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

Roelof Oosterhuis
University of Groningen

August 16, 2018

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

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

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

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

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

1 **Pythagorean triples and Fermat’s last theorem, case $n = 4$**  
   1.1 Parametrisation of Pythagorean triples (over $\mathbb{N}$ and $\mathbb{Z}$) . . . . . . . . . 5  
   1.2 Fermat’s last theorem, case $n = 4$ . . . . . . . . . . . . . . . . 10

2 **The quadratic form $x^2 + Ny^2$**  
   2.1 Definitions and auxiliary results . . . . . . . . . . . . . . . . . 15  
   2.2 Basic facts if $N \geq 1$ . . . . . . . . . . . . . . . . . . . . . . . 16  
   2.3 Multiplication and division . . . . . . . . . . . . . . . . . . . . . 17  
   2.4 Uniqueness ($N > 1$) . . . . . . . . . . . . . . . . . . . . . . . . . 28  
   2.5 The case $N = 3$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . 32  
   2.6 Existence ($N = 3$) . . . . . . . . . . . . . . . . . . . . . . . . . . 42

3 **Fermat’s last theorem, case $n = 3$**  

45
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 $abc: (a::nat)\times b = c \wedge n$ 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 $a = 0$ $\vee$ $a = 1$ 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 $p$ $\wedge$ $p \mid a$ using prime-factor-nat[of $a$]
by blast
hence $h1$: $p \mid (c \wedge n)$ using 3 dvd-mult2[of $p a b$]
by presburger
hence $(p^n) \mid (c^n)$
using $p(1)$ prime-dvd-power-nat[of $p c n$]
by blast
moreover have $h2$: $\neg p \mid b$
using $p$ ⟨coprime $a b$⟩ coprime-common-divisor-nat[of $a b p$]
by auto
hence $\neg (p^n) \mid b$ using $n0 p$ (1)
by (auto intro: dvd-trans dvd-power[of $n p$])
ultimately have $(p^n) \mid a$ using 1-prems $p(1)$ prime-elem-divprod-pow[of $p a b n$]
by simp
then obtain $a'$ $c'$ where $ac$: $a = p^n \times a'$ $c = p \times c'$
using $h1$ dvdE[of $p^n a$]
dvdE[of $p c$]
prime-dvd-power-nat[of $p c n$] $p(1)$
by meson
hence $p^n \times (a' \times b) = p^n \times c'^n$ using 3
by (simp add: power-mult-distrib semiring-normalization-rules(18))
hence $a' \times b = c'^n$ using $p(1)$ by auto
moreover have coprime $a' b$ using 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 $p$ ⟨$a \times b = c \wedge n0$ 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 1(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 \( 0 < n \) and \( 0 \leq a \) and \( 0 \leq b \) and \((a::int) * b = c \leq n\) and coprime \( a \) \( b \)
shows \( \exists k. \ a = k^n \)
proof (cases \( a = 0 \))
case False
from \( \langle 0 \leq a \rangle \) \( \langle 0 \leq b \rangle \) \( a * b = c \leq n\) [symmetric] have \( 0 \leq c \leq n \)
  by simp
hence \( c^n = |c| \leq n \) using power-even-abs[of \( n \) \( c \)] zero-le-power-\( [of \ n \ c] \) by linarith
hence \( a * b = |c| \leq n\) using assms(4) by presburger
hence \( nat \ a * nat \ b = \langle nat |c| \rangle \ leq n\) using nat-mul-distib[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 \( \langle 0 \leq a \rangle \) \( \langle \text{coprime } a \ b \rangle \) have \( \text{coprime } (nat \ a) \ (nat \ b) \)
  using coprime-nat-abs-left-iff[of \( a \) \( nat \ b \)] by simp
ultimately have \( \exists k. \ nat \ a = k^n \)
  using int-relprime-power-divisors[of \( n \) \( nat \ a \) \( nat \ b \) \( nat |c| \)] assms(1) by blast
thus ?thesis using assms(2) \( \text{int-nat-eq } [of \ a \ b] \) 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: \( a \leq \langle b :: nat \rangle \) \( \implies \ (a-b)^2 = a^2 + b^2 - 2*a*b \)
proof
  assume a-ge-b: \( a \geq b \)
  hence \( a^2 - b^2 \geq b^2 \) by (simp only: power-mono)
  from a-ge-b have ab-ge-b2: \( a*b \geq b^2 \) by (simp add: power2-eq-square)
  have b*(a-b) + (a-b)^2 = a*(a-b) by (simp add: power2-eq-square diff-mult-distib)
  also have \( \ldots = a*b + a^2 + (b^2 - b^2) - 2*a*b \)
    by (simp add: mult-distib2 power2-eq-square)
  also with \( a-ge-b2 \) have \( \ldots = a*b + (a^2 - b^2) + b^2 - 2*a*b \) by simp
  also have \( \ldots = b*(a-b) + a^2 + b^2 - 2*a*b \) by auto
  also have \( \ldots = b*(a-b) + a^2 + b^2 - 2*a*b \) by simp
    finally show ?thesis by arith
qed

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

private lemma nat-power-inject-base: \[ \langle n \neq 0 \rangle ; \ a \leq b \leq n \ \implies (a::nat) = b \]
proof
  assume n \( \neq 0 \) and ab: \( \text{a} \leq b \leq n \)
  then obtain \( m \) where \( n = \text{Suc} \ m \) by (frule-tac \( n = \text{Suc} \ m \) in \( \text{not0-implies-Suc} \), auto)
  with \( ab \) have \( \text{a} \leq \text{Suc} \ m \) \( = \text{b} \leq \text{Suc} \ m \) and \( a \geq 0 \) and \( b \geq 0 \) by auto
  thus ?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 a22 = 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-mult-distrib2 add-mult-distrib mult.commute)
finally show \?thesis by (simp only: diff-mult-distrib)
qed
have a-nonzero: \( a \neq 0 \)
proof (rule ccontr)
  assume \( a = 0 \) hence \( a = 0 \) by simp
  with aodd have \( \text{odd } (0::nat) \) by simp
  thus 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 False by (simp add: power2-eq-square)
qed
ultimately show \?thesis by auto
qed
hence \( b^2 - c^2 \) 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 \(?g^2 \mid d \) by (simp only: gcd-dvd2)
  hence \(?g \mid d \) by simp
  hence \(?g \mid d \) by (simp only: gcd-greatest)
  with ab-relprime show \?thesis
    by (simp add: ac-simps gcd-eq-1-imp-coprime)
qed
have \( p^2: \text{prime } (2::nat) \) by simp
have factors-odd: \( \text{odd } (c-b) \land \text{odd } (c+b) \)
proof (auto simp only: ccontr)
assume even \((c-b)\)
with \(\mathsf{a2factor}\) have \(2 \div d\ a^2\) by \((\mathsf{simp\ only: dvd-mult})\)
with \(p2\) have \(2 \div d\ a\) by \(\mathsf{auto}\)
with \(a\mathsf{od}\) show \(\mathsf{False}\) by \(\mathsf{simp}\)
next
assume even \((c+b)\)
with \(\mathsf{a2factor}\) have \(2 \div d\ a^2\) by \((\mathsf{simp\ only: dvd-mult})\)
with \(p2\) have \(2 \div d\ a\) by \(\mathsf{auto}\)
with \(\mathsf{add}\) show \(\mathsf{False}\) by \(\mathsf{simp}\)
qed
have \(cb1\): \(c-b + (c+b) = 2*c\)
proof —
have \(c-b + (c+b) = ((c-b)+b)+c\) by \(\mathsf{simp}\)
also with \(b\mathsf{less-c}\) have \(\ldots = (c+b-b)+c\) by \((\mathsf{simp\ only: \ diff-associative})\)
also have \(\ldots = c+c\) by \(\mathsf{simp}\)
finally show \(\mathsf{thesis}\) by \(\mathsf{simp}\)
qed
have \(cb2\): \(2*b + (c-b) = c+b\)
proof —
have \(2*b + (c-b) = b+b + (c-b)\) by \(\mathsf{auto}\)
also have \(\ldots = b+((c-b)+b)\) by \(\mathsf{simp}\)
also with \(b\mathsf{less-c}\) have \(\ldots = b+(c+b-b)\) by \((\mathsf{simp\ only: \ diff-associative})\)
finally show \(\mathsf{thesis}\) by \(\mathsf{simp}\)
qed
have \(\mathsf{factors-relprime: coprime}\ (c-b) (c+b)\)
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 \(\mathsf{simp}\)
also with \(b\mathsf{less-c}\) have \(\ldots = (c+b-b)+c\) by \((\mathsf{simp\ only: \ diff-associative})\)
also have \(\ldots = c+c\) by \(\mathsf{simp}\)
finally show \(\mathsf{thesis}\) by \(\mathsf{simp}\)
qed
have \(?g = \gcd\ (c-b + (c+b)) (c+b)\) by \(\mathsf{simp}\)
with \(cb1\) have \(?g = \gcd\ (2*c) (c+b)\) by \((\mathsf{rule-tac\ a=\ c-b + (c+b)\ in\ back-subst})\)
\(\mathsf{hence\ g2c: ?g \div d\ 2*c}\) by \((\mathsf{simp\ only: gcd-dvd1})\)
\(\mathsf{have\ \gcd\ (c-b) (2*b + (c-b)) = \gcd\ (c-b) (2*b)}\)
using \(\gcd\text{-add2\! of\! c-b 2*b + (c-b)}\) by \((\mathsf{simp\ add: algebra-simps})\)
with \(cb2\) have \(?g = \gcd\ (c-b) (2*b)\) by \((\mathsf{rule-tac\ a=2*b + (c-b)\ in\ back-subst})\)
\(\mathsf{hence\ g2b: ?g \div d\ 2*b}\) by \((\mathsf{simp\ only: gcd-dvd2})\)
with \(g2c\) have \(?g \div d\ 2 * \gcd\ b\ c\) by \((\mathsf{simp\ only: gcd-greatest\ gcd-mult-distrib})\)
with \(\mathsf{bc-relprime}\) have \(?g \div d\ 2\) by \(\mathsf{simp}\)
moreover have \(?g \neq 0\)
using \(b\mathsf{less-c}\) by \(\mathsf{auto}\)
ultimately have \(1 \leq ?g \ ?g \leq 2\)
by \((\mathsf{simp-all\ add: dvd-imp-le})\)
then have \(g1or2: ?g = 2\ \lor \ ?g = 1\)
by \(\mathsf{arith}\)
moreover have \(?g \neq 2\)
proof
assume \(?g = 2\)
moreover have \( \text{?} q \, \text{dvd} \, c - b \)
by simp
ultimately show \( \text{False} \)
using factors-odd by simp
qed
ultimately show \( \text{?thesis} \)
by (auto intro: gcd-eq-1-imp-coprime)

qed
from \( a \, \text{factor} \, \text{have} \, (c-b)*(c+b) = a^2 + (2::nat) > 1 \) by auto
with factors-relprime have \( \exists \, k. \, c-b = k^2 \)
by (simp only: nat-relprime-power-divisors)
then obtain \( r \) where \( r: c-b = r^2 \) by auto
from \( a \, \text{factor} \, \text{have} \, (c+b)*(c-b) = a^2 + (2::nat) > 1 \) by auto
with factors-relprime have \( \exists \, k. \, c+b = k^2 \)
by (simp only: nat-relprime-power-divisors)
then obtain \( s \) where \( s: c+b = s^2 \) by auto
— now \( p := (s+r)/2 \) and \( q := (s-r)/2 \) is our solution
have rs-odd: \( \text{odd} \, r \land \text{odd} \, s \)
proof (auto dest: ccontr)
assume even \( r \) hence \( 2 \, \text{dvd} \, r \) by presburger
with \( r \) have \( 2 \, \text{dvd} \, (c-b) \) by (simp only: power2-eq-square dvd-mult)
with factors-odd show \( \text{False} \) by auto

next
assume even \( s \) hence \( 2 \, \text{dvd} \, s \) by presburger
with \( s \) have \( 2 \, \text{dvd} \, (c+b) \) by (simp only: power2-eq-square dvd-mult)
with factors-odd show \( \text{False} \) by auto

qed
obtain \( m \) where \( m: m = s-r \) by simp
from \( r \, s \) have \( r^2 \leq s^2 \) by arith
with \( \text{two0} \) have \( r \leq s \) by (rule-tac n=2 in nat-power-le-imp-le-base)
with \( m \) have \( m^2: s = r + m \) by simp
have even \( m \)
proof (rule ccontr)
assume odd \( m \) with rs-odd and \( m^2 \) show \( \text{False} \) by presburger

qed
then obtain \( q \) where \( m = 2*q \)
with \( m^2 \) have \( q: s = r + 2*q \) by simp
obtain \( p \) where \( p: p = r+q \) by simp
have \( c: c = p^2 + q^2 \)
proof
from \( cb1 \) and \( r \) and \( s \) have \( 2*c = r^2 + s^2 \) by simp
also with \( q \) have \( \ldots = 2*r^2 + 2*s^2 + 2*r*s*(2*q) \) by algebra
also have \( \ldots = 2*r^2 + 2*s^2 + 2*r*s*r \) by (simp add: power-mult-distrib)
also have \( \ldots = 2*(r^2 + 2*s*r + q^2) + 2*s^2 \) by (simp add: power2-eq-square)
also with \( p \) have \( \ldots = 2*p^2 + 2*s^2 \) by algebra
finally show \( \text{?thesis} \) by auto

qed
moreover have \( b: b = 2*p*q \)
proof
from \( cb2 \) and \( r \) and \( s \) have \( 2*b = s^2 - r^2 \) by arith
also with \( q \) have \( \ldots = (2*q)^2 + 2*r*(2*q) \) by (simp add: power2-sum)
also with \( p \) have \( \ldots = 4*q*p \) by (simp add: power2-eq-square add-mult-distrib2)
finally show \( ?\text{thesis} \) by \( \text{auto} \)
qed

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

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

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

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

private corollary \( \text{int-euclid-pyth-triples}: [ \ \text{coprime} (a::int) \ b; \ odd \ a; \ a^2 + b^2 = c^2 \]
\( \implies \exists \ p \ q. \ a = p^2 - q^2 \ \& \ b = 2*p*q \ \& \ |c| = p^2 + q^2 \ \& \ \text{coprime} \ p \ q \)
proof –
assume \( \text{ab-rel:} \ \text{coprime} \ a \ b \ \& \ \text{add: odd} \ a \ \& \ \text{abc:} \ a^2 + b^2 = c^2 \)
let \( ?a = \text{nat}[a] \)
let \( ?b = \text{nat}[b] \)
let \( ?c = \text{nat}[c] \)
have \( ab^2-\text{pos:} \ a^2 \geq 0 \ \& \ b^2 \geq 0 \) by \( \text{simp} \)
hence \( \text{nat}(a^2) + \text{nat}(b^2) = \text{nat}(a^2 + b^2) \) by \( \text{(simp only: nat-add-distrib)} \)
with \( \text{abc have} \ \text{nat}(a^2) + \text{nat}(b^2) = \text{nat}(c^2) \) by \( \text{presburger} \)
hence \( \text{nat}(a^2) + \text{nat}(b^2) = \text{nat}(c^2) \) by \( \text{simp} \)
hence new-abc: \( ?a^2 + ?b^2 = ?c^2 \)
by \( \text{(simp only: nat-mult-distrib power2-eq-square nat-add-distrib)} \)
moreover from \( \text{ab-rel have} \ \text{new-ab-rel: \ coprime} \ ?a \ ?b \)
by \( \text{(simp add: gcd-int-def)} \)
moreover have \( \text{new-a-odd: odd} \ ?a \ \text{using} \ \text{add} \)
by \( \text{simp} \)
ultimately have \( \exists \ p \ q. \ ?a = p^2 - q^2 \ \& \ ?b = 2*p*q \ \& \ ?c = p^2 + q^2 \ \& \ \text{coprime} \ p \ q \)
by \( \text{(rule-tac a=?a and b = ?b and c=?c in nat-euclid-pyth-triples)} \)
then obtain \( m \) and \( n \) where \( mn: \)
\( ?a = m^2 - n^2 \ \& \ ?b = 2*m*n \ \& \ ?c = m^2 + n^2 \ \& \ \text{coprime} \ m \ n \) by \( \text{auto} \)
have \( n^2 \leq m^2 \)
proof \( \text{(rule ccontr)} \)
1.1 Parametrisation of Pythagorean triples (over $\mathbb{N} \text{ and } \mathbb{Z}$)

assume $n^2 \leq m^2$ hence $n^2 > m^2$ by simp 
with $mn$ have $?a = 0$ by simp 
with new-a-odd show False by simp 
qed

moreover from $mn$ have int $?a = int(m^2 - n^2)$ and int $?b = int(2*m*n)$ 
and int $?c = int(m^2 + n^2)$ by auto

ultimately have $|a| = int(m^2) - int(n^2)$ and $|b| = int(2*m*n)$
and $|c| = int(m^2) + int(n^2)$ by (simp add: of-nat-diff)+
hence $absabc: |a| = (int m)^2 - (int n)^2 \land |b| = 2*(int m)*int n$
\land $|c| = (int m)^2 + (int n)^2$ by (simp add: power2-eq-square)

from $mn$ have $mn-rel$ coprime $(int m)$ $(int n)$ 
by (simp add: gcd-int-def)

show $\exists \ p \ q. \ a = p^2 - q^2 \land b = 2*p*q \land |c| = p^2 + q^2 \land \text{coprime p q}$
(is $\exists \ p \ q. \ ?Q \ p \ q$)

proof (cases)

assume apos: $a \geq 0$ then obtain $p$ where $p = int m$ by simp
hence $\exists \ q. \ ?Q \ p \ q$
proof (cases)

assume bpos: $b \geq 0$ then obtain $q$ where $q = int n$ by simp
with $p$ apos bpos $absabc$ $mn-rel$ have $?Q \ p \ q$ by simp
thus $?thesis$ by (rule exI)

next

assume $b \geq 0$ hence bneg: $b < 0$ by simp
then obtain $q$ where $q = - int n$ by simp
with $p$ apos bneg $absabc$ $mn-rel$ have $?Q \ p \ q$ by simp
thus $?thesis$ by (rule exI)

qed

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

next

assume $a \geq 0$ hence aneg: $a < 0$ by simp
then obtain $p$ where $p = int n$ by simp
hence $\exists \ q. \ ?Q \ p \ q$
proof (cases)

assume bpos: $b \geq 0$ then obtain $q$ where $q = int m$ by simp
with $p$ aneg bpos $absabc$ $mn-rel$ have $?Q \ p \ q$
by (simp add: ac-simps)
thus $?thesis$ by (rule exI)

next

assume $b \geq 0$ hence bneg: $b < 0$ by simp
then obtain $q$ where $q = - int m$ by simp
with $p$ aneg bneg $absabc$ $mn-rel$ 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

$$a^4 + b^4 = c^2 \land \text{coprime } a \land bc \neq 0 \land a \text{ odd.}$$

**Proof** —

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

from `ab-relprime` have $2b^2relprime$: `coprime (a^2) (b^2)`

by `simp`

moreover from `uvabc` have `gcd` $a v dvd gcd (a^2)$ `by` `presaburger`

moreover from `uvabc` have `gcd` $a v dvd (a^2) + (b^2)^2 = c^2` `by` `simp`

ultimately obtain $u$ and $v$ where `uvabc`

$$a^2 = u^2 - v^2 \land b^2 = 2uv + c^2 \land \text{cooprime } u \land v$$

by `(frule_tac a=a^2 in int-euclid-pyth-triples, auto)`

with `abc0` have `u0`: $u \neq 0 \land v \neq 0` `by` `auto`

have `abrelprime`: `coprime a v`

proof —

have `gcd a v dvd gcd (a^2)` `by` `(simp add: power2-eq-square)`

moreover from `uvabc` have `gcd` $v dvd (a^2 u dvd gcd (b^2) (a^2)`

by `simp`

with `2b2relprime` have `gcd` $a v dvd (1::int)`

by `(simp add: ac-simps)`

ultimately have `gcd` $a v dvd 1` `by` `(rule dvd-trans)`

then show `thesis`

by `(simp add: gcd-eq-1-imp-coprime)`

qed

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

from `uvabc` have `a^2 + v^2 = u^2` `by` `simp`

with `as-relprime` and `aodd` obtain $k$ and $l$ where

`klau`: $a = k^2 - l^2 \land v = 2kl \land |a| = k^2 + l^2` `and` `kl-rel`: `coprime k l`

by `(frule_tac a=a in int-euclid-pyth-triples, auto)`

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

for `coprime k`, $l$ and $k^2 + l^2$

from `uvabc` have `even (b^2)` `by` `simp`

hence even $b$ `by` `simp`

then obtain $m$ where `bm`: $b = 2m` using `evenE` `by` `blast`

have `|k|*|l|*|k^2+l^2| = m^2` `by` `(simp only: power2-eq-square ac-simps)`

also have `... = |b^2|` `by` `simp`

also with `uvabc` have `... = 2v|v||u|` `by` `(simp add: abs-mult)`

also with `klau` have `... = 2|k^2+l^2|` `by` `simp`

also have `... = 4|k|*|l|*|k^2+l^2|` `by` `(auto simp add: abs-mult)`

finally show `thesis` `by` `simp`

qed

moreover have `(2::nat) > 1` `by` `auto`
moreover from \( kl-rel \) have coprime \(|k| |l| \) by simp
moreover have coprime \(|l| \) \((|k|^2+1^2)\)

proof –
from \( kl-rel \) have coprime \( (k \cdot k) l \)
by simp
hence coprime \( (k \cdot k+l \cdot l) l \) using gcd-add-mult \([of \ l \ \ l \ \ k \cdot k]\)
by (simp add: ac-simps gcd-eq-1-imp-coprime)
hence coprime \( l (k^2+1^2) \)
by (simp add: power2-eq-square ac-simps)
thus \( \neg \)thesis by simp

qed
moreover have coprime \(|k^2+1^2| \) \(|k| \)
proof –
from \( kl-rel \) have coprime \( l k \)
by (simp add: ac-simps)
hence coprime \( l \cdot l \) \(k \cdot k\)
by simp
hence coprime \( l \cdot l+k \cdot k \) \(k \cdot k\)
using gcd-add-mult \([of \ k \ \ k \ \ l \ \ l]\)
by (simp add: ac-simps gcd-eq-1-imp-coprime)
hence coprime \( k \cdot k+1 \cdot 1 \) \(k \)
by (simp add: power2-eq-square ac-simps)
thus \( \neg \)thesis by simp

qed
ultimately have \( \exists x y z. [|k| = x^2 \land |l| = y^2 \land |k^2+1^2| = z^2 \)
using int-relprime-power-divisors\([of \ 2 \ |k| \ |l| \ * \ |k^2+1^2| \ m]\)
int-relprime-power-divisors\([of \ 2 \ |k| \ |k^2+1^2| \ m]\)
int-relprime-power-divisors\([of \ 2 \ |l| \ * \ |k^2+1^2| \ m]\)
by (simp-all add: ac-simps)
then obtain \( \alpha \ \beta \ \gamma \) where \( \text{albega:} \)
\(|k| = \alpha^2 \land |l| = \beta^2 \land |k^2+1^2| = \gamma^2 \)
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 \( \neg \)thesis by simp

qed
moreover have \( l^2 = \beta^4 \)
proof –
from \( \text{albega} \) have \(|l|^2 = (\beta^2)^2 \) by simp
thus \( \neg \)thesis by simp

qed
moreover have \( \gamma^2: k^2 + l^2 = \gamma^2 \)
proof –
have \( k^2 \geq 0 \land l^2 \geq 0 \) by simp
with \( \text{albega} \) show \( \neg \)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 \( \alpha \ \beta \ \text{relprime-coprime: coprime} \ \alpha \ \beta \)
proof (rule classical)
let \( \gamma = \gcd \alpha \beta \)
assume \( \neg \text{coprime } \alpha \beta \)
than have \( \text{gnot1}: \gamma \neq 1 \)
by (auto intro: gcd-eq-1-imp-coprime)
have \( \gamma > 1 \)
proof –
  have \( \gamma \neq 0 \)
  proof
    assume \( \gamma = 0 \)
    hence \( \text{nat } |\alpha|=0 \) by simp
    hence \( \alpha=0 \) by arith
    with \( \alpha \beta a 0 \) show \( \text{False} \) by simp
  qed
  hence \( \gamma > 0 \) by auto
  with \( \text{gnot1} \) show \( \text{thesis} \) by linarith
qed
moreover have \( \gamma \mid \gcd k l \)
proof –
  have \( \gamma \mid \alpha \land \gamma \mid \beta \) by auto
  with \( \alpha \beta a \) have \( \gamma \mid |k| \land \gamma \mid |l| \)
  by (simp add: power2-eq-square mult.commute)
  hence \( \gamma \mid k \land \gamma \mid l \) by simp
  thus \( \text{thesis} \) by simp
qed
ultimately have \( \gcd k l \neq 1 \) by fastforce
with \( k l \text{-rel} \) show \( \text{thesis} \) by auto
qed
— choose \( p \) and \( q \) in the right way
have \( \exists p q. p \cdot 4 + q \cdot 4 = \gamma \cdot 2 \land p \cdot q \cdot \gamma \neq 0 \land \text{odd } p \land \text{coprime } p q \)
proof –
  have \( \text{odd } \alpha \lor \text{odd } \beta \)
  proof (rule ccontr)
    assume \( \neg (\text{odd } \alpha \lor \text{odd } \beta) \)
    hence \( \text{even } \alpha \land \text{even } \beta \) by simp
    then have \( 2 \mid \alpha \land 2 \mid \beta \) by simp
    then have \( 2 \mid \gcd \alpha \land 2 \mid \beta \) by simp
    with \( \alpha \beta \text{-relprime} \) show \( \text{False} \) by auto
  qed
moreover
  \{ assume \( \text{odd } \alpha \)
  with \( \text{newabc } \alpha \beta a 0 \) \( \alpha \beta \text{-relprime} \) obtain \( p q \) where
    \( p=\alpha \land q=\beta \land p \cdot 4 + q \cdot 4 = \gamma \cdot 2 \land p \cdot q \cdot \gamma \neq 0 \land \text{odd } p \land \text{coprime } p q \)
  by auto
  hence \( \text{thesis} \) by auto \}
moreover
  \{ assume \( \text{odd } \beta \)
  with \( \text{newabc } \alpha \beta a 0 \) \( \alpha \beta \text{-relprime} \) obtain \( p q \) where
    \( q=\alpha \land p=\beta \land p \cdot 4 + q \cdot 4 = \gamma \cdot 2 \land p \cdot q \cdot \gamma \neq 0 \land \text{odd } p \land \text{coprime } p q \)
  by (auto simp add: ac-simps)
  hence \( \text{thesis} \) by auto \}
ultimately show \( \text{thesis} \) by auto
qed
— show the solution is smaller

moreover have $\gamma^2 < c^2$

proof —
from gamma2 klavu have $\gamma^2 \leq |u|$ 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 v2non0: $0 \neq v^2$

by simp
also have h1: $\ldots \leq |u|$ by simp
also have h2: $\ldots \leq |c|^2$ using self-le-power[of $|c|$ 2] h1 h2 h3 uvabc by linarith
finally show $?thesis$ by simp
qed
ultimately show $?thesis$ by auto
qed

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

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

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

case (0 x)

have $x^2 \geq 0$ by (rule zero-le-power2)
with v2non0 have $0 < v^2$ by (auto simp add: less-le)
thus $?thesis$ by auto
qed

also with uvabc have $\ldots \leq |c|$ by auto
also have $\ldots \leq |c|^2$ using self-le-power[of $|c|$ 2] h1 h2 h3 uvabc by linarith
also have $\ldots \leq c^2$ by simp

The theorem. Puts equation in requested shape.

private lemma no_rewritten_fermat4:
$\neg \exists (a::int) b. (a^4 + b^4 = c^2 \land a*b*c \neq 0 \land odd a \land coprime a b)$

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

case (0 x)

have $x^2 \geq 0$ by (rule zero-le-power2)
with v2non0 have $0 < v^2$ by (auto simp add: less-le)
thus $?thesis$ by auto
qed

ultimately show $?thesis$ by auto
qed

1.2 Fermat’s last theorem, case $n = 4$
let \( ?c = (z \div ?g)^2 \)
assume \( xyz0 \): \( x \times y \times z \neq 0 \)
— divide out the g.c.d.
hence \( x \neq 0 \lor y \neq 0 \) by simp
then obtain \( a \ b \) where \( ab \): \( x = ?g \times a \land y = ?g \times b \land \text{coprime } a \ b \)
using gcd-coprime-exists[of \( x \ y \)] by (auto simp: mult.commute)
moreover have \( abc \): \( a^4 + b^4 = ?c^2 \land a \times b \times ?c \neq 0 \)
proof —
  have \( zgab \): \( z^4 = ?g^4 \times (a^4+b^4) \)
  proof —
  from \( ab \) have \( z^4 = (?g \times a)^4+(?g \times b)^4 \) by simp
  thus \( ?thesis \) by (simp only: power-mult-distrib distrib-left)
  qed
have \( cgz \): \( z^2 = ?c \times ?g^2 \)
proof —
from \( zgab \) have \( ?g^4 \text{ dvd } z^4 \) by simp
hence \( ?g \text{ dvd } z \) by simp
hence \( z \div ?g \times ?g = z \) 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 \( g0 \): \( ?g \neq 0 \) by simp
have \( a^4 + b^4 = ?c^2 \)
proof —
  have \( ?c^2 \times ?g^4 = (a^4+b^4) \times ?g^4 \)
  proof —
  have \( ?c^2 \times ?g^4 = (?c \times ?g^2)^2 \) by algebra
   also with \( cgz \) have \( \ldots = (z^2)^2 \) by simp
   also have \( \ldots = z^4 \) by algebra
   also with \( zgab \) have \( \ldots = ?g^4 \times (a^4+b^4) \) by simp
   finally show \( ?thesis \) by simp
  qed
with \( g0 \) show \( ?thesis \) by auto
qed
moreover from \( ab \) \( xyz0 \) \( c0 \) have \( a \times b \times ?c \neq 0 \) by auto
ultimately show \( ?thesis \) by simp
qed
— choose the parity right
have \( \exists \ p \ q \ p^4 + q^4 = ?c^2 \land p \times q \times ?c \neq 0 \land \text{odd } p \land \text{coprime } p \ q \)
proof —
  have \( \text{odd } a \lor \text{odd } b \)
  proof (rule contr)
    assume \( \neg(\text{odd } a \lor \text{odd } b) \)
    hence \( 2 \text{ dvd } a \land 2 \text{ dvd } b \) by simp
    hence \( 2 \text{ dvd } \text{gcd } a \ b \) by simp
    with \( ab \) show False by auto
  qed
moreover
  \{ assume \( \text{odd } a \)
      then obtain \( p \ q \) where \( p = a \) and \( q = b \) and \( \text{odd } p \) by simp
      with \( ab \) \( abc \) have \( ?thesis \) by auto \}
moreover
The quadratic form \( x^2 + Ny^2 \)

2. The quadratic form \( x^2 + Ny^2 \)

theory Quad-Form

imports

\texttt{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 \( \exists \cdot \)thesis

proof (cases \( 2 \cdot (a \mod n) \leq n \))

case True

end

end
hence \(2 \times |a - k \times n| \leq n\) using \(h\) pos-mod-sign \(a\) by \(auto\)
thus \(?thesis\) by \(blast\)

next
case \(False\)
hence \(2 \times (n - a \mod n) \leq n\) by \(auto\)
have \(a - (k+1) \times n = a \mod n - n\) using \(h\) by \((simp \ add: \ algebra-simps)\)
hence \(2 \times |a - (k+1) \times n| \leq n\) using \(h\) pos-mod-bound[\(of\ n\ a\)] \(a\) \(False\) by \(fastforce\)
thus \(?thesis\) by \(blast\)
qed

lemma prime-power-dvd-cancel-right:
\[
p ^ \cdot n \ d v d \ a \ i f \ \text{prime} (p;:'a::semiring-gcd) \ \\
\n\n\nproof –
\from that have coprime \(p\ b\)
by \((auto \ intro: \ prime-imp-coprime)\)
with that show \(?thesis\)
by \((simp \ add: \ coprime-dvd-mult-left-iff)\)
qed

definition
is-qfN :: \(int \Rightarrow \ int \Rightarrow \ bool\) where
\[
is-qfN \ A \ N \leftarrow (\exists \ x \ y. \ A = \ x ^ \cdot 2 + N \times y ^ \cdot 2)
\]
definition
is-cube-form :: \(int \Rightarrow \ int \Rightarrow \ bool\) where
\[
is-cube-form \ a \ b \leftarrow (\exists \ p \ q. \ a = \ p ^ \cdot 3 - 9 \times p \times q ^ \cdot 2 \ \\
\wedge \ b = 3 \times p ^ \cdot 2 \times q - 3 \times q ^ \cdot 3)
\]

private lemma abs-eq-impl-unitfactor: |\(a::int| = |b| \implies \ \exists \ u. \ a = u \times b \wedge |u|=1
proof –
assume |\(a| = |b|

hence \(a = 1 \times b \vee a = (-1) \times b\) by \(arith\)
then obtain \(u\) where \(a = u \times b \wedge (u=1 \vee u=\neg 1)\) by \(blast\)
thus \(?thesis\) by \(auto\)
qed

private lemma prime-3-nat: \(prime (3::nat)\) by \(auto\)

2.2 Basic facts if \(N \geq 1\)

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

\[ a \cdot b \geq a^2 \geq 0 \]

by auto

moreover have \( a^2 \geq 0 \)

by (rule zero-le-power2)

ultimately show \(?\)thesis by arith

qed

\textbf{lemma} qfN-zero: \[ (N::int) \geq 1; a^2 + N \cdot b^2 = 0 \] \implies (a = 0 \land b = 0)

\textbf{proof} –

assume \( N: N \geq 1 \) and \( ab: a^2 + N \cdot b^2 = 0 \)

show \(?\)thesis

proof (rule ccontr, auto)

assume \( a \neq 0 \)

hence \( a^2 > 0 \)

by simp

moreover have \( N \cdot b^2 \geq 0 \)

proof (cases)

assume \( b = 0 \)

thus \(?\)thesis 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)

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)

hence \( N \cdot b^2 > 0 \)

by simp

moreover 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

qed

2.3 Multiplication and division

\textbf{lemma} qfN-mult1: \[ ((\cdot::int)^2 + N \cdot b^2) \cdot (c^2 + N \cdot d^2) = (a \cdot c + N \cdot b \cdot d) \cdot 2 + N \cdot (a \cdot d - b \cdot c)^2 \]

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

\textbf{lemma} qfN-mult2: \[ ((\cdot::int)^2 + N \cdot b^2) \cdot (c^2 + N \cdot d^2) = (a \cdot c - N \cdot b \cdot d) \cdot 2 + N \cdot (a \cdot d + b \cdot c)^2 \]

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

\textbf{corollary} is-qfN-mult: is-qfN \( A \cdot N \) \implies is-qfN \( B \cdot N \) \implies is-qfN \( (A \cdot B) \cdot N \)

by (unfold is-qfN_def, auto, auto simp only: qfN-mult1)

\textbf{corollary} is-qfN-power: \( (\cdot::nat)^0 \) \implies is-qfN \( A \cdot N \) \implies is-qfN \( (A \cdot n) \cdot N \)

by (induct n, auto, case-tac n=0, auto simp add: is-qfN-mult)

\textbf{lemma} qfN-div-prime:

fixes \( p :: \cdot \cdot \cdot \cdot \cdot \)


assumes \(\exists u. v. a \cdot 2 + N \cdot q \cdot 2\) and \((p \cdot 2 + N \cdot q \cdot 2) \text{ dvd } (a \cdot 2 + N \cdot b \cdot 2)\)

shows \(\exists v. e \cdot 2 + N \cdot v \cdot 2 = (u \cdot 2 + N \cdot v \cdot 2) \times (p \cdot 2 + N \cdot q \cdot 2)\)

\(\wedge (\exists e. a = p \cdot u + e \cdot N \cdot q \cdot v \wedge b = p \cdot v - e \cdot q \cdot u \wedge |e| = 1)\)

proof –

let \(?P = p \cdot 2 + N \cdot q \cdot 2\)

let \(?A = a \cdot 2 + N \cdot b \cdot 2\)

from \(\exists u. v. a \cdot 2 + N \cdot q \cdot 2\) obtain \(U\) where \(U: ?A = ?P \cdot U\) by (auto simp only: dvd-def)

have \(\exists e. ?P \text{ dvd } b \cdot p + e \cdot a \cdot q \wedge |e| = 1\)

proof –

have \(?P \text{ dvd } (b \cdot p + a \cdot q) \cdot (b \cdot p - a \cdot q)\)

proof –

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

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

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

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

qed

with \(\exists e. ?P \text{ dvd } (b \cdot p + a \cdot q) \lor ?P \text{ dvd } (b \cdot p - a \cdot q)\)

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

moreover

\{ assume \(?P \text{ dvd } b \cdot p + a \cdot q\)

hence \(?P \text{ dvd } b \cdot p + 1 \cdot a \cdot q \wedge |1| = (1::int)\) by simp \}

moreover

\{ assume \(?P \text{ dvd } b \cdot p - a \cdot q\)

hence \(?P \text{ dvd } b \cdot p + (-1) \cdot a \cdot q \wedge |-1| = (1::int)\) by simp \}

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

qed

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

by (auto simp only: dvd-def)

have \(?P \text{ dvd } a \cdot p - e \cdot N \cdot b \cdot q\)

proof (cases)

assume \(e1: e = 1\)

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

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

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

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

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

finally have \((a \cdot p - e \cdot N \cdot b \cdot q) \cdot 2 + ?P \cdot 2 \cdot (U - N \cdot v \cdot 2)\)

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

hence \(?P \cdot 2 \text{ dvd } (a \cdot p - e \cdot N \cdot b \cdot q) \cdot 2\) by (rule dvdI)

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

next

assume \(\neg e = 1\) with \(e\) have \(e1: e = -1\) by auto

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

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

by (simp add: qfN-mult1)

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

by (simp only: power2-minus)

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

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

finally have \((a \cdot p - e \cdot N \cdot b \cdot q) \cdot 2 + ?P \cdot 2 \cdot (U - N \cdot v \cdot 2)\)

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

hence \(?P \cdot 2 \text{ dvd } (a \cdot p - e \cdot N \cdot b \cdot q) \cdot 2\) by (rule dvdI)
thus \( \text{thesis by simp} \)

\text{qed}

then obtain \( u \) where \( u \colon a \ast p - e \ast N \ast b \ast q = \text{?P} \ast u \) by (auto simp only: dvd-def)

from \( e \) have e2-1: \( e \ast e = 1 \)

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

have \( a = p \ast u + e \ast N \ast q \ast v \)

\text{proof –}

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

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

also with \( v \ u \) have \( \ldots = p \ast (a \ast p - e \ast N \ast b \ast q) + (e \ast N \ast q) \ast (b \ast p + e \ast a \ast q) \)

by simp

also have \( \ldots = a \ast (p \ast 2 + e \ast e \ast N \ast q \ast 2) \)

by (simp add: power2-cq-square distrib-left ac-simps right-diff-distrib)

also with e2-1 have \( \ldots = a \ast ?P \) by simp

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

moreover from \( \text{ass} \) have \( ?P \neq 0 \) by auto

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

\text{qed}

moreover have \( b = p \ast v - e \ast q \ast u \)

\text{proof –}

have \((p \ast v - e \ast q \ast u) \ast ?P = p \ast (?P \ast v) - (e \ast q) \ast (?P \ast u)\)

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

also with \( v \ u \) have \( \ldots = p \ast (b \ast p + e \ast a \ast q) - e \ast q \ast (a \ast p - e \ast N \ast b \ast q) \) by simp

also have \( \ldots = b \ast (p \ast 2 + e \ast e \ast N \ast q \ast 2) \)

by (simp add: power2-cq-square distrib-left ac-simps right-diff-distrib)

also with e2-1 have \( \ldots = b \ast ?P \) by simp

finally have \((b - (p \ast v - e \ast q \ast u)) \ast ?P = 0 \) by auto

moreover from \( \text{ass} \) have \( ?P \neq 0 \) by auto

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

\text{qed}

moreover have \( ?A = (a \ast 2 + N \ast v \ast 2) \ast ?P \)

\text{proof (cases)}

assume \( e = 1 \)

with \( a \) and \( b \) 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 \( b \) show \( \text{thesis by (simp add: qfN-mult2 ac-simps)} \)

\text{qed}

moreover from \( e \) have \( |e| = 1 \).

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

\text{qed}

corollary qfN-div-prime-weak:

\[ \begin{aligned}
\text{prime} \ (p \ast 2 + N \ast q \ast 2) :: \text{int};
(p \ast 2 + N \ast q \ast 2) \ \text{dvd} \ (a \ast 2 + N \ast b \ast 2)
\implies \exists \ u \ v. \ a \ast 2 + N \ast b \ast 2 = (u \ast 2 + N \ast \upsilon \ast 2) \ast (p \ast 2 + N \ast q \ast 2)
\end{aligned} \]

apply (subgoal_tac \( \exists \ u \ v. \ a \ast 2 + N \ast b \ast 2 = (u \ast 2 + N \ast v \ast 2) \ast (p \ast 2 + N \ast q \ast 2) \)

\land \ (\exists \ e. \ a = p \ast u + e \ast N \ast q \ast v \ \land \ b = p \ast v - e \ast q \ast u \ \land \ |e| = 1), \ bleach) \]

apply (rule qfN-dive-prime, auto)

done

corollary qfN-div-prime-general: \[ \begin{aligned}
\text{prime} \ P; \ P \ \text{dvd} \ A; \ \text{is-qfN} \ A \ N; \ \text{is-qfN} \ P \ N
\implies \exists \ Q. \ A = Q \ast P \ \land \ \text{is-qfN} \ Q \ N
\end{aligned} \]
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 \( P \) \&\& dvd \( A \) \&\& \( P^n = p^2 + N*q^2 \)
  \( A^n = a^2 + N*b^2 \) \&\& coprime \( a \& b \) \&\& coprime \( P \& N*q \) \&\& \( n \geq 0 \)
  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 \( A \& n \geq 0 \) by simp
  hence \( P^n \) dvd \( A^n \) by simp
  then obtain \( U \) where \( U^n = U*P^n \) 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 \( P^n \) 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 \( \ldots = b^2 + p^2 + b^2 + N*q^2 - b^2 + N*q^2 - a^2 + q^2 \)
          by (simp add: power-mult-distrib)
        also with \( ass \) have \( \ldots = b^2 + P^n - q^2 + A^n \)
          by (simp only: ac-simps distrib-right distrib-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 \( P \) 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 \( (b*p + a*q) + (b*p - a*q) \&\& P \) 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)
            using \( prime-dvd-multD \) by blast
            hence \( P \) dvd \( 2 \) \&\& \( P \) dvd \( b*p \& P \) dvd \( a*q \) by auto
            moreover have \( \neg P \) dvd \( 2 \)
              proof (rule ccontr, simp)
                assume \( pdvd2: P \) dvd \( 2 \)
                have \( P \leq 2 \)
2.3 Multiplication and division

proof (rule ccontr)
  assume ¬ P ≤ 2 hence P≠2: P > 2 by simp
  moreover from ass have P > 1 by (simp add: prime-int-iff)
  ultimately have P≠2 by auto
  qed

moreover have ¬ P dvd p ∧ δ P dvd a*q by auto
proof (auto dest: ccontr)
  assume Pdvdp: P dvd p
  hence P dvd pˆ2 by (simp only: dvd-mul power2_eq_square)
  with PdvdPn have P dvd p δ P dvd P·N=q by (simp add: power2_eq_square)
  with P dvd p by blast
moreover
  { assume P dvd (q+q)
    hence P dvd q using prime-dvd-multD ass by blast
  }
ultimately have P dvd N·q by fastforce
with PdvdP have P dvd gcd p · (N·q) by simp
with P dvd N·q by auto
with P dvd gcd p · (N·q) by auto
with P dvd gcd p · (N·q) by auto
with P dvd gcd p · (N·q) by auto
with P dvd gcd p · (N·q) by auto
with P dvd gcd p · (N·q) by auto
with P dvd gcd p · (N·q) by auto
qed
ultimately have P dvd a ∧ P dvd b by auto
with P dvd a by simp
with P dvd b by simp
with P dvd a by simp
with P dvd b by simp
ultimately have ?thesis by auto
The quadratic form $x^2 + Ny^2$

**proof** (cases)

**assume** $e = 1$

from $U$ have $(P^\circ n)^2 \cdot U = A^\circ n \cdot P^\circ n$ by (simp add: power2-eq-square ac-simps)

also with $e$ have ... = $(a*p - e*N*b*q)^2 + N*(b*p + e*a*q)^2$

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

also with $v$ have ... = $(a*p - e*N*b*q)^2 + (P^\circ n)^2 * (N*v)^2$

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

**finally** have $(a*p - e*N*b*q)^2 = (P^\circ n)^2 * U - (P^\circ n)^2 * N*v^2$ by simp

also have ... = $(P^\circ n)^2 * (U - N*v^2)$ by (simp only: right-diff-distrib)

**finally** have $(P^\circ n)^2 dvd (a*p - e*N*b*q)^2$ by (rule dvdI)

thus $\theta$ by simp

**next**

**assume** $e = -1$ with $e$ have $e1$: $e = -1$ by auto

from $U$ have $(P^\circ n)^2 * U = A^\circ n * P^\circ n$ 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 ... = $(a*p - e*N*b*q)^2 + N*(b*p + e*a*q)^2$

by (simp only: power2-minus)

also with $v$ and $ass$ have ... = $(a*p - e*N*b*q)^2 + N*v^2 * (P^\circ n)^2$

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

**finally** have $(a*p - e*N*b*q)^2 = (P^\circ n)^2 * U - (P^\circ n)^2 * N*v^2$ by simp

also have ... = $(P^\circ n)^2 * (U - N*v^2)$ by (simp only: right-diff-distrib)

**finally** have $(P^\circ n)^2 dvd (a*p - e*N*b*q)^2$ by (rule dvdI)

thus $\theta$ by simp

**qed**

then obtain $v$ where $v$: $b*p + e*a*q = P^\circ n*v$ and $e$: $|e| = 1$

by (auto simp only: dvd-def)

**have** $P^\circ n dvd a*p - e*N*b*q$

**proof**

**assume** $P^\circ n dvd b*p + a*q$

**hence** $P^\circ n dvd b*p + 1*a*q$ and $|I| = (1::int)$ by simp

**moreover**

**assume** $P^\circ n dvd b*p - a*q$

**hence** $P^\circ n dvd b*p + (-1)*a*q$ and $|-I| = (1::int)$ by simp

ultimately show $\theta$ by blast

**qed**
ultimately show \(?thesis\) by auto

qed

moreover have \(b: b = p \cdot v - e \cdot q \cdot u\)

proof

from ass have \((p \cdot v - e \cdot q \cdot u) \cdot P \cdot n = p \cdot (P \cdot n \cdot v) - (e \cdot q) \cdot (P \cdot n \cdot u)\)

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

also with \(v \cdot u\) have \(\ldots = p \cdot (b \cdot p + e \cdot a \cdot q) - e \cdot q \cdot (a \cdot p - e \cdot N \cdot b \cdot q)\) by simp

also have \(\ldots = b \cdot (p \cdot 2 + e \cdot e \cdot N \cdot q \cdot 2)\)

by (simp add: power2-eq-square distrib-left ac-simps right-diff-distrib)

also with \(e^2 - 1\) and ass have \(\ldots = b \cdot P \cdot n\) by simp

finally have \((b - (p \cdot v - e \cdot q \cdot u)) \cdot P \cdot n = 0\) by auto

moreover from ass have \(P \cdot n \neq 0\)

by (unfold prime-int-iff, auto)

ultimately show \(?thesis\) by auto

qed

moreover have \(A \cdot n = (u \cdot 2 + N \cdot v \cdot 2) \cdot P \cdot n\)

proof (cases)

assume \(e = 1\)

with \(a\) and \(b\) and ass show \(?thesis\) 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 \(?thesis\) 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 \(w \cdot \text{dvd} u\) \(\text{w dvd v}\)

then have \(w \cdot \text{dvd} u \cdot p + v \cdot (e \cdot N \cdot q) \wedge w \cdot \text{dvd} v \cdot p - u \cdot (e \cdot q)\)

by simp

with \(a\) \(b\) show \(w \cdot \text{dvd} a\) \(\text{w dvd b}\)

by (auto simp only: ac-simps)

qed

moreover from \(e\) and ass have \(|e| = 1 \wedge A \cdot n = a \cdot 2 + N \cdot b \cdot 2 \wedge P \cdot n = p \cdot 2 + N \cdot q \cdot 2\) by simp

ultimately show \(?thesis\) by auto

qed

lemma \text{qfN-primedivisor-not}:

assumes \(\text{ass: } \text{prime } P \wedge Q > 0 \wedge \text{is-qfN } (P \cdot Q)\) \(N \wedge \neg \text{is-qfN } P\) \(N\)

shows \(\exists R.\) \((\text{prime } R \wedge R \cdot \text{dvd} Q \wedge \neg \text{is-qfN } R\) \(N\)

proof (rule contr, auto)

assume \(\text{ass2: } \forall R.\) \(R \cdot \text{dvd} Q \longrightarrow \text{prime } R \longrightarrow \text{is-qfN } R\) \(N\)

define \(ps\) where \(ps = \text{prime-factorization } (\text{nat } Q)\)

from ass have \(ps: (\forall p \in \text{set-mset } ps\cdot \text{prime } p) \wedge Q = \text{int } (\prod i \in \# ps.\ i)\)

by (auto simp: ps-def prod-mset-prime-factorization-int)

have \(\text{ps-lemma: } (\forall p \in \text{set-mset } ps\cdot \text{prime } p) \wedge \text{is-qfN } (P \cdot \text{int}(\prod i \in \# ps.\ i))\) \(N\)

\(\wedge (\forall R.\) \((\text{prime } R \wedge R \cdot \text{dvd} \text{int}(\prod i \in \# ps.\ i)) \longrightarrow \text{is-qfN } R\) \(N\)\)

\(\Longrightarrow False\)

(is \(?B\) \(ps \Longrightarrow False\))

proof (induct \(ps\))

case empty hence \(\text{is-qfN } P\) \(N\) by simp

with ass show False by simp
next
case (add p ps)
  hence ass3: ?B ps \implies False
  and IH: ?B \( ps + \{\#p\}\) by simp-all
  hence p: prime (int p) and int p dvd int(\[ i \in \#ps + \{\#p\} \]. i) by auto
moreover with IH have pgfN: is-qfN (int p) \[ N \]
  and int p dvd P*int(\[ i \in \#ps + \{\#p\} \]. i) by simp
  and is-qfN (P*int(\[ i \in \#ps + \{\#p\} \]. i)) \[ N \]
by auto
ultimately obtain S where S: P*int(\[ i \in \#ps + \{\#p\} \]. i) = S*(int p) \land is-qfN
S \[ N \]
using qfN-div-prime-general by blast
hence \((int p)+(P* int(\[ i \in \#ps \]. i) - S) = 0\) by auto
with p S have is-qfN (P*int(\[ i \in \#ps \]. i)) \[ N \]
  by (auto simp add: prime-int-iff)
moreover from IH have \( \forall p \in \text{set-mset ps. prime p} \)
  by simp
moreover from IH have \( \forall R. \text{prime R \land R dvd int(\[ i \in \#ps \]. i) \implies is-qfN } R \[ N \]
by auto
ultimately have ?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:
  \[
  \text{prime } (p^2+N*q^2::int); \text{ odd } (p^2+N*q^2); p \neq 0; N \geq 1 \\
  \implies \exists a b. (p^2+N*q^2)^3 = a^2 + N*b^2 \land \text{coprime } a (N*b)
  \]
proof --
  let \( ?P = p^2+N*q^2 \)
  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 \( ?a = p*(p^2 - 3*N*q^2) \)
  let \( ?b = q*(3*p^2 - N*q^2) \)
  have abP: ?P^3 = ?a^2 + N*?b^2 by (simp add: eval-nat-numeral field-simps)
  have ?P dvd p if h1: gcd ?p \( ?a \neq 1 \)
proof

let \( h = \gcd b a \)

have \( h \geq 0 \) by simp

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

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

moreover

\{ assume \( h = 0 \)

hence \( a = 0 \land b = 0 \)

by auto

with \( a b P \)

have \( P \cdot 3 = 0 \)

by auto

with \( P \)

have False by (unfold prime-int-iff, auto)

hence \( \neg \text{thesis by simp} \)

moreover

\{ assume \( h > 1 \)

then have \( \exists g. \prime g \land g \mid h \)

using prime-factor-int [of \( h \)] by auto

then obtain \( g \) where \( g \): \( \prime g \) \( g \mid h \)

by blast

then have \( g \mid a \land g \mid b \) by simp

with \( g \) have \( g 1: g \mid q \lor g \mid 3 \cdot p^2 - N \cdot q^2 \)

and \( g 2: g \mid p \lor g \mid 3 \cdot p^2 - 3 \cdot N \cdot q^2 \)

by (auto dest: prime-dvd-multD)

from \( g \) have \( gpos: g \geq 0 \) by (auto simp only: prime-int-iff)

have \( g \mid P \)

proof (cases)

assume \( g \mid p \)

hence \( gNq: g \mid N \cdot q^2 \) by (auto simp add: dvd-def power2-eq-square)

show \( \neg \text{thesis} \)

proof (cases)

assume \( gp: g \mid p \)

hence \( g \mid p^2 \) by (auto simp add: dvd-def power2-eq-square)

with \( gNq \) show \( \neg \text{thesis} \) by auto

next

assume \( \neg g \mid p \) with \( gq \)

have \( g \mid p^2 - 3 \cdot N \cdot q^2 \) by auto

moreover from \( gNq \)

have \( g \mid 4 \cdot (N \cdot q^2) \) by (rule dvd-mult)

ultimately have \( g \mid p^2 - 3 \cdot (N \cdot q^2) + 4 \cdot (N \cdot q^2) \)

by (simp only: ac_simps dvd-add)

moreover have \( p^2 - 3 \cdot (N \cdot q^2) + 4 \cdot (N \cdot q^2) = p^2 + N \cdot q^2 \) by arith

ultimately show \( \neg \text{thesis} \) by simp

qed

next

assume \( \neg g \mid q \) with \( g1 \)

have \( gpq: g \mid 3 \cdot p^2 - N \cdot q^2 \) by simp

show \( \neg \text{thesis} \)

proof (cases)

assume \( g \mid p \)

hence \( \neg g \mid 4 \cdot p^2 \) by (auto simp add: dvd-def power2-eq-square)

with \( gpq \)

have \( g \mid 4 \cdot p^2 - (3 \cdot p^2 - N \cdot q^2) \) by (simp only: dvd-diff)

moreover have \( 4 \cdot p^2 - (3 \cdot p^2 - N \cdot q^2) = p^2 + N \cdot q^2 \) by arith

ultimately show \( \neg \text{thesis} \) by simp

next
assume \( \neg \) \( g \) dvd \( p \) with \( g^2 \) have \( g \) dvd \( p^2 - 3 \ast \NW - q^2 \) by auto
with \( \mbox{gcd} \) have \( g \) dvd \( 3 \ast p^2 - 3 \ast \NW - q^2 - (p^2 - 3 \ast \NW - q^2) \)
  by (simp only: dvd-diff)
moreover have \( 3 \ast p^2 - 3 \ast \NW - q^2 - (p^2 - 3 \ast \NW - q^2) = 2 \ast \?P \) by auto
ultimately have \( g \) dvd \( 2 \ast \?P \) by simp
with \( g \) have \( g \) dvd \( 2 \) \( \lor \) \( g \) dvd \( \?P \) by (simp only: prime-dvd-multD)
moreover have \( \neg \) \( g \) dvd \( 2 \)
proof (rule ccontr, simp)
  assume \( \neg \) \( g \) dvd \( 2 \)
  have \( g \leq 2 \)
  proof (rule ccontr)
    assume \( \neg \) \( g \leq 2 \)
    hence \( g > 2 \) by simp
  
  more over have \( \neg \) \( g \) dvd \( 2 \) by (auto simp only: zdvd-not-zless)
  with \( \neg \) \( g \) dvd \( 2 \) show False by simp
  qed
moreover have \( \neg \) \( \neg \) \( g \) dvd \( 2 \)
  proof (rule ccontr)
    assume \( \neg \) \( g \) dvd \( 2 \)
    have \( g = 1 \)
    proof (simp add: prime-int-iff)
      with \( g \) have \( \?P \) dvd \( p \) \( \lor \) \( \?P \) dvd \( p^2 - 3 \ast \NW - q^2 \)
        by (auto dest: prime-dvd-multD)
      moreover have \( \neg \) \( \?P \) dvd \( 3 \ast \NW - q^2 \)
        by (simp only: dvd-refl dvd-mul)
      ultimately have \( \neg \) \( \?P \) dvd \( 4 \ast p^2 \) by auto
      with \( \neg \) \( \?P \) dvd \( 4 \) \( \lor \) \( \neg \) \( \?P \) dvd \( p^2 \)
        by (simp only: prime-dvd-multD)
      moreover have \( \neg \) \( \?P \) dvd \( 4 \) by auto
      proof (rule ccontr, simp)
        assume \( \neg \) \( \?P \) dvd \( 4 \)
        have \( \?P \leq 4 \)
        proof (rule ccontr)
          assume \( \neg \) \( \?P \leq 4 \)
          hence \( \?P > 4 \) by simp
moreover have \((\odot::\text{int}) < 4\) by \text{auto} \\
ultimately have \(\neg\ ?P \text{ dvd } 4\) by \text{(auto simp only: zdvd-not-zless)} \\
with \text{Pdvd4} show \text{False} by \text{simp} \\
q b \ultim a t y \h a \ve r \(\neg \ ?P \text{ dvd } 4\)
proof \text{ (rule ccontr, simp)} \\
assume \(\neg \ ?P = 2 \lor \neg \ ?P = 4\)
with \text{Podd} show \text{False} by \text{blast} \\
q b 
ultimately have \(\neg \ ?P = 3\) by \text{auto} \\
with \text{Pdvd4} have \((3::\text{int}) \text{ dvd } 4\) by \text{simp} \\
thus \text{False} by \text{arith} \\
q b 
ultimately show \text{?thesis} by \text{auto} \\
q b 
ultim a t y \h a \ve r \(\neg \ ?P \text{ dvd } p\)
if \h 1: \text{gcd } N \ ?a \neq 1 \\
proof \\
let \(\ ?h = \text{gcd } N \ ?a\) \\
have \(\ ?h \geq 0\) by \text{simp} \\
with \h 1 have \(\ ?h = 0 \lor \ ?h = 1 \lor \ ?h > 1\) by \text{arith} \\
moreover \\
{ \text{assume } \neg \ ?h = 0 \lor \neg \ ?h = 1 \lor \neg \ ?h > 1 \text{ by } \text{auto} } \\
moreover \\
{ \text{assume } \neg \ ?h = 0 \lor \neg \ ?h = 1 \lor \neg \ ?h > 1 \text{ by } \text{auto} } \\
then have \exists g. \text{prime } g \land g \text{ dvd } \ ?h \\
using \text{prime-factor-int [of } \ ?h]\text{ by auto} \\
then obtain g where g: \text{prime } g \text{ dvd } \ ?h \\
by \text{blast} \\
with g have \text{g dvd } N \ \text{and } \text{gcd } \ ?a \text{ by } \text{auto} \\
with g have \text{g dvd } p\cdot p^2 - N\cdot (3\cdot p\cdot q^2) \\
by \text{(auto simp only: right-diff-distrib ac-simps)} \\
with g have \text{g dvd } p\cdot p^2 - N\cdot (3\cdot p\cdot q^2) + N\cdot (3\cdot p\cdot q^2) \\
by \text{(simp only: dvd-add dvd-mult2)} \\
with g have g\cdot p\cdot p\cdot p\cdot p\cdot p \text{ by simp} \\
with g have g\cdot p\cdot p \text{ by (simp add: prime-dvd-multD power2-eq-square)} \\
with g have g\cdot p \text{ by (auto dest: prime-dvd-multD)} \\
with g have g\cdot p \text{ by (simp add: power2-eq-square)} \\
with g\cdot p \text{ by (auto dest: prime-int-iff)} \\
with g\cdot p \text{ by (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 \( \neg ?P \ dvd p \)
proof (rule ccontr, clarsimp)
assume \( P \vdw p \): \( ?P \ dvd p \)
have \( p^2 \geq ?P^2 \)
proof (rule ccontr)
assume \( \neg p^2 \geq ?P^2 \) hence \( p^2 < ?P^2 \) by simp
moreover have \( p^2 > 0 \) by simp
ultimately have \( \neg ?P^2 \ dvd p^2 \) by (simp add: zdvd-not-zless)
with \( P \vdw p \) 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 \( p^2 > ?P \) by (auto simp add: power2-eq-square)
hence \( \neg neg \): \( N*q^2 < 0 \) by auto
show False
proof (simp only: zdvd-not-zless)
have is-gfN \((0^2 + N*q^2)\) \( N \) by (auto simp only: is-gfN-def)
with \( N \) have \( 0 + N*q^2 \geq 0 \) 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:
[ \( \text{prime } (a^2+N*b^2:int); \ N > 1; \ a^2+N*b^2 = c^2+N*d^2 \) ]
\( \implies (|a| = |c| \land |b| = |d|) \)
proof (clarsimp)
let \( ?P = a^2+N*b^2 \)
assume \( P: \text{prime } ?P \) \( \text{and } N: \ N > 1 \) \( \text{and } abcdN: \ ?P = c^2 + N*d^2 \)
have mult: \( (a*d+b*c)*(a*d-b*c) = ?P*(d^2-b^2) \)
proof (simp only: zdvd-not-zless)
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 \( ?P \ dvd a*d + b*c \lor ?P \ dvd a*d - b*c \)
proof (simp only: zdvd-not-zless)
from mult have \( ?P \ dvd (a*d+b*c)*(a*d-b*c) \) by simp
with $P$ show $\$thesis$ by (auto dest: prime-dvd-multD)
qd
moreover
{
assume $\$P\ dvd\ a\ \ast\ d\ +\ b\ \ast\ c$
then obtain $Q$ where $Q$: $a\ \ast\ d\ +\ b\ \ast\ c = \$P\ \ast\ Q$ by (auto simp add: dvd-def)
from $abcdN$ have $\$P\ \ast\ 2 = (a\ \ast\ 2 + N\ \ast\ b\ \ast\ 2) \ast (c\ \ast\ 2 + N\ \ast\ d\ \ast\ 2)$
by (simp add: power2-eq-square)
also have $... = (a\ \ast\ c - N\ \ast\ b \ast d) \ast 2 + N \ast (a\ \ast\ d + b \ast c) \ast 2$ by (rule qfN-mult2)
also with $Q$ have $... = (a \ast c - N \ast b \ast d) \ast 2 + N \ast Q \ast 2 \ast Q \ast 2$ by (simp add: ac-simps power-mul-distrib)
also have $... \geq N \ast Q \ast 2 \ast Q \ast 2 \ast ?P \ast 2$ by simp
finally have $pos$: $?P \ast 2 \geq ?P \ast 2 \ast (Q \ast 2 \ast N)$ by (simp add: ac-simps)
have $b \ast 2 = d \ast 2$
proof (rule ccontr)
assume $b \ast 2 \neq d \ast 2$
with $P$ mult $Q$ have $Q \neq 0$ by (unfold prime-int-iff, auto)
hence $Q \ast 2 > 0$ by simp
moreover with $N$ have $Q \ast 2 \ast N > Q \ast 2 \ast 1$ by (simp only: zmult-zless-mono2)
ultimately have $Q \ast 2 \ast N > 1$ by arith
moreover with $P$ have $?P \ast 2 > 0$ by (simp add: prime-int-iff)
ultimately have $?P \ast 2 \ast 1 < ?P \ast 2 \ast (Q \ast 2 \ast N)$ by (simp only: zmult-zless-mono2)
with $pos$ show $False$ by simp
qd
}
moreover
{
assume $\$P\ dvd\ a\ \ast\ d\ -\ b\ \ast\ c$
then obtain $Q$ where $Q$: $a\ \ast\ d\ -\ b\ \ast\ c = \$P\ \ast\ Q$ by (auto simp add: dvd-def)
from $abcdN$ have $\$P\ \ast\ 2 = (a\ \ast\ 2 + N\ \ast\ b\ \ast\ 2) \ast (c\ \ast\ 2 + N\ \ast\ d\ \ast\ 2)$
by (simp add: power2-eq-square)
also have $... = (a\ \ast\ c + N\ \ast\ b \ast d) \ast 2 + N \ast (a\ \ast\ d - b \ast c) \ast 2$ by (rule qfN-mult1)
also with $Q$ have $... = (a \ast c + N \ast b \ast d) \ast 2 + N \ast Q \ast 2 \ast ?P \ast 2$
by (simp add: ac-simps power-mul-distrib)
also have $... \geq N \ast Q \ast 2 \ast ?P \ast 2$ by simp
finally have $pos$: $?P \ast 2 \geq ?P \ast 2 \ast (Q \ast 2 \ast N)$ by (simp add: ac-simps)
have $b \ast 2 = d \ast 2$
proof (rule ccontr)
assume $b \ast 2 \neq d \ast 2$
with $P$ mult $Q$ have $Q \neq 0$ by (unfold prime-int-iff, auto)
hence $Q \ast 2 > 0$ by simp
moreover with $N$ have $Q \ast 2 \ast N > Q \ast 2 \ast 1$ by (simp only: zmult-zless-mono2)
ultimately have $Q \ast 2 \ast N > 1$ by arith
moreover with $P$ have $?P \ast 2 > 0$ by (simp add: prime-int-iff)
ultimately have $?P \ast 2 \ast 1 < ?P \ast 2 \ast (Q \ast 2 \ast N)$ by (simp only: zmult-zless-mono2)
with $pos$ show $False$ by simp
qd
}
ultimately have $bd$: $b \ast 2 = d \ast 2$ by blast
moreover with $abcdN$ have $a \ast 2 = c \ast 2$ by auto
ultimately show $\$thesis$ by (auto simp only: power2-eq-iff)
qd

lemma qfN-square-prime:
assumes $ass$:
prime ($p \ast 2 + N \ast q \ast 2 :: int$) $\land$ $N > 1 \land (p \ast 2 + N \ast q \ast 2) \ast 2 = r \ast 2 + N \ast s \ast 2 \land$ coprime $r s$
shows $|r| = |p^2 - N*q^2| \land |s| = |2*p*q|

proof

let $\mathcal{P} = p^2 + N*q^2$
let $\mathcal{A} = r^2 + N*s^2$

from ass have $\mathcal{P} > 1$ by (simp add: prime-int-iff)
from ass have $\mathcal{APP}: \mathcal{A} = \mathcal{P} * \mathcal{A}$ by (simp only: power2-eq-square)
with ass have prime $\mathcal{P} \land \mathcal{P} dvd \mathcal{A}$ by (simp add: dvdI)
then obtain $u \in \mathbb{Q}$ where $u$:

$hence |u| = |p| \land |v| = |q|$ by (auto dest: qfN-prime-unique)
then obtain $f \in \mathbb{Q}$ where $f$:

$|f| = 1$ and $g: v = g*q \land |g| = 1$

by (blast dest: abs-eq-iml-unifactor)
with $\mathcal{uw}e$ have $r = f*p*p + (e*q)*N*q*q \land s = g*p*q - (e*f)*p*q$ by simp
hence $\mathcal{rs}: r = f*p^2 + (e*q)*N*q^2 \land s = (g - e*f)*p*q$
by (auto simp only: power2-eq-square left-diff-distrib)
moreover have $s \neq 0$

proof (rule ccontr, simp)
assume $s0: \neg s = 0$

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 $\mathcal{A} = 1$ by simp
moreover have $\mathcal{P}^2 > 1$

proof
from $PI$ have $1 < \mathcal{P}$ by (simp add: prime-int-iff)

hence $\mathcal{P}^2 > 1^2$ by (simp only: power-strict-mono)
thus $\mathcal{thesis}$ by auto

qed

moreover from ass have $\mathcal{A} = \mathcal{P}^2$ by simp
ultimately show False by auto

qed

ultimately have $g \neq e*f$ by auto
moreover from $f \in \mathbb{Q}$ $\mathcal{uw}e$ have $|g| = |e*f|$ unfolding abs-mult by presburger
ultimately have $gef: g = -(e*f)$ by arith
from $\mathcal{uw}e$ have $e * \neg (e * f) = -f$

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

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

hence $|r| = |f| * |p^2 - N*q^2|$
$\land |s| = |e|*|f|*|2*p*q|

by (auto simp add: abs-mult)

with $\mathcal{uw}e$ $f \in \mathbb{Q}$ show $\mathcal{thesis}$ by (auto simp only: mult-1-left)

qed

lemma qfN-cube-prime:

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

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

proof
2.4 Uniqueness (N > 1)

\[ \text{let } \forall P = p^2 + N * q^2 \]
\[ \text{let } \forall A = a^2 + N * b^2 \]

from \text{ass have coprime a b by blast}
from \text{ass have } P1: \forall P > 1 \text{ by (simp add: prime-int-iff)}
with \text{ass have APP: } \forall A = \forall P * \forall P^2 \text{ by (simp add: power2-eq-square power3-eq-cube)}
with \text{ass have prime } \forall P \land \forall P \text{ dvd } \forall A \text{ by (simp add: dvdI)}

then obtain \( u \) \( v \) \( e \) where \( u \):
\[ \forall A = (a^2 + N * v^2) * \forall P \land a = p * u + e * N * q * v \land b = p * v - e * q * u \land |e| = 1 \]
by (frule-tac \( p = p \) \( \text{in} \) \( qfN-div-prime \), \text{auto})

have \text{coprime } u \text{ v}
proof (rule coprime1)
\begin{itemize}
\item fix \( c \)
\item assume \( \text{c dvd u c dvd v} \)
\item with \( \text{wee have c dvd a c dvd b} \)
\item by simp-all
\item with \((\text{coprime a b)}\) \text{show is-unit c}
\item by (rule coprime-common-divisor)
\end{itemize}
\text{qed}

with \( P1 \) \text{ uve APP ass have prime } \forall P \land N > 1 \land \forall P^2 = a^2 + N * v^2 \]
\land \text{coprime u v by (auto simp add: ac-simps)}

\text{hence } |u| = |p^2 - N * q^2| \land |v| = |2 * p * q| \text{ by (rule qfN-square-prime)}

then obtain \( f \) \( g \) \begin{itemize}
\item where \( f: u = f * (p^2 - N * q^2) \land |f| = 1 \)
\item and \( g: v = g * (2 * p * q) \land |g| = 1 \) by (blast dest: \text{abs-eq-impl-unifactor})
\item with \( \text{we have a = p * f * (p^2 - N * q^2) + e * N * q * g * 2 * p * q} \)
\item \text{and } b = p * g * 2 * p * q - e * q * f * (p^2 - N * q^2) \text{ by auto}
\end{itemize}

\begin{itemize}
\item hence \( a: a = f * p * p^2 + f * N * p * q^2 \) \text{ by (auto simp add: distrib-left ac-simps)}
\item \text{hence } Pa: \forall P \text{ dvd a by auto}
\item \text{have e * f = g using f2 power2-eq-square[of f] cfg by simp}
\item \text{with ab have b = g * p * p^2 * q + g * N * q * q^2 by auto}
\item \text{hence b = (g * q) * ?P by (auto simp add: distrib-left ac-simps)}
\item \text{hence } ?P \text{ dvd b by auto}
\item \text{with Pa have } ?P \text{ dvd gcd a b by simp}
\item \text{with ass have } ?P \text{ dvd 1 by auto}
\end{itemize}

\begin{itemize}
\item with \( P1 \) \text{ show False by auto}
\end{itemize}
\text{qed}

moreover from \( f \) \( g \) \text{ uve have } |e| = |f * g| \text{ unfolding abs-mult by auto}
ultimately have \( c = -(f * g) \) by \text{arith}

\begin{itemize}
\item hence e * g = -f * f = -g using f2 g2 unfolding power2-eq-square by auto
\item with ab have a = f * p * p^2 - 3 * f * N * p * q^2 \land b = 3 * g * p^2 * q - g * N * q * q^2 \text{ by (simp add: mult.assoc)}
\item hence a = f * (3 * 3 * N * p * q^2) \land b = g * (3 * p^2 * q - N * q^3)
\end{itemize}
by (auto simp only: right-diff-distrib ac-simps power2-eq-square power3-eq-cube)
with \(fg\) show ?thesis by (auto simp add: abs-mult)
qed

2.5 The case \(N = 3\)

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

**Proof**
- let \(?A = a^2 + 3 \cdot b^2\)
- assume \(\text{even} \ ?A\)
  - have \((\text{odd} \ a \land \text{odd} \ b) \lor (\text{even} \ a \land \text{even} \ b)\)
  - proof (rule contr, auto)
    - assume \(\text{even} \ a \land \text{odd} \ b\)
    - hence \((\text{even} \ (a^2)) \land \text{odd} \ (b^2)\)
      - by (auto simp add: power2-eq-square)
    - moreover have \(\text{odd} \ 3\) by simp
    - ultimately have \(?A\) by simp
    - with \(\text{even}\) show False by simp
  - next
    - assume \(\text{odd} \ a \land \text{even} \ b\)
    - hence \((\text{odd} \ (a^2)) \land \text{even} \ (b^2)\)
      - by (auto simp add: power2-eq-square)
    - moreover hence \((\text{even} \ (b^2 \cdot 3))\) by simp
    - ultimately have \(?A\) by simp
    - with \(\text{even}\) show False by simp
- qed

moreover
- \{ assume \(\text{even} \ a \land \text{even} \ b\)
  - then obtain \(c\) \(d\) where \(\text{abcd}: a = 2 \cdot c \land b = 2 \cdot d\) using evenE[of a] evenE[of b]
  - by meson
    - hence \(?A = 4 \cdot (c^2 + 3 \cdot d^2)\) by (simp add: power-mult-distrib)
    - moreover have \(\text{is-qfN} (c^2 + 3 \cdot d^2) 3\) by (unfold is-qfN-def, auto)
      - ultimately have ?thesis by blast \}
- moreover
- \{ assume \(\text{odd} \ a \land \text{odd} \ b\)
  - then obtain \(c\) \(d\) where \(\text{abcd}: a = 2 \cdot c + 1 \land b = 2 \cdot d + 1\) using oddE[of a] oddE[of b]
  - by meson
    - have \(\text{odd} \ (c - d) \lor \text{even} \ (c - d)\) by blast
    - moreover
      - \{ assume \(\text{even} \ (c - d)\)
        - then obtain \(e\) where \(c - d = 2 \cdot e\) using evenE by blast
          - with \(\text{abcd}\) have \(e1: a - b = 4 \cdot e\) by arith
            - hence \(e2: a + 3 \cdot b = 4 \cdot (e + b)\) by auto
              - have \(4 \cdot ?A = (a + 3 \cdot b)^2 + 3 \cdot (a - b)^2\)
                - by (simp add: eval-nat-numeral field-simps)
              - also with \(e1\) \(e2\) have \(\ldots\) = \((4 \cdot (e + b))^2 + 3 \cdot (4 \cdot e)^2\) by (simp(no_asm simp))
              - finally have \(?A = 4 \cdot ((e + b)^2 + 3 \cdot e^2)\) by (simp add: eval-nat-numeral field-simps)
                - moreover have \(\text{is-qfN} ((e + b)^2 + 3 \cdot e^2) 3\) by (unfold is-qfN-def, auto)
                  - ultimately have ?thesis by blast \}
      - moreover
        - \{ assume \(\text{odd} \ (c - d)\)
then obtain e where \( c - d = 2e + 1 \) using oddE by blast
with abcd have e1: \( a + b = 4(e + d + 1) \) by auto
hence e2: \( a - 3b = 4(e + d - b + 1) \) by auto
have \( 4 \cdot ?A = (a - 3b)^2 + 3(a + b)^2 \)
  by (simp add: eval-nat-numeral field-simps)
also with e1 e2 have \( \ldots = (4(e + d - b + 1) - 2 + 3(e + d + 1) - 2) \)
  by (simp (no-asmsimp))
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 \( ((e + d - b + 1) - 2 + 3(e + d + 1) - 2) \)
  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: \[ is-qfN A 3; even A \]
\[ \implies \exists B. A = 4B \land is-qfN B 3 \]
proof –
assume even A and is-qfN A 3
then obtain a b where A = a^2 + 3b^2
  and \( (a^2 + 3b^2) \) by (unfold is-qfN-def, auto)
thus \( ?thesis \) by (auto simp add: qf3-even)
qed

lemma qf3-oddprime-divisor-not:
assumes ass: prime P \land odd P \land Q > 0 \land is-qfN (P \cdot 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 contr, simp)
assume ass2: \( \forall R. R dvd Q \implies prime R \implies even R \lor is-qfN R 3 \)
(is ?A Q)
obtain n::nat where n = nat Q by auto
with ass have n: \( Q = int n \) by auto
have \( (n > 0 \land is-qfN (P \cdot int n) 3 \land \neg ?A (int n) ) \implies False \) (is ?B n \implies False)
proof (induct n rule: less-induct)
case (less n)
hence IH: \( !m. m < n \land ?B m \implies False \)
  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 \cdot 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 \cdot 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 even: \( \neg \) odd \((\text{int } n)\)
hence even \((\text{int } n) \times P) \text{ by simp}

with \( Bn \) have \( \text{even } (P \times \text{int } n) \land \text{is-qfN } (P \times \text{int } n) 3 \) by \( \text{simp add: ac-simps} \)
hence \( \exists B. P \times (\text{int } n) = 4 \times B \land \text{is-qfN } B 3 \) by \( \text{simp only: qf3-even-general} \)
then obtain \( B \) where \( B : P \times (\text{int } n) = 4 \times B \land \text{is-qfN } B 3 \) by auto
hence \( 2^2 \times \text{dvd } (\text{int } n) \times P \) by \( \text{simp add: ac-simps} \)
moreover have \( \neg 2 \times \text{dvd } P \)

proof \( \text{(rule ccontr, simp)} \)
assume \( 2 \times \text{dvd } P \)
with \( \text{ass have odd } P \land \text{even } P \) by simp
thus \( \text{False by simp} \)

qed

moreover have \( \text{prime } (2 :: \text{int}) \) by simp
ultimately have \( 2^2 \times \text{dvd int } n \)
by \( \text{(rule-tac p=2 in prime-power-dvd-cancel-right)} \)
then obtain \( \text{im :: int where int } n = 4 \times \text{im} \) by \( \text{(auto simp add: dvd-def)} \)
moreover obtain \( m :: \text{nat where m = nat im by auto} \)
ultimately have \( m : n = 4 \times m \) by \( \text{arith} \)
with \( B \) have \( \text{is-qfN } (P \times \text{int } m) 3 \) by auto
moreover from \( m \) \( Bn \) have \( m > 0 \) by auto
moreover from \( m \) \( Bn \) have \( \?A (\text{int } m) \) by auto
ultimately have \( \text{Bm : } \?B m \) by simp
from \( \text{Bn m have m < n by arith} \)
with \( \text{IH Bm show False by auto} \)

qed

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

qed

lemma \( \text{qf3-oddprimedivisor:} \)
\[
\begin{array}{l}
\text{prime } (P :: \text{int}) ; \text{odd } P ; \text{coprime } a b ; \text{P dvd } (a^2 + 3 b^2) \\
\Rightarrow \text{is-qfN } P 3
\end{array}
\]

proof \( \text{(induct } P \text{ arbitrary; a b rule:infinite-descent0-measure[where } V \equiv \lambda P. \text{nat } | P]) \)
case \( (0 x) \)
moreover hence \( x = 0 \) by \( \text{arith} \)
ultimately show \( \?A \text{ case by (simp add: prime-int-iff)} \)

next

case \( \text{smaller } x \)
then obtain \( a b \text{ where } abx : \text{prime } x \land \text{odd } x \land \text{coprime } a b \)
\( \land x \times \text{dvd } (a^2 + 3 b^2) \land \neg \text{is-qfN } x 3 \) by auto
then obtain \( M \) where \( M : a^2 + 3 b^2 = x \times M \) by \( \text{(auto simp add: dvd-def)} \)
let \( \?A = a^2 + 3 b^2 \)
from \( abx \) have \( x | 0 : x > 0 \) by \( \text{(simp add: prime-int-iff)} \)
then obtain \( m \) where \( 2 \times (a - m \times x) \leq x \) by \( \text{(auto dest: best-division-abs)} \)
with \( abx \) have \( 2 \times |a - m \times x| \leq x \) \( \text{using odd-two-times-div-two-succ[of } x] \) by presburger
then obtain \( c \) where \( cm : c = a - m \times x \land 2 \times |c| < x \) by auto
from \( x | 0 \) obtain \( n \) where \( 2 \times |b - n \times x| \leq x \) by \( \text{(auto dest: best-division-abs)} \)
with \( abx \) have \( 2 \times |b - n \times x| < x \) \( \text{using odd-two-times-div-two-succ[of } x] \) by presburger
then obtain \( d \) where \( dv : d = b - n \times x \land 2 \times |d| < x \) by auto
let \( \?C = c^2 + 3 d^2 \)
have \( C3: \text{is-qfN} \ y \ C \) by (unfold is-qfN-def, auto)

have \( C0: \ y \ C > 0 \)

proof

have \( \text{hlp} (3::\text{int}) \geq 1 \) by simp

have \( \ y \ C \geq 0 \) by simp

hence \( \ y \ C = 0 \lor \ y \ C > 0 \) by arith

moreover

{ assume \( \ y \ C = 0 \)

with \( \text{hlp} \) have \( c=0 \land d=0 \) by (rule qfN-zero)

with \( \text{cm dn} \) have \( a = m \cdot x \land b = n \cdot x \) by simp

hence \( x \\text{ dvd} a \land x \\text{ dvd} b \) by simp

hence \( x \\text{ dvd} \\gcd a b \) by simp

with \( \text{abx} \) have False by (auto simp add: prime-int-iff)

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

qed

have \( x \\text{ dvd} \ y \ C \)

proof

have \( \ y \ C = \lceil c \rceil \cdot 2 + 3 \cdot \lceil d \rceil \cdot 2 \) by (simp only: power2-abs)

also with \( \text{cm dn} \) have \( \ldots = (a \cdot m \cdot x) \cdot 2 + 3 \cdot (b \cdot n \cdot x) \cdot 2 \) by simp

also have \( \ldots = a \cdot 2 - 2 \cdot a \cdot (m \cdot x) + (m \cdot x) \cdot 2 + 3 \cdot (b \cdot 2 - 2 \cdot b \cdot (n \cdot x) + (n \cdot x) \cdot 2) \)

by (simp add: algebra-simps power2-eq-square)

also with \( \text{abx M} \) have \( \ldots = x \cdot M - x \cdot (2 \cdot a \cdot m + 3 \cdot 2 \cdot b \cdot n) + x \cdot 2 \cdot (m \cdot 2 + 3 \cdot n \cdot 2) \)

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

finally show \( \ y \ C = x \cdot (M - (2 \cdot a \cdot m + 3 \cdot 2 \cdot b \cdot n) + x \cdot (m \cdot 2 + 3 \cdot n \cdot 2)) \)

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

qed

then obtain \( y \) where \( \ y \ C = x \cdot y \) by (auto simp add: dvd-def)

have \( \text{yx:} \ y < x \)

proof (rule ccontr)

assume \( \neg \ y < x \) hence \( xy: x \cdot y \leq 0 \) by simp

have \( \text{hlp:} \ 2 \cdot \lceil c \rceil \geq 0 \land 2 \cdot \lceil d \rceil \geq 0 \land (3::\text{nat}) > 0 \) by simp

from \( y \) have \( 4 \cdot x \cdot y = 2 \cdot 2 \cdot c \cdot 2 + 3 \cdot 2 \cdot 2 \cdot d \cdot 2 \) by simp

hence \( 4 \cdot x \cdot y = (2 \cdot \lceil c \rceil \cdot 2 + 3 \cdot (2 \cdot \lceil d \rceil) \cdot 2 \)

by (auto simp add: power-mult-distrib)

with \( \text{cm dn hlp} \) have \( 4 \cdot x \cdot y < x \cdot 2 + 3 \cdot (2 \cdot \lceil d \rceil) \cdot 2 \)

and \( (3::\text{int}) > 0 \land (2 \cdot \lceil d \rceil) \cdot 2 < x \cdot 2 \)

using power-strict-mono [of \( 2 \cdot \lceil b \rceil \) \( x \cdot 2 \) \( b \)]

by auto

hence \( x \cdot 4 \cdot x < x \cdot 2 + 3 \cdot x \cdot 2 \) by (auto)

also have \( \ldots = x \cdot 4 \cdot x \) by (simp add: power2-eq-square)

finally have contr: \( (x \cdot y) \cdot (4 \cdot x) > 0 \) by (auto simp add: right-diff-distrib)

show False

proof (cases)

assume \( \neg \ x \cdot y \cdot 0 \) with contr show False by auto

next

assume \( \neg \ x \cdot y \cdot 0 \) with \( xy \) have \( x \cdot y \cdot 0 \) by simp

moreover from \( x \cdot 0 \) have \( 4 \cdot x > 0 \) by simp

ultimately have \( 4 \cdot x \cdot (x \cdot y) < 4 \cdot x \cdot 0 \) by (simp only: zmult-zless-mono2)

with contr show False by auto

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

qed

have $y0$: $y > 0$
proof (rule ccontr)
assume $\neg y > 0$
hence $y \leq 0$ by simp
moreover have $y \neq 0$
proof (rule ccontr)
assume $\neg y \neq 0$ hence $y = 0$ by simp
with $y$ and $C0$ show False by auto
qed
ultimately have $y < 0$ by simp
with $x0$ have $x + y < x \cdot 0$ by (simp only: zmult-zless_mono2)
with $C0 \ y$ show False by simp
qed

let $?g = gcd \ c \ d$

have $c \neq 0 \lor d \neq 0$
proof (rule ccontr)
assume $\neg (c \neq 0 \lor d \neq 0)$ hence $c = 0 \land d = 0$ by simp
with $C0$ show False by simp

then obtain $e \ f$ where $ef$: $e = ?g \cdot e \land d = ?g \cdot f \land \text{coprime} \ e \ f$
using gcd-coprime-exists[of $c \ d$] gcd-pos-int[of $c \ d$] by (auto simp: mult.commute)
have $g2\text{nonzero}$: $?g^2 \neq 0$
proof (rule ccontr, simp)
assume $c = 0 \land d = 0$
with $C0$ show False by simp

let $?E = e^2 + 3 \cdot f^2$
have $E3$: is-qfN $?E$ 3 by (unfold is-qfN_def, auto)
have $CgE$: $?C = ?g^2 \cdot ?E$
proof
have $?g^2 \cdot ?E = (?g \cdot e)^2 + 3 \cdot (?g \cdot f)^2$
  by (simp add: distrib_left power_mult_distrib)
with $ef$ show $\text{thesis}$ by simp

hence $?g^2 \text{ dvd } ?C$ by (simp add: dvd_def)
with $y$ have $g2\text{dvdxy}$: $?g^2 \text{ dvd } y \cdot x$ by (simp add: ac_simps)
moreover have $\text{coprime} \ x \ (?g^2)$
proof
let $?h = gcd \ ?g \ x$
have $?h \text{ dvd } ?g \ y \land ?g \text{ dvd } c$ by blast+
hence $?h \text{ dvd } c$ by (rule dvd_trans)
have $?h \text{ dvd } ?g \ y \land ?g \text{ dvd } d$ by blast+
hence $?h \text{ dvd } d$ by (rule dvd_trans)
have $?h \text{ dvd } x$ by simp
hence $?h \text{ dvd } m \cdot x$ by (rule dvd_mult)
with $?h \text{ dvd } c$ have $?h \text{ dvd } c + m \cdot x$ by (rule dvd_add)
with $cm$ have $?h \text{ dvd } a$ by simp
from $?h \text{ dvd } x$ have $?h \text{ dvd } n \cdot x$ by (rule dvd_mult)
with $?h \text{ dvd } d$ have $?h \text{ dvd } d + n \cdot x$ by (rule dvd_add)
with $dn$ have $?h \text{ dvd } b$ by simp
with $?h \text{ dvd } a$ have $?h \text{ dvd } gcd \ a \ b$ by simp
with \( abz \) have \( \tilde{h} \ dvd \ 1 \) by simp
hence \( \tilde{h} = 1 \) by simp
hence coprime \( (\tilde{g}'^2) \ x \) by (auto intro: gcd-eq-1-imp-coprime)
thus \( \tilde{\text{thesis}} \) by (simp only: ac-simps)

qed

ultimately have \( \tilde{g}'^2 \ d dvd \ y \)
  by (auto simp add: ac-simps coprime-dvd-mult-right-iff)

then obtain \( w \) where \( w = \tilde{g}'^2 \ast w \) by (auto simp add: dvd-def)
with \( CgE \ y \ g2nonzero \) have \( \tilde{E} = x \ast w \) 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 \( w\neg \): \( w<0 \)
    have \( \tilde{g}'^2 \geq 0 \) by (rule zero-le-power2)
    with \( g2nonzero \) have \( \tilde{g}'^2 > 0 \) by arith
    with \( w\neg \) have \( \tilde{g}'^2 \ast w < \tilde{g}'^2 \ast 0 \) by (simp only: zmult-zless-mono2)
    with \( w y0 \) have \( \text{False} \) by auto \}

  ultimately show \( \text{False} \) by blast
  qed

have \( w-le-y \): \( w \leq y \)

proof (rule ccontr)
  assume \( \neg w \leq y \)
  hence \( w>Y \) by simp
  have \( \tilde{g}'^2 = 1 \lor \tilde{g}'^2 > 1 \)
  proof –
    have \( \tilde{g}'^2 \geq 0 \) by (rule zero-le-power2)
    hence \( \tilde{g}'^2 =0 \lor \tilde{g}'^2 > 0 \) by auto
    with \( g2nonzero \) show \( \tilde{\text{thesis}} \) by arith
  qed

  moreover
  \{ assume \( \tilde{g}'^2 =1 \) with \( w wY \) have \( \text{False} \) by simp \}
  moreover
  \{ assume \( g1: \tilde{g}'^2 >1 \)
    with \( \langle w>0 \rangle \) have \( w\ast 1 < w\ast 2 \) by (auto dest: zmult-zless-mono2)
    with \( w \) have \( w < y \) by (simp add: ac-simps)
    with \( wY \) have \( \text{False} \) by auto \}

  ultimately show \( \text{False} \) by blast
  qed

from \( E3 \ abx \langle \ast \rangle \) have
  \( \text{prime} x \land \text{odd} x \land w > 0 \land \text{is-gfN} (x\ast w) \ 3 \land \neg \text{is-gfN} x \ 3 \) by simp

then obtain \( z \) where \( z: \text{prime} z \land \text{odd} z \land z \ d dvd \ w \land \neg \text{is-gfN} z \ 3 \)
  by (frule-tac \( P=x \) in \( qf3-oddprimedivisor-not \), auto)

from \( E3 \) have \( w d dvd \ ?E \) by simp
with \( z \) have \( z \ d dvd \ ?E \) by (auto dest: ded-trans)
with \( z \ e \ f \) have \( \text{prime} z \land \text{odd} z \land \text{coprime} e f \land z \ d dvd \ ?E \land \neg \text{is-gfN} z \ 3 \)
  by auto

moreover have \( \text{nat}|z| < \text{nat}|x| \)

proof –


have $z \leq w$
proof (rule ccontr)
  assume $\neg z \leq w$ hence $w < z$ by auto
with ($w > 0$) have $\neg z \ dvd w$ by (rule zdvd-not-zless)
with $z$ show False by simp
qed
with $w \leq y$ $x$ have $z < x$ by simp
with $z$ have $|z| < |x|$ by (simp add: prime-int-iff)
thus $\neg$thesis by auto
qed
ultimately show $\neg$case by auto
qed

definition lemma $qf3$-cube-prime-impl-cube-form:
assumes $ab$-relprime: coprime $a$ $b$ and $abP$: $P \cdot 3 = a^2 + 3 \cdot b^2$
and $P$: prime $P \land$ odd $P$
shows is-cube-form $a$ $b$
proof
  from $abP$ have $qfP3$: is-qfN $(P \cdot 3) \ 3$ by (auto simp only: is-qfN-def)
  have $P$-dP3$: $P \ dvd P \cdot 3$ by (simp add: eval-nat-numeral)
  with $abP$-relprime $P$ have $qfP$: is-qfN $P \ 3$ by (simp add: $qf3$-oddprimedivisor)
  then obtain $p$ $q$ where $pq$: $P = p \cdot 2 + 3 \cdot q^2$ by (auto simp only: is-qfN-def)
  with $P$ $abP$-relprime have $prime$ $(p \cdot 2 + 3 \cdot q^2) \land (3::int) > 1$
  hence $ab$: $|a| = |p \cdot 3 - 3 \cdot 3 \cdot p \cdot q^2| \land |b| = |3 \cdot p^2 \cdot q - 3 \cdot q^3|$
  by (rule $qfN$-cube-prime)
  hence $a$: $a = p \cdot 3 - 9 \cdot p \cdot q^2 \lor a = -(p \cdot 3) + 9 \cdot p \cdot q^2$ by arith
  from $ab$ have $b$: $b = 3 \cdot p^2 \cdot q - 3 \cdot q^3$ $\lor$ $b = -(3 \cdot p^2 \cdot q) + 3 \cdot q^3$ by arith
  obtain $r$ $s$ where $r$: $r = -p$ and $s$: $s = -q$ by simp
  show $\neg$thesis
proof (cases)
  assume $a1$: $a = p \cdot 3 - 9 \cdot p \cdot q^2$
  show $\neg$thesis
proof (cases)
  assume $b1$: $b = 3 \cdot p^2 \cdot q - 3 \cdot q^3$
  with $a1$ show $\neg$thesis by (unfold is-cube-form-def, auto)
next
  assume $\neg b$: $b = 3 \cdot p^2 \cdot q - 3 \cdot q^3$
  with $b$ have $b = -3 \cdot p^2 \cdot q + 3 \cdot q^3$ by simp
  with $s$ have $b = 3 \cdot p^2 \cdot s - 3 \cdot s^3$ by simp
  moreover from $a1$ $s$ have $a = p \cdot 3 - 9 \cdot p \cdot s^2$ by simp
  ultimately show $\neg$thesis by (unfold is-cube-form-def, auto)
qed
next
  assume $\neg a$: $a = p \cdot 3 - 9 \cdot p \cdot q^2$
  with $a$ have $a = -(p \cdot 3) + 9 \cdot p \cdot q^2$ by simp
  with $r$ have $ar$: $a = r \cdot 3 - 9 \cdot r \cdot q^2$ by simp
  show $\neg$thesis
proof (cases)
  assume $b1$: $b = 3 \cdot p^2 \cdot q - 3 \cdot q^3$
  with $r$ have $b = 3 \cdot r^2 \cdot q - 3 \cdot q^3$ by simp
  with $ar$ show $\neg$thesis by (unfold is-cube-form-def, auto)
next
assume \( b = 3*p^2*q - 3*q^3 \)
with \( b \) have \( b = -3*p^2*q + 3*q^3 \) by simp
with \( r \) have \( b = 3*r^2*s - 3*s^3 \) by simp
moreover from \( r s \) have \( a = r^3 - 9*r*s^2 \) by simp
ultimately show \( \text{thesis} \) by (unfold is-cube-form-def, auto)
qed

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

\textbf{proof} –
assume \( a b; c d; \) is-cube-form \( c d \) and \( e: \) \( |e| = 1 \)
from \( a b \) obtain \( p q \) where \( a = p^3 - 9*p^2*q^2 \wedge b = 3*p^2*q - 3*q^3 \)
by (auto simp only: is-cube-form-def)
from \( c d \) obtain \( r s \) where \( c = r^3 - 9*r*s^2 \wedge d = 3*r^2*s - 3*s^3 \)
by (auto simp only: is-cube-form-def)
let \( ?t = p*r + c*3*q*s \\
let \( ?u = p*s - e*r*q \\
have \( e2: e^2=1 \)
\textbf{proof} –
from \( e \) have \( e=1 \vee e=-1 \) by linarith
moreover
\hspace{1em} \{ assume \( e=1 \) hence \( \text{thesis} \) by auto \}
moreover
\hspace{1em} \{ assume \( e=-1 \) hence \( \text{thesis} \) by simp \}
ultimately show \( \text{thesis} \) 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 \( a*c + e*3*b*d = ?t^3 - 9*?t*?u^2 \)
\textbf{proof} –
have \( ?t^3 = 9*?t+?u^2 = p^3*r^3 + e*9*p^2*q*r^2*s + e^2*27*p^2*q^2*r*s^2 + e^3*27*p^2*q^3*s^3 + 9*p^2*q^2*r^2*s^2 + e^2*18*p^2*q^2*r^2*s - e^2*9*p^2*q^2*(r*r^2) - e^2*7*p^2*q^2*(s*s^2) + e^2*54*p^2*q^2*r^2*s^2 - e^2*27*(q^2)*r^2*s \\
by (simp add: eval-nat-numeral field-simps)
also with \( e2 e3 \) have \( \ldots = p^3*r^3 + e*27*p^2*q*r^2*s + 81*p^2*q^2*r^2*s^2 + e^2*72*p^2*q^2*s^3 + 9*p^2*q^2*r^3 - e^2*27*p^2*q^2*s^3 - e^2*27*p^3^3*r^2*s \\
by (simp add: power2-eq-square power3-eq-cube)
also with \( p q r s \) have \( \ldots = a*c + e*3*b*d \\
by (simp only: left-diff-distrib right-diff-distrib ac-simps)
finally show \( \text{thesis} \) by auto
qed

moreover have \( a*d-e*b*c = 3*?t^2*?u - 3*?u^3 \)
\textbf{proof} –
have \( 3*?t^2*?u - 3*?u^3 = \)
\hspace{1em} \( 3*(p^2)^2*r^2*s + e^3*p^2*q*(r*r^2) + e^2*18*p^2*q*r*s^2 \\
- e^2*18*p^2*q^2*r^2*s + e^2*27*p^2*q^2*(s*s^2) - e^2*27*(q^2)*r^2*s \\
- 3*p^3^3*s^3 + e*9*p^2*q^2*r*s^2 - e^2*9*p^2*q^2*r^2*s + e^3*3*r^3^3 \\
by (simp add: eval-nat-numeral field-simps)
also with \( c2 \) \( c3 \) have \( \ldots = 3*p^3*r^2*s - c*3*p^2*q*r^3 + c*18*p^2*q*r*s^2 - 18*p*q^2*r^2 + 27*p^2*q^2 + c*3*q^3*r^2 - 3*p^3+s^2 - c*9*p^2*q*r^2 - 9*p^2*q^2 + c*3*r^3 * q^3 \)

by (simp add: power2-eq-square power3-eq-cube)

also with \( pq \) \( rs \) have \( \ldots = a*d - c*b*c \)

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 \( \text{qf3-cube-primelist-impl-cube-form: } \Pi (\forall \text{ps. prime } p \in \text{ps}) \text{. odd } (\Pi (\Pi i \in \text{ps. } i)) \) \( \Rightarrow \)

(\Pi (a \in \text{ps. } a \text{. coprime } a \text{. b } \Rightarrow a^2 + 3*b^2 = (\Pi (\Pi i \in \text{ps. } i)) ) \Rightarrow \text{is-cube-form a b) \)

proof (induct ps)

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

have b0: \( b = 0 \)

proof (rule contra)

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: \( (a=1 \lor a=-1) \) by (auto simp add: power2-eq-square zmult-eq-1-iff)

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

with a1 and b0 have \( a = p^3 - 9*p^2*q^2 \land b = 3*p^2*q - 3*p^3 * q^3 \) by auto

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

next

case (add p ps) hence \( \text{ass: coprime a b } \land \text{ odd } (\Pi (\Pi i \in \text{ps. } i)) \land a^2 + 3*b^2 = (\Pi (\Pi i \in \text{ps. } i)) \Rightarrow \text{is-cube-form u v} \)

(\Pi \text{p} \text{. p} \text{. int} \) \( \land \text{ odd } (\Pi (\Pi i \in \text{ps. } i)) \Rightarrow \text{is-cube-form u v} \)

by auto

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

by simp

let \( ?w = \text{int} (\Pi (\Pi i \in \text{ps. } i)) \)

let \( ?X = \text{int} (\Pi (\Pi i \in \text{ps. } i)) \)

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

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

have pw: \( ?w = ?p \ast ?X \land \text{odd } ?p \land \text{odd } ?X \)

proof (safe)

have \( (\Pi (\Pi i \in \text{ps. } i)) \) \( = p \ast (\Pi (\Pi i \in \text{ps. } i)) \) by simp

thus \( \text{wpx: } ?w = ?p \ast ?X \) by (auto simp only: of-nat-mult [symmetric])

with \text{ass show even } ?p \Rightarrow \text{False by auto}

from \( \text{wpx: } ?w = ?X \ast ?p \) by simp

with \text{ass show even } ?X \Rightarrow \text{False by simp}

qed

have is-qfN \( ?p 3 \)

proof –
2.5 The case \( N = 3 \)

from \( \text{ass} \) \( \text{have} \) \( a^2+3*b^2 = (\exists p\exists X \cdot 3 \) \( \text{by} \) (simp add: mult.commute)

hence \( \exists p \) dvd \( a^2+3*b^2 \) \( \text{by} \) (simp add: eval-nat-numeral field-simps)

moreover from \( \text{ass} \) \( \text{have} \) prime \( \exists p \) and coprime \( a \) \( \text{by} \) simp-all

moreover from \( \text{pw} \) \( \text{have} \) odd \( \exists p \) \( \text{by} \) simp

ultimately show \( \exists \text{thesis} \) \( \text{by} \) (simp add: qf3-oddprimedivisor)

qed

then obtain \( \alpha \beta \) where alphabeta: \( \exists p = \alpha^2 + 3*\beta^2 \)

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

have \( \alpha \neq 0 \)

proof (rule ccontr, simp)

assume \( \alpha = 0 \) with alphabeta have \( 3 \) dvd \( \exists p \) \( \text{by} \) auto

with \( \text{pw} \) \( \text{have} \) \( w3: \exists d \) dvd \( \exists w \) \( \text{by} \) (simp only: dvd-mult2)

then obtain \( v \) where \( \exists w = 3*v \) \( \text{by} \) (auto simp add: dvd-def)

with \( \text{ass} \) \( \text{have} \) \( vab: 27*v^3 = a^2 + 3*b^2 \) \( \text{by} \) simp

hence \( \alpha^2 = 3*(9*v^3 - b^2) \) \( \text{by} \) auto

hence \( 3 \) dvd \( \alpha^2 \) \( \text{by} \) (unfold dvd-def, blast)

moreover have prime \( 3::\text{int} \) \( \text{by} \) simp

ultimately have \( \exists a3: \exists d \) dvd \( \exists a \) using prime-dvd-power-int[of \( 3::\text{int} \) \( a \)] \( \text{by} \) fastforce

then obtain \( \exists c \) \( \text{where} \) \( c: a = 3*c \) \( \text{by} \) (auto simp add: dvd-def)

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

hence \( b^2 = 3*(3*v^3 - c^2) \) \( \text{by} \) auto

hence \( 3 \) dvd \( b^2 \) \( \text{by} \) (unfold dvd-def, blast)

moreover have prime \( 3::\text{int} \) \( \text{by} \) simp

ultimately have \( \exists 3 \) dvd \( \exists b \) using prime-dvd-power-int[of \( 3::\text{int} \) \( b \)] \( \text{by} \) fastforce

with \( \exists a3: \exists 3 \) dvd gcd \( a \) \( \text{by} \) simp

with \( \text{ass} \) \( \text{show} \) \( False \) \( \text{by} \) simp

qed

moreover from alphabeta \( \text{pw} \) \( \text{have} \)

prime \( (\alpha^2 + 3*\beta^2) \) \( \land \) odd \( (\alpha^2+3*\beta^2) \) \( \land\) \( (3::\text{int} \geq 1 \) \( \text{by} \) auto

ultimately obtain \( \exists c \) \( \exists d \) \( \text{where} \) \( \text{cdp:} \)

\( (\alpha^2+\beta^2) \cdot 3 = \exists c^2+3*d^2 \) \( \land \) \( \text{coprime} \( u \) \( \exists v \) \( \exists (\exists e: a = e*u+e*3*d+v \) \( \land \) \( b = c*v-e*d+u \) \( \land \) \( |e| = 1 \) \( \) \( ) \)

by (rule-tac \( A=\exists w \) \( \text{and} \) \( n=3 \) in qfN-power-div-prime, auto)

then obtain \( \exists u \) \( \exists v \) \( \exists \text{where} \) \( u^2+3*b^2 = (u^2+3*v^2)*(c^2+3*d^2) \)

\( \land \) \( \text{coprime} \( u \) \( \exists v \) \( \land a = c*u+e*3*d+v \) \( \land b = c*v-e*d+u \) \( \land \) \( |e| = 1 \) \( \) \( \) \( \) \( ) \) blast

moreover have is-cube-form \( u \) \( \exists v \)

proof —

have \( \forall X: u^2+3*v^2 = \forall X^3 \)

proof —

from \( \text{ass} \) \( \text{have} \) \( p0: \exists p \neq 0 \) \( \text{by} \) (simp add: prime-int-iff)

from \( \text{pw} \) \( \text{have} \) \( \exists p3*\exists X^3 = \exists p3*3 \) \( \text{by} \) (simp add: power-mult-distrib)

also with \( \text{ass} \) \( \text{have} \) \( \ldots = \exists a^2+3*b^2 \) \( \text{by} \) simp

also with \( \text{we} \) \( \text{have} \) \( \ldots = (u^2+3*v^2)*(c^2+3*d^2) \) \( \text{by} \) auto

also with \( \text{cdp} \) \( \text{alphabeta} \) \( \text{have} \) \( \ldots = \exists p3* (u^2+3*v^2) \) \( \text{by} \) (simp only: ac-simps)

finally have \( \exists p3*(u^2+3*v^2-\exists X^3) = 0 \) \( \text{by} \) auto

with \( p0 \) \( \text{show} \) \( \exists \text{thesis} \) \( \text{by} \) auto

qed

with \( \text{pw} \) \( \text{IH} \) \( \text{we} \) \( \text{show} \) \( \exists \text{thesis} \) \( \text{by} \) simp

qed

moreover have is-cube-form \( c \) \( \exists d \)
2 The quadratic form $x^2 + Ny^2$

proof

have coprime c d
proof (rule coprimeI)
  fix f
  assume f dvd c and f dvd d
  then have f dvd c*v + d*(e*3*v) ∧ f dvd c*v - d*(e*u)
    by simp
  with have f dvd a and f dvd b
    by (auto simp only: ac-simps)
  with ⟨coprime a b⟩ show is-unit f
    by (rule coprime-common-divisor)
  qed
ultimately show is-cube-form a b
by (simp only: cube-form-mult)
qed

lemma qf3-cube-impl-cube-form:
  assumes ass: coprime a b ∧ a^2 + 3*b^2 = w^3 ∧ odd w
  shows is-cube-form a b
proof
  have 0 ≤ w^3 using ass not-sum-power2-lt-zero[of a b]
    zero-le-power2[of b]
  by linarith
  hence 0 < w using ass by auto arith
  define M where M = prime-factorization (nat w)
  from ⟨w > 0⟩ have (∀p∈set-mset M. prime p) ∧ w = int (∏i∈#M. i)
    by (auto dest: qf3-cube-primelist-impl-cube-form)
  with ass show ?thesis
by (auto dest: qf3-cube-primelist-impl-cube-form)
qed

2.6 Existence ($N = 3$)

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

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

lemma Legendre-zmult: [ p > 2; prime p ]
  ⇒ (Legendre (a*b) p) = (Legendre a p)*(Legendre b p)
proof
  assume p2: p > 2 and prp: prime p
  from prp have prp': prime (nat p)
    by simp
  let ?p12 = nat(((p) - 1) div 2)
  let ?Labp = Legendre (a*b) p
  let ?Lap = Legendre a p
  let ?Lbp = Legendre b p
  have h1: ((nat p - 1) div 2) = nat ((p - 1) 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
    by (simp only: power-mult-distrib cong-sym)
  moreover have [?Lap * ?Lbp = a^?p12*b^?p12] (mod p)
2.6 Existence \((N = 3)\)

using euler-criterion[of nat \(p\)] \(p\2 prp' \ h t\) by (simp add: cong-mult)
ultimately have \(\Box L a p \ast \Box L b p = \Box L a b p\) (mod \(p\))
using cong-trans by blast
then obtain \(\n k\) where \(\Box L a b p = (\Box L a p \ast \Box L b p) + p \ast k\)
by (auto simp add: cong-iff-lin-int)
have \(k = 0\)
proof (rule ccontr)
  assume \(k \neq 0\) hence \(|k| = 1 \lor |k| > 1\) by arith
  moreover have \(|k| > 1\)
  with \(p\2\) have \(|k| \ast p > 2\) by auto
  moreover have \(|k| \ast p > 2\) by auto
  moreover have \(|p| = p\) by auto
ultimately have \(|k| \ast p > 2\) by (auto simp only: abs-mult)
moreover have \(|k| \ast p > 2\) by auto
ultimately have \(|k| \ast p = k \ast p\) by auto
ultimately have \(|k| \ast p = k \ast p\) by (auto simp add: Legendre-def)
ultimately have \(|k| \ast p = k \ast p\) by auto
ultimately show \(\Box L a b p = 0 \lor \Box L a b p = -1\)
  by (auto simp add: Legendre-def)
ultimately show False by auto
qed

with \(k\) show \(\Box \)thesis by auto
qed

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

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

**proof** –
  let \(\Box p = 6 \ast m + 1\)
  let \(\Box L = Legendre (-3) \Box p\)
  let \(\Box L 1 = Legendre (-1) \Box p\)
  let \(\Box L 3 = Legendre 3 \Box p\)
  assume \(p\) : prime \(\Box p\)
from \(p\) have \(p'\) : prime (nat \(\Box p\)) by simp
have neg1cube: \((-1 :: int) \ast 3 = -1\) by simp
have \(m1\) : \(m \geq 1\)
proof (rule ccontr)
  assume \(\n m \geq 1\) hence \(m \leq 0\) by simp
  with \(p\) show False by (auto simp add: prime-int-iff)
qed
hence \(p n 3\) : \(\Box p \neq 3\) and \(p 2\) : \(\Box p > 2\) by auto
with \(p\) have \(\Box L = (Legendre (-1) \Box p) \ast (Legendre 3 \Box p)\)
  by (rule-tac a = -1 and b = 3 in Legendre-zmult, auto)
moreover have \([Legendre (-1) \Box p = (-1) \ast nat m] (mod \(\Box p\))\)
proof –
  have \(nat(\Box (p - 1) \ div 2) = (nat \Box p - 1) \ div 2\) by auto
  hence \([\Box L 1 = (-1) \ast (nat(\Box (p - 1) \ div 2))] (mod \(\Box p\))\)
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 have (−1::int) ^3 = (-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-altdef-int 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-altdef-int)
  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 [1 = ?L] (mod ?p) by (auto simp add: cong-sym)
  hence ?p dvd 1 - ?L by (simp only: cong-altdef-sym)
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
Fermat’s last theorem, case $n = 3$

3 Fermat’s last theorem, case $n = 3$

theory Fermat3
imports Quad-Form
begin

context
begin

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

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

private lemma nat-relprime-power-divisors:
  assumes n0: 0 < n and abc: (a::nat)*b = c^n and relprime: coprime a b
  shows \exists k. a = k^n
using assms proof (induct c arbitrary: a b rule: nat-less-induct)
case (1 c)
  show ?case
  proof (cases a > 1)
case False
  hence a = 0 ∨ 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] ded-power-same[of p c n] by blast
moreover have h2: ¬ p dvd b
  using (coprime a b) coprime-common-divisor-nat[of a b p] by auto
hence ¬ (p "n) dvd b using n0 p(1) dvd-power[of n p] gcd-nat.trans by blast
ultimately have (p "n) dvd a
  using 1.prems p(1) prime-elm-dvdpow[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-distr semiring-normalization-rules(18))
  hence a' * b = c' "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] n0 prime-gt-Suc-0-nat
  by simp-all
hence c' < c using ac(2) by simp
ultimately obtain k where a' = k' "n using 1(1) n0 by presburger
hence a = (p * k) "n using ac(1) by (simp add: power-mult-distr)
thus ?thesis by blast
qed

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

private lemma factor-sum-cubes: (x::int)^3 + y^3 = (x+y)*(x^2 - x*y + y^2)
Fermat's last theorem, case \( n = 3 \)

**Private lemma** two-not-abs-cube: \(|x^3| = (2\cdot\text{int}) \implies False\)

**proof**
- **assume** \(|x^3|=2\)
- **hence** \(x^32\cdot\text{|x|}=2\) by (simp add: power-abs)
- **have** \(|x| \geq 0\) by simp
- **moreover**
  - **assume** \(|x|=0\) ∨ \(|x|=1\) ∨ \(|x|=2\)
  - **with** \(x^32\) **have** False by (auto simp add: power-0-left)
- **moreover**
  - **assume** \(|x|>2\)
  - **moreover have** \((0::\text{int}) \leq 2\) and \((0::\text{nat}) < 3\) by auto
  - **ultimately have** \(|x|^3 > 2^3\) by (simp only: power-strict-mono)
  - **with** \(x^32\) **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:
\(\neg (\exists v w. v^3 + w^3 = x^3 \land v \cdot w \cdot x \neq 0 \land \text{even } (x::\text{int}) \land \text{coprime } v w)\)

**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** \((\text{smaller } x)\)
  - **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** \(\exists \alpha \beta \gamma. ?P \alpha \beta \gamma \land \text{nat}|\gamma^3| < \text{nat}|x^3|\)
**proof**
  - **obtain** coprime \(p\) and \(q\) such that \(v = p + q\) and \(w = p - q\)
  - **have** \(vw\text{Odd}: odd\ v \land odd\ w\)
**proof** (rule ccontr, case-tac odd \(v\), simp-all)
  - **assume** \(vc\text{even}: even\ v\)
    - **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** \(2\text{Odd}\ v \land 2\text{Odd}\ w\) by auto
  - **hence** \(2\text{Odd}\ gcd\ v\ w\) 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
Fermat’s last theorem, case \( n = 3 \)

**Proof**

1. **Assume** \( \neg \neg 3 \vdash p \)\(^2\) \( + 3q \)\(^2\)\( \equiv 2 \)\( \ast p \)\(^2\) \( + 3q \)\(^2\)\( \leq 2 \)\( \ast p \)\(^2\) by \( \text{simp} \)

2. With \( \text{vux} \) have \( \text{odd } (x \cdot 3) \) by \( \text{(simp add: add.commute)} \)

3. **Hence** \( \text{odd } x \) by \( \text{simp} \)

4. With \( \text{vux} \) show \( \text{False by auto} \)

**QED**

**Hence** \( \text{even } (v+w) \land \text{even } (v-w) \) by \( \text{simp} \)

5. **Then obtain** \( p \ q \) where \( pq: v+w = 2 \ast p \land v-w = 2 \ast q \)

6. Using \( \text{evenE[of } v+w; \text{ evenE[of } v-w; \text{ by meson} \}

7. **Hence** \( vw: v = p+q \land w = p-q \) by \( \text{auto} \)

8. Show that \( x^3 = (2p)(p^2 + 3q^2) \) and that these factors are

9. — either coprime (first case), or have 3 as g.c.d. (second case)

10. **Have** \( vwpq: v \cdot 3 + w \cdot 3 = (2 \ast p) \ast (p^2 + 3q^2) \)

**Proof**

11. Have \( 2 \ast (v^3 + w^3) = 2 \ast (v+w) \ast (v^2 - v \ast w + w^2) \)

12. By \( \text{(simp only: factor-sum-cubes)} \)

13. Also from \( pq \) have \( \ldots = 4 \ast p \ast (v^2 - v \ast w + w^2) \) by \( \text{auto} \)

14. Also have \( \ldots = p \ast ((v+w)^2 + 3 \ast (v-w)^2) \)

15. By \( \text{(simp add: eval-nat-numeral field-simps)} \)

16. Also with \( pq \) have \( \ldots = p \ast ((2 \ast p)^2 + 3 \ast (2 \ast q)^2) \) by \( \text{simp} \)

17. Also have \( \ldots = 2 \ast (2 \ast p) \ast (p^2 + 3q^2) \) by \( \text{(simp add: power-mult-distrib)} \)

18. **Finally show** \( \text{?thesis by simp} \)

**QED**

**Let** \( ?g = \text{gcd } (2 \ast p) \ast (p^2 + 3 \ast q^2) \)

19. **Have** \( g1: ?g \geq 1 \)

**Proof** (rule \( \text{ccontr} \))

20. Assume \( \neg ?g \geq 1 \)

21. Then have \( ?g < 0 \lor ?g = 0 \) unfolding \( \text{not-le by arith} \)

22. Moreover have \( ?g \geq 0 \) by \( \text{simp} \)

23. Ultimately have \( ?g = 0 \) by \( \text{arith} \)

24. **Hence** \( p = 0 \) by \( \text{simp} \)

25. With \( vwpq \) \( vwx : 0 < \text{nat} | x \cdot 3 | \) show \( \text{False by auto} \)

**QED**

**Have** \( gOdd: \text{odd } ?g \)

26. **Proof** (rule \( \text{ccontr} \))

27. Assume \( \neg \text{odd } ?g \)

28. **Hence** \( \text{2 dvd } p \cdot 2 + 3 \ast q \cdot 2 \) by \( \text{simp} \)

29. **Then obtain** \( k \) where \( k: p \cdot 2 + 3 \ast q \cdot 2 = 2 \ast k \) by \( \text{(auto simp add: dvd-def)} \)

30. **Hence** \( 2 \ast (k - 2 \ast q \cdot 2) = p \cdot 2 - q \cdot 2 \) by \( \text{auto} \)

31. Also have \( \ldots = (p+q) \ast (p-q) \) by \( \text{(simp add: power2-cq-square algebra-simps)} \)

32. **Finally have** \( v \ast w = 2 \ast (k - 2 \ast q \cdot 2) \) using \( vw \) by \( \text{presburger} \)

33. **Hence** \( \text{even } (v \ast w) \) by \( \text{auto} \)

34. **Hence** \( \text{even } (v) \lor \text{even } (w) \) by \( \text{simp} \)

35. With \( vwOdd \) show \( \text{False by simp} \)

**QED**

**Then have** \( \text{even-odd-p-q: even } p \land \text{odd } q \lor \text{odd } p \land \text{even } q \)

36. By \( \text{auto} \)

37. — first case: \( p \) is not a multiple of 3; hence \( 2p \) and \( p^2 + 3q^2 \)

38. — are coprime; hence both are cubes

39. \{ assume \( p3: \neg 3 \vdash p \)

40. Have \( g3: \neg 3 \vdash ?g \)

41. **Proof** (rule \( \text{ccontr} \))

42. **Assume** \( \neg \neg 3 \vdash p \) and \( \neg ?g \) hence \( 3 \vdash 2 \ast p \) by \( \text{simp} \)

43. **Hence** \( \text{even } p \land \neg \text{odd } ?g \)
Fermat's last theorem, case $n = 3$

```
hence $(3 :: int) dvd 2 \land 3 dvd p$
with $p^3$ show False by arith
qed
```

```
from $\langle \text{coprime } v \text{ w} \rangle$ have $pq$-relprime: coprime $p$ $q$
proof (rule coprime-imp-coprime)
  fix $c$
  assume $c$ dvd $p$ and $c$ dvd $q$
  then have $c$ dvd $p + q$ and $c$ dvd $p - q$
    by simp-all
  with vw show $c$ dvd $v$ and $c$ dvd $w$
    by simp-all
qed
```

```
moreover from $\langle \text{coprime } p \text{ q} \rangle$ have coprime $p$ $(q^2)$
by simp
then have factors-relprime: coprime $(2 \ast p) (p^2 + 3 \ast q^2)$
proof (rule coprime-imp-coprime)
  fix $c$
  assume $q2p$: $c$ dvd $2 \ast p$ and $gpq$: $c$ dvd $p^2 + 3 \ast q^2$
  have coprime $2$ $c$
    using $q2p$ gpq even-odd-p-q dvd-trans $[of 2 \ c \ p^2 + 3 \ast q^2]$
    by auto
  with $q2p$ show $c$ dvd $p$
    by (simp add: coprime-dvd-mult-left-iff ac-simps)
then have $c$ dvd $p^2$
  by (simp add: power2-eq-square)
with $gpq$ have $c$ dvd $3 \ast q^2$
  by (simp add: dvd-add-right-iff)
moreover have coprime $3$ $c$
  using $c$ dvd $p$ $p3$ dvd-trans $[of 3 \ c \ p]$ by (auto intro: prime-imp-coprime)
ultimately show $c$ dvd $q^2$
  by (simp add: coprime-dvd-mult-right-iff ac-simps)
```

```
moreover from $vwx$ $vwpq$ have $pxx$: $(2 \ast p) \ast (p^2 + 3 \ast q^2) = x \ast 3$ by auto
ultimately have $\exists \ c. \ 2 \ast p = c \ast 3$ by (simp add: int-relprime-odd-power-divisors)
then obtain $c$ where $c = c \ast 3 = 2 \ast p$ by auto
from $pxx$ factors-relprime have coprime $(p^2 + 3 \ast q^2) (2 \ast p)$
  and $(p^2 + 3 \ast q^2) \ast (2 \ast p) = x \ast 3$ by (auto simp add: ac-simps)
  with $d$ factors-relprime show $d = d \ast 3$ by simp
```

```
have odd $d$
proof (rule ccontr)
  assume $\neg$ odd $d$
  hence even $(d \ast 3)$ by simp
  hence $2$ dvd $d \ast 3$ by simp
moreover have $2$ dvd $2 \ast p$ by (rule dvd-triv-left)
ultimately have $2$ dvd $gcd (2 \ast p) (d \ast 3)$ by simp
  with $d$ factors-relprime show False by simp
```

```
with $d$ $pq$-relprime have coprime $p$ $q$ $\land$ $p^2 + 3 \ast q^2 = d \ast 3$ $\land$ odd $d$
  by simp
```
Fermat’s last theorem, case \( n = 3 \)

\[ a^3 + b^3 = c^3 \]

**Proof**

1. **Case** \( a \in \mathbb{N} \)
   - Assume \( \gcd(a, b) = 1 \)
   - Then \( \gcd(a + b, a^2 + b^2) = 1 \)

2. **Case** \( b \in \mathbb{N} \)
   - Assume \( \gcd(a, b) = 1 \)
   - Then \( \gcd(a + b, a^2 + b^2) = 1 \)

3. **Case** \( a, b, c \in \mathbb{N} \)
   - Assume \( \gcd(a, b, c) = 1 \)
   - Then \( \gcd(a + b + c, a^2 + b^2 + c^2) = 1 \)

4. **Case** \( a, b, c \not\in \mathbb{N} \)
   - Assume \( \gcd(a, b, c) = 1 \)
   - Then \( \gcd(a + b + c, a^2 + b^2 + c^2) = 1 \)

5. **Case** \( a, b, c \not\in \mathbb{N} \)
   - Assume \( \gcd(a, b, c) = 1 \)
   - Then \( \gcd(a + b + c, a^2 + b^2 + c^2) = 1 \)

**Conclusion**

Fermat’s last theorem is true for all \( n \geq 3 \).
\[2\ast a = \gamma^3 \land a - 3\ast b = \alpha^3 \land a + 3\ast b = \beta^3 \text{ by auto}\]
— show this is a (smaller) solution

\[\text{hence } \alpha^3 + \beta^3 = \gamma^3 \text{ by auto}\]

moreover have \(\alpha\ast\beta\ast\gamma \neq 0\)

proof (rule ccontr, safe)

assume \(\alpha \ast \beta \ast \gamma = 0\)

with \(\text{albega}\ \text{ab}\) have \(p=0\) by (auto simp add: power-0-left)

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

qed

moreover have even \(\gamma\)

proof –

have even \((2\ast a)\) by simp

with \(\text{albega}\ \text{have even } (\gamma^3)\) by simp

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

qed

moreover have coprime \(\alpha\ \beta\)

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

fix \(h\)

assume \(\text{ha; } h\ \text{dvd } \alpha\ \text{and } \text{hb; } h\ \text{dvd } \beta\)

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

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

with \(\text{albega}\) show \(h\ \text{dvd } a - 3\ast b\ \land h\ \text{dvd } a + 3\ast b\) by auto

qed

moreover have \(\text{nat}\gamma^3 < \text{nat}\gamma^3\)

proof –

let \(\text{?A} = p^2 + 3\ast q^2\)

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

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

also with \(\text{albega}\) have \(
\gamma^3 \ast((a + 3\ast b)\ast(a - 3\ast b)\ast\text{?A})\) by auto

finally have eq: \(\lvert x^3\rvert = \lvert \gamma^3\rvert \ast \lvert((a + 3\ast b)\ast(a - 3\ast b)\ast\text{?A})\rvert\)

by (auto simp add: abs-mult)

with \((0 < \text{nat}\gamma^3)\) have \((\lvert(a + 3\ast b)\ast(a - 3\ast b)\ast\text{?A}\rvert > 0\) by auto

hence eqpos: \((\lvert(a + 3\ast b)\ast(a - 3\ast b)\rvert > 0\) by auto

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

proof –

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

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

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

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

moreover

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

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

moreover

\{ assume \(\text{A1: } ?A = 1\)

have \(q=0\)

proof (rule ccontr)

assume \(q \neq 0\)

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

hence \(3\ast q^2 > 1\) by arith

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

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

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

qed

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

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

hence \( \text{False} \) by (rule two-not-abs-cube) 

ultimately show \(?\)thesis by auto

qed

ultimately have
\[ |(a+3b)\cdot(a-3b)| < |(a+3b)\cdot(a-3b)| \cdot |A| \]

by (simp only: \( \text{zn} \)-mult-zless-mono2)

with \( eqpos \) have \(|(a+3b)\cdot(a-3b)| \cdot |A| > 1 \) by arith

hence \(|(a+3b)\cdot(a-3b)| \cdot |A| > 1 \) by (auto simp add: \( \text{abs} \)-mult)

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

proof –

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

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

qed

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

by (rule \( \text{zn} \)-mult-zless-mono2)

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

thus \(?\)thesis by arith

qed

ultimately have \(?\)thesis by auto 

moreover

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

— factors are coprime; hence both are cubes

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

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

moreover have \( 3 \) dvd \( 3\cdot(3r^2 + q^2) \) by (rule \( \text{dvd} \)-triv-left)

ultimately have \( pq3 : 3 \) dvd \( p^2 + 3q^2 \) by (simp add: \( \text{power} \)-mult-distrib)

moreover from \( p3 \) have \( 3 \) dvd \( 2p \) by (rule \( \text{dvd} \)-mult)

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

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

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

proof –

from \( g3 \) obtain \( k \) where \( k : \gamma = 3k \) by (auto simp add: \( \text{dvd} \)-def)

have \( k = 1 \)

proof (rule \( \text{ccontr} \))

assume \( k \neq 1 \)

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

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

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

with \( k \) have \( hq : 3h \) dvd \( \gamma \) by (auto simp add: \( \text{mult} \)-dvd-mono)

hence \( 3h \) dvd \( p^2 + 3q^2 \) and \( hp : 3h \) dvd \( 2p \) by auto
then obtain \( s \) where \( s \): \( p \cdot 2 + 3 \cdot q \cdot 2 = (3 \cdot h) \cdot s \)
\( \) by \((\text{auto simp add: dvd-def})\)
with \( r \) have \( \text{rg}: 3 \cdot r \cdot 2 + q \cdot 2 = h \cdot s \) \( \) by \((\text{simp add: power-mult-distrib})\)
from \( hp \) \( r \) have \( 3 \cdot h \cdot d \cdot d \cdot d \cdot 3 \cdot (2 \cdot r) \) \( \) by \(\text{simp}\)
moreover have \((3::\text{int}) \neq 0\) \( \) by \(\text{simp}\)
ultimately have \( h \cdot d \cdot d \cdot 2 \cdot r \) \( \) by \((\text{rule zdvd-mult-cancel})\)
with \( h \) have \( h \cdot d \cdot d \cdot 2 \vee h \cdot d \cdot d \cdot r \)
\( \) by \((\text{auto dest: prime-dvd-multD})\)
moreover have \( - h \cdot d \cdot d \cdot 2 \)
proof \((\text{rule ccontr, simp})\)
assume \( h \cdot d \cdot d \cdot 2 \)
with \( h \) have \( h=2\) using \(\text{zdvd-not-zless[of 2 h]}\) \( \) by \((\text{auto simp: prime-int-iff})\)
with \( hg \) have \( 2 \cdot 3 \cdot d \cdot v \cdot q \) \( \) by \(\text{auto}\)
hence \( 2 \cdot d \cdot v \cdot q \) \( \) by \((\text{rule dvd-mult-left})\)
with \( g\text{Odd}\) show \( \text{False by simp}\)
qed
ultimately have \( \text{hr}: h \cdot d \cdot d \cdot r \) \( \) by \(\text{simp}\)
then obtain \( t \) where \( r = h \cdot t \cdot t \) \( \) by \((\text{auto simp add: dvd-def})\)
hence \( t: r \cdot 2 = h \cdot (h \cdot t \cdot t \cdot 2) \) \( \) by \((\text{auto simp add: power2-eq-square})\)
with \( \text{rg}: h \cdot s = h \cdot (3 \cdot h \cdot t \cdot t \cdot 2) + q \cdot 2 \) \( \) by \(\text{simp}\)
hence \( q \cdot 2 = h \cdot (s - 3 \cdot h \cdot t \cdot t \cdot 2) \) \( \) by \((\text{simp add: right-diff-distrib})\)
hence \( h \cdot d \cdot v \cdot q \cdot 2 \) \( \) by \(\text{simp}\)
with \( h \) have \( h \cdot d \cdot v \cdot q \) \( \) using \(\text{prime-dvd-multD[of h q q]}\)
\( \) by \((\text{simp add: power2-eq-square})\)
with \( hr \) have \( h \cdot d \cdot v \cdot q \cdot r \) \( \) by \(\text{simp}\)
with \( h \cdot q\text{-relprime}\) show \( \text{False by (unfold prime-def, auto)}\)
qed
with \( k \) \( r \) have \( 3 = \gcd (2 \cdot (3 \cdot r)) (3 \cdot (3 \cdot r) \cdot 2 + 3 \cdot q \cdot 2) \) \( \) by \(\text{auto}\)
also have \( \ldots = \gcd (3 \cdot (2 \cdot r)) (3 \cdot (3 \cdot r) \cdot 2 + q \cdot 2) \)
\( \) by \((\text{simp add: power-mult-distrib})\)
also have \( \ldots = 3 \cdot \gcd (2 \cdot r) (3 \cdot r \cdot 2 + q \cdot 2) \) \( \) using \(\text{gcd-mult-distrib-int[of 3]}\) \( \) by \(\text{auto}\)
finally have \( \text{coprime} (2 \cdot r) (3 \cdot r \cdot 2 + q \cdot 2) \)
\( \) by \((\text{auto dest: gcd-eq-1-imp-coprime})\)
moreover have \( \text{coprime} 9 (3 \cdot r \cdot 2 + q \cdot 2) \)
using \((\text{coprime v w})\) proof \((\text{rule coprime-imp-coprime})\)
fix \( h::\text{int}\)
assume \( \neg \text{is-unit } h \)
assume \( h9: h \cdot d \cdot v \cdot 9 \) and \( hrq: h \cdot d \cdot v \cdot d \cdot d \cdot d \cdot 3 \cdot r \cdot 2 + q \cdot 2 \)
have \( \text{prime} (3::\text{int}) \)
\( \) by \(\text{simp}\)
moreover from \( vh \) \( d \cdot d \cdot v \cdot 9 \) have \( h \cdot d \cdot d \cdot 2 \)
\( \) by \(\text{simp}\)
ultimately obtain \( k \) where \( \text{normalize } h = 3 ^ k \)
\( \) by \((\text{rule divides-primepow})\)
with \( \neg \text{is-unit } h \) \( \) have \( \theta < k \)
\( \) by \(\text{simp}\)
with \((\text{normalize } h = 3 ^ k)\) \( \) have \( |h| = 3 \cdot 3 ^ k \cdot (k - 1) \)
\( \) by \((\text{cases k})\) \(\text{simp-all}\)
then have \( 3 \cdot d \cdot d \cdot [h] .. \)
then have \( 3 \cdot d \cdot d \cdot h \)
\( \) by \(\text{simp}\)
then have $3 \mid 3 \cdot r^2 + q^2$
  using $hrq$ by (rule dvd-trans)
then have $3 \mid q^2$
  by presburger
then have $3 \mid q$
  using prime-dvd-power-int [of $3 \cdot q$] by auto
with $p3$ have $3 \mid p + q$ and $3 \mid p - q$
  by simp-all
with $vw$ have $3 \mid v$ and $3 \mid w$
  by simp-all
with $⟨\text{coprime } v \ w⟩$ have is-unit ($3 :: \text{int}$)
  by (rule coprime-common-divisor)
then show $h \mid v$ and $h \mid w$
  by simp-all
qed
ultimately have $\text{coprime } (2 \cdot r \cdot 9) \cdot (3 \cdot r^2 + q^2)$
  by (simp only: coprime-mult-left-iff)
then show ?thesis
  by (simp add: ac-simps)
qed
moreover have $rqx$:
  $(18 \cdot r) \ast (q^2 + 3 \cdot r^2) = x^3$
proof –
from $vwx \ wpq$ have $x^3 = 2 \ast p \ast (p^2 + 3 \cdot q^2)$ by auto
also with $r$ have $\ldots = 2 \ast (3 \cdot r) \ast (9 \cdot r^2 + 3 \cdot q^2)$
  by (auto simp add: power2-eq-square)
finally show ?thesis by auto
qed
ultimately have $\exists c. 18 \cdot r = c^3$
  by (simp add: int-relprime-odd-power-divisors)
then obtain $c1$ where $c1$:
  $c1^3 = 3 \ast (6 \cdot r)$ by auto
hence $3 \mid c1$ and prime ($3 :: \text{int}$) by auto
hence $3 \mid c1$ using prime-dvd-power[of $3$] by fastforce
with $c1$ obtain $c$ where $c$:
  $3 \cdot c^3 = 2 \cdot r$
  by (auto simp add: power-mult-distrib dvd-def)
from $rqx$ factors-relprime have coprime $(q^2 + 3 \cdot r^2) \cdot (18 \cdot r)$
  and $(q^2 + 3 \cdot r^2) \ast (18 \ast r) = x^3$ by (auto simp add: ac-simps)
  hence $\exists d. q^2 + 3 \cdot r^2 = d^3$
    by (simp add: int-relprime-odd-power-divisors)
then obtain $d$ where $d$:
  $q^2 + 3 \cdot r^2 = d^3$ by auto
have odd $d$
proof (rule ccontr)
  assume $\neg$ odd $d$
  hence $2 \mid d \cdot 3$ by simp
  moreover have $2 \mid 2 \ast (9 \ast r)$ by (rule dvd-triv-left)
  ultimately have $2 \mid gcd (2 \ast (9 \ast r)) \cdot (d^3)$ by simp
  with $d$ factors-relprime show False by auto
qed
with $d$ qr-relprime have coprime $q \ r \land q^2 + 3 \cdot r^2 = d^3 \land$ odd $d$
  by simp
hence is-cube-form $q \ r$ by (rule qf3-cube-impl-cube-form)
then obtain $a \ b$ where $q = a^3 - 9 \cdot a \cdot b^2 \land r = 3 \ast a^2 \ast b - 3 \ast b^3$
  by (unfold is-cube-form-def, auto)
hence \( ab \): \( q = a^* (a + 3 * b) * (a - 3 * b) \land r = b^* (a + b) * (a - b) * 3 \)
by (simp add: eval-nat-numeral field-simps)
with \( c \) have abc: \( (2 * b) * (a + b) * (a - b) = c^* 3 \) by auto
from qr-relprime ab have ab-relprime: coprime a b
by (auto intro: coprime-imp-coprime)
then have ab1: coprime \((2 * b) (a + b)\)
proof (rule coprime-imp-coprime)
fix \( h \)
assume h2b: \( h \ dvd 2 + b \) and hab: \( h \ dvd a + b \)
have even \( h \)
proof
assume even \( h \)
then have even \((a + b)\)
using hab by (rule dvd-trans)
then have even \((a + 3 * b)\)
by simp
with \( ab \) have even \( q \) even \( r \)
by auto
then show False
using coprime-common-divisor-int qr-relprime by fastforce
qed
with h2b show \( h \ dvd b \)
using coprime-dvd-mult-right-iff \([of h 2 b]\) by simp
with hab show \( h \ dvd a \)
using dvd-diff \([of h a + b a - b]\) by simp
qed
from ab1 have ab2: coprime \((a + b) (a - b)\)
proof (rule coprime-imp-coprime)
fix \( h \)
assume hab1: \( h \ dvd a + b \) and hab2: \( h \ dvd a - b \)
then show \( h \ dvd 2 + b \) using dvd-diff \([of h a + b a - b]\) by fastforce
qed
from ab1 have ab3: coprime \((a - b) (2 * b)\)
proof (rule coprime-imp-coprime)
fix \( h \)
assume hab: \( h \ dvd a - b \) and h2b: \( h \ dvd 2 + b \)
have \( a - b + 2 * b = a + b \) by simp
then show \( h \ dvd a + b \) using hab h2b dvd-add \([of h a - b 2 + b]\) by presburger
qed
then have \([simp]: even b \longleftrightarrow odd a\)
by simp
have \( \exists k t m. 2 + b = k^* 3 \land a + b = t^* 3 \land m = a - b = m^* 3 \)
using abc ab1 ab2 ab3
int-relprime-odd-power-divisors \([of 3 2 * b (a + b) * (a - b) c]\)
int-relprime-odd-power-divisors \([of 3 a + b (2 * b) * (a - b) c]\)
int-relprime-odd-power-divisors \([of 3 a - b (2 * b) * (a + b) c]\)
by simp (simp add: ac-simps, simp add: algebra-simps)
then obtain \( \alpha \beta \gamma \) where a1: \( 2 + b = \gamma^* 3 \land a - b = \alpha^* 3 \land a + b = \beta^* 3 \)
by auto
then obtain \( \alpha \) where \( \alpha = -\alpha 1 \) by auto
— show this is a (smaller) solution
with a1 have a2: \( \alpha^* 3 = b - a \) by auto
with $a1$ have $\alpha\cdot 3 + \beta\cdot 3 = \gamma\cdot 3$ by auto
moreover have $\alpha\cdot \beta\cdot \gamma \neq 0$
proof (rule ccontr, safe)
  assume $\alpha \cdot \beta \cdot \gamma = 0$
  with $a1$ $a2$ $ab$ have $r=0$ by (auto simp add: power-0-left)
  with $r$ $vwpq$ $vx$ show False by auto
qed
moreover have even $\gamma$
proof
  have even $\gamma$ by simp
  with $a1$ have even $(\gamma\cdot 3)$ by simp
  thus $\exists$thesis by simp
qed
moreover have coprime $\alpha$ $\beta$
using $ab2$ proof (rule coprime-imp-coprime)
  fix $h$
  assume ha: $h$ dvd $\alpha$ and $hb$: $h$ dvd $\beta$
  then have $h$ dvd $\alpha\cdot \alpha\cdot 2$ and $h$ dvd $\beta\cdot \beta\cdot 2$ by simp-all
  then have $h$ dvd $\alpha\cdot \alpha\cdot 2$ and $h$ dvd $\beta\cdot \beta\cdot 2$ by (auto simp only: power-Suc)
  with $a1$ $a2$ have $h$ dvd $b - a$ and $h$ dvd $a + b$ by auto
  then show $h$ dvd $a + b$ and $h$ dvd $a - b$
    by (simp-all add: dvd-diff-commute)
qed
moreover have $nat\{\gamma\cdot 3\} < nat\{x\cdot 3\}$
proof
  let $?A = p\cdot 2 + 3\cdot q\cdot 2$
  from $vwx$ $vwpq$ have $x\cdot 3 = 2*p*?A$ 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 $\ldots = \gamma\cdot 3 * (9*(a+b)*(a-b)*?A)$ by auto
  finally have eq: $|x\cdot 3| = |\gamma\cdot 3| * |9*(a+b)*(a-b)*?A|$
    by (auto simp add: abs-mult)
  with $0 < nat\{x\cdot 3\}$ 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 $|\gamma\cdot 3| > 0$
proof
  from eq have $|\gamma\cdot 3| = 0$ \Longrightarrow $|x\cdot 3|=0$ by auto
  with $0 < nat\{x\cdot 3\}$ show $\exists$thesis by auto
qed
ultimately have $|\gamma\cdot 3| * 1 < |\gamma\cdot 3| * |9*(a+b)*(a-b)*?A|$
  by (rule smult-zless- mono2)
  with eq have $|x\cdot 3| > |\gamma\cdot 3|$ by auto
  thus $\exists$thesis by arith
qed
ultimately have $\exists$thesis by auto 
ultimately show $\exists$thesis by auto
qed
thus $\exists$case by auto
qed

The theorem. Puts equation in requested shape.
theorem fermat-3:

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

shows \(x*y*z = 0\)

proof (rule ccontr)

let \(\bar{g} = \gcd x \ y\)

let \(\bar{c} = z \div \bar{g}\)

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 \(a^3 + b^3 = z^3\) and \(a \cdot b \neq 0\) by auto

— make both sides even

from \(a \cdot b\) have coprime \((a \cdot 3) \ (b \cdot 3)\)

by simp

have \(\exists \ (u \ w) \ w^3 + v^3 = w^3 \land u*v*w \neq 0\) by auto

proof —

let \(\bar{Q} u v w = u^3 + v^3 = w^3 \land u*v*w \neq 0\) by auto

have even \(a \lor even b \lor even ?c\) by simp

proof (rule ccontr)

assume \(\neg(\text{even } a \lor \text{even } b \lor \text{even } ?c)\)

hence aodd: odd \(a\) and \(odd \ b\) and \(odd \ ?c\) by auto

hence even \((c^3 - b^3)\) by simp

moreover from \(abc\) have \(c^3 - b^3 = a^3\) by simp

ultimately have even \((a^3)\) by simp
Fermat's last theorem, case $n = 3$

hence even $(a)$ by simp
with odd show False by simp
qed
moreover
{} assume even $(a)$
then obtain $u \ w \ w$ where $uvwabc: u = -b \ w = ?c \ w = a \ w$ by auto
moreover with $abc$ have $u*v*w \neq 0$ by auto
moreover have $uvw: u^3 + v^3 = w^3$
proof
from $uvwabc$ have $u^3 + v^3 = (1+b)^3 + ?c^3$ by simp
also have $(1)^3^3 + b^3 + ?c^3$ by (simp only: power-mult-distrib)
also have $(1)^3^3 + b^3 + ?c^3$ by auto
also with $abc$ and $uvwabc$ have $\ldots = w^3$ by auto
finally show $\text{thesis by simp}$
qed
moreover have coprime $u \ v$
using $(a^3) (b^3)$: proof (rule coprime-imp-coprime)
fix $h$
assume $hu: h \ dvd u \ and \ h \ dvd v$
with $uvwabc$ have $h \ dvd ?c^2$ by (simp only: dvd-mult2)
with $abc$ have $h \ dvd a^3 + b^3$ using power-Suc[of $?c^3$]
moreover from $hu \ uvwabc$ have $h \ dvd b^2$ by simp
ultimately have $h \ dvd a^3 + b^3$ using power-Suc[of $b^3$]
qed
ultimately have $Q u \ w \ w$ using (even $a$) by simp
hence $\text{thesis by auto}$ }
moreover
{} assume even $b$
then obtain $u \ w \ w$ where $uvwabc: u = -a \ w = ?c \ w = b \ w$
by auto
moreover with $abc$ have $u*v*w \neq 0$ by auto
moreover have $uvw: u^3 + v^3 = w^3$
proof
from $uvwabc$ have $u^3 + v^3 = (1+a)^3 + ?c^3$ by simp
also have $(1)^3 + a^3 + ?c^3$ by (simp only: power-mult-distrib)
also have $(1)^3 + a^3 + ?c^3$ by auto
also with $abc$ and $uvwabc$ have $\ldots = w^3$ by auto
finally show $\text{thesis by simp}$
qed
moreover have coprime $u \ v$
using $(a^3) (b^3)$: proof (rule coprime-imp-coprime)
fix $h$
assume $hu: h \ dvd u \ and \ h \ dvd v$
with $uvwabc$ have $h \ dvd ?c^2$ by (simp only: dvd-mult2)
with $abc$ have $h \ dvd a^3 + b^3$ using power-Suc[of $?c^3$]
moreover from $hu \ uvwabc$ have $h \ dvd a^2$ by simp
ultimately have $h \ dvd a^3 + b^3 - a^3$
using power-Suc[of $a^3$]
moreover have coprime $u \ v$
using $(a^3)$ (b^3): proof (rule coprime-imp-coprime)
fix $h$
assume $hu: h \ dvd u \ and \ h \ dvd v$
with $uvwabc$ have $h \ dvd ?c^2$ by (simp only: dvd-mult2)
with $abc$ have $h \ dvd a^3 + b^3$ using power-Suc[of $?c^3$]
moreover from $hu \ uvwabc$ have $h \ dvd a^2$ by simp
ultimately have $h \ dvd a^3 + b^3 - a^3$
using power-Suc[of $a^3$]
qed
ultimately have \( \exists u v w \) using (even b) by simp
  hence thesis by auto }
moreover
  { assume even ?c
    then obtain u v w where uvwabc: \( u = a \land v = b \land w = ?c \land \) even w
      by auto
    with abc ab have thesis by auto }
ultimately show thesis by auto
qed

hence \( \exists w. \exists u v. u^3 + v^3 = w^3 \land u \neq v \land \) coprime u v
by auto
— show contradiction using the earlier result
thus False by (auto simp only: no-rewritten-fermat3)

end

References


