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

Roelof Oosterhuis
University of Groningen

June 11, 2019

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

$$\text{coprime} \hspace{1mm} ab = c^n \implies \exists k : |a| = k^n.$$ 

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].
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 $\exists k. a = k^n$
using assms proof (induct arbitrary: $a$ $b$ rule: nat-less-induct)
  case (1 $c$)
  show $?case$
  proof (cases $a > 1$)
    case False
    hence $a = 0 \lor a = 1$ by linarith
    thus $?thesis$ using $n0$ power-one zero-power by (simp only: eq-sym-conv) blast
  next
    case True
    then obtain $p$ where $p$ : prime $p$ $p$ dvd $a$ using prime-factor-nat[of $a$]
      by blast
    hence $h1: p$ dvd $(c^n)$ using 1(3) dvd-mult2[of $p$ $a$ $b$] by presburger
    hence $(p^n)$ dvd $(c^n)$
      using $p$(1) prime-dvd-power-nat[of $p$ $c$ $n$] dvd-power-same[of $p$ $c$ $n$] by blast
    moreover have $h2: \neg p$ dvd $b$
      using $p$⟨coprime $a$ $b$⟩ coprime-common-divisor-nat[of $a$ $b$ $p$]
      by auto
    hence $\neg (p^n)$ dvd $b$
      using $n0$ $p$(1) by (auto intro: dvd-trans dvd-power[of $n$ $p$])
    ultimately have $(p^n)$ dvd $a$
      using 1.prems $p$(1) prime-elem-divprod-pow[of $p$ $a$ $b$ $n$] by simp
    then obtain $a'$ $c'$ where $ac: a = p^n * a'$ $c = p * c'$
      using $h1$ dvdE[of $p^n$ $a$] dvdE[of $p$ $c$] prime-dvd-power-nat[of $p$ $c$ $n$] $p$(1) by meson
    hence $p^n * (a' * b) = p^n * c'^n$ using 1(3)
      by (simp add: power-mult-distrib semiring-normalization-rules(18))
    hence $a' * b = c'^n$ using $p$(1) by auto
    moreover have coprime $a'$ $b$ using $I(4)$ $ac$(1)
      by (simp add: ac-simps)
    moreover have $0 < b$ $0 < a$ using $h2$ dvd-0-right gr0I True by fastforce+
    then have $0 < c$ $1 < p$
      using $p$ ⟨$a * b = c^n$⟩ $n0$ nat-0-less-mult-iff[of $a$ $b$] $n0$
      by (auto simp add: prime-gt-Suc-0-nat)
    hence $c' < c$ using ac(2) by simp
    ultimately obtain $k$ where $a' = k^n$ using $I$(1) $n0$ by presburger
    hence $a = (p*k)^n$ using $ac$(1) by (simp add: power-mult-distrib)
    thus $?thesis$ by blast
    qed
  qed
private lemma int-relprime-power-divisors:
  assumes \( \theta < n \) and \( \theta \leq a \) and \( \theta \leq b \) and \((a::int) \ast b = c \) and \( \text{coprime } a \ast b \)
  shows \( \exists k. a = k^n \)
proof (cases \( a = 0 \))
  case False
  from \( \{ \theta \leq a \} \) \( \theta \leq b \) \( a \ast b = c \) \( \text{symmetric} \) have \( \theta \leq c \) \( c^n \)
  by simp
  hence \( c^n = |c|^n \) using power-even-abs[of \( n \) \( c \)] zero-le-power-eq[of \( c \) \( n \)] by linarith
  hence \( a \ast b = |c|^n \) using assms(4) by presburger
  hence \( \text{nat} \ a \ast \text{nat} \ b = |\text{nat} \ c|^n \) using nat-mult-distrib[of \( a \) \( b \)] assms(2)
  by (simp add: nat-power-eq)
moreover have \( 0 \leq b \) using assms mult-less-0-iff[of \( a \) \( b \)] False by auto
with \( \{ \theta \leq a \} \) (coprime \( a \) \( b \)) have coprime \( \text{nat}(a) \text{nat}(b) \) by simp
ultimately have \( \exists \ k. \text{nat} \ a = k^n \)
  using nat-relprime-power-divisors[of \( n \) \( \text{nat} \ a \) \( \text{nat} \ b \) \( \text{nat}(c) \)] assms(1) by blast
thus \( \theta \text{thesis using assms(2) int-nat-eq[of \( a \)] by fastforce} \)
qed (simp add: zero-power[of \( n \) assms(1)])

Proof of Fermat’s last theorem for the case \( n = 4 \):
\[
\forall x, y, z : x^4 + y^4 = z^4 \implies xyz = 0.
\]

private lemma nat-power2-diff: \( a \geq (b::nat) \implies (a-b)^2 = a^2 + b^2 - 2*a*b \)
proof −
  assume \( a\geq b: a \geq b \)
  hence \( a^2-b^2 \) \( \geq b^2 \) by (simp only: power-mono)
  from \( a\geq b \) have \( ab\geq b^2 \) \( a*b \geq b^2 \) by (simp add: power2-2-eq-square)
  have \( b^2 (a-b) + (a-b)^2 = a^2 (a-b) \) by (simp add: power2-2-eq-square diff-mult-distrib)
  also have \( \ldots = a*b + a^2 + (b^2 - b^2) - 2*a*b \)
  by (simp add: diff-mult-distrib2 power2-2-eq-square)
  also with \( a\geq b^2 \) have \( \ldots = a^2 + (a^2 - b^2) + b^2 - 2*a*b \) by simp
  also with \( ab\geq b^2 \) have \( \ldots = (a*b - b^2) + a^2 + b^2 - 2*a*b \) by auto
  also have \( \ldots = b^2 (a-b) + a^2 + b^2 - 2*a*b \)
  by (simp only: diff-mult-distrib2 power2-2-eq-square mult.commute)
  finally show \( \theta \text{thesis by arith} \)
qed

private lemma nat-power-le-imp-le-base: \( [ n \neq 0 \; a^n \leq b^n ] \implies (a::nat) \leq b \)
proof −
  assume \( n \neq 0 \) and \( ab: a^n \leq b^n \)
  then obtain \( m \) where \( n = \text{Suc} \; m \) by (frule-tac \( n=n \) in \( \text{not0-implies-Suc}, \text{auto} \))
  with \( ab \) have \( a \geq 0 \) and \( a^ \text{Suc} m \leq b^ \text{Suc} m \) and \( b \geq 0 \) by auto
  thus \( \theta \text{thesis by (rule-tac } n=m \text{ in power-le-imp-le-base}) \)
qed

private lemma nat-power-inject-base: \( [ n \neq 0 \; a^n = b^n ] \implies (a::nat) = b \)
proof −
  assume \( n \neq 0 \) and \( ab: a^n = b^n \)
  then obtain \( m \) where \( n = \text{Suc} \; m \) by (frule-tac \( n=n \) in \( \text{not0-implies-Suc}, \text{auto} \))
  with \( ab \) have \( a^ \text{Suc} m = b^ \text{Suc} m \) and \( a \geq 0 \) and \( b \geq 0 \) by auto
  thus \( \theta \text{thesis by (rule power-inject-base}) \)
qed
1.1 Parametrisation of Pythagorean triples (over \( \mathbb{N} \) and \( \mathbb{Z} \))

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 \( \exists \ p \ q. \ a = p^2 - q^2 \land b = 2*p*q \land c = p^2 + q^2 \land \text{coprime} p q \)
proof –
  have two0: \((2::nat) \neq 0\) by simp
from abc have a2cb: \(a^2 = c^2 - b^2\) by arith
  — factor \(a^2\) in coprime factors \((c - b)\) and \((c + b)\); hence both are squares
have a2factor: \(a^2 = (c-b)*(c+b)\)
proof –
  have \(c*b - c*b = 0\) by simp
with a2cb have \(a^2 = c*c + c*b - c*b - b*b\) by (simp add: power2-eq-square)
  also have \(\ldots = c*(c+b) - b*(c+b)\)
  by (simp add: add-distrib mult-distrib mult.commute)
finally show ?thesis by (simp only: diff-distrib)
qed
have a-nonzero: \(a \neq 0\)
proof (rule ccontr)
  assume \(\neg a \neq 0\) hence \(a = 0\) by simp
  with aodd have \(\text{odd} (0::nat)\) by simp
  thus \(\text{False}\) by simp
qed
have b-less-c: \(b < c\)
proof –
  from abc have \(b^2 \leq c^2\) by auto
  with two0 have \(b \leq c\) by (rule-tac n=2 in nat-power-le-imp-le-base)
  moreover have\( b \neq c\)
  proof
    assume \(b=c\) with a2cb have \(a^2 = 0\) by simp
    with a-nonzero show \(\text{False}\) by (simp add: power2-eq-square)
  qed
ultimately show ?thesis by auto
qed
hence b2-le-c2: \(b^2 \leq c^2\) by (simp add: power-mono)
have bc-relprime: coprime b c
proof –
  from b2-le-c2 have cancelb2: \(c^2 - b^2 + b^2 = c^2\) by auto
  let \(?g = \gcd b c\)
  have \(?g^2 = \gcd (b^2) (c^2)\) by simp
  with cancelb2 have \(?g^2 = \gcd (b^2) (c^2 - b^2 + b^2)\) by simp
  hence \(?g^2 = \gcd (b^2) (c^2 - b^2)\) using gcd-add2[of b^2 c^2 - b^2]
    by (simp add: algebra-simps del: gcd-add1)
  with a2cb have \(?g^2 \text{ dvd } a^2\) by (simp only: gcd-dvd2)
  hence \(?g \text{ dvd } a \land \text{gcd} a b\) by simp
  hence \(?g \text{ dvd } \text{gcd} a b\) by (simp only: gcd-greatest)
  with ab-relprime show ?thesis
    by (simp add: ac-simps gcd-eq-1-imp-coprime)
qed
have p2: \(\text{prime} (2::nat)\) by simp
have factors-odd: \(\text{odd} (c-b) \land \text{odd} (c+b)\)
proof (auto simp only: ccontr)
assume even \((c-b)\)
with \(a\#factor\) have \(2 \vdvd a \cdot 2\) by \((simp\ only: dvd-mult2)\)
with \(p2\) have \(2 \vdvd a\) by auto
with \(a\#odd\) show False by simp

next
assume even \((c+b)\)
with \(a\#factor\) have \(2 \vdvd a \cdot 2\) by \((simp\ only: dvd-mult)\)
with \(p2\) have \(2 \vdvd a\) by auto
with \(a\#odd\) show False by simp

qed
have \(cb1\): \(c-b + (c+b) = 2*c\)
proof —
have \(c-b + (c+b) = ((c-b)+b)+c\) by simp
also with \(b-less-c\) have \(\ldots = (c+b-b)+c\) by \((simp\ only: diff-add-assoc)\)
also have \(\ldots = c+c\) by simp
finally show \(?thesis\) by simp

qed
have \(cb2\): \(2*b + (c-b) = c+b\)
proof —
have \(2*b + (c-b) = b+b + (c-b)\) by auto
also have \(\ldots = b + ((c-b)+b)\) by simp
also with \(b-less-c\) have \(\ldots = b + (c+b-b)\) by \((simp\ only: diff-add-assoc)\)
finally show \(?thesis\) by simp

qed
have \(factors-relprime\): \(coprime\ (c-b) (c+b)\)
proof —
let \(?g = gcd\ (c-b) (c+b)\)
have \(cb1\): \(c-b + (c+b) = 2*c\)
proof —
have \(c-b + (c+b) = ((c-b)+b)+c\) by simp
also with \(b-less-c\) have \(\ldots = (c+b-b)+c\) by \((simp\ only: diff-add-assoc)\)
also have \(\ldots = c+c\) by simp
finally show \(?thesis\) by simp

qed
have \(?g = gcd\ (c-b + (c+b)) (c+b)\) by simp
with \(cb1\) have \(?g = gcd\ (2*c) (c+b)\) by \((rule-tac\ a=c-b + (c+b)\) in back-subst)\)

dc:\ ?g \vdvd 2*c by \((simp\ only: gcd-dvd1)\)

have \(gcd\ (c-b) (2*b + (c-b)) = gcd\ (c-b) (2*b)\)
using \(gcd-add2\) of \(c-b 2*b + (c-b)\) by \((simp\ add: algebra-simps)\)
with \(cb2\) have \(?g = gcd\ (c-b) (2*b)\) by \((rule-tac\ a=2*b + (c-b)\) in back-subst)\)

hence \(g2b\): \(?g \vdvd 2*b\) by \((simp\ only: gcd-dvd2)\)

with \(g2c\) have \(?g \vdvd 2 * gcd\ b\ cd\) by \((simp\ only: gcd-greatest\ gcd-mult-distrib-nat)\)
with \(bc-relprime\) have \(?g \vdvd 2\) by simp

moreover have \(?g \neq 0\)
using \(b-less-c\) by auto

ultimately have \(1 \leq ?g\) \(?g \leq 2\)
by \((simp-all\ add: dvd-imp-le)\)
then have \(g1or2\): \(?g = 2 \lor ?g = 1\)
by arith
moreover have \(?g \neq 2\)

proof
assume \(?g = 2\)
moreover have \( q \) dvd \( c - b \)
by simp
ultimately show False
using factors-odd by simp
qed
ultimately show \( \text{thesis} \)
by (auto intro: gcd-eq-1-imp-coprime)

1.1 Parametrisation of Pythagorean triples (over \( \mathbb{N} \) and \( \mathbb{Z} \))
finally show \( ?\text{thesis} \) by auto
qed

moreover have \( a: a = p \cdot 2 - q \cdot 2 \)

proof -

from \( p \) have \( p \geq q \) by simp
hence \( p^{2} \cdot 2 \geq q^{2} \) by (simp only: power-mono)
from \( a^2 \cdot 2 \) and \( b \) and \( c \) have \( a^2 = (p^2 + q^2)^2 - (2 + p + q)^2 \) by simp
also have \( \ldots = (p^2)^2 + (q^2)^2 - 2 \cdot (p^2)^2 \cdot (q^2)^2 \)
by (auto simp add: power2-sum power-mult-distrib ac-simps)
also with \( p^{2} \cdot 2 \) \( q^{2} \) have \( \ldots = (p^2 - q^2)^2 \) by (simp only: nat-power2-diff)
finally have \( a^2 = (p^2 - q^2)^2 \) by simp
with \( \\text{two0} \) show \( ?\text{thesis} \) by (rule-tac n=2 in nat-power-inject-base)
qed

moreover have \( \text{coprime} \ p \ q \)

proof -

let \( ?k = \text{gcd} \ p \ q \)
have \( ?k \ \text{dvd} \ p \ \wedge \ ?k \ \text{dvd} \ q \) by simp
with \( b \) and \( a \) have \( ?k \ \text{dvd} \ a \ \wedge \ ?k \ \text{dvd} \ b \)
by (simp add: power2-eq-square)
hence \( ?k \ \text{dvd} \ \text{gcd} \ a \ b \) by (simp only: gcd-greatest)
with \( \text{ab-relprime} \) show \( ?\text{thesis} \)
by (auto intro: gcd-eq-1-imp-coprime)
qed

ultimately show \( ?\text{thesis} \) by auto
qed

Now for the case of integers. Based on \( \text{nat-euclid-pyth-triples} \).

private corollary \( \text{int-euclid-pyth-triples} \): \[ \begin{align*}
\text{coprime} \ (a::\text{int}) \ b; \ \text{odd} \ a; \\
\text{a}^2 + \text{b}^2 = \text{c}^2
\end{align*} \]
\( \Rightarrow \exists \ p \ q. \ a = p^2 - q^2 \ \wedge \ b = 2 \cdot p \cdot q \ \wedge \ |c| = p^2 + q^2 \ \wedge \ \text{coprime} \ p \ q \)

proof -

assume \( \text{ab-rel} \): \( \text{coprime} \ a \ b \) and \( \text{aodd} \): \( \text{odd} \ a \) and \( \text{abc} \): \( \text{a}^2 + \text{b}^2 = \text{c}^2 \)

let \( ?a = \text{nat}[a] \)
let \( ?b = \text{nat}[b] \)
let \( ?c = \text{nat}[c] \)

have \( \text{ab2-pos} \): \( \text{a}^2 \geq 0 \ \wedge \ \text{b}^2 \geq 0 \) by simp
hence \( \text{nat}(\text{a}^2) + \text{nat}(\text{b}^2) = \text{nat}(\text{a}^2 + \text{b}^2) \) by (simp only: nat-add-distrib)
with \( \text{abc} \) have \( \text{nat}(\text{a}^2) + \text{nat}(\text{b}^2) = \text{nat}(\text{c}^2) \) by presburger
hence \( \text{nat}([\text{a}]^2) + \text{nat}([\text{b}]^2) = \text{nat}([\text{c}]^2) \) by simp
hence \( \text{new-abc} \): \( ?a^2 + ?b^2 = ?c^2 \)
by (simp only: nat-mult-distrib power2-eq-square nat-add-distrib)

moreover from \( \text{ab-rel} \) have \( \text{new-ab-rel} \): \( \text{coprime} \ ?a \ ?b \)
by (simp add: gcd-int-def)

moreover have \( \text{new-a-odd} \): \( \text{odd} \ ?a \ \text{using} \ \text{aodd} \)
by simp

ultimately have
\( \exists \ p \ q. \ ?a = p^2 - q^2 \ \wedge \ ?b = 2 \cdot p \cdot q \ \wedge \ ?c = p^2 + q^2 \ \wedge \ \text{coprime} \ p \ q \)
by (rule-tac a=?a and b=?b and c=?c in nat-euclid-pyth-triples)

then obtain \( m \) and \( n \) where \( mn \):
\( ?a = m^2 - n^2 \ \wedge \ ?b = 2 \cdot m \cdot n \ \wedge \ ?c = m^2 + n^2 \ \wedge \ \text{coprime} \ m \ n \) by auto

have \( n^2 \leq m^2 \)
proof (rule ccontr)
1.1 Parametrisation of Pythagorean triples (over \( N \) and \( Z \))

assume \( n \cdot 2 \leq m \cdot 2 \) hence \( n \cdot 2 > m \cdot 2 \) by simp

with \( mn \) have \(?a = 0 \) by simp

with new-a-odd show False by simp

qed

moreover from \( mn \) have \( \text{int } ?a = \text{int}(m \cdot 2 - n \cdot 2) \) and \( \text{int } ?b = \text{int}(2 \cdot m \cdot n) \)

and \( \text{int } ?c = \text{int}(m \cdot 2 + n \cdot 2) \) by auto

ultimately have \( |a| = \text{int}(m \cdot 2) - \text{int}(n \cdot 2) \) and \( |b| = \text{int}(2 \cdot m \cdot n) \)

and \( |c| = \text{int}(m \cdot 2) + \text{int}(n \cdot 2) \) by (simp add: af-nat-diff)+

hence \( \|a\| = (\text{int } m)^2 - (\text{int } n)^2 \land |b| = 2 \cdot (\text{int } m) \cdot \text{int } n \)

\( \land |c| = (\text{int } m)^2 + (\text{int } n)^2 \) by (simp add: power2-eq-square)

from \( mn \) have \( \text{mn-rel: coprime } (\text{int } m) (\text{int } n) \)

by (simp add: gcd-int-def)

show \( \exists \ p q. \ a = p \cdot 2 - q \cdot 2 \land b = 2 \cdot p \cdot q \land |c| = p \cdot 2 + q \cdot 2 \land \text{coprime } p q \)

(is \( \exists \ p q. \ ?Q p q \)

proof (cases)

assume apos: \( a \geq 0 \) then obtain \( p \) where \( p = \text{int } m \) by simp

hence \( \exists \ q. \ ?Q p q \)

proof (cases)

assume bpos: \( b \geq 0 \) then obtain \( q \) where \( q = \text{int } n \) by simp

with \( p \) apos bpos mn-rel have \( ?Q p q \) by simp

thus \( ?thesis \) by (rule exI)

next

assume \( \neg b \geq 0 \) hence bneg: \( b < 0 \) by simp

then obtain \( q \) where \( q = - \text{int } n \) by simp

with \( p \) apos bneg mn-rel have \( ?Q p q \) by simp

thus \( ?thesis \) by (rule exI)

qed

thus \( ?thesis \) by (simp only: exI)

next

assume \( \neg a \geq 0 \) hence aneg: \( a < 0 \) by simp

then obtain \( p \) where \( p = \text{int } n \) by simp

hence \( \exists \ q. \ ?Q p q \)

proof (cases)

assume bpos: \( b \geq 0 \) then obtain \( q \) where \( q = \text{int } m \) by simp

with \( p \) aneg bpos mn-rel have \( ?Q p q \)

by (simp add: ac-simps)

thus \( ?thesis \) by (rule exI)

next

assume \( \neg b \geq 0 \) hence bneg: \( b < 0 \) by simp

then obtain \( q \) where \( q = - \text{int } m \) by simp

with \( p \) aneg bneg mn-rel have \( ?Q p q \)

by (simp add: ac-simps)

thus \( ?thesis \) by (rule exI)

qed

thus \( ?thesis \) by (simp only: exI)

qed
1.2 Fermat’s last theorem, case $n = 4$

Core of the proof. Constructs a smaller solution over $\mathbb{Z}$ of
\[ a^4 + b^4 = c^2 \land \text{coprime } a b \land abc \neq 0 \land a \text{ odd}. \]

**private lemma** smaller-fermat4:
**assumes** $abc: (a::int) \land a^4 + b^4 = c^2$ and $abc0: ab \land c \neq 0$ and $aodd: \text{odd } a$

**shows**
\[ \exists p q r \quad (p^*4 + q^*4 = r^*2 \land p^*q^*r \neq 0 \land \text{odd } p \land \text{coprime } p q \land r^*2 < c^*2) \]

**proof**

— put equation in shape of a pythagorean triple and obtain $u$ and $v$

**from** $\text{ab-relprime}$ **have** $ab2relprime$: $\text{coprime } (a^*2) (b^*2)$

**by** $\text{simp}$

**moreover from** $\text{aoddl have odds } (a^*2)$ **by** $\text{presburger}$

**moreover from** $\text{abc have } (a^*2)^*2 + (b^*2)^*2 = c^*2$ **by** $\text{simp}$

**ultimately obtain** $u$ and $v$ where $uvabc$:
\[ a^*2 = u^*2 - v^*2 \land b^*2 = 2u^*v \land |c| = u^*2 + v^*2 \land \text{coprime } u v \]

**by** ($\text{frule-tac a=a^*2 int euclid-pyth-triples, auto}$)

**with** $abc0$ **have** $uv0$: $u \neq 0 \lor v \neq 0$ **by** $\text{auto}$

**have** $\text{av-relprime: coprime } a v$

**proof**

— make again a pythagorean triple and obtain $k$ and $l$

**from** $uvabc$ **have** $a^*2 + v^*2 = u^*2$ **by** $\text{simp}$

**with** $\text{av-relprime and aoddl obtain } k l$ where

$klaov: a = k^*2 - l^*2 \land v = 2k^*l \land |a| = k^*2 + l^*2$ and $k-l: \text{coprime } k l$

**by** ($\text{frule-tac a=a in int euclid-pyth-triples, auto}$)

— prove $b = 2m$ and $k(k^2 + l^2) = m^2$, for coprime $k$, $l$ and $k^2 + l^2$

**from** $uvabc$ **have even** $(b^*2)$ **by** $\text{simp}$

**hence even** $b$ **by** $\text{simp}$

**then obtain** $m$ **where** $bm: b = 2m$ **using** $\text{evenE}$ **by** $\text{blast}$

**have** $|k| = |l| = k^*2 + l^*2 = m^*2$

**proof**

— from $bm$ **have** $4*m^*2 = b^*2$ **by** (simp only: $\text{power2-eq-square ac-simps}$)

**also have** $\ldots = |b^*2|$ **by** $\text{simp}$

**also with** $uvabc$ **have** $\ldots = 2|v||a|$ **by** (simp add: $\text{abs-mult}$)

**also with** $klaov$ **have** $\ldots = 2|2k*l||k^*2 + l^*2|$ **by** $\text{simp}$

**also have** $\ldots = 4*|k|*|l|*k^*2 + l^*2$ **by** (auto simp add: $\text{abs-mult}$)

**finally show** $?thesis$ **by** $\text{simp}$

**qed**

**moreover have** $(2::\text{nat}) > 1$ **by** $\text{auto}$
moreover from \( kl-rel \) have coprime \(|k| \wedge |l| \) by simp
moreover have coprime \(|l| \wedge (|k^2 + l^2|) \)
proof –
from \( kl-rel \) have coprime \((k+k*l) \) \( l \)
by simp
hence coprime \((k+k*l*l) \) \( l \) using gcd-add-mult \(|of \ l \ k*k| \)
by (simp add: ac-simps gcd-eq-1-imp-coprime)
hence coprime \( l \) \((k^2+l^2) \)
by (simp add: power2-eq-square ac-simps)
thus ?thesis by simp
qed
moreover have coprime \(|k^2 + l^2| \wedge |k| \)
proof –
from \( kl-rel \) have coprime \( l \) \( k \)
by (simp add: ac-simps)
hence coprime \((l*l+k+k*l) \) \( k \) using gcd-add-mult\(|of \ k \ k*l| \)
by (simp add: ac-simps gcd-eq-1-imp-coprime)
hence coprime \( k \) \((k^2+l^2) \)
by (simp add: power2-eq-square ac-simps)
thus ?thesis by simp
qed
ultimately have \( \exists \ x \ y \ z. \ |k| = x^2 \wedge |l| = y^2 \wedge |k^2 + l^2| = z^2 \)
using int-relprime-power-divisors\(|of \ 2 \ |k| \ |l| \ wedge |k^2 + l^2| \ m| \)
int-relprime-power-divisors\(|of \ 2 \ |k| \ |l| \ wedge |k^2 + l^2| \ m| \)
int-relprime-power-divisors\(|of \ 2 \ |k^2 + l^2| \ |k*l| \ m| \)
by (simp-all add: ac-simps)
then obtain \( \alpha \ \beta \ \gamma \) where \( \text{albega} \):
\(|k| = \alpha^2 \wedge |l| = \beta^2 \wedge |k^2 + l^2| = \gamma^2 \)
by auto
— show this is a new solution
have \( k^2 = \alpha^4 \)
proof –
from \( \text{albega} \) have \(|k|^2 = (\alpha^2)^2 \) by simp
thus ?thesis by simp
qed
moreover have \( l^2 = \beta^4 \)
proof –
from \( \text{albega} \) have \(|l|^2 = (\beta^2)^2 \) by simp
thus ?thesis by simp
qed
moreover have \( \gamma^2 \): \( k^2 + l^2 = \gamma^2 \)
proof –
have \( k^2 \geq 0 \wedge l^2 \geq 0 \) by simp
with \( \text{albega} \) show ?thesis by auto
qed
ultimately have \( \text{newabc} \): \( \alpha^4 + \beta^4 = \gamma^2 \) by auto
from \( uv0 \ klavu \ \text{albega} \) have \( \text{albega0} \): \( \alpha \beta \gamma \neq 0 \) by auto
— show the coprimality
have alphabeta-relprime: coprime \( \alpha \beta \)
proof (rule classical)
let \( g = \gcd \alpha \beta \)

assume \( \neg \text{coprime } \alpha \beta \)

then have \( \text{gnot1: } g \neq 1 \)

by (auto intro: gcd-eq-1-imp-coprime)

have \( g > 1 \)

proof

have \( g \neq 0 \)

proof

assume \( g = 0 \)

hence \( \text{nat } |\alpha| = 0 \) by simp

hence \( \alpha = 0 \) by arith

with albega0 show False by simp

qed

hence \( g > 0 \) by auto

with gnot1 show \( \text{thesis by linarith} \)

qed

moreover have \( g \text{ dvd } \gcd k l \)

proof

have \( g \text{ dvd } \alpha \wedge g \text{ dvd } \beta \) by auto

with albega have \( g \text{ dvd } |k| \wedge g \text{ dvd } |l| \)

by (simp add: power2-eq-square mult.commute)

hence \( g \text{ dvd } k \wedge g \text{ dvd } l \) by simp

thus \( \text{thesis by simp} \)

qed

ultimately have \( \gcd k l \neq 1 \) by fastforce

with kl-rel show \( \text{thesis by auto} \)

qed

— choose \( p \) and \( q \) in the right way

have \( \exists p q. p^4 + q^4 = \gamma^2 \wedge p \neq 0 \wedge \text{odd } p \wedge \text{coprime } p q \)

proof

have odd \( \alpha \vee \text{odd } \beta \)

proof (rule ccontr)

assume \( \neg (\text{odd } \alpha \vee \text{odd } \beta) \)

hence \( \text{even } \alpha \wedge \text{even } \beta \) by simp

then have \( 2 \text{ dvd } \alpha \wedge 2 \text{ dvd } \beta \) by simp

then have \( 2 \text{ dvd } \gcd \alpha \beta \) by simp

with alphabeta-relprime show False by auto

qed

moreover

\{ assume \( \text{odd } \alpha \)

with newabc albega0 alphabeta-relprime obtain \( p q \) where

\( p = \alpha \wedge q = \beta \wedge p^4 + q^4 = \gamma^2 \wedge p \neq 0 \wedge \text{odd } p \wedge \text{coprime } p q \)

by auto

hence \( \text{thesis by auto} \) \}

moreover

\{ assume \( \text{odd } \beta \)

with newabc albega0 alphabeta-relprime obtain \( p q \) where

\( q = \alpha \wedge p = \beta \wedge p^4 + q^4 = \gamma^2 \wedge p \neq 0 \wedge \text{odd } p \wedge \text{coprime } p q \)

by (auto simp add: ac-simps)

hence \( \text{thesis by auto} \) \}

ultimately show \( \text{thesis by auto} \)

qed
1.2 Fermat’s last theorem, case $n = 4$  

— show the solution is smaller  
moreover have $\gamma^2 < c^2$

proof –
from $\gamma^2 \leq |u|$ by simp
also have $h1: \ldots \leq |u|^2$ using self-le-power[of $|u|$ 2] $uv0$ by auto
also have $h2: \ldots \leq u^2$ by simp
also have $h3: \ldots < u^2 + v^2$

proof –
from $uv0$ have $v^2 \neq 0$ by simp
with $v^2 \neq 0$ have $0 < v^2$ by (auto simp add: less_le)
thus $\vdash \text{thesis by auto}$
qed
also with $uvabc$ have $\ldots \leq |c|$ by auto
also have $\ldots \leq c^2$ by simp
finally show $\vdash \text{thesis by simp}$
qed
ultimately show $\vdash \text{thesis by auto}$
qed

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

private lemma no-rewritten-fermat4:
$\neg (\exists (a::int) b. (a^4 + b^4 = c^2 \land a*b*c \neq 0 \land \text{odd } a \land \text{coprime } a \ b))$

proof (induct c rule: infinite-descent0-measure[where $V=\lambda c. \text{nat}(c^2)$])

case (0 x)
have $x^2 \geq 0$ by (rule zero-line)
with $0 < x^2$ by (auto simp add: less_le)
thus $\vdash \text{thesis by auto}$
qed
next

case (smaller x)
then obtain $a b$ where $a^4 + b^4 = x^2$ and $a*b*x \neq 0$
and $\text{odd } a$ and $\text{coprime } a \ b$ by auto
hence $\exists p q r. (p^4 + q^4 = r^2 \land p*q*r \neq 0 \land \text{odd } p$
$\land \text{coprime } p \ q \ r^2 < x^2$) by (rule smaller-fermat4)
then obtain $p q r$ where $pqr$: $p^4 + q^4 = r^2 \land p*q*r \neq 0 \land \text{odd } p$
$\land \text{coprime } p \ q \ r^2 < x^2$ by auto
have $r^2 \geq 0$ and $x^2 \geq 0$ by (auto simp only: zero-line)

hence $\text{int}(\text{nat}(r^2)) = r^2 \land \text{int}(\text{nat}(x^2)) = x^2$ by auto

with $pqr$ have $\text{int}(\text{nat}(r^2)) < \text{int}(\text{nat}(x^2))$ by auto
hence $\text{nat}(r^2) < \text{nat}(x^2)$ by presburger

with $pqr$ show $\vdash \text{thesis by auto}$
qed

The theorem. Puts equation in requested shape.

theorem fermat-4:
assumes $\text{ass: } (x::int)^4 + y^4 = z^4$
shows $x*y*z = 0$
proof (rule ccontr)
let $?g = gcd x y$
Pythagorean triples and Fermat’s last theorem, case \( n = 4 \)

let \( c = (z \div \gcd) \cdot 2 \)
assume \( xyz0 : x+y+z \neq 0 \)
— divide out the g.c.d.
hence \( x \neq 0 \lor y \neq 0 \) by simp
then obtain \( a \ b \) where \( ab : x = \gcd \cdot a \land y = \gcd \cdot b \land \text{coprime} \ a \ b \)
using \( \gcd:\text{-}\coprime:\text{exists}[of \ x \ y] \) by (auto simp: mult.commute)
moreover have \( abc : a^4 + b^4 = c^2 \land a \cdot b \cdot c \neq \) 0
proof
have \( zgab : z^4 = (a^4 + b^4) \cdot c^2 \)
proof
from \( ab \) have \( z^4 = (\gcd \cdot a)^4 + (\gcd \cdot b)^4 \) by simp
thus ?thesis by (simp only: power2-eq-square ac-simps)
qed
have \( cgz : z^2 = c \cdot \gcd^2 \)
proof
from \( zgab \) have \( \gcd^4 \mid z^4 \) by simp
hence \( \gcd \mid z \) by simp
hence \( (z \div \gcd) \cdot \gcd = z \) by (simp only: ac-simps dvd-mult-div-cancel)
with \( ab \) show ?thesis by (auto simp only: power2-eq-square ac-simps)
qed
with \( xyz0 \) have \( c0 : c \neq 0 \) by (auto simp add: power2-eq-square)
from \( xyz0 \) have \( g0 : \gcd \neq 0 \) by simp
have \( a^4 + b^4 = c^2 \)
proof
have \( c^2 \cdot \gcd^4 = (a^4 + b^4) \cdot \gcd^4 \)
proof
have \( c^2 \cdot \gcd^4 = (\gcd \cdot a^2)^2 \cdot \gcd^2 \) by algebra
also with \( cgz \) have \( \ldots = (z^2)^2 \) by simp
also have \( \ldots = z^4 \) by algebra
also with \( zgab \) have \( \ldots = \gcd^4 \cdot (a^4 + b^4) \) by simp
finally show ?thesis by simp
qed
with \( g0 \) show ?thesis by auto
qed
moreover from \( ab \ xyz0 \) \( c0 \) have \( a \cdot b \cdot c \neq 0 \) by auto
ultimately show ?thesis by simp
qed
— choose the parity right
have \( \exists p \ q \ p^4 + q^4 = c^2 \land p \cdot q \cdot c \neq 0 \land \text{odd} \ p \land \text{coprime} \ p \ q \)
proof
have \( \neg\text{odd} a \lor \text{odd} b \)
proof (rule \text{contra})
assume \( \neg(\text{odd} a \lor \text{odd} b) \)
hence \( 2 \mid d \div d \) by simp
hence \( 2 \mid d \) by simp
with \( ab \) show False by auto
qed
moreover
{ assume odd \( a \)
  then obtain \( p \ q \) where \( p = a \) and \( q = b \) and odd \( p \) by simp
  with \( ab \) \( abc \) have ?thesis by auto }
moreover
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: \((n::int) > 0 \implies \exists k. 2 \cdot |a - k \cdot n| \leq n\)
proof –
assume a: \(n > 0\)
define k where k = a div n
have h: \(a - k \cdot n = a \mod n\) by (simp add: div-mult-mod-eq algebra-simps k-def)
thus \(\text{thesis}\)
proof (cases \(2 \cdot (a \mod n) \leq n\))
case True
hence $2 \cdot |a - k \cdot n| \leq n$ using $h$ pos-mod-sign $a$ by auto
thus $?thesis$ by blast
next
case False
hence $2 \cdot (n - a \mod n) \leq n$ by auto
have $a - (k+1) \cdot n = a \mod n - n$ using $h$ by (simp add: algebra-simps)
hence $2 \cdot |a - (k+1) \cdot n| \leq n$ using $h$ pos-mod-bound[of $n$ $a$] a False by fastforce
thus $?thesis$ by blast
qed
definition is-qfN :: int $\Rightarrow$ int $\Rightarrow$ bool where
is-qfN $A$ $N$ $\leftrightarrow$ ($\exists$ $x$ $y$. $A = x^2 + N \cdot y^2$)
definition is-cube-form :: int $\Rightarrow$ int $\Rightarrow$ bool where
is-cube-form $a$ $b$ $\leftrightarrow$ ($\exists$ $p$ $q$. $a = p^3 - 9 \cdot p \cdot q^2 \land b = 3 \cdot p^2 \cdot q - 3 \cdot q^3$)

2.2 Basic facts if $N \geq 1$

lemma qfN-pos: [ $N \geq 1$; is-qfN $A$ $N$ ] $\Rightarrow$ $A \geq 0$
proof
assume $N$: $N \geq 1$ and is-qfN $A$ $N$
then obtain $a$ $b$ where $ab$: $A = a^2 + N \cdot b^2$ by (auto simp add: is-qfN-def)
have $N \cdot b^2 \geq 0$
proof (cases)
assume $b = 0$ thus $?thesis$ by auto
next
assume $b = 0$ hence $b^2 > 0$ by simp
moreover from $N$ have $N > 0$ by simp
ultimately have $N \cdot b^2 > N \cdot 0$ by (auto simp only: zmult-zless-mono2)
thus $?thesis$ by auto
2.3 Multiplication and division

lemma qfN-zero: \[ \[ (N::int) \geq 1; a^2 + N \cdot b^2 = 0 \] \implies (a = 0 \land b = 0) \]
proof -
assume N: N \geq 1 and abN: a^2 + N \cdot b^2 = 0
show \?thesis
proof (rule ccontr, auto)
assume a \neq 0 hence a^2 > 0 by simp
moreover from N have N > 0 by simp
ultimately have N \cdot b^2 > N \cdot 0 by (auto simp only: zmult-zless-mono2)
thus \?thesis by auto
qed
ultimately have a^2 + N \cdot b^2 > 0 by arith
with abN show False by auto
next
assume b \neq 0 hence b^2 > 0 by simp
moreover from N have N > 0 by simp
ultimately have N \cdot b^2 > N \cdot 0 by (auto simp only: zmult-zless-mono2)
ultimately have a^2 \geq 0 by (rule zero-le-power2)
ultimately have a^2 + N \cdot b^2 > 0 by arith
with abN show False by auto
qed

2.3 Multiplication and division

lemma qfN-mult1: \[ ((a::int))^2 + N \cdot b^2 \cdot (c^2 + N \cdot d^2) \]
\[ = (a + c + N \cdot b \cdot d)^2 + N \cdot (a \cdot d - b \cdot c)^2 \]
by (simp add: eval-nat-numeral field-simps)

lemma qfN-mult2: \[ ((a::int))^2 + N \cdot b^2 \cdot (c^2 + N \cdot d^2) \]
\[ = (a - c + N \cdot b \cdot d)^2 + N \cdot (a \cdot d + b \cdot c)^2 \]
by (simp add: eval-nat-numeral field-simps)

corollary is-qfN-mult: \[ is-qfN A N \implies is-qfN B N \implies is-qfN (A \cdot B) N \]
by (unfold is-qfN-def, auto, auto simp only: qfN-mult1)

corollary is-qfN-power: \[ (n::nat) > 0 \implies is-qfN A N \implies is-qfN (A \cdot n) N \]
by (induct n, auto, case-tac n=0, auto simp add: is-qfN-mult)

lemma qfN-div-prime:
  fixes p :: int
assumes \( \text{prime} \ (p^2+Nq^2) \land (p^2+Nq^{-2}) \\vdash (a^2+Nb^2) \) 

shows \( \exists \ v \ u. \ a^2+Nb^2 = (u^2+Nv^2)*(p^2+Nq^2) \) 
\( \land (\exists \ e. \ a = p*u+e*Nq*v \land b = p*v - e*q*u \land |e| = 1) \)

proof

let \( ?P = p^2+Nq^2 \)

let \( ?A = a^2+Nb^2 \)

from \( \text{ass} \) obtain \( U \) where \( U: ?A = ?P*U \) by (auto simp only: dvd-def)

have \( \exists \ e. \ ?P \vdash b*p + e*a*q \land |e| = 1 \) 
proof

have \( ?P \vdash (b*p + a*q)*(b*p - a*q) \)

proof

have \( (b*p + a*q)*(b*p - a*q) = b^2*?P - q^2*?A \)

by (simp add: eval-nat-numeral field-simps)

also from \( U \) have \( \ldots = (b^2 - q^2*U)*?P \) by (simp add: field-simps)

finally show \( \text{thesis} \) by simp

qed

with \( \text{ass} \) have \( ?P \vdash (b*p + a*q) \lor ?P \vdash (b*p - a*q) \)

by (simp add: nat-abs-mult-distrib prime-int-iff prime-dvd-mult-iff)

moreover

\{ assume \( ?P \vdash b*p + a*q \) 
  hence \( ?P \vdash b*p + 1*a*q \land |1| = (1::int) \) by simp \}

moreover

\{ assume \( ?P \vdash b*p - a*q \) 
  hence \( ?P \vdash b*p + (-1)*a*q \land |-1| = (1::int) \) by simp \}

ultimately show \( \text{thesis} \) by blast

qed

then obtain \( v \ e \) where \( v: b*p + e*a*q = ?P*v \) and \( e: |e| = 1 \) 

by (auto simp only: dvd-def)

have \( ?P \vdash a*p - e*N*b*q \)

proof (cases)

assume \( e1: e = 1 \)

from \( U \) have \( U \vdash ?P^2 = ?A \vdash ?P \) by (simp add: power2-eq-square)

also with \( e1 \) have \( \ldots = (a*p-e*N*b*q)^2 + N*(b*p+e*a*q)^2 \)

by (simp only: qN-mult2 add.commute mult-1-left)

also with \( v \) have \( \ldots = (a*p-e*N*b*q)^2 + N*v^2*?P^2 \)

by (simp only: power-mult-distrib ac-simps)

finally have \( (a*p-e*N*b*q)^2 = ?P^2*(U-N*v^2) \)

by (simp add: ac-simps left-diff-distrib)

hence \( ?P^2 \vdash (a*p - e*N*b*q)^2 \) by (rule dvdI)

thus \( \text{thesis} \) by simp

next

assume \( \neg e = 1 \) with \( e: e = -1 \) by auto

from \( U \) have \( U \vdash ?P^2 = ?A \vdash ?P \) by (simp add: power2-eq-square)

also with \( e1 \) have \( \ldots = (a*p-e*N*b*q)^2 + N*(-(b*p+e*a*q))^2 \)

by (simp add: qN-mult1)

also have \( \ldots = (a*p-e*N*b*q)^2 + N*(b*p+e*a*q)^2 \)

by (simp only: power2-minus)

also with \( v \) have \( \ldots = (a*p-e*N*b*q)^2 + N*v^2*?P^2 \)

by (simp only: power-mult-distrib ac-simps)

finally have \( (a*p-e*N*b*q)^2 = ?P^2*(U-N*v^2) \)

by (simp add: ac-simps left-diff-distrib)

hence \( ?P^2 \vdash (a*p-e*N*b*q)^2 \) by (rule dvdI)
thus ?thesis by simp

qed

then obtain u where u: a*p - e*N*b*q = ?P*u by (auto simp only: dvd-def)

from e have e2-1: e * e = 1

using abs-mult-self-eq [of e] by simp

have a: a = p*u + e*N*q*v proof

have (p*u + e*N*q*v)*?P = p*(?P*u) + (e*N*q)*(?P*v)

by (simp only: distrib-right ac-simps)

also with v u have ... = p*(a*p - e*N*b*q) + (e*N*q)*(b*p + e*a*q) by simp

also have ... = a*(p^2 + e*e*N*q^2)

by (simp add: power2-eq-square distr left-diff-distrib)

also with e2-1 have ... = a * ?P by simp

finally have (a-(p*u+e*N*q*v))*?P = 0 by auto

moreover from ass have ?P ≠ 0 by auto

ultimately show ?thesis by simp

qed

moreover have: b = p*v - e*q*u

proof (cases)

assume e=1

with a and b show ?thesis by (simp add: qfN-mult1 ac-simps)

next

assume ¬ e=1 with e have e=−1 by simp

with a and b show ?thesis by (simp add: qfN-mult2 ac-simps)

qed

moreover have ?A = (a^2 + N*v^2)*?P

proof

assume e=1

with a and b show ?thesis by simp

next

assume ¬ e=1 with e have e=−1 by simp

with a and b show ?thesis by simp

qed

moreover have |e| = 1 .

ultimately show ?thesis by blast

qed

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)

apply (subgoal_tac [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), blast)

apply (rule qfN-div-prime, auto)

done

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
apply (subgoal-tac $\exists\ u\ v.\ A = (u^2 + N*v^2)*P$)
apply (unfold is-qfN-def, auto)
apply (simp only: qfN-div-prime-weak)
done

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 $\exists\ u\ v.\ a^2 + N*b^2 = (u^2 + N*v^2)*(p^2 + N*q^2)$ ∧ coprime $u\ v$
∧ ($\exists\ e.\ a = p*u + e*N*q*v$ ∧ $b = p*v - e*q*u$ ∧ $|e| = 1$)
proof –
from $ass$ have $P$ dvd $A$ ∧ $n > 0$ by simp
hence $P^n$ dvd $A^n$ by simp
then obtain $U$ where $U: A^n = U*P^n$ by (auto simp only: dvd-def ac-simps)
from $ass$ have coprime $a\ b$
by blast
have $\exists\ e.\ P^n$ dvd $b*p + e*a*q$ ∧ $|e| = 1$
proof –
have $Pn$-dvd-prod: $P^n$ dvd $(b*p + a*q)*(b*p - a*q)$
proof –
have $(b*p + a*q)*(b*p - a*q) = (b*p)^2 - (a*q)^2$
by (simp add: power2-eq-square algebra-simps)
also have $\ldots = b^2*p^2 + b^2*N*q^2 - b^2*p*N*q^2 - a^2*q^2$
by (simp add: power-mult-distrib)
also with $ass$ have $\ldots = b^2*P^n - q^2*A^n$
by (simp only: ac-simps distrub-right distrub-left)
also with $U$ have $\ldots = (b^2 - q^2*U)*P^n$ by (simp only: left-diff-distrib)
finally show ?thesis by (simp add: ac-simps)
qed
have $P^n$ dvd $(b*p + a*q) \lor P^n$ dvd $(b*p - a*q)$
proof –
have $PdvdPn$: $P$ dvd $P^n$
proof –
from $ass$ have $\exists\ m.\ n = Suc\ m$ by (simp add: not0-implies-Suc)
then obtain $m$ where $n = Suc\ m$ by auto
hence $P^n = P^{*(P^m)}$ by auto
thus ?thesis by auto
qed
have $\neg P$ dvd $b*p + a*q$ \lor $\neg P$ dvd $b*p - a*q$
proof (rule ccontr, simp)
assume $P$ dvd $b*p + a*q$ ∧ $P$ dvd $b*p - a*q$

hence $P$ dvd $(b*p + a*q) + (b*p - a*q) \land P$ dvd $(b*p + a*q) - (b*p - a*q)$
by (simp only: dvd-add, simp only: dvd-diff)

hence $P$ dvd $2*(b*p)$ ∧ $P$ dvd $2*(a*q)$ by (simp only: mult-2, auto)
with $ass$ have $(P$ dvd $2 \lor P$ dvd $b*p) \land (P$ dvd $2 \lor P$ dvd $a*q)$
using prime-dvd-multD by blast
hence $P$ dvd $2 \lor (P$ dvd $b*p \land P$ dvd $a*q)$ by auto
moreover have $\neg P$ dvd $2$
proof (rule ccontr, simp)
assume $pdvd2$: $P$ dvd $2$

hence $P \leq 2$
proof (rule ccontr)
  assume \( \neg P \leq 2 \) hence \( P > 2 \) by simp
  with pdvd2 show False by (simp add: zdvd-not-zless)
qed

moreover from ass have \( P > 1 \) by (simp add: prime-int-iff)
ultimately have \( P=2 \) by auto
with ass have \( \text{odd } 2 \) by simp
thus False by simp
qed

ultimately have \( P \text{ dvd } b \^ P \land P \text{ dvd } a \^ q \) by auto
with ass have \( \text{gcd } p (N^*q) \) by simp
using prime-dvd-multD by blast
moreover have \( \neg P \text{ dvd } b \land \neg P \text{ dvd } q \)
  proof (auto dest: ccontr)
    assume \( P \text{ dvd } (q^*q) \)
    hence \( P \text{ dvd } q \) using prime-dvd-multD ass by blast
  
ultimately have \( P \text{ dvd } (N^*q) \) by fastforce
with PdvdP have \( P \text{ dvd } (N^*q) \) by simp
with ass show False by (simp add: prime-int-iff)

next
assume \( P \text{ dvd } q \)
  hence \( P \text{ dvd } (q^*q) \) by simp
  hence \( P \text{ dvd } N^*q \) by simp
  hence \( P \text{ dvd } N^*q^*q \) by simp
  hence \( P \text{ dvd } N^*q^*q^*q \) by (simp add: power2-eq-square ac-simps)
  with PdvdPn have \( P \text{ dvd } N^*q^*q^*q \) by (simp only: dvd-diff)
  with ass show \( \neg P \text{ dvd } b \land \neg P \text{ dvd } a \)
  proof (auto dest: prime-dvd-multD)
    assume \( \neg P \text{ dvd } b \land \neg P \text{ dvd } a \)
    with \( \text{gcd } b \land \text{gcd } a \) by auto
  
ultimately show \?thesis by auto

qed

ultimately have \( P \text{ dvd } b \land P \text{ dvd } a \land \neg P \text{ dvd } b \land \neg P \text{ dvd } a \)
with \( P_n \text{-dvd-prod} \) and ass have \( P \text{-dvd } b \^ P \land \neg P \text{-dvd } a \)
  by (rule-tac \( b \)\(+\)a\) in prime-power-dvd-cancel-right, auto simp add: mult.commute)
moreover
{ assume \( \neg P \text{ dvd } b \land \neg P \text{ dvd } a \)
  with \( P_n \text{-dvd-prod} \) and ass have \( P \text{-dvd } b \land \neg P \text{-dvd } a \)
    by (rule-tac a\(+\)a in prime-power-dvd-cancel-right, simp) }
ultimately show \?thesis by auto
The quadratic form $x^2 + Ny^2$

qed
moreover
{ assume P^n dvd b*p + a*q
  hence P^n dvd b*p + 1*a*q ∧ |I| = (1::int) by simp }
moreover
{ assume P^n dvd b*p - a*q
  hence P^n dvd b*p + (-1)*a*q ∧ |I| = (1::int) by simp }
ultimately show "thesis by blast"

qed
then obtain v e where v: b*p + e*a*q = P^n*v and e: |e| = 1
by (auto simp only: dvd-def)
have P^n dvd a*p - e*N*b*q
proof (cases)
  assume e1: e = 1
  from U have (P^n)^2*U = A^n*P^n by (simp add: power2-eq-square ac-simps)
  also with e1 ass have ... = (a*p - e*N*b*q)^2 + N*(b*p + e*a*q)^2
    by (simp only: qfN-mult2 add.commute mult-1-left)
  also with v have ... = (a*p - e*N*b*q)^2 + (P^n)^2*N*v^2
    by (simp only: power-mult-distrib ac-simps)
  finally have (a*p - e*N*b*q)^2 = (P^n)^2*U - (P^n)^2*N*v^2 by simp
  also have ... = (P^n)^2 * (U - N*v^2) by (simp only: right-diff-distrib)
  finally have (P^n)^2 dvd (a*p - e*N*b*q)^2 by (rule dvdI)
  thus "thesis by simp"

next
  assume e1: e = -1 with e have e1: e = -1 by auto
  from U have (P^n)^2*U = A^n*P^n by (simp add: power2-eq-square)
  also with e1 ass have ... = (a*p - e*N*b*q)^2 + N*(-(b*p + e*a*q))^2
    by (simp add: qfN-mult1)
  also have v and ass have ... = (a*p - e*N*b*q)^2 + N*v^2*(P^n)^2
    by (simp only: power-mult-distrib ac-simps)
  finally have (a*p - e*N*b*q)^2 = (P^n)^2*U - (P^n)^2*N*v^2 by simp
  also have ... = (P^n)^2 * (U - N*v^2) by (simp only: right-diff-distrib)
  finally have (P^n)^2 dvd (a*p - e*N*b*q)^2 by (rule dvdI)
  thus "thesis by simp"

qed
then obtain u where u: a*p - e*N*b*q = P^n*u by (auto simp only: dvd-def)
from e have e2-1: e * e = 1
  using abs-mult-self-eq [of e] by simp
have a: a = p*u + e*N*q*v
proof -
  from ass have (p*u + e*N*q*v)*P^n = p*(P^n*u) + (e*N*q)*(P^n*v)
    by (simp only: distrib-right ac-simps)
  also with v and u have ... = p*(a*p - e*N*b*q) + (e*N*q)*(b*p + e*a*q)
    by simp
  also have ... = a*(p^2 + e*e*N*q^2)
    by (simp add: power2-eq-square distrib-left ac-simps right-diff-distrib)
  also with e2-1 and ass have ... = a*P^n by simp
  finally have (a - (p*u + e*N*q*v))*P^n = 0 by auto
  moreover from ass have P^n ≠ 0
    by (unfold prime-int-iff , auto)
ultimately show \( \text{thesis} \) by auto
qed
moreover have \( b: b = p*v - e*q*u \)
proof –
  from ass have \((p*v - e*q*u)*P^n = p*(P^n*v) - (e*q)*(P^n*u)\)
    by (simp only: left-diff-distrib ac-simps)
  also with \( v \) and \( u \) have \( \ldots = p*(b*p + e*a*q) - e*q*(a*p - e*N*b*q) \) by simp
  also have \( \ldots = b*(p^2 + e*e*N*q^2) \)
    by (simp add: power2-eq-square distrib-left ac-simps right-diff-distrib)
  also with \( e2 \) and ass have \( \ldots = b*P^n \) by simp
finally have \((b - (p*v - e*q*u))*P^n = 0 \) by auto
moreover from ass have \( P^n \neq 0 \)
by (unfold prime-int-iff, auto)
ultimately show \( \text{thesis} \) by auto
qed
moreover have \( A^n = (u^2 + N*v^2)*P^n \)
proof (cases)
  assume \( e = -1 \)
  with \( a \) and \( b \) and ass show \( \text{thesis} \) by (simp add: qfN-mult1 ac-simps)
next
  assume \( \neg e = -1 \) with \( e \) have \( e = -1 \) by simp
  with \( a \) and \( b \) and ass show \( \text{thesis} \) by (simp add: qfN-mult2 ac-simps)
qed
moreover have \( \text{coprime} u v \)
using \( \text{coprime} a \) b
proof (rule coprime-imp-coprime)
fix \( w \)
assume \( w \text{ dvd} u \) \( w \text{ dvd} v \)
then have \( w \text{ dvd} u*p + v*(e*N*q) \wedge w \text{ dvd} v*p - u*(e*q) \)
  by simp
  with \( a \) \text{ and } \( b \) \text{ and } ass show \( \text{thesis} \) by (auto simp only: ac-simps)
qed
moreover from \( e \) and ass have
\[ |e| = 1 \wedge A^n = a^2 + N*b^2 \wedge P^n = p^2 + N*q^2 \]
ultimately show \( \text{thesis} \) by auto
qed

lemma qfN-primedivisor-not:
assumes \( \text{ass: prime } P \wedge Q > 0 \wedge \text{is-qfN } (P*Q) \wedge \neg \text{is-qfN } P \wedge N \)
shows \( \exists R. (\text{prime } R \wedge R \text{ dvd } Q \wedge \neg \text{is-qfN } R \wedge N) \)
proof (rule contr, auto)
assume \( \text{ass2: } \forall R. R \text{ dvd } Q \rightarrow \text{prime } R \rightarrow \text{is-qfN } R \wedge N \)
define \( ps \) where \( ps = \text{prime-factorization } (\text{nat } Q) \)
from ass have \( ps:(\forall p \in \text{set-mset } ps. \text{ prime } p) \wedge Q = \text{ int} (\bigprod i \in \# ps. i) \)
  by (auto simp: ps-def prod-mset-prime-factorization-int)
have \( ps \text{-lemma: } (\forall p \in \text{set-mset } ps. \text{ prime } p) \wedge \text{is-qfN } (P*\text{int}(\bigprod i \in \# ps. i)) \wedge (\forall R. (\text{prime } R \wedge R \text{ dvd } Q \wedge \neg \text{is-qfN } R \wedge N)) \rightarrow \text{False} \)
(is \( ?B ps \rightarrow \text{False} \))
proof (induct \( ps \))
case empty hence \( \text{is-qfN } P \wedge N \) by simp
with ass show \( \text{False} \) by simp
24 2 The quadratic form $x^2 + Ny^2$

next

\[ (add \ p \ ps) \]

**hence** $\exists B \ ps \Rightarrow False$

and $IH: \exists B (ps + \{#p\})$ by simp-all

hence $p: prime (int \ p)$ and $int \ p \ dvd \ int(\prod_{i \in #ps + \{#p\}} i)$ by auto

moreover with $IH$ have $pgfN: \ is-qfN (int \ p) \ N$

and $int \ p \ dvd \ P \ * \ int(\prod_{i \in #ps + \{#p\}} i)$ and $is-qfN (P * int(\prod_{i \in #ps + \{#p\}} i)) \ N$

by auto

ultimately obtain $S$ where $S: P * int(\prod_{i \in #ps + \{#p\}} i) = S * (int \ p) \land \ is-qfN \ S \ N$

using $qfN-div-prime-general$ by blast

hence $(\prod p * int(\prod_{i \in #ps + \{#p\}} i) - S) = 0$ by auto

with $p \ S$ have $is-qfN (P * int(\prod_{i \in #ps + \{#p\}} i)) \ N$ by (auto simp add: prime-int-iff)

moreover from $IH$ have $\forall R. \ prime \ R \land R \ dvd \ int(\prod_{i \in #ps + \{#p\}} i) \longrightarrow \ is-qfN \ R \ N$

by auto

ultimately have $\exists B \ ps \ by \ simp$

with $ass3$ show $False \ by \ simp$

qed

with $ps \ ass2 \ ass \ show \ False \ by \ auto$

qed

**lemma** $prime-factor-int$:

fixes $k :: int$

assumes $|k| \neq 1$

obtains $p$ where $prime \ p \ p \ dvd \ k$

proof (cases $k = 0$)

case True

then have $prime (2 :: int)$ and $2 \ dvd \ k$

by simp-all

with that show $thesis$

by blast

next

case False

with $assms$ $prime-divisor-exists$ [of $k$] obtain $p$ where $prime \ p \ p \ dvd \ k$

by auto

with that show $thesis$

by blast

qed

**lemma** $qfN-oddprime-cube$:

\[ prime (p^2 + N * q^2 :: int); \ odd (p^2 + N * q^2); \ p \neq 0; \ N \geq 1 \]

\[ \Rightarrow \ \exists a \ b. (p^2 + N * q^2)^3 = a^2 + N * b^2 \land \ coprime \ a (N * b)$

proof –

let $\forall P = p^2 + N * q^2$

assume $P: \ prime \ ?P \ and \ Podd: \ odd \ ?P \ and \ p0: \ p \neq 0 \ and \ N1: \ N \geq 1$

have $suc23: \ 3 = Suc 2$ by simp

let $\forall a = p * (p^2 - 3 * N * q^2)$

let $\forall b = q * (3 * p^2 - N * q^2)$

have $abP: \ P = a^2 + N * b^2$ by (simp add: eval-nat-numeral field-simps)

have $\forall P \ dvd \ p$ if $h1: \ gcd \ ?b \ ?a \neq 1$
2.3 Multiplication and division

proof –
let \(?h = \text{gcd} \ ?b \ ?a\)

have \(h2: \ ?h \geq 0\) by simp

hence \(?h = 0 \lor \ ?h = 1\) by arith

with \(h1\) have \(?h = 0 \lor \ ?h > 1\) by auto

moreover
{ assume \(?h = 0\)
  hence \(?a = 0 \land \ ?b = 0\)
    by auto
  with \(abP\) have \(?P \cdot 3 = 0\)
    by auto
  with \(P\) have \(\text{False}\)
    by (unfold prime-int-iff, auto)
  hence \(?\text{thesis by simp}\) }

moreover
{ assume \(?h > 1\)
  then have \(\exists \ g. \ \text{prime} \ g \land \ ?h\)
    using prime-factor-int [of \(?h\)] by auto
  then obtain \(g\) where \(?a = 0 \land \ ?b = 0\)
    by blast
  then have \(?a \land \ ?b\) by simp
  with \(g1\) have \(g dvd \ ?a\) by simp
  with \(g2\) have \(?P\) by (auto dest: prime-dvd-multD)
  from \(g\) have \(?P\) by (auto simp only: prime-int-iff)
  have \(g dvd \ ?P\)
  proof (cases)
    assume \(g dvd q\)
    hence \(?Nq: \ ?h\) by (auto simp add: dvd-def power2-eq-square)
    show \(?\text{thesis}\)
    proof
    assume \(?a\)
    hence \(?p2\) by (auto simp add: dvd-def power2-eq-square)
    moreover have \(?p2\) by (simp only: dvd-diff)
    ultimately show \(?\text{thesis}\) by simp
    next
  assume \(?a\)
  hence \(?p2\) by (auto simp add: dvd-def power2-eq-square)
  moreover have \(?p2\) by (simp only: dvd-diff)
  ultimately show \(?\text{thesis}\) by simp
qed

next
{ assume \(?g dvd q\) with \(g1\) have \(gpq: \ ?a\) by simp
  show \(?\text{thesis}\)
  proof (cases)
    assume \(?g dvd p\)
    hence \(?gNq: \ ?h\) by (auto simp add: dvd-def power2-eq-square)
    with \(?Nq\) show \(?\text{thesis}\) by auto
    next
  assume \(?g dvd p\) with \(g2\) have \(?P\) by (auto simp only: prime-int-iff)
  moreover have \(?Nq\) by (rule dvd-mult)
  ultimately have \(?P\) by (simp only: ac-simps dvd-add)
  moreover have \(?p2\) by (arith)
  ultimately show \(?\text{thesis}\) by simp
qed

next
{ assume \(?g dvd q\) with \(g1\) have \(gpq: \ ?a\) by simp
  show \(?\text{thesis}\)
  proof (cases)
    assume \(?g dvd p\)
    hence \(?g4p2\) by (auto simp add: dvd-def power2-eq-square)
    with \(?gpq\) have \(?P\) by (simp only: dvd-diff)
    moreover have \(?P\) by (arith)
    ultimately show \(?\text{thesis}\) by simp
    next
  assume \(?g dvd p\)
  hence \(?g4p2\) by (auto simp add: dvd-def power2-eq-square)
  with \(?gpq\) have \(?P\) by (simp only: dvd-diff)
  moreover have \(?P\) by (arith)
  ultimately show \(?\text{thesis}\) by simp
next
assume \( \neg g \text{ dvd } p \) with \( g \) have \( g \text{ dvd } p^2 - 3*N*q^2 \) by auto
with gpd dvd 3*p^2 - N*q^2 - (p^2 - 3*N*q^2)
by (simp only: dvd-diff)
moreover have \( 3*p^2 - N*q^2 - (p^2 - 3*N*q^2) = 2*?P \) by auto
ultimately have \( g \text{ dvd } 2*?P \) by simp
with \( g \) have \( g \text{ dvd } 2 \lor g \text{ dvd } ?P \) by (simp only: prime-dvd-multD)
moreover have \( \neg g \text{ dvd } 2 \)
proof (rule ccontr, simp)
assume \( g \text{ dvd } 2 \)
have \( g \leq 2 \)
proof (rule ccontr)
assume \( g \leq 2 \) hence \( g > 2 \) by simp
moreover have \( \langle 0::int \rangle < 2 \) by auto
ultimately have \( \neg g \text{ dvd } 2 \) by (auto simp only: zdvd-not-zless)
with \( g \text{ dvd } 2 \) show False by simp
qed
moreover from \( g \) have \( g \geq 2 \) by (simp add: prime-int-iff)
ultimately have \( g = 2 \) by auto
with \( g \) have \( 2 \text{ dvd } ?a \land 2 \text{ dvd } ?b \) by auto
hence \( 2 \text{ dvd } ?a^2 \land 2 \text{ dvd } N*?b^2 \)
by (simp add: power2-eq-square)
with \( abP \) have \( 2 \text{ dvd } ?P^3 \) by (simp only: dvd-add)
hence even \( (?P^3) \) by auto
moreover have odd \( (?P^3) \) using \( Podd \) by simp
ultimately show False by auto
qed
ultimately show \( \text{thesis} \) by simp
qed
with \( P \) have \( g \) pos have \( g = 1 \lor g = ?P \)
by (simp add: prime-int-iff)
with \( g \) have \( ?P \) by (simp add: prime-int-iff)
with \( g \) have \( Pab: ?P \text{ dvd } ?a \land ?P \text{ dvd } ?b \) by auto
have \( \text{thesis} \)
proof
from \( Pab \) have \( ?P \text{ dvd } p \lor ?P \text{ dvd } p^2 - 3*N*q^2 \)
by (auto dest: prime-dvd-multD)
moreover
\{
assume \( ?P \text{ dvd } p^2 - 3*N*q^2 \)
moreover have \( ?P \text{ dvd } 3*(p^2 + N*q^2) \)
by (auto simp only: dvd-refl dvd-mult)
ultimately have \( ?P \text{ dvd } p^2 - 3*N*q^2 + 3*(p^2+N*q^2) \)
by (simp only: dvd-add)
hence \( ?P \text{ dvd } 4*p^2 \) by auto
with \( P \) have \( ?P \text{ dvd } 4 \lor ?P \text{ dvd } p^2 \)
by (simp only: prime-dvd-multD)
moreover have \( \neg ?P \text{ dvd } 4 \)
proof (rule ccontr, simp)
assume \( P\text{dvd4: } ?P \text{ dvd } 4 \)
have \( ?P \leq 4 \)
proof (rule ccontr)
assume \( \neg ?P \leq 4 \) hence \( ?P > 4 \) by simp
moreover have \( (0::\mathbb{N}) < 4 \) by auto
ultimately have \( \neg \, ?P \, \text{dvd} \, 4 \) by \( \text{auto \ simp \ only: \ zdvd-not-zless} \)
with \( P \, \text{dvd} \, 4 \) show \( \text{False} \) by simp
qed
moreover have \( ?P \geq 2 \) by \( \text{auto \ simp \ add: \ prime-int-iff} \)
moreover have \( ?P \neq 2 \land ?P \neq 4 \)
proof (rule ccontr, simp)
  assume \( ?P = 2 \lor ?P = 4 \) hence even \( ?P \) by fastforce
  with \( P \, \text{odvd} \) show \( \text{False} \) by blast
qed
ultimately have \( ?P = 3 \) by auto
with \( P \, \text{dvd} \) have \( (3::\mathbb{N}) \, \text{dvd} \, 4 \) by simp
thus \( \text{False} \) by arith
qed
ultimately show \( ?\text{thesis} \) by auto
qed

moreover have \( ?P \, \text{dvd} \, p \) if \( h1 \): \( \text{gcd} \, N \, ?a \neq 1 \)
proof
let \( ?h = \text{gcd} \, N \, ?a \)
  have \( h2 \): \( ?h \geq 0 \) by simp
  hence \( ?h = 0 \lor ?h = 1 \lor ?h > 1 \) by arith
  with \( h1 \) have \( ?h = 0 \lor ?h > 1 \) by auto
moreover
  \{ assume \( ?h = 0 \) hence \( N = 0 \land ?a = 0 \)
    by auto
    hence \( N = 0 \) by arith
    with \( N1 \) have \( \text{False} \) by auto
    hence \( ?\text{thesis} \) by simp \}
moreover
  \{ assume \( ?h > 1 \)
    then have \( \exists \, g. \, \text{prime} \, g \land g \, \text{dvd} \, ?h \)
      using \( \text{prime-factor-int \ [of \ ?h]} \) by auto
    then obtain \( g \) where \( g \, \text{prime} \, g \, \text{dvd} \, ?h \)
      by blast
    hence \( g \, \text{dvd} \, N \) and \( g \, \text{dvd} \, ?a \) by auto
    hence \( g \, \text{dvd} \, p \cdot p \cdot 2 - N \cdot (3 \cdot p \cdot q \cdot 2) \)
      by \( \text{auto \ simp \ only: \ right-diff-distrib \ ac-simps} \)
    with \( g \, \text{dvd} \)
      have \( g \, \text{dvd} \, p \cdot p \cdot 2 - N \cdot (3 \cdot p \cdot q \cdot 2) + N \cdot (3 \cdot p \cdot q \cdot 2) \)
      by \( \text{simp \ only: \ dvald \ add \ dvald-mult2} \)
    hence \( g \, \text{dvd} \, p \cdot p \cdot 2 \) by simp
    with \( g \) have \( g \, \text{dvd} \, p \lor g \, \text{dvd} \, p \cdot p \)
      by \( \text{simp \ add: \ prime-dvd-multD \ power2-eq-square} \)
    with \( g \) have \( g \, \text{dvd} \) by \( \text{auto \ dest: \ prime-dvd-multD} \)
    hence \( g \, \text{dvd} \, p \cdot 2 \) by \( \text{simp \ add: \ power2-eq-square} \)
    with \( g \, \text{dvd} \)
      have \( g \, \text{dvd} \, ?P \) by auto
    from \( g \, \text{have} \, g \geq 0 \) by \( \text{simp \ add: \ prime-int-iff} \)
    with \( g \) have \( ?P \, \text{g} \) have \( g = 1 \lor g = ?P \)
      by \( \text{auto \ dest: \ primes-dvd-imp-eq} \)
with \( g \) have \( g = ?P \) by (auto simp only: prime-int-iff)
with \( gp \) have \( ?thesis \) by simp }
ultimately show \( ?thesis \) by auto
qed
moreover have \(~ ?P \) dvd \( p \)
proof (rule ccontr, clarsimp)
assume \( Pdvdp: ?P \) dvd \( p \)
have \( p^2 \geq ?P^2 \)
proof (rule ccontr)
assume \(~ p^2 \geq ?P^2 \)
hence \( p \not= ?P \)
\( p^2 < ?P^2 \) by simp
moreover with \( p0 \) have \( p^2 > 0 \) by simp
ultimately have \(~ ?P^2 \) dvd \( p^2 \) by (simp add: zdvd-not-zless)
with \( Pdvdp \) show \( False \) by simp
qed
moreover with \( P \) have \( ?P * 1 < ?P * ?P \)
unfolding prime-int-iff by (auto simp only: zmult-zless-mono2)
ultimately have \( p^2 > ?P^2 \) by (auto simp add: power2-eq-square)
hence \( neg: N * q^2 < 0 \) by auto
show \( False \)
proof –
have is-qfN \( (0^2 + N * q^2) \) \( N \) by (auto simp only: is-qfN-def)
with \( N1 \) have \( 0^2 + N * q^2 \geq 0 \) by (rule qfN-pos)
with \( neg \) show \( False \) by simp
qed
qed
ultimately have \( gcd ?a ?b = 1 \) \( gcd ?a N = 1 \)
by (auto simp add: ac-simps)
then have coprime \( ?a \) \( ?b \) coprime \( ?a N \)
by (auto simp only: gcd-eq-1-imp-coprime)
then have coprime \( ?a \) \( (N * ?b) \)
by simp
with \( abP \) show \( ?thesis \)
by blast
qed

2.4 Uniqueness \( (N > 1) \)

lemma qfN-prime-unique:
[ \( prime (a^2 + N*b^2 :: int); N > 1; a^2 + N*b^2 = c^2 + N*d^2 \) ]
\( \Rightarrow \) \( (|a| = |c| \land |b| = |d|) \)
proof –
let \( ?P = a^2 + N*b^2 \)
assume \( P: prime ?P \) and \( N: N > 1 \) and \( abcdN: ?P = c^2 + N*d^2 \)
have mutl: \( (a*d + b*c)*(a*d - b*c) = ?P*(d^2 - b^2) \)
proof –
have \( (a*d + b*c)*(a*d - b*c) = (a^2 + N*b^2)*d^2 - b^2*(c^2 + N*d^2) \)
by (simp add: eval-nat-numeral field-simps)
with \( abcdN \) show \( ?thesis \) by (simp add: field-simps)
qed
have \( ?P \) dvd \( a*d + b*c \) \or \( ?P \) dvd \( a*d - b*c \)
proof –
from mutl have \( ?P \) dvd \( (a*d + b*c)*(a*d - b*c) \) by simp
with \( P \) show \(?thesis\) by (auto dest: prime-dvd-multD)
qed

moreover
\{ assume \(?P\) dvd \(a\cdot d + b\cdot c\)
then obtain \( Q \) where \( Q\colon a\cdot d + b\cdot c = ?P\cdot Q\) by (auto simp add: dvd-def)
from \( abcdN\) have \(?P^2 = (a\cdot c + N\cdot b\cdot d)^2 + N\cdot (a\cdot d + b\cdot c)^2\) by (simp add: power2-eq-square)
also have \(d\cdot b = d\cdot 2\) by simp
finally have pos: \(?P^2 \geq ?P\cdot 2\cdot (Q^2\cdot 2\cdot N)\) by (simp add: ac-simps)
prove (rule ccontr)
assume \( b\cdot 2 \neq d\cdot 2\)
with \( P \) mult \( Q \) have \( Q \neq 0\) by (unfold prime-int-iff, auto)
hence \( Q^2 > 0\) by simp
moreover with \( N\) have \( Q^2\cdot 2\cdot N > Q^2\cdot 2\cdot 1\) by (simp only: zmult-zless-mono2)
ultimately have \( Q^2\cdot 2\cdot N > 1\) by arith
moreover with \( P\) have \( ?P^2 > 0\) by (simp add: prime-int-iff)
ultimately have \(?P^2\cdot 1 < ?P^2\cdot (Q^2\cdot 2\cdot N)\) by (simp only: zmult-zless-mono2)
with pos show False by simp
qed \}

moreover
\{ assume \(?P\) dvd \(a\cdot d - b\cdot c\)
then obtain \( Q \) where \( Q\colon a\cdot d - b\cdot c = ?P\cdot Q\) by (auto simp add: dvd-def)
from \( abcdN\) have \(?P^2 = (a\cdot c + N\cdot b\cdot d)^2 + N\cdot (a\cdot d - b\cdot c)^2\) by (rule qfN-mult2)
also have \(d\cdot b = d\cdot 2\) by simp
finally have pos: \(?P^2 \geq ?P\cdot 2\cdot (Q^2\cdot 2\cdot N)\) by (simp add: ac-simps)
prove (rule ccontr)
assume \( b\cdot 2 \neq d\cdot 2\)
with \( P \) mult \( Q \) have \( Q \neq 0\) by (unfold prime-int-iff, auto)
hence \( Q^2 > 0\) by simp
moreover with \( N\) have \( Q^2\cdot 2\cdot N > Q^2\cdot 2\cdot 1\) by (simp only: zmult-zless-mono2)
ultimately have \( Q^2\cdot 2\cdot N > 1\) by arith
moreover with \( P\) have \( ?P^2 > 0\) by (simp add: prime-int-iff)
ultimately have \(?P^2\cdot 1 < ?P^2\cdot (Q^2\cdot 2\cdot N)\) by (simp only: zmult-zless-mono2)
with pos show False by simp
qed \}

ultimately have \( bd\colon b\cdot 2 = d\cdot 2\) by blast
moreover with \( abcdN\) have \( a\cdot 2 = c\cdot 2\) by auto
ultimately show \(?thesis\) by (auto simp only: power2-eq-iff)
qed

lemma qfN-square-prime:
assumes \( a\cdot c + N\cdot b\cdot d \)
shows \(?P\cdot 2\cdot N\cdot s\cdot 2 = r\cdot 2\cdot N\cdot s\cdot 2\) by (auto simp add: power2-eq-square)
shows \(|r| = |p^2 - N \cdot q^2| \land |s| = |2 \cdot p \cdot q|\)

proof

- let \(\exists P = p^2 + N \cdot q^2\)
- let \(\exists A = r^2 + N \cdot s^2\)

from ass have \(P1: \exists P > 1\) by (simp add: prime-int-iff)
from ass have \(APP: \exists A = \exists P \cdot \exists P\) by (simp only: power2-eq-square)
with ass have \(prime \, \exists P \land \exists P \text{ ded } \exists A\) by (simp add: dvdI)

then obtain \(u, v, e, where\)

\(|\exists A = (u^2 + N \cdot v^2) \cdot \exists P \land r = p \cdot u + e \cdot N \cdot q \cdot v\land s = p \cdot v - e \cdot q \cdot u \land |e| = 1\)

by (frule-tac \(p=p\) in qfN-div-prime, auto)

with \(APP \, P1 \, ass \, have \prime (u^2 + N \cdot v^2) \land N > 1 \land u^2 + N \cdot v^2 = \exists P\)

by auto

hence \(|u| = |p| \land |v| = |q|\) by (auto dest: qfN-prime-unique)

then obtain \(f, g where\)

\(|f = f \cdot p \land |f| = 1\) and \(g: v = g \cdot q \land |g| = 1\)

by (blast dest: abs-eq-impl-unitfactor)

with \(we\ have\ \(r = f \cdot p \cdot p + (e \cdot g) \cdot N \cdot q \cdot q\land s = g \cdot p \cdot q - (e \cdot f) \cdot p \cdot q\) by simp

hence \(rs: r = f \cdot p^2 + (e \cdot g) \cdot N \cdot q^2 \land s = (g - e \cdot f) \cdot p \cdot q\)

by (auto simp only: power2-eq-square left-diff-distrib)

moreover have \(s \neq 0\)

proof (rule contr, simp)

assume \(s0: s=0\)

hence \(gcd \, r, s = |r|\) by simp

with ass have \(|r| = 1\) by simp

hence \(r^2 = 1\) by (auto simp add: power2-eq-1-iff)

with \(s0\ have\ \exists A = 1\) by simp

moreover have \(\exists P^2 > 1\)

proof

- from \(P1\ have\ 1 < \exists P \land (0::int) \leq 1 \land (0::nat) < 2\) by auto

hence \(\exists P^2 > 1^2\) by (simp only: power-strict-mono)

thus \(\exists thesis\ by\ auto\)

qed

moreover from ass have \(\exists A = \exists P^2\) by simp

ultimately show \(False\ by\ auto\)

qed

ultimately have \(g \neq e \cdot f\) by auto

moreover from \(f, g\ we\ have\ |g| = |e \cdot f|\) unfolding abs-mult by presburger

ultimately have \(gef: g = -(e \cdot f)\) by arith

from \(we\ have\ e \cdot s = (e \cdot f) = - f\)

using abs-mult-self-eq \([of e]\) by simp

hence \(r = f \cdot (p^2 - N \cdot q^2) \land s = (-e \cdot f) \cdot 2 \cdot p \cdot q\) using \(rs\ gef\ unfolding\ right-diff-distrib\)

by auto

hence \(|r| = |f| \cdot |p^2 - N \cdot q^2|\)

\(\land |s| = |e| \cdot |f| \cdot 2 \cdot p \cdot q|\)

by (auto simp add: abs-mult)

with \(we\ f, g\ show\ \exists thesis\ by\ (auto\ simp\ only:\ mult-1-left)\)

qed

lemma qfN-cube-prime:

assumes \(ass: prime (p^2 + N \cdot q^2::int) \land N > 1\)
\land \((p^2 + N \cdot q^2) \cdot 3 = a^2 + N \cdot b^2 \land\ coprime\ a\ b\)

shows \(|a| = |p^3 - 3 \cdot N \cdot p \cdot q^2|\) and \(|b| = |3 \cdot p^2 \cdot q - N \cdot q^3|\)

proof


2.4 Uniqueness \((N > 1)\)

let \(?P = p \cdot 2 + N \cdot q \cdot 2\)
let \(?A = a \cdot 2 + N \cdot b \cdot 2\)
from ass have coprime \(?a, b\) by blast
from ass have \(P1: ?P > 1\) by (simp add: prime-int-iff)
with ass have \(APP: ?A = ?P \cdot ?P \cdot 2\) by (simp add: power2-eq-square power3-eq-cube)
with ass have prime \(?P \wedge ?P \cdot \text{dvd} ?A\) by (simp add: dvdI)
then obtain \(u \cdot v \cdot e\) where \(uve\):
  \(?A = (a \cdot 2 + N \cdot v \cdot 2) \cdot ?P + a = p \cdot u + e \cdot N \cdot q \cdot v \wedge b = p \cdot v - e \cdot q \cdot u \wedge |e| = 1\)
  by (frule-tac \(p \cdot p\) in \(q \cdot N\)-div-prime, auto)
have coprime \(?u\) \(?v\)
proof (rule coprimeI)
  fix \(?c\)
  assume \(?c\) \(?dvd\) \(?u\) \(?c\) \(?dvd\) \(?v\)
  with \(uve\) have \(?c\) \(?dvd\) \(?a\) \(?c\) \(?dvd\) \(?b\)
  by simp-all
  with (coprime \(?a\) \(?b\)) show is-unit \(?c\)
  by (rule coprime-common-divisor)
qed
with \(P1\) \(uve\) \(ass\) have prime \(?P \wedge N > 1 \wedge ?P \cdot 2 = a \cdot 2 + N \cdot v \cdot 2\)
  \wedge coprime \(?u\) \(?v\) by (auto simp add: ac-simps)
hence \(|u| = |p \cdot 2 - N \cdot q \cdot 2|\) \wedge \(|v| = |2 \cdot p \cdot q|\) by (rule \(q \cdot N\)-square-prime)
then obtain \(?f\) \(?g\) where \(f: u = f \cdot (p \cdot 2 - N \cdot q \cdot 2) \wedge |f| = 1\)
  and \(?g:: v = g \cdot (2 \cdot p \cdot q)\) \wedge \(|g| = 1\) by (blast dest: abs-eq-impl-unifactor)
with \(uve\) have \(?a = p \cdot f \cdot (p \cdot 2 - N \cdot q \cdot 2) + e \cdot N \cdot q \cdot g \cdot 2 \cdot p \cdot q\)
  \wedge \(?b = p \cdot g \cdot 2 \cdot p \cdot q - e \cdot q \cdot f \cdot (p \cdot 2 - N \cdot q \cdot 2)\) by auto
hence \(ab: a = f \cdot p \cdot p \cdot 2 + -f \cdot N \cdot p \cdot q \cdot 2 + 2 \cdot e \cdot g \cdot N \cdot p \cdot q \cdot 2\)
  \wedge \(?b = 2 \cdot g \cdot p \cdot 2 \cdot q - e \cdot f \cdot p \cdot 2 \cdot q + e \cdot f \cdot N \cdot q \cdot q \cdot 2\)
  by (auto simp add: ac-simps right-diff-distrib power2-eq-square)
from \(?f\) have \(f^2: f^2 = 1\)
  using abs-mult-self-eq [of \(?f\)] by (simp add: power2-eq-square)
from \(?g\) have \(g^2: g^2 = 1\)
  using abs-mult-self-eq [of \(?g\)] by (simp add: power2-eq-square)
have \(?c \neq f \cdot g\)
proof (rule ccontr, simp)
  assume \(?c:: f \cdot g\)
  with \(?ab\) \(?g\) have \(?a = f \cdot p \cdot p \cdot 2 + f \cdot N \cdot p \cdot q \cdot 2\) by (auto simp add: power2-eq-square)
  hence \(?a = (f \cdot p) \cdot ?P\) by (auto simp add: distrib-left ac-simps)
  hence \(?Pa: ?P\) \(?dvd\) \(?a\) by auto
  have \(?e \cdot f = g\) using \(?f^2\) \(?power2-eq-square\)[of \(?f\)] \(?efg\) by simp
  with \(?ab\) \(?have\) \(?b = g \cdot p \cdot 2 \cdot q + g \cdot N \cdot p \cdot q \cdot 2\) by auto
  hence \(?b = (g \cdot q) \cdot ?P\) by (auto simp add: distrib-left ac-simps)
  hence \(?P\) \(?dvd\) \(?b\) by auto
  with \(?Pa\) \(?have\) \(?P\) \(?dvd\) \(?gcd\) \(?a\) \(?b\) by simp
  with \(?ass\) \(?have\) \(?P\) \(?dvd\) \(?1\) by auto
  with \(?P1\) \(?show\) False by auto
qed
moreover from \(?f\) \(?g\) \(uve\) \(have\) \(|e| = |f \cdot g|\) unfolding abs-mult by auto
ultimately have \(?c = -(f \cdot g)\) by arith
hence \(?e \cdot g = -f \cdot e \cdot f = -g\) using \(?f^2\) \(?g^2\) unfolding power2-eq-square by auto
with \(?ab\) \(?have\) \(?a = f \cdot p \cdot p \cdot 2 - 3 \cdot f \cdot N \cdot p \cdot q \cdot 2\) \wedge \(?b = 3 \cdot g \cdot p \cdot 2 \cdot q - g \cdot N \cdot q \cdot q \cdot 2\)
  by (simp add: mult.assoc)
  hence \(?a = f \cdot (3 \cdot p \cdot 3 - 3 \cdot N \cdot p \cdot q \cdot 2)\) \wedge \(?b = g \cdot (3 \cdot p \cdot 2 \cdot q - N \cdot q \cdot 3)\)
2.5 The case \( N = 3 \)

**Lemma:** \( qf3\text{-even}: \) even \((a^2 + 3b^2)\) \( \implies \exists \ B. \ a^2 + 3b^2 = 4B \wedge \text{is-qfN} \ B \ 3 \)

**Proof:**

- let \( ?A = a^2 + 3b^2 \)
- assume even: even \( ?A \)
- have \((\text{odd } a \wedge \text{odd } b) \vee (\text{even } a \wedge \text{even } b)\)
  - proof (rule condr, auto)
    - assume even \( a \) and odd \( b \)
    - hence \((\text{odd } a^2)\) and \( \text{odd } (b^2)\)
      - by (auto simp add: power2-eq-square)
    - moreover have odd \( 3 \) by simp
    - ultimately have odd \( ?A \) by simp
    - with even show False by simp
  - next
    - assume odd \( a \) and even \( b \)
    - hence \((\text{odd } a^2)\) and \( \text{even } (b^2)\)
      - by (auto simp add: power2-eq-square)
    - moreover hence even \((b^2+3)\) by simp
    - ultimately have odd \((b^2+3+a^2)\) by simp
    - hence odd \( ?A \) by (simp add: ac-simps)
    - with even show False by simp
  - qed
- moreover
  - \{ assume even \( a \) \wedge even \( b \)\}
  - then obtain \( c \) \( d \) where \( abcd: \ a = 2c \wedge \ b = 2d \) using evenE[of \( a \)] evenE[of \( b \)]
    - by meson
    - hence \( ?A = 4(c^2 + 3d^2) \) by (simp add: power-mult-distrib)
    - moreover have is-qfN \((c^2 + 3d^2)\) \( 3 \) by (unfold is-qfN-def, auto)
    - ultimately have \( \text{thesis by blast} \}
  - moreover
    - \{ assume odd \( a \) \wedge odd \( b \) \}
    - then obtain \( c \) \( d \) where \( abcd: \ a = 2c + 1 \wedge \ b = 2d + 1 \) using oddE[of \( a \)] oddE[of \( b \)]
      - by meson
    - have odd \((c-d)\) \vee even \((c-d)\) by blast
    - moreover
      - \{ assume even \((c-d)\) \}
      - then obtain \( e \) where \( c-d = 2e \) using evenE by blast
        - with \( abcd \) have \( e1: \ a-b = 4e \) by arith
        - hence \( e2: \ a+3b = 4(e+b) \) by auto
        - have \( 4\times ?A = (a+3b)^2 + 3(a-b)^2 \)
          - by (simp add: eval-nat-numeral field-simps)
        - also with \( e1 \) \( e2 \) have \( \ldots = (4(e+b))^2 + 3(4e)^2 \) by (simp(no-asm-simp))
      - finally have \( ?A = 4((e+b)^2 + 3e^2) \) by (simp add: eval-nat-numeral field-simps)
        - moreover have is-qfN \((e+b)^2 + 3e^2)\) \( 3 \) by (unfold is-qfN-def, auto)
      - ultimately have \( \text{thesis by blast} \}
    - moreover
      - \{ assume odd \((c-d)\) \}
then obtain $c$ where $c - d = 2c + 1$ using oddE by blast
with abcd have $e1$: $a+b = 4*(e+d+1)$ by auto
hence $e2$: $a - 3*b = 4*(e+d-b+1)$ by auto
have $4*A = (a - 3*b)^2 + 3*(a+b)^2$
  by (simp add: eval-nat-numeral field-simps)
also with $e1$ $e2$ have $... = (4*(e+d-b+1)^2 + 3*(e+d+1)^2)^2$
  by (simp (no-asm-simp))
finally have $?A = 4*((e+d-b+1)^2 + 3*(e+d+1)^2)$
  by (simp add: eval-nat-numeral field-simps)
moreover have $is-qfN ((e+d-b+1)^2 + 3*(e+d+1)^2) 3$
  by (unfold is-qfN-def, auto)
ultimately show $?thesis$ by blast }
ultimately have $?thesis$ by auto }
ultimately show $?thesis$ by auto
qed

lemma qf3-even-general: $[ is-qfN A 3; even A ]$
  $\Rightarrow \exists B. A = 4*B \land is-qfN B 3$
proof -
  assume even A and $is-qfN A 3$
  then obtain $a \ b$ where $A = a^2 + 3*b^2$
    and even ($a^2 + 3*b^2$) by (unfold is-qfN-def, auto)
  thus $?thesis$ by (auto simp add: qf3-even)
qed

lemma qf3-oddprime-factor-not:
  assumes ass: prime P \land odd P \land Q>0 \land is-qfN (P*Q) 3 \land \neg is-qfN P 3
  shows $\exists R. prime R \land odd R \land R dvd Q \land \neg is-qfN R 3$
proof (rule ccontr, simp)
  assume ass2: $\forall R. R dvd Q \longrightarrow prime R \longrightarrow even R \lor is-qfN R 3$
  (is $?A Q$)
  obtain $n::nat$ where $n = nat Q$ by auto
with ass have $n$: $Q = int n$ by auto
have $(n > 0 \land is-qfN (P*int n) 3 \land \neg A(int n)) \Longrightarrow False$ (is $?B n \Longrightarrow False$)
proof (induct $n$ rule: less-induct)
case (less n)
  hence $IH$: $!m. m<n \land ?B m \Longrightarrow False$
  and $Bn$: $?B n$ by auto
show $False$
proof (cases)
  assume odd: $odd (int n)$
  from $Bn$ ass have prime P \land int n > 0 \land is-qfN (P*int n) 3 \land \neg is-qfN P 3$
    by simp
  hence $\exists R. prime R \land R dvd int n \land \neg is-qfN R 3$
    by (rule qfN-primedivisor-not)
  then obtain $R$ where $R$: prime R \land R dvd int n \land \neg is-qfN R 3$ by auto
  moreover with odd have odd R
  proof -
    from $R$ obtain $U$ where $int n = R*U$ by (auto simp add: dvd-def)
    with odd show $?thesis$ by auto
  qed
  moreover from $Bn$ have $?A (int n)$ by simp
ultimately show \( \text{False by auto} \)

next

assume \( \text{even: } \neg \text{ odd (int } n) \)
hence even ((int \( n \)) * \( P \)) by simp

with \( B n \) have \( \text{even (P*int } n) \land \text{ is-gfN (P*int } n) \) \( 3 \) by (simp add: ac-simps)

hence \( \exists B. \ P*(\text{int } n) = 4*B \land \text{ is-gfN } B \) \( 3 \) by auto

then obtain \( B \) where \( B; \ P*(\text{int } n) = 4*B \land \text{ is-gfN } B \) \( 3 \) by auto

hence \( 2^2 \text{ dvd } (\text{int } n)*P \) by (simp add: ac-simps)

moreover have \( \neg 2 \text{ dvd } P \)

proof (rule ccontr, simp)

assume \( 2 \text{ dvd } P \)

with \( \text{ass have odd } P \land \text{ even } \) by simp

thus \( \text{False by simp} \)

qed

moreover have \( \text{prime } (2::\text{int}) \) by simp

ultimately have \( 2^2 \text{ dvd } \text{int } n \)

by (rule-tac \( p=2 \) in prime-power-dvd-cancel-right)

then obtain \( \text{im::int where } \text{int } n = 4*\text{im} \) by (auto simp add: dvd-def)

moreover obtain \( m::\text{nat where } m = \text{nat im } \) by auto

ultimately have \( m; \ n = 4*m \) by arith

with \( \text{B have is-gfN } (P*\text{int } m) \) \( 3 \) by auto

moreover from \( m Bn \) have \( m > 0 \) by auto

moreover from \( m Bn \) have \( ?A (\text{int } m) \) by auto

ultimately have \( Bn; \ ?B m \) by simp

from \( Bn m \) have \( m < n \) by arith

with \( III Bm \) show False by auto

qed

qed

with \( \text{ass ass2 } n \) show \( \text{False by auto} \)

qed

lemma \( \text{gf3-oddprimedivisor} \):

\[
\begin{align*}
\text{prime (P::int); odd } P; \text{ coprime a b; } P \text{ dvd } (a^2+3*b^2) \\
\implies \text{is-gfN } P \ 3
\end{align*}
\]

proof (induct \( P \) arbitrary: \( a \) \( b \) rule: \( \text{infinite-descent0-measure[where } V=\lambda P. \text{ nat}[P]] \))

case \( (0 \ x) \)

moreover hence \( x = 0 \) by arith

ultimately show \( \neg \text{case by (simp add: prime-int-iff)} \)

next

case \( \text{smaller } x \)

then obtain \( \text{a b where abx: prime } x \land \text{ odd } x \land \text{ coprime a b} \)

\land \( x \text{ dvd } (a^2+3*b^2) \land \neg \text{ is-gfN } x \) \( 3 \) by auto

then obtain \( M \) where \( M; a^2+3*b^2 = x*M \) by (auto simp add: dvd-def)

let \( ?A = a^2 + 3*b^2 \)

from \( \text{abx have } x0; \ x > 0 \) by (simp add: prime-int-iff)

then obtain \( m \) where \( 2*(a-m*x)\leq x \) by (auto dest: \( \text{best-division-abs} \))

with \( \text{abx have } \delta*(a-m*x)\leq x \) using \( \text{odd-two-times-div-two-succ[of } x \) \( \text{by presburger} \)

then obtain \( c \) where \( c = a-m*x \land 2*|c| < x \) by auto

from \( x0 \) obtain \( n \) where \( 2*(b-n*x)\leq x \) by (auto dest: \( \text{best-division-abs} \))

with \( \text{abx have } \delta*(b-n*x)\leq x \) using \( \text{odd-two-times-div-two-succ[of } x \) \( \text{by presburger} \)

then obtain \( d \) where \( \text{dv: } d = b-n*x \land 2*|d| < x \) by auto

let \( ?C = c^2+3*d^2 \)
have C3: is-qfN ?C 3 by (unfold is-qfN-def, auto)
have C0: ?C > 0
proof
  have hlp: (3::int) ≥ 1 by simp
  have ?C ≥ 0 by simp
  hence ?C = 0 ∨ ?C > 0 by arith
moreover
  { assume ?C = 0
    with hlp have c=0 ∧ d=0 by (rule qfN-zero)
    with cm dn have a = m*x ∧ b = n*x by simp
    hence x dvd a ∧ x dvd b by simp
    hence x dvd gcd a b by simp
    with abx have False by (auto simp add: prime-int-iff) }
ultimately show ?thesis by blast
qed
have x dvd ?C
proof
  have ?C = |c|^2 + 3*d^2 by (simp only: power2-abs)
  also with cm dn have ... = (a−m*x)^2 + 3*(b−n*x)^2 by simp
  also have ... = a^2 − 2*a*(m*x) + (m*x)^2 + 3*(b^2 − 2*b*(n*x) + (n*x)^2)
    by (simp add: algebra-simps power2-eq-square)
  also with abx M have ... = x*M − x*(2*a*m + 3*a*b*n) + x^2*(m^2 + 3*n^2)
    by (simp only: power-mult-distrib distrib-left ac-simps, auto)
  finally show ?C = x^2(M − (2*a*m + 3*a*b*n) + x*(m^2 + 3*n^2))
    by (simp add: power2-eq-square distrib-left right-diff-distrib)
  qed
then obtain y where y: ?C = x*y by (auto simp add: dvd-def)
have yx: y < x
proof (rule ccontr)
  assume ¬ y < x hence xy: x−y ≤ 0 by simp
  have hlp: 2|c| ≥ 0 ∧ 2|d| ≥ 0 ∧ (3::nat) > 0 by simp
  from y have 4*x*y = 2^2*c^2 + 3*2^2*d^2 by simp
  hence 4*x*y = (2|c|)^2 + 3*(2|d|)^2
    by (auto simp add: power-mult-distrib)
  with cm dn hlp have 4*x*y < x^2 + 3*(2|d|)^2
    and (3::int) > 0 ∧ (2|d|)^2 < x^2
    using power-strict-mono [of 2|b| 2 for b]
    by auto
  hence x*4*y < x^2 + 3*x^2 by (auto)
  also have ... = x*4*x by (simp add: power2-eq-square)
  finally have contr: (x−y)*(4*x) > 0 by (auto simp add: right-diff-distrib)
  show False
proof (cases)
  assume x−y = 0 with contr show False by auto
next
  assume ¬ x−y = 0 with xy have x−y < 0 by simp
  moreover from x0 have 4*x > 0 by simp
  ultimately have 4*x*(x−y) < 4*x*0 by (simp only: zmult-zless-mono2)
  with contr show False by auto
qed
The quadratic form $x^2 + Ny^2$

\[\text{prove (rule ccontr)}\]
\[\text{assume } \neg y > 0\]
\[\text{hence } y \leq 0 \text{ by simp}\]
\[\text{moreover have } y \neq 0\]
\[\text{proof (rule ccontr)}\]
\[\text{assume } \neg y \neq 0 \text{ hence } y=0 \text{ by simp}\]
\[\text{with } y \text{ and } C0 \text{ show False by auto}\]
\[\text{qed}\]
\[\text{ultimately have } y < 0 \text{ by simp}\]
\[\text{with } x0 \text{ have } x*y < x*0 \text{ by (simp only: zmult-zless-mono2)}\]
\[\text{with } C0 \text{ y show False by simp}\]
\[\text{qed}\]
\[\text{let } ?g = \text{gcd c d}\]
\[\text{have } c \neq 0 \text{ } \lor \text{ } d \neq 0\]
\[\text{proof (rule ccontr)}\]
\[\text{assume } \neg (c \neq 0 \text{ } \lor \text{ } d \neq 0)\]
\[\text{hence } c=0 \text{ } \land \text{ } d=0 \text{ by simp}\]
\[\text{with } C0 \text{ show False by simp}\]
\[\text{qed}\]
\[\text{then obtain } e \text{ and } f \text{ where} \quad ef: \ c = ?g*e \land \ d = ?g*f \land \ \text{coprime e f}\]
\[\text{using gcd-coprime-exists[of c d] gcd-pos-int[of c d] by (auto simp: mult.commute)}\]
\[\text{have g2nonzero: } \neg ?g^2 \neq 0\]
\[\text{proof (rule ccontr, simp)}\]
\[\text{assume } c=0 \text{ } \land \text{ } d=0\]
\[\text{with } C0 \text{ show False by simp}\]
\[\text{qed}\]
\[\text{let } ?E = e^2 + 3*f^2\]
\[\text{have E3: is-qfN } ?E \text{ 3 by (unfold is-qfN-def, auto)}\]
\[\text{have CgE: } ?C = ?g^2 \ast ?E\]
\[\text{proof -}\]
\[\text{have } ?g^2 \ast ?E = (?g*e)^2 + 3*(?g*f)^2\]
\[\text{by (simp add: distrib-left power-mult-distrib)}\]
\[\text{with } ef \text{ show } ?\text{thesis by simp}\]
\[\text{qed}\]
\[\text{hence } ?g^2 \text{ dvd } C \text{ by (simp add: dvd-def)}\]
\[\text{with } y \text{ have g2dvdxy: } ?g^2 \text{ dvd } y*x \text{ by (simp add: ac-simps)}\]
\[\text{moreover have coprime x (} ?g^2)\]
\[\text{proof -}\]
\[\text{let } ?h = \text{gcd } ?g \text{ x}\]
\[\text{have } ?h \text{ dvd } ?y \text{ and } \neg ?g \text{ dvd c by blast+}\]
\[\text{hence } ?h \text{ dvd c by (rule dvd-trans)}\]
\[\text{have } ?h \text{ dvd } ?y \text{ and } \neg ?g \text{ dvd d by blast+}\]
\[\text{hence } ?h \text{ dvd d by (rule dvd-trans)}\]
\[\text{have } ?h \text{ dvd x by simp}\]
\[\text{hence } ?h \text{ dvd m*x by (rule dvd-mult)}\]
\[\text{with } ?h \text{ dvd c have } ?h \text{ dvd c+m*x by (rule dvd-add)}\]
\[\text{with cm have } ?h \text{ dvd a by simp}\]
\[\text{from } ?h \text{ dvd x have } ?h \text{ dvd n*x by (rule dvd-mult)}\]
\[\text{with } ?h \text{ dvd d have } ?h \text{ dvd d+n*x by (rule dvd-add)}\]
\[\text{with dn have } ?h \text{ dvd b by simp}\]
\[\text{with } ?h \text{ dvd a have } ?h \text{ dvd gcd a b by simp}
with \(abz\) have \(?h\ \text{dvd}\ 1\) by simp
hence \(?h = 1\) by simp
hence \(\text{coprime}\ (?g^2)\ x\) by (auto intro: \(\text{gcd-eq-1-imp-coprime}\))
thus \(\text{thesis}\) by (simp only: \(\text{ac-simps}\))

qed
ultimately have \(?g^2\ \text{dvd}\ y\)
by (auto simp add: \(\text{ac-simps\ \ coprime-dvd-mult-right-iff}\))
then obtain \(w\) where \(w = ?g^2 * w\) by (auto simp add: dvd-def)
with \(CgE\ y\ g2\nonzero\) have \(Ewx\): \(?E = x * w\) by auto
have \(w > 0\)
proof (rule ccontr)
assume \(\neg w > 0\) hence \(w \leq 0\) by auto
hence \(w = 0\lor w < 0\) by auto
moreover
\{ assume \(w = 0\) with \(w y0\) have \(\text{False}\) by auto \}
moreover
\{ assume \(wneg: w < 0\)
  \(\text{have}\ ?g^2 \geq 0\) by (rule \(\text{zero-le-power2}\))
  with \(g2\nonzero\) have \(?g^2 > 0\) by arith
  with \(wneg\) have \(?g^2 + w < ?g^2 + 0\) by (simp only: \(\text{zmult-zless-mono2}\))
  with \(w y0\) have \(\text{False}\) by auto \}
ultimately show \(\text{False}\) by blast

qed
have \(w - \text{le-y}: w \leq y\)
proof (rule ccontr)
assume \(\neg w \leq y\)
hence \(w y: w > y\) by simp
have \(?g^2 = 1\lor ?g^2 > 1\)
proof – 
  \(\text{have}\ ?g^2 \geq 0\) by (rule \(\text{zero-le-power2}\))
  hence \(?g^2 = 0\lor ?g^2 > 0\) by auto
  with \(g2\nonzero\) show \(\text{thesis}\) by arith
qed
moreover
\{ assume \(?g^2 = 1\) with \(w y\) have \(\text{False}\) by simp \}
moreover
\{ assume \(g1: ?g^2 > 1\)
  with \(<w>0\) have \(w * 1 < w * ?g^2\) by (auto dest: \(\text{zmult-zless-mono2}\))
  with \(w\) have \(w < y\) by (simp add: \(\text{ac-simps}\))
  with \(wy\) have \(\text{False}\) by auto \}
ultimately show \(\text{False}\) by blast

qed
from \(E\ text{Ex E3}\ abx\ <w>0\) have
  \(\text{prime}\ x\land\ \text{odd}\ x\land \ w > 0\land \ \text{is-qfN}\ (x+w)\ 3\land \neg \text{is-qfN}\ x\ 3\) by simp
then obtain \(z\) where \(z: \text{prime}\ z\land\ \text{odd}\ z\land\ z\ \text{dvd}\ w\land \neg \text{is-qfN}\ z\ 3\)
by (frule-tac \(P=x\) in \(\text{qf3-oddprimedivisor-not}\), auto)
from \(E\ text{Ex}\ have\ w\ \text{dvd}\ \text{?E}\ by\ simp\)
with \(z\ \text{have}\ w\ \text{dvd}\ \text{?E}\) by (auto dest: \(\text{dvd-trans}\))
with \(z\ \text{ef}\) have \(\text{prime}\ z\land\ \text{odd}\ z\land\ \text{coprime}\ e\ f\land\ z\ \text{dvd}\ \text{?E}\land \neg \text{is-qfN}\ z\ 3\)
by auto
moreover have \(nat|z| < nat|x|\)
proof –
have $z \leq w$
proof (rule ccontr)
  assume $\neg z \leq w$ hence $w < z$ by auto
with ($w > 0$) have $\neg z \text{ dvd } w$ by (rule zdvd-not-zless)
with $z$ show False by simp
qed
with $w \text{ le } y x$ have $z < x$ by simp
with $z$ have $|z| < |x|$ by (simp add: prime-int-iff)
thus $\text{?thesis}$ by auto
qed
ultimately show $\text{?case}$ by auto
qed

lemma $\text{qf3-cube-prime-impl-cube-form}$:
  assumes $\text{ab-relprime}$: coprime $a \text{ and } b$
and $P$: prime $P$ \and odd $P$
shows $\text{is-cube-form a b}$
proof --
  from $\text{abP}$ have $\text{qfP3}$: $\text{is-qfN (} P^\circ 3 \text{)}$ by (auto simp only: is-qfN-def)
  have $\text{PdP3}$: $P \text{ dvd } P^\circ 3$ by (simp add: eval-nat-numeral)
  with $\text{abP}$ $\text{ab-relprime P}$ have $\text{qfP}$: $\text{is-qfN P 3}$ by (simp add: qf3-oddprimedivisor)
  then obtain $p \text{ q}$ where $pq$: $P = p^2 + 3q^2$ by (auto simp only: is-qfN-def)
  with $P \text{ abP}$ $\text{ab-relprime P}$ have primediv $\text{prime (} p^2 + 3q^2 \text{)}$ \and \((3::int) > 1\)
  \and $\text{(p^2+3*q^2)^3 = a^2+3*b^2 \and coprime a b}$ by auto
hence $ab$: $|a| = |p^3 - 3*3*p*q^2| \land |b| = |3*p^2*q - 3*q^3|$
  by (rule qfN-cube-prime)
  hence $a = p^3 - 9*p*q^2 \lor a = -(p^3) + 9*p*q^2$ by arith
  from $ab$ have $b\text{ b = 3*p^2*q - 3*q^3 \lor b = -(3*p^2*q) + 3*q^3}$ by arith
  obtain $r \text{ s}$ where $r = -p$ \and $s = -q$ by simp
  show $\text{?thesis}$
proof (cases)
  assume $a1$: $a = p^3 - 9*p*q^2$
  show $\text{?thesis}$
proof (cases)
    assume $b1$: $b = 3*p^2*q - 3*q^3$
    with $a1$ show $\text{?thesis}$ by (unfold is-cube-form-def, auto)
next
  assume $\neg b = 3*p^2*q - 3*q^3$
  with $b$ have $b = -3*p^2*q + 3*q^3$ by simp
  with $s$ have $b = 3*p^2*s - 3*s^3$ by simp
  moreover from $a1 \text{ s}$ have $a = p^3 - 9*p*s^2$ by simp
  ultimately show $\text{?thesis}$ by (unfold is-cube-form-def, auto)
qed
next
  assume $\neg a = p^3 - 9*p*q^2$
  with $a$ have $a = -(p^3) + 9*p*q^2$ by simp
  with $r$ have $ar$: $a = r^3 - 9*r*q^2$ by simp
  show $\text{?thesis}$
proof (cases)
  assume $b1$: $b = 3*p^2*q - 3*q^3$
  with $r$ have $b = 3*r^2*q - 3*q^3$ by simp
  with $ar$ show $\text{?thesis}$ by (unfold is-cube-form-def, auto)
2.5 The case $N = 3$

next
assume $b = 3*p^2q - 3*q^3$
with $b$ have $b = -3*p^2q + 3*q^3$ by simp
with $r \cdot s$ have $b = 3*r^2s - 3*3^3$ by simp
moreover from $a$ have $a = r^3 - 9*r*3^2$ by simp
ultimately show $?thesis$ by (unfold is-cube-form-def, auto)
qed

lemma cube-form-mult: $[\text{is-cube-form a b; is-cube-form c d; } |e| = 1 ]$
$\implies \text{is-cube-form} (a*c+c*e*3*b*d) (a*d-e*b*c)$
proof -
assume $ab$: is-cube-form $a$ $b$ and $cd$: is-cube-form $c$ $d$ and $e$: $|e| = 1$
from $ab$ obtain $p q$ where $pq$: $a = p^3 - 9*p*q^2$ and $b = 3*p^2q - 3*q^3$
by (auto simp only: is-cube-form-def)
from $cd$ obtain $r s$ where $rs$: $c = r^3 - 9*r*s^2$ and $d = 3*r^2s - 3*s^3$
by (auto simp only: is-cube-form-def)
let $?t = p*r + e*3*q*s$
let $?u = p*s - e*r*q$
have $e2$: $c^2=1$
proof -
from $e$ have $e=1 \lor e=-1$ by linarith
moreover
{ assume $e=1$ hence $?thesis$ by auto }
moreover
{ assume $e=-1$ hence $?thesis$ by simp }
ultimately show $?thesis$ by blast
qed

hence $e*e^2 = e$ by simp

hence $e3$: $e^3 = e^3$ by (simp only: power2-eq-square power3-eq-cube)
have $aw+e3*b*d = 2*t^3 - 9*t^2+u^2$
proof -
have $?t^3 - 9*t*t+u^2 = p^3*r^3 + e*9*p^2q*r^2s + e^2*27*p^2q^2+2*r^2s^2$
+ $e^3*27q^3*r^3^2 - 9*p^22*r^2s^2 + e^1*18*p^2q*r^2s^2 - e^2*29*p^2q^2(s*r^2)^2$
- $e^2*27*p^2q^2*(s^2)^2 + e^2*25*p^2q^2*r^2s^2 - e^2*27*2*(q^2)*r^2s^2$
by (simp add: eval-nat-numeral field-simps)
also with $e2 e3$ have ... = $p^3*r^3 + e^2*27*p^2q^2*r^2s^2 + 81*p^2q^2*r^2s^2 + e^2*27q^3*r^3^3$
- $9*p^22*r^2s^2 - 9*p^2q^2*r^23 - e^2*27*p^2q^2*r^2s^3 - e^2*27q^3*r^2s^2$
by (simp add: power2-eq-square power3-eq-cube)
also with $pq rs$ have ... = $a*c + e*3*b*d$
by (simp only: left-diff-distrib right-diff-distrib ac-simps)
finally show $?thesis$ by auto
qed

moreover have $a*d-e*b*c = 3*?t^2*u - 3*?u^3$
proof -
have $3*?t^2*u - 3*?u^3 =$
$3*(p+2)*r^2s - e*3*p^2q*(r*r^2) + e^2*18*p^2q*r^2s^2$
- $e^2*27*p^2q^2*r^2s^2 + e^2*27*p^2q^2*(s^2)^2 - e^2*27*(q^2)*r^2s^2$
- $3*p^3+s^3 + e^2*9*p^2q*r^2s^2 - e^2*29*p^2q^2*r^2s^2 + e^3*3*r^3^3$
by (simp add: eval-nat-numeral field-simps)
also with \( e_2 e_3 \) have \( \ldots = 3^3 p^2 q^2 r^2 s - e_3^3 p^2 q^2 r^2 s^2 - 18^3 p^3 q^2 r^2 s^3 - 27^3 p^4 q^2 r^2 s^3 - e_2^3 q^3 r^3 s^2 - 2 \sum \cdot p^3 s^2 r^2 s - 9^3 p^3 s^2 r^3 s \) by (simp add: power2-eq-square power3-eq-cube)
also with \( p q r s \) have \( \ldots = a + c + e b + c \) by (simp only: left-diff-distrib right-diff-distrib ac-simps)
finally show \( \text{thesis} \) by auto
qed
ultimately show \( \text{thesis} \) by (auto simp only: is-cube-form-def)
qed

**lemma** \( q^3 \text{-cube-primelist-impl-cube-form} \): \( \bigwedge \forall p \in \text{set-mset ps. prime p} \). odd \( (\prod i \in \# ps. i) \) \( \implies \) (!! a b. coprime a b \( \implies a^2 + 3 b^2 = (\text{int}(\prod i \in \# ps. i))^3 \)) \( \implies \) is-cube-form a b

**proof** (induct ps)

case empty hence ab1: \( a^2 + 3 b^2 = 1 \) by simp

have \( b^0: b=0 \)

proof (rule ccontr)

assume \( b \neq 0 \)

hence \( b^2 > 0 \) by simp

hence \( 3 b^2 > 1 \) by arith

with ab1 have \( a^2 < 0 \) by arith

moreover have \( a^2 \geq 0 \) by (rule zero-le-power2)

ultimately show \( \text{False} \) by auto

qed

with ab1 have a1: \( (a=1 \vee a=-1) \) by (auto simp add: power2-eq-square zmult-eq-1-iff)

then obtain \( p \) and \( q \) where \( p=a \) and \( q=(0::\text{int}) \) by simp

with a1 and \( b^0 \) have \( a = p^3 - 9^3 p^2 q^2 \wedge b = 3^3 p^2 q - 3^3 q^3 \) by auto

thus is-cube-form a b by (auto simp only: is-cube-form-def)

next

case (add p ps) hence ass: \( \text{coprime a b \wedge odd (\prod i \in \# ps + \{\# p\}. i) \wedge a^2 + 3 b^2 = \text{int}(\prod i \in \# ps + \{\# p\}. i)^3 \wedge (\forall a \in \text{set-mset ps. prime a}) \wedge \text{prime (int p)} \) and \( \text{IH} \): \( \forall u v. \text{coprime } u v \wedge u^2 + 3 v^2 = \text{int}(\prod i \in \# ps. i)^3 \wedge \text{odd (int}(\prod i \in \# ps. i)) \implies \text{is-cube-form u v} \)

by auto

then have \( \text{coprime a b} \)

by simp

let \( \exists w = \text{int (} (\prod i \in \# ps + \{\# p\}. i) \) \nlet \( \exists X = \text{int (} (\prod i \in \# ps. i) \)

let \( \exists p = \text{int p} \)

have ge3-1: (\(3::\text{int}\)) \(\geq 1 \) by auto

have \( p w: \exists w = ? p \ast ? X \wedge \text{odd } ? p \wedge \text{odd } ? X \)

proof (safe)

have \( \exists w = \text{int (} (\prod i \in \# ps + \{\# p\}. i) \) \) \( ? p \ast \text{int (} (\prod i \in \# ps. i) \)

thus \( \exists w = ? p \ast ? X \)

by (auto simp only: of-nat-mult [symmetric])

with \( \text{ass show even } ? p \implies \text{False by auto} \)

from \( \exists w \) have \( \exists w = ? X \ast ? p \) by simp

with \( \text{ass show even } ? X \implies \text{False by simp} \)

qed

have \( \text{is-\text{-}qfN } ? p \ 3 \)

proof —
2.5 The case $N = 3$

from ass have $a^2 + 2 \cdot b^2 = (\exists p \cdot ?p \cdot X \cdot ?p \cdot X)$ by (simp add: mult.commute)

hence $?p \cdot dvd a^2 + 3 \cdot b^2$ by (simp add: eval-nat-numeral field-simps)

moreover from ass have prime $?p$ and coprime $a \ b$ by simp-all

moreover from $pw$ have odd $?p$ by simp

ultimately obtain $?thesis$ by (simp add: qf3-oddprimedivisor)

 qed

then obtain $\alpha \ \beta$ where alphabeta: $?p = \alpha^2 + 3 \cdot \beta^2$

by (auto simp add: is-qfN-def)

have $\alpha \neq 0$

proof (rule ccontr, simp)

assume $\alpha = 0$ with alphabeta have $3 \ dvd \ ?p$ by auto

with $pw$ have $w3$: $3 \ dvd \ ?w$ by (simp only: dvd-mult2)

then obtain $v$ where $?w = 3^*v$ by (auto simp add: dvd-def)

with ass have $vab$: $27^*v^3 = a^2 + 3^*b^2$ by simp

hence $a^2 = 3^*(9^*v^3 - b^2)$ by auto

hence $3 \ dvd \ a^2$ by (unfold dvd-def, blast)

moreover have prime $3^::int$ by simp

ultimately have $a3$: $3 \ dvd \ a$ using prime-dvd-power-int[of $3^::int \ b \ 2$] by fastforce

then obtain $c$ where $c = 3^*c$ by (auto simp add: dvd-def)

with $vab$ have $27^*v^3 = 9^*c^2 + 3^*b^2$ by (simp add: power-mult-distrib)

hence $b^2 = 3^*(3^*v^3 - c^2)$ by auto

hence $3 \ dvd \ b^2$ by (unfold dvd-def, blast)

moreover have prime $3^::int$ by simp

ultimately have $3 \ dvd \ b$ using prime-dvd-power-int[of $3^::int \ b \ 2$] by fastforce

with $a3$ have $3 \ dvd \ gcd \ a \ b$ by simp

with $ass$ show $False$ by simp

moreover from alphabeta $pw$ have $\alpha^2 + 3^*\beta^2 = 1$

ultimately obtain $c \ d$ where $cdp$:

$(\alpha^2 + 3^*\beta^2)^3 = c^2 + 3^*d^2 \land \ coprime \ c \ (3^*d)$

by (blast dest: qfN-oddprime-cube)

with ass have $\exists \ u \ v. \ a^2 + 3^*b^2 = (u^2 + 3^*v^2)^*(c^2 + 3^*d^2)$

by (rule-tac $A = ?w$ and $n=3$ in qfN-power-div-prime, auto)

then obtain $u \ v \ e$ where $wab$: $a^2 + 3^*b^2 = (u^2 + 3^*v^2)^*(c^2 + 3^*d^2)$

by (rule-tac $A = ?w$ and $n=3$ in qfN-power-div-prime, auto)

finally have $?p^3 \cdot (u^2 + 3^*v^2 - ?X \cdot ?p \cdot X) = 0$ by auto

with $p0$ show $?thesis$ by auto

qed

with $pw \ IH$ have show $?thesis$ by simp

qed

moreover have is-cube-form $c \ d$
2.6 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 \((\frac{a}{p})(\frac{b}{p}) = \frac{ab}{p^2}\), where \(p\) is an odd prime.

**Lemma** Legendre-zmult: \([ p > 2; \text{prime } p ]\)

\[ \Rightarrow (\text{Legendre } (a*b) \ p) = (\text{Legendre } a \ p)*(\text{Legendre } b \ p) \]

**Proof** –

- Assume \(p^2; p > 2\) and prp: prime \(p\)
- From prp have prp’: prime (nat \(p\))
- By simp
- Let \(?p12 = \text{nat}((p - 1) \text{ div } 2)\)
- Let \(?Labp = \text{Legendre } (a*b) \ p\)
- Let \(?Lap = \text{Legendre } a \ p\)
- Let \(?Lbp = \text{Legendre } b \ p\)
- Have h1: \((\text{nat } p - 1) \text{ div } 2) = \text{nat } ((p - 1) \text{ div } 2)\) using \(p2\) by auto
- Hence \([?Labp = (a*b)^{(?p12)}] \mod p\) using prp p2 euler-criterion[of nat \(p\) a*b]
- By auto
- Hence \([a^{(?p12)} * b^{(?p12)} = ?Labp] \mod p\)
- By (simp only: power-mult-distrib cong-sym)
- Moreover have \([?Lap * ?Lbp = a^{(?p12)*b^{(?p12)}}] \mod p\)
using euler-criterion[of nat p] p2 prp' h1 by (simp add: cong-mult)
ultimately have [?Labp * ?Lbp = ?Labp] (mod p)
using cong-trans by blast
then obtain k where: ?Labp = (?Labp?Lbp) + p * k
by (auto simp add: cong-iff-lin)
have k=0
proof (rule ccontr)
assume k ≠ 0 hence |k| = 1 ∨ |k| > 1 by arith
moreover have k1: |k| > 1
  with p2 have |k|*p > 2 by auto }
moreover
{ assume k1: |k| > 1
  with p2 have |k|*p < |k|*p
    by (simp only: zmult-2less-2mono2)
  with k1 have |k|*p > 2 by arith }
ultimately have |k|*p > 2 by auto
moreover from p2 have |p| = p by auto
ultimately have k*p > 2 by (auto simp only: abs-mult)
moreover from k have ?Labp − ?Labp?Lbp = k*p by auto
ultimately have |?Labp − ?Labp?Lbp| > 2 by auto
moreover have ?Labp = 1 ∨ ?Labp = 0 ∨ ?Labp = −1
  by (simp add: Legendre-def)
moreover have ?Labp?Lbp = 1 ∨ ?Labp?Lbp = 0 ∨ ?Labp?Lbp = −1
  by (auto simp add: Legendre-def)
ultimately show False by auto
qed
with k show ?thesis by auto
qed

Now show \((\frac{2}{p}) = +1\) for primes \(p \equiv 1 \text{ mod } 6\).

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

**proof**

- let \(?p = 6*m+1\)
- let \(?L = \text{Legendre} (-3) \ ?p\)
- let \(?L1 = \text{Legendre} (-1) \ ?p\)
- let \(?L3 = \text{Legendre} 3 \ ?p\)
  assume \(p\): prime \(?p\)
  from \(p\) have \(p\): prime \((\text{nat } ?p)\) by simp
  have neg1cube: \((-1::int) ^ 3 = -1\) by simp
  have \(m1\): \(m \geq 1\)
  proof (rule ccontr)
    assume \(\neg \ m \geq 1\) hence \(m \leq 0\) by simp
    with \(p\) show False by (auto simp add: prime-int-iff)
  qed
  hence \(pn3\): \(?p \neq 3\) and \(p2\): \(?p > 2\) by auto
  with \(p\) have ?L = (Legendre \((-1) \ p\)) * (Legendre 3 ?p)
    by (frule-tac a=-1 and b=3 in Legendre-zmult, auto)
  moreover have [Legendre \((-1) \ p = (-1) \ nat m\) (mod ?p)]
    proof
      have nat((?p − 1) div 2) = (nat ?p − 1) div 2 by auto
      hence [?L1 = (-1) * (nat((?p − 1) div 2))] (mod ?p)
moreover have nat ((?p - 1) div 2) = 3* nat m
proof –
  have (?p - 1) div 2 = 3*m by auto
  hence nat((?p - 1) div 2) = nat (3*m) by simp
moreover have (3::int) ≥ 0 by simp
ultimately show ?thesis by (simp add: nat-mult-distrib)
qed
moreover have neg1cube (-1::int) *(3*nat m) = (-1) ^ nat m
  by (simp only: power-mult)
ultimately show ?thesis by auto
qed
moreover have ?L3 = (-1) ^ nat m
proof –
  have ?L3 * (Legendre ?p 3) = (-1) ^ nat m
proof –
  have nat ((3 - 1) div 2 * ((6 * m + 1 - 1) div 2)) = 3*nat m by auto
  hence ?L3 * (Legendre ?p 3) = (-1::int) ^ (3*nat m)
using Quadratic-Reciprocity-int[of 3 ?p] p' pn3 p2 by fastforce
with neg1cube show ?thesis by (simp add: power-mult)
qed
moreover have Legendre ?p 3 = 1
proof –
  have [1^2 = ?p] (mod 3) by (unfold cong-iff-dvd-diff dvd-def, auto)
  hence QuadRes 3 ?p by (unfold QuadRes-def, blast)
moreover have - [?p = 0] (mod 3)
proof (rule ccontr, simp)
  assume [?p = 0] (mod 3)
  hence 3 dvd ?p by (simp add: cong-iff-dvd-diff)
  moreover have 3 dvd 6*m by (auto simp add: dvd-def)
  ultimately have 3 dvd ?p - 6*m by (simp only: dvd-diff)
  hence (3::int) dvd 1 by simp
thus False by auto
qed
ultimately show ?thesis by (unfold Legendre-def, auto)
qed
ultimately show ?thesis by auto
qed
ultimately have ![L = (-1) ^ (nat m) * (-1) ^ (nat m)] (mod ?p)
  by (metis cong-scalar-right)
  hence ![L = (-1) ^ ((nat m) + (nat m))] (mod ?p) by (simp only: power-add)
moreover have (nat m) + (nat m) = 2*(nat m) by auto
ultimately have ![L = (-1) ^ (2*(nat m))] (mod ?p) by simp
  hence ![L = ((-1) ^ 2) ^ (nat m)] (mod ?p) by (simp only: power-mult)
  hence ![L = ?L] (mod ?p) by (auto simp add: cong-sym)
  hence ![p dvd 1 - ?L] by (simp only: cong-iff-dvd-diff)
moreover have ![L = -1 ∨ ![L = 0 ∨ ![L = 1] by (simp add: Legendre-def)
ultimately have ![p dvd 2 ∨ ![p dvd 1 ∨ ![L = 1] by auto
moreover
  assume ![p dvd 2 ∨ ![p dvd 1
  with p2 have False by (auto simp add: zdvd-not-zless)
ultimately show ?thesis by auto
3 Fermat’s last theorem, case \( n = 3 \)

theory Fermat3

begin

context

begin

Proof of Fermat’s last theorem for the case \( n = 3 \):

\[
\forall x, y, z : \quad x^3 + y^3 = z^3 \implies xyz = 0.
\]

private lemma nat-relprime-power-divisors:

assumes \( n0: 0 < n \) and \( abc: (a::nat)*b = c \cdot n \) and \( relprime: coprime a b \)

shows \( \exists k. \quad a = k \cdot n \)

using assms proof (induct c arbitrary: a b rule: nat-less-induct)

case (1 c)

show ?case

proof (cases a > 1)

qed
case False
  hence \( a = 0 \lor a = 1 \) by linarith
  thus ?thesis using \( n \)0 power-one-zero-power by (simp only: eq-sym-conv) blast
next

case True
  then obtain \( p \) where \( p \)\: prime \( p \) dvd \( a \) using prime-factor-nat[of \( a \)] by blast
  hence \( h1 \): \( p \) dvd \( (c \cdot n) \) using \( 1(3) \) dvd-mult2[of \( p \) \( a \) \( b \)] by presburger
  hence \( (p \cdot n) \) dvd \( (c \cdot n) \)
    using \( p(1) \) prime-dvd-power-nat[of \( p \) \( c \) \( n \)] ded-power-same[of \( p \) \( c \) \( n \)] by blast
  moreover have \( h2 \): \( \neg \) \( p \) dvd \( b \)
    using \( \neg \) \( (p \cdot n) \) dvd \( b \) using \( n \)0 \( p(1) \) dvd-power[of \( n \) \( p \)] gcd-nat.trans by blast
  ultimately have \( (p \cdot n) \) dvd \( a \)
    using \( \{ \)prems \( p(1) \)\: prime-elm-divprod-pow \( \} \) of \( a \) \( b \) \( n \)
    by simp
  then obtain \( a' \) \( c' \) where \( ac \): \( a = p' \cdot n \ast a' \) \( c = p \ast c' \)
    using \( h1 \) dvdE[of \( p' \cdot n \) \( a \) \( p \cdot c \)]\: prime-dvd-power-nat[of \( p \) \( c \) \( n \)] \( p(1) \)
    by meson
  hence \( p' \cdot n \ast (a' \ast b) = p' \cdot n \ast c' \cdot n \)
    using \( 1(3) \)
    by (simp add: power-mult-distrib semiring-normalization-rules(18))
  hence \( a' \ast b = c' \cdot n \)
    using \( p(1) \) by auto
  moreover have \( coprime a' \) \( b \) using \( 1(4) \) ac\( (1) \)
    by simp
  moreover have \( 0 < b < 0 < a \) using \( h2 \) dvd-0-right gr0I \( True \) by fastforce+
  then have \( 0 < c < 1 < p \)
    using \( p(1) \) \( 1(3) \) nat-0-less-mult-iff[of \( a \) \( b \) \( n \)0 prime-gt-Suc-0-nat
    by simp-all
  hence \( c' < c \) using ac\( (2) \) by simp
  ultimately obtain \( k \)
    where \( a' = k' \cdot n \)
    using \( 1(1) \) \( n \)0 by presburger
  hence \( a = (p \ast k') \cdot n \)
    using ac\( (1) \) by (simp add: power-mult-distrib)
  thus ?thesis by blast
qed

private lemma int-relprime-odd-power-divisors:
  assumes \( \text{odd } n \) and \( (a::\text{int}) \ast b = c \cdot n \) and \( \text{coprime } a \) \( b \)
  shows \( \exists k. \ a = k' \cdot n \)
proof –
  from \( \text{assms have } |a| \ast |b| = |c| \cdot n \)
    by (simp add: abs-mult [symmetric] power-abs)
  then have \( \text{nat } |a| \ast \text{nat } |b| = \text{nat } |c| \cdot n \)
    by (simp add: nat-mult-distrib [of \( |a| \) \( b \), symmetric] nat-power-eq)
  moreover have \( \text{coprime } (\text{nat } |a|) \)
    (\( \text{nat } |b| \)) using \( \text{assms}(3) \)
    \( \text{gcd-int-def } \)
    by fastforce
  ultimately have \( \exists k. \ \text{nat } |a| = k' \cdot n \)
    using nat-relprime-power-divisors[of \( \text{nat } |a| \)
    nat \( |b| \) nat \( |c| \] \( \text{assms}(1) \)
    by blast
  then obtain \( k' \)
    where \( k' : \text{nat } |a| = k' \cdot n \)
    by blast
  moreover define \( k \)
    where \( k = \text{int } k' \)
  ultimately have \( k : |a| = k' \cdot n \)
    using int-nat-eq[of \( |a| \)] of-nat-power[of \( k' \) \( n \)]
    by force
    \{ assume \( a \neq k' \cdot n \)
      with \( k \) have \( a = -(k' \cdot n) \)
      by arith
    \}
  hence \( a = (-k') \cdot n \)
    using \( \text{assms}(1) \)
    \( \text{power-minus-odd } \)
    by simp
  thus ?thesis by blast
qed

private lemma factor-sum-cubes: \((x::\text{int})^3 + y^3 = (x+y)(x^2 - x \cdot y + y^2)\)
Fermat’s last theorem, case $n = 3$

by (simp add: eval-nat-numeral field-simps)

private lemma two-not-abs-cube: $|x^3| = (2::int) \Rightarrow \text{False}$
proof
- assume $|x^3| = 2$
  hence $x^3: |x^3| = 2$ by (simp add: power-abs)
  have $|x| \geq 0$ by simp
moreover
{} assume $|x| = 0 \lor |x| = 1 \lor |x| = 2$
  with $x^3$ have False by (auto simp add: power-0-left)
moreover
{} assume $|x| > 2$
  moreover have $(0::int) \leq 2$ and $(0::nat) < 3$ by auto
  ultimately have $|x^3| > 2^3$ by (simp only: power-strict-mono)
  with $x^3$ have False by simp
ultimately show False by arith
qed

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

private lemma no-rewritten-fermat3:
~ $\exists v w. v^3+w^3 = x^3 \land v\cdot w \cdot x \neq 0 \land \text{even } (x::int) \land \text{coprime } v\ w$
proof (induct $x$ rule: infinite-descent0-measure[where $V=\lambda x. \text{nat} |x^3|$])
case ($0\ x$) hence $x^3 = 0$ by arith
  hence $x=0$ by auto
  thus ?case by auto
next
case (smaller $x$)
then obtain $v\ w$ where $vwx: v^3+w^3=x^3 \land v\cdot w\cdot x \neq 0 \land \text{even } x \land \text{coprime } v\ w$ (is ?P $v\ w\ x$)
  by auto
then have coprime $v\ w$
  by simp
have $\exists \alpha \beta \gamma. \ ?P \ \alpha \beta \gamma \land \text{nat} |\gamma^3\rangle < \text{nat} |x^3|$ 
proof 
- obtain coprime $p$ and $q$ such that $v = p+q$ and $w = p-q$
  have $vw\text{Odd}: \text{odd } v \land \text{odd } w$
  proof (rule ccontr, case-tac odd $v$, simp-all)
    assume $vc: \text{even } v$
    hence even $(v^3)$ by simp
  moreover from $vwx$ have even $(x^3)$ by simp
  ultimately have even $(x^3-v^3)$ by simp
moreover from $vwx$ have $x^3-v^3 = w^3$ by simp
ultimately have even $(w^3)$ by simp
  hence even $w$ by simp
  with $ve$ have $2 \cdot \text{dvd } v \land 2 \cdot \text{dvd } w$ by auto
  hence $2 \cdot \text{dvd } \text{gcd } v\ w$ by simp
  with $vwx$ show False by simp
next
  assume odd $v$ and even $w$
  hence odd $(v^3)$ and even $(w^3)$
    by auto

qed
hence \( \text{odd } (w^3 + v^3) \) by simp
with \( \text{vux} \) have \( \text{odd } (x^3) \) by (simp add: add.commute)
hence odd \( x \) by simp
with \( \text{vux} \) show False by auto
qed

hence even \((v+w)\) \& even \((v-w)\) by simp
then obtain \( p \ q \) where \( pq: v+w = 2*p \ \& \ v-w = 2*q \)
using evenE[of \( v+w \)] evenE[of \( v-w \)] by meson
hence \( vw: v = p+q \ \& \ w = p-q \) by auto
— show that \( x^3 = (2p)(p^2 + 3q^2) \) and that these factors are
— either coprime (first case), or have 3 as g.c.d. (second case)
have \( vwpq: v^3 + w^3 = (2*p)*(p^2 + 3*q^2) \)
proof –
  have \( 2*(v^3 + w^3) = 2*(v+w)*(v^2 - v*w + w^2) \)
  by (simp only: factor-sum-cubes)
also from \( pq \) have \( \ldots = 4*p*(v^2 - v*w + w^2) \) by auto
also have \( \ldots = p*((v+w)^2 + 3*(v-w)^2) \)
  by (simp add: eval-nat-numeral field-simps)
also with \( pq \) have \( \ldots = p*((2*p)^2 + 3*(2*q)^2) \) by simp
also have \( \ldots = 2*(2*p)*(p^2+3*q^2) \) by (simp add: power-mult-distrib)
finally show ?thesis by simp
qed

let \( ?g = \text{gcd } (2 \times p) \ (p^2 + 3 * q^2) \)
have \( g1: ?g \geq 1 \)
proof (rule ccontr)
  assume \(~ ?g \geq 1 \)
  then have \( ?g < 0 \lor ?g = 0 \) unfolding not-le by arith
  moreover have \( ?g \geq 0 \) by simp
  ultimately have \( ?g = 0 \) by arith
  hence \( p = 0 \) by simp
with \( vwpq \) have \(0 < \text{nat} |x^3|\) show False by auto
qed

have gOdd: odd \( ?g \)
proof (rule ccontr)
  assume \(~ odd ?g \)
hence \( \text{2 dvd } p^2 + 3*q^2 \) by simp
then obtain \( k \) where \( k: p^2 + 3*q^2 = 2*k \) by (auto simp add: dvd-def)
hence \( 2*(k - 2*q^2) = p^2 - q^2 \) by auto
also have \( \ldots = (p+q)*(p-q) \) by (simp add: power2-eq-square algebra-simps)
finally have \( v*w = 2*(k - 2*q^2) \) using \( vw \) by presburger
hence even \((v*w)\) by auto
hence even \((v)\) \& even \((w)\) by simp
with \( vwOdd \) show False by simp
qed

then have even-odd-p-q: even \( p \ \& \ odd q \lor odd p \ \& \ even q \)
  by auto
— first case: \( p \) is not a multiple of 3; hence \( 2p \) and \( p^2 + 3q^2 \)
— are coprime; hence both are cubes
\{ assume \( p3: \neg 3 \text{ dvd } p \)
  have g3: \( \neg 3 \text{ dvd } ?g \)
  proof (rule ccontr)
    assume \( \neg \neg 3 \text{ dvd } ?g \) hence \( 3 \text{ dvd } 2*p \) by simp
  \}

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

\[
\begin{align*}
&\text{hence } (3::\text{int}) \text{ dvd } 2 \lor 3 \text{ dvd } p \\
&\quad \text{using } \text{prime-dvd-multD} \text{[of 3]} \text{ by } \text{(fastforce simp add: prime-dvd-mult-iff)} \\
&\quad \text{with } p3 \text{ show } \text{False by arith} \\
&\text{qed} \\
&\text{from } \langle \text{coprime } v \text{ w} \rangle \text{ have } \text{pq-relprime: coprime } p \text{ q} \\
&\text{proof } \text{(rule coprime-imp-coprime)} \\
&\quad \text{fix } c \\
&\quad \text{assume } c \text{ dvd } p \text{ and } c \text{ dvd } q \\
&\quad \text{then have } c \text{ dvd } p + q \text{ and } c \text{ dvd } p - q \\
&\quad \quad \text{by simp-all} \\
&\quad \text{with } vw \text{ show } c \text{ dvd } v \text{ and } c \text{ dvd } w \\
&\quad \quad \text{by simp-all} \\
&\text{qed} \\
&\text{from } \langle \text{coprime } p \text{ q} \rangle \text{ have } \text{coprime } p \ (q^2) \\
&\quad \text{by simp} \\
&\text{then have } \text{factors-relprime: coprime } (2 * p) \ (p^2 + 3 * q^2) \\
&\text{proof } \text{(rule coprime-imp-coprime)} \\
&\quad \text{fix } c \\
&\quad \text{assume } g2p: c \text{ dvd } 2 * p \text{ and } gpq: c \text{ dvd } p^2 + 3 * q^2 \\
&\quad \text{have coprime } 2 \ c \\
&\quad \quad \text{using } g2p \text{ gpq even-odd-p-q dvd-trans [of 2 c p]} \\
&\quad \quad \text{by auto} \\
&\quad \text{with } g2p \text{ show } c \text{ dvd } p \\
&\quad \quad \text{by } \text{(simp add: coprime-dvd-mult-left-iff ac-simps)} \\
&\quad \text{then have } c \text{ dvd } p^2 \\
&\quad \quad \text{by } \text{(simp add: power2-eq-square)} \\
&\quad \text{with } gpq \text{ have } c \text{ dvd } 3 * q^2 \\
&\quad \quad \text{by } \text{(simp add: dvd-add-right-iff)} \\
&\quad \text{moreover have } \text{coprime } 3 \ c \\
&\quad \quad \text{using } c \text{ dvd } p \text{ p3 dvd-trans [of 3 c p]} \\
&\quad \quad \text{by } \text{(auto intro: prime-imp-coprime)} \\
&\quad \text{ultimately show } c \text{ dvd } q^2 \\
&\quad \quad \text{by } \text{(simp add: coprime-dvd-mult-right-iff ac-simps)} \\
&\text{qed} \\
&\text{moreover from } vwx \text{ vwpq have } \text{pqx: } (2 * p)* (p^2 + 3 * q^2) = x^3 \text{ by auto} \\
&\text{ultimately have } \exists \ c. \ 2 * p = c^3 \text{ by } \text{(simp add: int-relprime-odd-power-divisors)} \\
&\text{then obtain } c \text{ where } c: c^3 = 2 * p \text{ by auto} \\
&\text{from } \text{pqx factors-relprime have } \text{coprime } (p^2 + 3 * q^2) \ (2 * p) \\
&\quad \text{and } (p^2 + 3 * q^2)*(2 * p) = x^3 \text{ by } \text{(auto simp add: ac-simps)} \\
&\text{hence } \exists \ d. \ p^2 + 3 * q^2 = d^3 \text{ by } \text{(simp add: int-relprime-odd-power-divisors)} \\
&\text{then obtain } d \text{ where } d: p^2 + 3 * q^2 = d^3 \text{ by auto} \\
&\text{have odd } d \\
&\text{proof } \text{(rule ccontr)} \\
&\quad \text{assume } \neg \text{ odd } d \\
&\quad \text{hence even } (d^3) \text{ by simp} \\
&\quad \text{hence } 2 \text{ dvd } d^3 \text{ by simp} \\
&\quad \text{moreover have } 2 \text{ dvd } 2 * p \text{ by } \text{(rule dvd-triv-left)} \\
&\quad \text{ultimately have } 2 \text{ dvd } \gcd (2 * p) \ (d^3) \text{ by simp} \\
&\quad \text{with } d \text{ factors-relprime show False by simp} \\
&\text{qed} \\
&\text{with } d \text{ pq-relprime have } \text{coprime } p \text{ q} \land p^2 + 3 * q^2 = d^3 \land \text{add } d \\
&\quad \text{by simp}
Fermat's last theorem, case $n = 3$

hence $\exists$ have

proof (from $\langle$)

then obtain $a \ b$ where $p = a^3 - 9*a*b^2 \land q = 3*a^2*b - 3*b^3$

by (unfold is-cube-form-def, auto)

hence $ab: p = a*(a+3*b)*(a-3*b) \land q = b*(a+b)*(a-b+3)$

by (simp add: eval-nat-numeral field-simps)

with $c$ have $abc: (2*a)*(a+3*b)*(a-3*b) = c^3$ by auto

from $pq$-relprime $ab$ have $ab$-relprime: coprime $a \ b$

by (auto intro: coprime-imp-coprime)

then have $ab1$: coprime $(2 \ a)$ $(a + 3 \ b)$

proof (rule coprime-imp-coprime)

fix $h$

assume $h2a$: $h \ dvd \ 2 \ a$ and $hab$: $h \ dvd \ a + 3 \ b$

have coprime $2 \ h$

using $ab$ even-odd-p-q $h \ dvd$-trans $[of \ 2 \ h \ a + 3 \ b]$

by auto

with $h2a$ show $h \ dvd \ a$

by (simp add: coprime-dvd-mult-left-iff ac-simps)

with $hab$ have $h \ dvd \ 3 \ b$ and $\neg \ 3 \ dvd \ h$

using dvd-trans $[of \ 3 \ h \ a] \ ab (\neg \ 3 \ dvd \ p)$

by (auto simp add: dvd-add-right-iff)

moreover have coprime $3 \ h$

using $\neg \ 3 \ dvd \ h$ by (auto intro: prime-imp-coprime)

ultimately show $h \ dvd \ b$

by (simp add: coprime-dvd-mult-left-iff ac-simps)

qed

then have $[simp]$: even $b \longleftrightarrow$ odd $a$

and $ab3$: coprime $a$ $(a + 3 \ b)$

by simp-all

from $\langle$coprime $a \ b$ have $ab4$: coprime $a$ $(a - 3 \ b)$

proof (rule coprime-imp-coprime)

fix $h$

assume $h2a$: $h \ dvd \ a$ and $hab$: $h \ dvd \ a - 3 \ b$

then show $h \ dvd \ a$

by simp

with $hab$ have $h \ dvd \ 3 \ b$ and $\neg \ 3 \ dvd \ h$

using dvd-trans $[of \ 3 \ h \ a] \ ab (\neg \ 3 \ dvd \ p) \ dvd-add-right-iff [of \ h \ a - 3 \ b]$

by auto

moreover have coprime $3 \ h$

using $\neg \ 3 \ dvd \ h$ by (auto intro: prime-imp-coprime)

ultimately show $h \ dvd \ b$

by (simp add: coprime-dvd-mult-left-iff ac-simps)

qed

from $ab1$ have $ab2$: coprime $(a + 3 \ b)$ $(a - 3 \ b)$

by (rule coprime-imp-coprime)

(use dvd-add $[of \ - \ a + 3 \ b \ a - 3 \ b]$ in simp-all)

have $\exists k \ l \ m. \ 2 \ a = k \cdot 3 \land a + 3 \ b = l \cdot 3 \land a - 3 \ b = m \cdot 3$

using $ab2 \ ab3 \ ab4 \ abc$

int-relprime-odd-power-divisors $[of \ 3 \ 2 \ a \ (a + 3 \ b) \ (a - 3 \ b) \ c]$

int-relprime-odd-power-divisors $[of \ 3 \ (a + 3 \ b) \ 2 \ a \ (a - 3 \ b) \ c]$

int-relprime-odd-power-divisors $[of \ 3 \ (a - 3 \ b) \ 2 \ a \ (a + 3 \ b) \ c]$

by auto (auto simp add: ac-simps)

then obtain $\alpha \ \beta \ \gamma$ where $algebra:
\[ 2 \cdot a = \gamma \cdot 3 \land a - 3 \cdot b = \alpha \cdot 3 \land a + 3 \cdot b = \beta \cdot 3 \text{ by auto} \]

This shows \( a \) is a (smaller) solution.

**hence** \( \alpha \cdot 3 + \beta \cdot 3 = \gamma \cdot 3 \text{ by auto} \)

**moreover have** \( \alpha \cdot \beta \cdot \gamma \neq 0 \)

**proof (rule ccontr, safe)**

**assume** \( \alpha \cdot \beta \cdot \gamma = 0 \)

**with** \( \text{algebra ab have } p \cdot 0 \text{ by (auto simp add: power-0-left)} \)

**with** \( \text{vwpq vwx show False by auto} \)

**qed**

**moreover have** \( \text{even } \gamma \)

**proof**

**have** \( (2 \cdot a) \text{ by simp} \)

**with** \( \text{algebra have } (\gamma \cdot 3) \text{ by simp} \)

**thus** \( \theta \text{thesis by simp} \)

**qed**

**moreover have** \( \text{coprime } \alpha \beta \)

**using ab2 proof (rule coprime-imp-coprime)**

**fix** \( h \)

**assume** \( h \text{ dvd } \alpha \text{ and } h \text{ dvd } \beta \)

**then have** \( h \text{ dvd } \alpha \cdot \alpha \cdot 2 \land h \text{ dvd } \beta \cdot \beta \cdot 2 \text{ by simp} \)

**then have** \( h \text{ dvd } \alpha \cdot \text{Suc } 2 \land h \text{ dvd } \beta \cdot \text{Suc } 2 \text{ by (auto simp only: power-Suc)} \)

**with** \( \text{algebra show } h \text{ dvd } a - 3 \cdot b \text{ h dvd } a + 3 \cdot b \text{ by auto} \)

**qed**

**moreover have** \( \text{nat } | \gamma \cdot 3 | < \text{nat } | x \cdot 3 | \)

**proof**

**let** \( ?A = p \cdot 2 + 3 \cdot q \cdot 2 \)

**from vwx vwpq have** \( x \cdot 3 = 2 \cdot p \cdot ?A \text{ by auto} \)

**also with** \( ab \text{ have } \ldots = 2 \cdot a \cdot (a + 3 \cdot b) \cdot (a - 3 \cdot b) \cdot ?A \text{ by auto} \)

**also with** \( \text{algebra have } \ldots = \gamma \cdot 3 \cdot (a + 3 \cdot b) \cdot (a - 3 \cdot b) \cdot ?A \text{ by auto} \)

**finally have** \( \text{eq: } | x \cdot 3 | = | \gamma \cdot 3 | \cdot | (a + 3 \cdot b) \cdot (a - 3 \cdot b) \cdot ?A | \)

**by (auto simp add: abs-mult)**

**with** \( 0 < \text{nat } | x \cdot 3 | \) \( \text{have } (1 + 3 \cdot b) \cdot (a - 3 \cdot b) \cdot ?A > 0 \text{ by auto} \)

**hence** \( \text{eqpos: } (1 + 3 \cdot b) \cdot (a - 3 \cdot b) > 0 \text{ by auto} \)

**moreover have** \( \text{Ag1: } | ?A | > 1 \)

**proof**

**have** \( \text{Agf3: is-qfN } ?A 3 \text{ by (auto simp add: is-qfN-def)} \)

**moreover have** \( \text{triv3b: } (3::\text{int}) \geq 1 \text{ by simp} \)

**ultimately have** \( ?A \geq 0 \text{ by (simp only: qfN-pos)} \)

**hence** \( ?A > 1 \lor ?A = 0 \lor ?A = 1 \text{ by arith} \)

**moreover**

**{ assume** \( ?A = 0 \text{ with } \text{triv3b have } p = 0 \land q = 0 \text{ by (rule qfN-zero)} \)

**with** \( \text{vwpq vwx have False by auto } \)

**moreover**

**{ assume** \( A1: ?A = 1 \)

**have** \( q = 0 \)

**proof (rule ccontr)**

**assume** \( q \neq 0 \)

**hence** \( q \cdot 2 > 0 \text{ by simp} \)

**hence** \( 3 \cdot q \cdot 2 > 1 \text{ by arith} \)

**moreover have** \( p \cdot 2 \geq 0 \text{ by (rule zero-le-power2)} \)

**ultimately have** \( ?A > 1 \text{ by arith} \)

**with** \( A1 \text{ show False by simp} \)
Fermat’s last theorem, case \( n = 3 \)

qed

with \( pq\text{-relprime} \) have \(|p| = 1 \) by simp

with \( vwq \ vwx \ A1 \) have \(|x^3| = 2 \) by auto

hence False by (rule two-not-abs-cube)

ultimately show \(?thesis\) by auto

qed

ultimately have

\(|(a + 3b)\ast(a - 3b)|1 < |(a + 3b)\ast(a - 3b)\ast| ?A|\)

by (simp only: zmult-zless-mono2)

with \( egpos \) have \(|(a + 3b)\ast(a - 3b)\ast| ?A| > 1 \) by arith

hence \(|(a + 3b)\ast(a - 3b)\ast| ?A| > 1 \) by (auto simp add: abs-mul)

moreover have \(|\gamma \cdot 3| > 0 \)

proof –

from eq have \(|\gamma \cdot 3| = 0 \implies |x^3| = 0 \) by auto

with \( 0 < \text{nat}|x^3| \) show \(?thesis\) by auto

qed

ultimately have \(|\gamma \cdot 3| \ast 1 < |\gamma \cdot 3| \ast |(a + 3b)\ast(a - 3b)\ast| ?A|\)

by (rule zmult-zless-mono2)

with \( eq\) have \(|x^3| \) \(|\gamma \cdot 3| \) by auto

thus \(?thesis\) by arith

qed

ultimately have \(?thesis\) by auto

moreover

— second case: \( p = 3r \) and hence \( x^3 = (18r)(q^2 + 3r^2) \) and these

— factors are coprime; hence both are cubes

\{ assume \( p3: 3 \) dvd \( p \)

then obtain \( r \) where \( r: p = 3\ast r \) by (auto simp add: dvd-def)

moreover have \( 3 \) dvd \( 3\ast(3\ast r^2 + q^2) \) by (rule dvd-triv-left)

ultimately have \( pq3: 3 \) dvd \( p\ast 2 + 3\ast q^2 \) by (simp add: power-mul-distrib)

moreover from \( p3 \) have \( 3 \) dvd \( 2\ast p \) by (rule dvd-mul)

ultimately have \( g3: 3 \) dvd \( q \) by simp

from \( \langle \text{coprime} \ v \ w \rangle \) have \( qr\text{-relprime}: \text{coprime} \ q \ r \)

proof (rule coprime-imp-coprime)

fix \( h \)

assume \( hq: h \) dvd \( q \) h dvd \( r \)

with \( r \) have \( h \) dvd \( p \) by simp

with \( hq\) have \( h \) dvd \( p + q \) h dvd \( p - q \)

by simp-all

with \( vw\) show \( h \) dvd \( v \) h dvd \( w \)

by simp-all

qed

have \( \text{factors-relprime}: \text{coprime} \ (18\ast r) \ (q^2 + 3\ast r^2) \)

proof –

from \( g3 \) obtain \( k \) where \( k: \ ?g = 3\ast k \) by (auto simp add: dvd-def)

have \( k = 1 \)

proof (rule econtr)

assume \( k \neq 1 \)

with \( g1 \) \( k \) have \( k > 1 \) by auto

then obtain \( h \) where \( h: \text{prime} \ h \land h \) dvd \( k \)

using \( \text{prime-divisor-exists}[\text{of} \ k] \) by auto

with \( k \) have \( hq: 3\ast h \) dvd \( ?g \) by (auto simp add: mult-dvd-mono)

hence \( 3\ast h \) dvd \( p^2 + 3\ast q^2 \) and \( hp: 3\ast h \) dvd \( 2\ast p \) by auto
then obtain \( s \) where \( s \cdot p^2 + 3q^2 = (3h)s \)
by (auto simp add: dvd-def)
with \( r \) have \( rgq: 3r^2 + q^2 = h*s \) by (simp add: power-mult-distrib)
from \( hp \) have \( 3 + h \cdot d \cdot d \cdot 3 + (2*r) \) by simp
moreover have \( 3\cdot\text{int} \neq 0 \) by simp
ultimately have \( h \cdot d \cdot d \cdot 2 + r \) by (rule zdvd-mult-cancel)
with \( h \) have \( h \cdot d \cdot d \cdot 2 \lor h \cdot d \cdot d \cdot r \)
by (auto dest: prime-dvd-multD)
moreover have \( \sim h \cdot d \cdot d \cdot 2 \)
proof (rule ccontr, simp)
assume \( h \cdot d \cdot d \cdot 2 \)
with \( h \) have \( h=2 \) using zdvd-not-zless[of 2 \( h \)] by (auto simp: prime-int-iff)
with \( hg \) have \( 2\cdot3 \cdot d \cdot v \cdot d \cdot q \) by auto
hence \( 2 \cdot d \cdot v \cdot d \cdot q \) by (rule dvd-mult-left)
with \( g\text{Odd} \) show \( \text{False} \) by simp
qed
ultimately have \( hr: h \cdot d \cdot d \cdot r \) by simp
then obtain \( t \) where \( r = h\cdot t \) by (auto simp add: dvd-def)
hence \( t: r^2 = h\cdot(h\cdot t^2) \) by (auto simp add: power2-eq-square)
with \( rgq \) have \( h\cdot s = h\cdot(3\cdot h\cdot t^2) + q^2 \) by simp
hence \( q^2 = h\cdot(s - 3\cdot h\cdot t^2) \) by (simp add: right-diff-distrib)
hence \( h \cdot d \cdot v \cdot d \cdot q^2 \) by simp
with \( h \) have \( h \cdot d \cdot v \cdot d \cdot q \) using prime-dvd-multD[of \( h \cdot q \cdot q \)]
by (simp add: power2-eq-square)
with \( hr \) have \( h \cdot d \cdot v \cdot d \cdot g \cdot d \cdot q \) by simp
with \( h \) \( qr\)-relprime show \( \text{False} \) by (unfold prime-def, auto)
qed
with \( k \) \( r \) have \( 3 = \text{gcd} (2\cdot(3\cdot r)) \cdot ((3\cdot r)^2 + 3 \cdot q^2) \) by auto
also have \( \ldots = \text{gcd} (3\cdot (2\cdot r)) \cdot (3\cdot (3\cdot r)^2 + q^2) \)
by (simp add: power-mult-distrib)
also have \( \ldots = 3 \cdot \text{gcd} (2\cdot r) \cdot (3\cdot r^2 + q^2) \) using gcd-mult-distrib-int[of \( 3 \)]
by auto
finally have \( \text{coprime} (2\cdot r) \cdot (3\cdot r^2 + q^2) \)
by (auto dest: gcd-eq-1-imp-coprime)
moreover have \( \text{coprime} 9 \cdot (3\cdot r^2 + q^2) \)
using \( \langle \text{coprime} v \rangle \) proof (rule coprime-imp-coprime)
fix \( h :: \text{int} \)
assume \( \sim \text{is-unit} \) \( h \)
assume \( h9: h \cdot d \cdot v \cdot d \cdot 9 \) and \( hrq: h \cdot d \cdot v \cdot d \cdot 3 \cdot r^2 + q^2 \)
have \( \text{prime} (3\cdot\text{int}) \)
by simp
moreover from \( vh \) \( d \cdot v \) \( d \cdot 9 \) \( h \) have \( h \cdot d \cdot v \cdot d \cdot 3^2 \)
by simp
ultimately obtain \( k \) where \( \text{normalize} \) \( h = 3 \cdot k \)
by (rule divides-primpow)
with \( \sim \text{is-unit} \) \( h \) have \( 0 < k \)
by simp
with \( \langle \text{normalize} \rangle \) \( h = 3 \cdot k \) have \( |h| = 3 \cdot 3 \sim (k - 1) \)
by (cases \( k \)) simp-all
then have \( 3 \cdot d \cdot v \cdot d \) \ldots
then have \( 3 \cdot d \cdot v \cdot d \) 
by simp
then have \(3 \text{ dvd } 3 \cdot r^2 + q^2\)

using \(hrq\) by \(\text{rule dvd-trans}\)

then have \(3 \text{ dvd } q^2\)

by \(\text{presburger}\)

then have \(3 \text{ dvd } q\)

using \(\text{prime-dvd-power-int} \ [\text{of } 3 \ q 2]\) by \(\text{auto}\)

with \(p\) have \(3 \text{ dvd } p + q \text{ and } 3 \text{ dvd } p - q\)

by \(\text{simp-all}\)

with \(vw\) have \(3 \text{ dvd } p \text{ and } 3 \text{ dvd } q\)

by \(\text{simp-all}\)

with \(\langle \text{coprime } v \ w \rangle\) have \(\text{is-unit } (3::\text{int})\)

by \(\text{auto}\)

with \(p^3\) have \(3 \text{ dvd } p + q \text{ and } 3 \text{ dvd } p - q\)

by \(\text{simp-all}\)

ultimately have \(3 \text{ dvd } v \text{ and } 3 \text{ dvd } w\)

by \(\text{simp-all}\)

qed

ultimately have \(\langle 2 \ast r \ast 9 \rangle \ (3 \ast r^2 + q^2)\)

by \(\text{simp only: coprime-mult-left-iff}\)

then show \(?\text{thesis}\)

by \(\text{simp add: ac-simps}\)

qed

moreover have \(rqx:\ (18 \ast r) \ast (q^2 + 3 \ast r^2) = x^3\)

proof –

from \(vwx\ wpq\) have \(x^3 = 2 \ast p \ast (p^2 + 3 \ast q^2)\) by \(\text{auto}\)

also with \(r\) have \(\ldots = 2 \ast (3 \ast r) \ast (9 \ast r^2 + 3 \ast q^2)\)

by \(\text{auto simp add: power2-eq-square}\)

finally show \(?\text{thesis}\) by \(\text{auto}\)

qed

ultimately have \(\exists \ c.\ 18 \ast r = c^3\)

by \(\text{simp add: int-relprime-odd-power-divisors}\)

then obtain \(c1\) where \(c1:\ c1^3 = 3 \ast (6 \ast r)\) by \(\text{auto}\)

hence \(3 \text{ dvd } c1^3\) and \(\text{prime } (3::\text{int})\) by \(\text{auto}\)

hence \(3 \text{ dvd } c1\) using \(\text{prime-dvd-power}\ [\text{of } 3]\) by \(\text{fastforce}\)

with \(c1\) obtain \(c\) where \(c:\ 3 \ast c^3 = 2 \ast r\)

by \(\text{auto simp add: power-mult-distrib dvd-def}\)

from \(rqx\ \text{factors-relprime have coprime } (q^2 + 3 \ast r^2) \ (18 \ast r)\)

and \((q^2 + 3 \ast r^2) \ast (18 \ast r) = x^3\) by \(\text{auto simp add: ac-simps}\)

hence \(\exists \ d.\ q^2 + 3 \ast r^2 = d^3\)

by \(\text{simp add: int-relprime-odd-power-divisors}\)

then obtain \(d\) where \(d: q^2 + 3 \ast r^2 = d^3\) by \(\text{auto}\)

have \(\text{odd } d\)

proof \(\text{rule ccontr}\)

assume \(\neg \ \text{odd } d\)

hence \(2 \ast d \ast d^3\) by \(\text{simp}\)

moreover have \(2 \text{ dvd } 2 \ast (9 \ast r)\) by \(\text{rule dvd-triv-left}\)

ultimately have \(2 \text{ dvd } \gcd (2 \ast (9 \ast r)) \ (d^3)\) by \(\text{simp}\)

with \(d\) \text{factors-relprime show } \text{False} \ by \(\text{auto}\)

qed

with \(d\) \text{qr-relprime have coprime } q \ r \ \wedge \ q^2 + 3 \ast r^2 = d^3 \ \wedge \ \text{odd } d\)

by \(\text{simp}\)

hence \(\text{is-cube-form } q \ r\) by \(\text{rule qf3-cube-impl-cube-form}\)

then obtain \(a\ b\) where \(q = a^3 - 9 \ast a \ast b^2 \ \wedge \ r = 3 \ast a^2 \ast b - 3 \ast b^3\)

by \(\text{unfold is-cube-form-def, auto}\)
hence \( ab\): \( q = a\ast (a+3\ast b)\ast (a-3\ast b) \wedge r = b\ast (a+b)\ast (a-b)\ast 3 \)
by (simp add: eval-nat-numeral field-simps)
with \( c \) have \( abc\): \( (2\ast b)\ast (a+b)\ast (a-b) = c^3 \) by auto
from qr-relprime \( ab \) have \( ab\)-relprime: \( \text{coprime } a \ b \)
by (auto intro: coprime-imp-coprime)
then have \( ab1\): \( \text{coprime } (2\ast b)\ (a+b) \)
proof (rule coprime-imp-coprime)
fix \( h \)
assume \( h2b\): \( h \ \text{dvd } 2\ast b \ \text{and } \ hab\): \( h \ \text{dvd } a+b \)
have \( \text{odd } h \)
proof
assume \( \text{even } h \)
then have \( \text{even } (a + b) \)
using \( \text{hab } \) by (rule dvd-trans)
then have \( \text{even } (a+3\ast b) \)
by simp
with \( ab\) have \( \text{even } q \ \text{even } r \)
by auto
then show \( \text{False} \)
using \( \text{coprime-common-divisor-int } \text{qr-relprime } \) by fastforce
qed
with \( h2b \) show \( h \ \text{dvd } b \)
using \( \text{coprime-dvd-mult-right-iff } \) [of \( h \ 2\ast b \)] by simp
with \( \text{hab } \) show \( h \ \text{dvd } a \)
using \( \text{dvd-diff } \) [of \( h \ a+b \ a-b \)] by simp
qed
from \( ab1 \) have \( ab2\): \( \text{coprime } (a+b)\ (a-b) \)
proof (rule coprime-imp-coprime)
fix \( h \)
assume \( \text{hab1}\): \( h \ \text{dvd } a+b \ \text{and } \ hab2\): \( h \ \text{dvd } a-b \)
then show \( h \ \text{dvd } 2\ast b \) using \( \text{dvd-diff } \) [of \( h \ a+b \ a-b \)] by fastforce
qed
from \( ab1 \) have \( ab3\): \( \text{coprime } (a-b)\ (2\ast b) \)
proof (rule coprime-imp-coprime)
fix \( h \)
assume \( hab\): \( h \ \text{dvd } a-b \) \( \text{and } \ h2b\): \( h \ \text{dvd } 2\ast b \)
have \( a-b+2\ast b = a+b \) by simp
then show \( h \ \text{dvd } a+b \) using \( \text{hab h2b dvd-add } \) [of \( h \ a-b \ 2\ast b \)] by presburger
qed
then have [simp]: \( \text{even } b \iff \text{odd } a \)
by simp
have \( \exists \ k \ l \ m. \ 2\ast b = k^3 \wedge a+b = l^3 \wedge a-b = m^3 \)
using \( \text{abc } ab1 \ ab2 \ ab3 \)
int-relprime-odd-power-divisors [of \( 3 \ 2 \ast b \ (a+b) \ast (a-b) \ c \)]
int-relprime-odd-power-divisors [of \( 3 \ a+b \ (2\ast b) \ast (a-b) \ c \)]
int-relprime-odd-power-divisors [of \( 3 \ a-b \ (2\ast b) \ast (a+b) \ c \)]
by simp (simp add: ac-simps, simp add: algebra-simps)
then obtain \( \alpha \beta \gamma \) where \( a1: \ 2\ast b = \gamma^3 \wedge a-b = \alpha 1^3 \wedge a+b = \beta^3 \)
by auto
then obtain \( \alpha \) where \( \alpha = -\alpha1 \) by auto
— show this is a (smaller) solution
with \( a1 \) have \( a2\): \( \alpha^3 = b-a \) by auto
with $a1$ have $\alpha^3 + \beta^3 = \gamma^3$ by auto
moreover have $\alpha \beta \gamma \neq 0$
proof (rule econstructor, safe)
assume $\alpha \beta \gamma = 0$
with $a1 \ a2 \ ab$ have $r=0$ by (auto simp add: power-0-left)
with $r \ vwpq \ vwx$ show False by auto
qed
moreover have even $\gamma$
proof –
have even $(2+b)$ by simp
with $a1$ have even $(\gamma^3)$ by simp
thus $\text{thesis}$ by simp
qed
moreover have coprime $\alpha \beta$
using $ab2$ proof (rule coprime-imp-coprime)
fix $h$
assume $ha$: $h \mid \alpha \ \text{and} \ hb$: $h \mid \beta$
then have $h \mid \alpha^2 \ \text{and} \ h \mid \beta^2$ by simp-all
then have $h \mid \alpha^{\text{Suc} \ 2} \ \text{and} \ h \mid \beta^{\text{Suc} \ 2}$ by (auto simp only: power-Suc)
with $a1 \ a2$ have $h \mid b - a \ \text{and} \ h \mid a + b$ by auto
then show $h \mid a + b \ \text{and} \ h \mid a - b$
by (simp-all add: dvd-diff-commute)
qed
moreover have $\text{nat} (\gamma^3) < \text{nat} (x^3)$
proof –
let $?A = p^2 + 3*q^2$
from $vwx \ vwpq$ have $x = 2*p^*?A$ by auto
also with $r$ have $\ldots = 6*r^*?A$ by auto
also with $ab$ have $\ldots = 2*b*(9*(a+b)*(a-b)^*?A)$ by auto
also with $a1$ have $\ldots = \gamma^3 *(9*(a+b)*(a-b)^*?A)$ by auto
finally have eq: $|x^3| = |\gamma^3| * |9*(a+b)*(a-b)^*?A|$ by (auto simp add: abs-mult)
with $\ldots < \text{nat} (x^3)$ have $|9*(a+b)*(a-b)^*?A| > 0$ by auto
hence $|(a+b)^*(a-b)^*?A| \geq 1$ by arith
hence $|9*(a+b)*(a-b)^*?A| > 1$ by arith
moreover have $|\gamma^3| > 0$
proof –
from eq have $|\gamma^3| = 0 \Longrightarrow |x^3| = 0$ by auto
with $\ldots < \text{nat} (x^3)$ show $\text{thesis}$ by auto
qed
ultimately have $|\gamma^3| * 1 < |\gamma^3| * |9*(a+b)*(a-b)^*?A|
by (rule zmult-zless-monot2)
with eq have $|x^3| > |\gamma^3|$ by auto
thus $\text{thesis}$ by arith
qed
ultimately have $\text{thesis}$ by auto
}
3 Fermat's last theorem, case $n = 3$

**Theorem fermat-3:**

**Assumes** `ass: (x::int)^3 + y^3 = z^3`

**Shows** `x*y*z=0`

**Proof (rule ccontr)**

- Let $\mathcal{Q} = \gcd x y$
- Let $c = z \div \mathcal{Q}$
- Assume `xyz0: x*y*z\neq0`
  - Divide out the g.c.d.

**Hence** $x \neq 0 \lor y \neq 0$ by `simp`

**Then obtain** $a b$ where $ab: x = \mathcal{Q}*a \land y = \mathcal{Q}*b \land \text{coprime } a b$

**Using** `gcd-coprime-exists[of x y]` by (auto `simp: mult.commute`)

**Moreover have** `abc: \mathcal{Q}*a^3 + b^3 = \mathcal{Q}*c^3` and `a*b*\mathcal{Q} \neq 0`

**Proof --**

- From `xyz0` have `g0: \mathcal{Q}\neq0` by `simp`
- Have `zgab: z^3 = \mathcal{Q}*a^3 + \mathcal{Q}*b^3` by `simp`
- Hence `\mathcal{Q}` divides `z` by `simp`
- Thus `?thesis` by (simp only: `power-mult-distrib distrib-left`)

**Qed**

**Moreover have** `a^3 + b^3 = \mathcal{Q}*c^3`

**Proof --**

- Have `\mathcal{Q}*c^3 + \mathcal{Q}*g^3 = (a^3 + b^3)*\mathcal{Q}*g^3` by `simp`
- Hence `\mathcal{Q}` divides `z` by `simp`
- Thus `?thesis` by (simp only: `ac-simps dvd-mult-div-cancel`)

**Qed**

**Moreover have** `a^3 + b^3 = \mathcal{Q}*c^3`

**Proof --**

- Have `\mathcal{Q}*c^3 + \mathcal{Q}*g^3 = (a^3 + b^3)*\mathcal{Q}*g^3` by `simp`
- Also with `cQz` have `z = a^3 + b^3` by `simp`
- Also with `zgab` have `\mathcal{Q}*a^3 + \mathcal{Q}*b^3` by `simp`
- Finally show `?thesis` by `simp`

**Qed**

- With `g0` show `?thesis` by `auto`

**Qed**

**Moreover from** $ab$ and $xyz0$ and $cQz$ have $a*b*\mathcal{Q} \neq 0$ by `auto`

**Ultimately show** `?thesis` by `simp`

**Qed**

- Make both sides even

**From** $ab$ have coprime $(a^3, b^3)$

**By** `simp`

- Have $\exists u v w. u^3 + v^3 = w^3 \land u*v*w\neq(0::int) \land \text{even } w \land \text{coprime } u v$

**Proof --**

- Let $\mathcal{Q} u v w = u^3 + v^3 = w^3 \land u*v*w\neq(0::int) \land \text{even } w \land \text{coprime } u v$
- Have even $a \lor$ even $b \lor$ even $\mathcal{Q}$

**Proof (rule ccontr)**

- Assume `~(even a \lor even b \lor even \mathcal{Q})`
- Hence `aOdd: odd a` and `odd b` by `auto`
- Hence even `\mathcal{Q} - b^3` by `simp`

**Moreover from** $abc$ have `\mathcal{Q} - b^3 = a^3` by `simp`

**Ultimately have** even $(a^3)$ by `auto`
Fermat’s last theorem, case $n = 3$

hence even (a) by simp
with aodd show False by simp
qed

moreover

{ assume even (a)
 then obtain $u \cdot v \cdot w$ where $uvwabc$: $u = -b \land v = ?c \land w = a \land$ even w
 by auto
moreover with $abc$ have $u \cdot v \cdot w \neq 0$ by auto
moreover have $uvw$: $u \cdot 3 + v \cdot 3 = w \cdot 3$
proof
 from $uvwabc$ have $u \cdot 3 + v \cdot 3 = (-1 \cdot b) \cdot 3 + ?c \cdot 3$ by simp
also have \ldots $= (-1) \cdot 3 + b \cdot 3 + ?c \cdot 3$ by (simp only; power-mult-distrib)
also have \ldots $= - (b \cdot 3) + ?c \cdot 3$ by auto
also with $abc$ and $uvwabc$ have \ldots $= w \cdot 3$ by auto
finally show \?thesis by simp
qed

moreover have coprime $u \cdot v$

using \langle coprime (a \cdot 3) (b \cdot 3) \rangle; proof (rule coprime-imp-coprime)
fix $h$
assume $hu$: $h \ dvd u$ and $h \ dvd v$
with $uvwabc$ have $h \ dvd ?c \cdot ?c \cdot 2$ by (simp only; dvd-mult2)
with $abc$ have $h \ dvd a \cdot 3 + b \cdot 3$ using power-Suc[of $?c \cdot 2$] by simp
moreover from $hu$ $uvwabc$ have $hb3$: $h \ dvd b \cdot b \cdot 2$ by simp
ultimately have $h \ dvd a \cdot 3 + b \cdot 3 + ?c \cdot 3$
using power-Suc[of $2$] dvd-diff [of $a \cdot 3 + b \cdot 3 + ?c \cdot 3$] by simp
with $hb3$ show $h \ dvd a \cdot 3 + b \cdot 3$ using power-Suc[of $2$] by auto
qed
ultimately have \? $(Q \ u \cdot v \cdot w$ using \langle even a \rangle by simp
hence \?thesis by auto }

moreover

{ assume even $b$
 then obtain $u \cdot v \cdot w$ where $uvwabc$: $u = -a \land v = ?c \land w = b \land$ even w
 by auto
moreover with $abc$ have $u \cdot v \cdot w \neq 0$ by auto
moreover have $uvw$: $u \cdot 3 + v \cdot 3 = w \cdot 3$
proof
 from $uvwabc$ have $u \cdot 3 + v \cdot 3 = (-1 \cdot a) \cdot 3 + ?c \cdot 3$ by simp
also have \ldots $= (-1) \cdot 3 + a \cdot 3 + ?c \cdot 3$ by (simp only; power-mult-distrib)
also have \ldots $= - (a \cdot 3) + ?c \cdot 3$ by auto
also with $abc$ and $uvwabc$ have \ldots $= w \cdot 3$ by auto
finally show \?thesis by simp
qed

moreover have coprime $u \cdot v$

using \langle coprime (a \cdot 3) (b \cdot 3) \rangle; proof (rule coprime-imp-coprime)
fix $h$
assume $hu$: $h \ dvd u$ and $h \ dvd v$
with $uvwabc$ have $h \ dvd ?c \cdot ?c \cdot 2$ by (simp only; dvd-mult2)
with $abc$ have $h \ dvd a \cdot 3 + b \cdot 3$ using power-Suc[of $?c \cdot 2$] by simp
moreover from $hu$ $uvwabc$ have $hb3$: $h \ dvd a \cdot a \cdot 2$ by simp
ultimately have $h \ dvd a \cdot 3 + b \cdot 3 + a \cdot 3$
using power-Suc[of $2$] dvd-diff [of $a \cdot 3 + b \cdot 3 + a \cdot 3$] by simp
with $hb3$ show $h \ dvd a \cdot 3$ and $h \ dvd b \cdot 3$ using power-Suc[of $2$] by auto
qed
ultimately have \( u \cdot v \cdot w \) using \( \text{even } b \) by simp
hence \( \text{thesis} \) by auto }
moreover
{ assume even \(?c\)
then obtain \( u \cdot v \cdot w \) where \( uvwabc: u = a \land v = b \land w = \text{?c } \land \text{even } w \)
by auto
with \( abc \) \( ab \) have \( \text{thesis} \) by auto }
ultimately show \( \text{thesis} \) by auto
qed

corollary fermat-mult3:
assumes \( xyz: (x::\text{int}) ^n + y^n = z^n \) and \( n: 3 \) \( \text{dvd n} \)
shows \( x \cdot y \cdot z = 0 \)
proof −
from \( n \) obtain \( m \) where \( n = m \cdot 3 \) by \( \text{auto simp only: ac-simps dvd-def} \)
with \( xyz \) have \( (x^m)^3 + (y^m)^3 = (z^m)^3 \) by \( \text{simp only: power-mult} \)
hence \( (x^m) \cdot (y^m) \cdot (z^m) = 0 \) by \( \text{rule fermat-3} \)
thus \( \text{thesis} \) by auto
qed

end

end

References


