dvd $n$
  shows $x \cdot y \cdot z = 0$
⟨proof⟩
end

References


