

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

Roelof Oosterhuis  
University of Groningen

August 21, 2007

## Abstract

This document gives a formal proof, verified by the proof assistant 'Isabelle'<sup>1</sup>, of the cases  $n = 3$  and  $n = 4$  (and all their multiples) of Fermat's Last Theorem: if  $n > 2$  then for all integers  $x, y, z$ :

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

Both proofs only use facts about the integers and are developed along the lines of the standard proofs, like in section 1 and 2 of Harold M. Edwards, *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, New York (etc.): Springer Verlag, 1977.

First, the framework of 'infinite descent' is being formalised and in both proofs there is a central role for the lemma

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

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

We remind the reader that the case  $n = 4$  of FLT, in contrast to the case  $n = 3$ , has already been formalised (in the proof assistant 'Coq')<sup>2</sup>. Moreover it should be mentioned that the parametrisation of the Pythagorean Triples can be found as number 23 on the list of 'top 100 mathematical theorems'.<sup>3</sup> This research is part of a M.Sc. thesis under supervision of Jaap Top and Wim H. Hesselink (RU Groningen). The author wants to thank Clemens Ballarin (TU München) and Freek Wiedijk (RU Nijmegen) for their support. More information: see <http://www.roelofosterhuis.nl/MScthesis.pdf>

---

<sup>1</sup>See <http://isabelle.in.tum.de/>

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

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

## Contents

<b>1</b>	<b>The proof method ‘infinite descent’</b>	<b>3</b>
<b>2</b>	<b>Powers, prime numbers and divisibility</b>	<b>4</b>
2.1	Auxiliary results . . . . .	4
2.2	Parity of integers . . . . .	7
2.3	Powers of natural numbers . . . . .	8
2.4	Powers of integers . . . . .	12
2.5	Facts about small powers of integers . . . . .	16
<b>3</b>	<b>Pythagorean triples and Fermat’s last theorem, case <math>n = 4</math></b>	<b>17</b>
3.1	Parametrisation of Pythagorean triples (over $\mathbb{N}$ and $\mathbb{Z}$ ) . . . . .	18
3.2	Fermat’s last theorem, case $n = 4$ . . . . .	23
<b>4</b>	<b>The quadratic form <math>x^2 + Ny^2</math></b>	<b>29</b>
4.1	Definitions and auxiliary results . . . . .	29
4.2	Basic facts if $N \geq 1$ . . . . .	29
4.3	Multiplication and division . . . . .	30
4.4	Uniqueness ( $N > 1$ ) . . . . .	41
4.5	The case $N = 3$ . . . . .	44
4.6	Existence ( $N = 3$ ) . . . . .	55
<b>5</b>	<b>Fermat’s last theorem, case <math>n = 3</math></b>	<b>58</b>

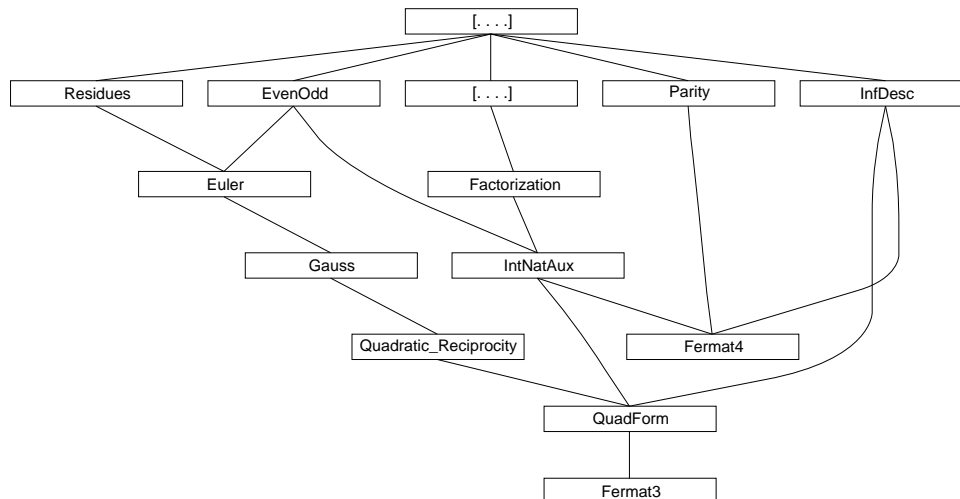


Figure 1: The dependence on existing files in the Isabelle library.

## 1 The proof method ‘infinite descent’

```
theory InfDesc
  imports Main
begin
```

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

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

**lemma** *nat-infinite-descent*:

```
[[ P 0; !!n. n>0 ==> ¬ P n ==> (∃ m::nat. m < n ∧ ¬P m) ]] ==> P n
by (induct n rule: less-induct, case-tac n>0, auto)
```

**lemmas** *infinite-descent*

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

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

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

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

**corollary** *nat-val-infinite-descent*:

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

**proof** –

```
obtain n where n = V x by auto
moreover have !!x. V x = (n::nat) ==> P x
proof (induct n rule: infinite-descent)
  case 0 — i.e.  $V(x) = 0$ 
  with ass0 show P x by auto
next — now  $n > 0$  and  $P(x)$  does not hold for some  $x$  with  $V(x) = n$ 
  case (smaller n)
  then obtain x where vxn:  $V x = n$  and  $V x > 0 \wedge \neg P x$  by auto
  with assn obtain y where  $V y < V x \wedge \neg P y$  by auto
  with vxn obtain m where  $m = V y \wedge m < n \wedge \neg P y$  by auto
  thus ?case by auto
```

**qed**

```
ultimately show P x by auto
```

**qed**

```

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

end

```

## 2 Powers, prime numbers and divisibility

```

theory IntNatAux
  imports
    ~~/src/HOL/NumberTheory/Factorization
    ~~/src/HOL/NumberTheory/EvenOdd
  begin

```

Contains lemmas about divisibility and coprimality of powers, as well as some results about parities and small powers. Most lemmas are developed for the integers as well as for the natural numbers.

### 2.1 Auxiliary results

**lemma** *make-relprime*:

$(a \neq 0 \vee b \neq 0) \implies \exists c d. a = \text{gcd}(a,b)*c \wedge b = \text{gcd}(a,b)*d \wedge \text{gcd}(c,d) = 1$

**proof** –

**assume** *ab0*:  $a \neq 0 \vee b \neq 0$

**let**  $?g = \text{gcd}(a,b)$

**have**  $?g \text{ dvd } a \wedge ?g \text{ dvd } b$  **by** *auto*

**then obtain**  $c d$  **where**  $abcd$ :  $a = ?g*c \wedge b = ?g*d$  **by** (*auto simp add: dvd-def*)

**moreover have**  $\text{gcd}(c,d)=1$

**proof** –

**from**  $abcd$  **have**  $?g*\text{gcd}(c,d)=?g$  **by** (*auto simp add: gcd-mult-distrib2*)

**moreover with**  $ab0$  **have**  $?g \neq 0$  **by** (*simp add: gcd-zero*)

**ultimately show** *?thesis* **by** *simp*

**qed**

**ultimately show** *?thesis* **by** *auto*

**qed**

**lemma** *factor-exists-general*:  $(a::\text{nat}) \neq 0 \implies (\exists ps. \text{primel } ps \wedge \text{prod } ps = a)$

**proof** –

**assume**  $a0$ :  $a \neq 0$

**show** *?thesis*

**proof** (*case-tac a=1*)

**assume**  $a=1$  **hence**  $\text{primel } [] \wedge \text{prod } [] = a$  **by** (*auto simp add: primel-def*)

**thus** *?thesis* **by** *auto*

**next**

**assume**  $a \neq 1$  **with**  $a0$  **have**  $a > \text{Suc } 0$  **by** *auto*

**thus** *?thesis* **by** (*rule factor-exists*)

**qed**

**qed**

**lemma** *make-zrelprime*:  $(a \neq 0 \vee b \neq 0)$

$\implies \exists c d. a = \text{zgcd}(a,b)*c \wedge b = \text{zgcd}(a,b)*d \wedge \text{zgcd}(c,d)=1$

**proof** –

```

assume  $ab0: a \neq 0 \vee b \neq 0$ 
let  $?g = \text{zgcd}(a,b)$ 
have  $?g \text{ dvd } a \wedge ?g \text{ dvd } b$  by auto
then obtain  $c \ d$  where  $abcd: a = ?g*c \wedge b = ?g*d$  by (auto simp add: dvd-def)
moreover have  $\text{zgcd}(c,d) = 1$ 
proof –
  from  $abcd$  have  $?g * \text{zgcd}(c,d) = ?g$ 
    by (auto simp add: zgcd-zmult-distrib2 zgcd-geq-zero)
  moreover with  $ab0$  have  $?g \neq 0$  by (auto simp add: zgcd-def gcd-zero)
  ultimately show  $?thesis$  by simp
qed
ultimately show  $?thesis$  by auto
qed

```

```

lemma int-nat-abs-eq-abs:  $\text{int}(\text{nat}|x::\text{int}|) = |x|$ 
by simp

```

```

lemma prime-impl-zprime-int:  $\text{prime}(a::\text{nat}) \implies \text{zprime}(\text{int } a)$ 
proof –
  assume  $pra: \text{prime } a$ 
  show  $\text{zprime}(\text{int } a)$ 
  proof –
    from  $pra$  have  $agr1: 1 < \text{int } a$  by (unfold prime-def, auto)
    moreover have  $!!m. m \geq 0 \wedge m \text{ dvd } \text{int } a \wedge m \neq \text{int } a \implies m=1$ 
    proof –
      { fix  $m$  assume  $m: m \geq 0 \wedge m \text{ dvd } \text{int } a \wedge m \neq \text{int } a$ 
        then obtain  $k::\text{int}$  where  $k: \text{int } a = m*k$  by (auto simp add: dvd-def)
        from  $m$  have  $\text{int}(\text{nat } m) = m$  by auto
        with  $k$  have  $\text{int } a = (\text{int}(\text{nat } m)) * k$  by simp
        hence  $\text{nat}(\text{int } a) = \text{nat}((\text{int}(\text{nat } m)) * k)$  by simp
        hence  $a = \text{nat}((\text{int}(\text{nat } m)) * k)$  by (simp only: nat-int)
        also have  $\dots = (\text{nat } m) * (\text{nat } k)$  by (simp add: nat-int nat-mult-distrib)
        finally have  $\text{nat } m \text{ dvd } a$  by auto
        with  $pra$  have  $\text{nat } m = a \vee \text{nat } m = 1$  by (auto simp add: prime-def)
        moreover from  $m$  have  $\text{nat } m \neq a$  by auto
        ultimately have  $\text{nat } m = 1$  by auto
        hence  $m = 1$  by arith }
      thus  $!!m. m \geq 0 \wedge m \text{ dvd } \text{int } a \wedge m \neq \text{int } a \implies m=1$  by auto
    }
  qed
  ultimately show  $?thesis$  by (auto simp add: zprime-def)
qed
qed

```

```

lemma zprime-factor-exists:  $(a::\text{int}) > 1 \implies \exists p. \text{zprime } p \wedge p \text{ dvd } a$ 
proof –
  assume  $a1: a > 1$  hence  $a: \text{int}(\text{nat } a) = a$  by (auto simp add: int-nat-eq)
  with  $a1$  have  $\text{nat } a > 1$  by auto
  hence  $\exists l. \text{primel } l \wedge \text{prod } l = \text{nat } a$  by (simp only: factor-exists)
  then obtain  $l$  where  $l: \text{primel } l \wedge \text{prod } l = \text{nat } a$  by (auto)
  show  $?thesis$ 
  proof (cases l)
    case Nil with  $l$  have  $\text{nat } a = 1$  by auto

```

```

with a1 show ?thesis by arith
next
case (Cons p ps)
with l have nat a = p*prod ps and p: prime p by (auto simp add: primel-def)
hence int (nat a) = (int p)*int(prod ps)
  by (auto simp add: int-mult)
with a p have zprime (int p)  $\wedge$  int p dvd a
  by (auto simp add: prime-impl-zprime-int)
thus ?thesis by blast
qed
qed

```

lemma best-division-abs:  $(x::int) > 0 \implies \exists n. 2 * |y - n*x| \leq x$

proof -

assume x0:  $x > 0$

then obtain b where  $b \geq 0 \wedge b < x \wedge [y = b] \pmod{x}$

by (blast dest: zcong-zless-unique)

hence x dvd (y-b) by (simp only: zcong-def)

then obtain m where  $y - b = x*m$  by (auto simp add: dvd-def)

hence m:  $b = y - m*x$  by (simp only: mult-ac)

show ?thesis

proof (cases)

assume  $2*|b| \leq x$

with m show ?thesis by auto

next

assume  $\neg 2*|b| \leq x$

with b have bx:  $2*b > x$  by auto

hence bx1:  $2*(x-b) < x$  by auto

from b have bx2:  $b-x < 0$  by auto

obtain n where  $n = m+1$  by simp

hence  $y - n*x = y - m*x - x$  by (simp only: zadd-zmult-distrib zmult-1)

with m have n:  $y - n*x = b-x$  by simp

with bx2 have pos:  $-y + n*x > 0$  by simp

moreover from n bx1 have  $2*(-y + n*x) < x$  by simp

ultimately have  $2*|y - n*x| < x$  by simp

hence  $2*|y - n*x| \leq x$  by (unfold zabs-def, auto)

thus ?thesis by auto

qed

qed

lemma best-odd-division-abs:  $[(x::int) > 0; x \in zOdd]$

$\implies \exists n. 2 * |y - n*x| < x$

proof -

assume  $x > 0$  and odd:  $x \in zOdd$

then obtain n where  $n: 2 * |y - n*x| \leq x$  by (auto dest: best-division-abs)

moreover have  $x \neq 2 * |y - n*x|$

proof (rule ccontr, clarsimp)

assume  $x = 2*|y - n*x|$

hence  $x \in zEven$  by (unfold zEven-def, auto)

with odd show False by (auto simp only: odd-iff-not-even)

qed

ultimately have  $2*|y - n*x| < x$  by simp

thus *?thesis* by *auto*  
qed

lemma *zprime-2*: *zprime 2*  
  apply (*auto simp add: zprime-def*)  
  apply (*frule zdvd-imp-le, simp*)  
  apply (*auto simp add: order-le-less dvd-def*)  
done

lemma *zgcd1-iff-no-common-primedivisor*:  
  (*zgcd(a,b)=1*) = ( $\neg(\exists p. \text{zprime } p \wedge p \text{ dvd } a \wedge p \text{ dvd } b)$ )  
proof (*rule ccontr, auto*)  
  fix *p* assume *ab*: *zgcd(a,b)=1* and *p dvd a* and *p dvd b* and *p*: *zprime p*  
  hence *p dvd a*  $\wedge$  *p dvd b* by *simp*  
  hence *p dvd zgcd(a,b)* by (*simp add: zgcd-greatest-iff*)  
  with *ab p* show *False* by (*unfold zprime-def, auto*)  
next  
  let *?g* = *zgcd(a,b)*  
  assume *g1*: *?g*  $\neq$  1 and *ps*:  $\forall p. \text{zprime } p \longrightarrow p \text{ dvd } a \longrightarrow \neg p \text{ dvd } b$   
  moreover have *?g*  $\neq$  0  
  proof (*rule ccontr, simp*)  
    assume *?g=0* hence *nat|a|=0*  $\wedge$  *nat|b|=0*  
    by (*unfold zgcd-def, auto simp add: gcd-zero*)  
    hence *a=0*  $\wedge$  *b=0* by *arith*  
    hence *2 dvd a*  $\wedge$  *2 dvd b* by *simp*  
    with *ps* show *False* by (*auto simp add: zprime-2*)  
  qed  
  moreover have *?g*  $\geq$  0 by (*rule zgcd-geq-zero*)  
  ultimately have *?g*  $>$  1 by *auto*  
  then obtain *p* where *zprime p*  $\wedge$  *p dvd ?g*  
    by (*frule-tac a=?g in zprime-factor-exists, auto*)  
  hence *zprime p*  $\wedge$  *p dvd a*  $\wedge$  *p dvd b* by (*simp add: zgcd-greatest-iff*)  
  with *ps* show *False* by *auto*  
qed

lemma *pos-zmult-pos*: *a*  $>$  (*0::int*)  $\implies$  *a\*b*  $>$  0  $\implies$  *b*  $>$  0  
  apply (*case-tac b = 0, auto*)  
  apply (*rule ccontr, subgoal-tac b < 0, auto*)  
  apply (*subgoal-tac a\*b < a\*0, auto dest: zmult-zless-mono2*)  
done

## 2.2 Parity of integers

lemma *power-preserves-even*: *n*  $>$  0  $\implies$  (*x*<sup>*n*</sup>  $\in$  *zEven*) = (*x*  $\in$  *zEven*)  
  apply (*induct n, auto simp add: even-times-either*)  
  apply (*case-tac n $\neq$ 0, auto dest: even-product*)  
done

lemma *power-preserves-odd*: *n*  $>$  0  $\implies$  (*x*<sup>*n*</sup>  $\in$  *zOdd*) = (*x*  $\in$  *zOdd*)  
  apply (*induct n, auto, rule odd-mult-odd-prop, auto*)  
  apply (*case-tac n $\neq$ 0, auto dest: odd-times-odd*)  
done

```

lemma even-plus-odd:  $a \in zEven \implies b \in zOdd \implies a+b \in zOdd$ 
  apply (auto simp add: zEven-def zOdd-def)
  apply (rule-tac x=k+ka in exI, auto)
done

```

```

lemma odd-plus-odd:  $\llbracket x \in zOdd; y \in zOdd \rrbracket \implies x+y \in zEven$ 
  apply (auto simp add: zOdd-def zEven-def)
  apply (rule-tac x=1+k+ka in exI, auto)
done

```

```

lemma odd-plus-odd:  $a \in zOdd \implies b \in zOdd \implies a+b \in zEven$ 
  apply (auto simp add: zEven-def zOdd-def)
  apply (rule-tac x=1+k+ka in exI, auto)
done

```

```

lemma even-plus-odd-prop1:  $a+b \in zOdd \implies a \in zOdd \implies b \in zEven$ 
  by (subgoal-tac a+b - a \in zEven, auto dest: odd-minus-odd)

```

```

lemma even-plus-odd-prop2:  $a+b \in zOdd \implies a \in zEven \implies b \in zOdd$ 
  by (subgoal-tac a+b - a \in zOdd, auto dest: odd-minus-even)

```

### 2.3 Powers of natural numbers

```

lemma gcd-1-power-left-distrib:  $gcd(a,b)=1 \implies gcd(a^n,b)=1$ 
  by (induct n, auto simp add: gcd-mult-cancel)

```

NB: the next (identical) lemma is just added to illustrate the difference between Isar and Isabelle scripting.

```

lemma alternative-gcd-1-power-left-distrib:  $gcd(a,b)=1 \implies gcd(a^n,b)=1$ 
proof -
  assume ab:  $gcd(a,b)=1$ 
  thus  $gcd(a^n,b)=1$ 
  proof (induct n)
    case 0
    show  $gcd(a^0,b)=1$  by auto
  next
    case (Suc n)
    hence  $gcd(a^n,b)=1$  by simp
    with ab have  $gcd(a*a^n,b)=1$  by (simp only: gcd-mult-cancel)
    thus  $gcd(a^{Suc n},b)=1$  by simp
  qed
qed

```

```

lemma gcd-1-power-distrib:  $gcd(a,b) = 1 \implies gcd(a^n,b^n)=1$ 
proof -
  assume  $gcd(a,b)=1$ 
  hence  $gcd(a^n,b)=1$  by (rule gcd-1-power-left-distrib)
  hence  $gcd(b,a^n)=1$  by (simp only: gcd-commute)
  hence  $gcd(b^n,a^n)=1$  by (rule gcd-1-power-left-distrib)
  thus  $gcd(a^n,b^n)=1$  by (simp only: gcd-commute)
qed

```

**lemma** *gcd-power-distrib*:  $\text{gcd}(a,b)^n = \text{gcd}(a^n, b^n)$

**proof** *cases*

**assume**  $a=0 \wedge b=0$

**thus** *?thesis* **by** (*auto simp add: power-0-left*)

**next**

**let**  $?g = \text{gcd}(a,b)$

**assume**  $\neg (a=0 \wedge b=0)$

**hence**  $a \neq 0 \vee b \neq 0$  **by** *simp*

**then obtain**  $c\ d$  **where**  $abcd: a = ?g*c \wedge b = ?g*d \wedge \text{gcd}(c,d)=1$

**by** (*frule-tac a=a in make-relprime, auto*)

**moreover have**  $(?g*c)^n = ?g^n * c^n \wedge (?g*d)^n = ?g^n * d^n$

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

**ultimately have**  $\text{gcd}(a^n, b^n) = ?g^n * \text{gcd}(c^n, d^n)$  **by** (*simp only: gcd-mult-distrib2*)

**moreover from**  $abcd$  **have**  $\text{gcd}(c^n, d^n) = 1$  **by** (*simp only: gcd-1-power-distrib*)

**ultimately show** *?thesis* **by** *simp*

**qed**

Useful lemma: if prime  $p|a^n$  then  $p|a$ .

**lemma** *prime-dvd-power*:  $\llbracket \text{prime } p; p \text{ dvd } a^n \rrbracket \implies p \text{ dvd } a$

**proof** (*induct n*)

**case** 0 **hence**  $\text{prime } p \wedge p = 1$  **by** *auto*

**thus** *?thesis* **by** *auto*

**next case** (*Suc n*) **hence** *IH*:  $\text{prime } p \wedge p \text{ dvd } a^n \implies p \text{ dvd } a$  **by** *auto*

**assume**  $p: \text{prime } p$  **and**  $p \text{ dvd } a^{\text{Suc } n}$

**hence**  $p \text{ dvd } a * a^n$  **by** *simp*

**with**  $p$  **have**  $p \text{ dvd } a \vee p \text{ dvd } a^n$  **by** (*simp add: prime-dvd-mult*)

**with** *IH* **and**  $p$  **show**  $p \text{ dvd } a$  **by** *auto*

**qed**

**lemma** *prime-power-dvd-cancel-right*:

$\llbracket \text{prime } p; \neg p \text{ dvd } b; p^n \text{ dvd } a*b \rrbracket \implies p^n \text{ dvd } a$

**proof** –

**assume**  $p: \text{prime } p$  **and**  $pb: \neg p \text{ dvd } b$

**hence**  $p1: p > 1$  **by** (*simp add: prime-def*)

**have**  $!!a. p^n \text{ dvd } a*b \longrightarrow p^n \text{ dvd } a$

**proof** (*induct n*)

**case** 0 **thus** *?case* **by** *auto*

**next**

**case** (*Suc n*) **hence** *IH*:  $!!a. p^n \text{ dvd } a*b \longrightarrow p^n \text{ dvd } a$  ..

**fix**  $a$  **show**  $p^{\text{Suc } n} \text{ dvd } a*b \longrightarrow p^{\text{Suc } n} \text{ dvd } a$

**proof** (*auto*)

**assume**  $ppnab: p * p^n \text{ dvd } a*b$

**hence**  $p \text{ dvd } a*b$  **by** (*rule dvd-mult-left*)

**with**  $p$  **have**  $p \text{ dvd } a \vee p \text{ dvd } b$  **by** (*rule prime-dvd-mult*)

**with**  $pb$  **have**  $p \text{ dvd } a$  **by** *simp*

**then obtain**  $k$  **where**  $apk: a = p * k$  **by** (*auto simp add: dvd-def*)

**with**  $ppnab$  **have**  $p * p^n \text{ dvd } p * (k*b)$  **by** (*auto simp add: mult-ac*)

**with**  $p1$  **have**  $p^n \text{ dvd } k*b$  **by** (*auto dest: dvd-mult-cancel*)

**with** *IH* **have**  $p^n \text{ dvd } k$  ..

**with**  $apk$  **show**  $p * p^n \text{ dvd } a$  **by** (*simp add: mult-dvd-mono*)

**qed**

qed  
 thus  $p^n \text{ dvd } a*b \implies p^n \text{ dvd } a$  ..  
 qed

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

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

**proof**

assume  $n \neq 0$   
 then obtain  $m$  where  $mn: n = \text{Suc } m$   
 by (*frule-tac n=n in not0-implies-Suc, auto*)  
 assume  $a^n \text{ dvd } b^n$   
 then obtain  $k$  where  $k: b^n = a^n * k$  by (*auto simp add: dvd-def*)  
 moreover have  $\text{gcd}(a^n, (a^n)*k) = (a^n) * \text{gcd}(1,k)$  by (*simp add: gcd-mult-distrib2*)  
 ultimately have  $\text{gcd}(a^n, b^n) = a^n$  by (*auto simp add: gcd-commute gcd-1*)  
 hence  $\text{gcd}(a,b)^n = a^n$  by (*simp add: gcd-power-distrib*)  
 with  $mn$  have  $a = \text{gcd}(a,b)$  by (*rule-tac n=m in power-inject-base, auto*)  
 moreover have  $\text{gcd}(a,b) \text{ dvd } b$  by (*rule gcd-dvd2*)  
 ultimately show  $a \text{ dvd } b$  by *simp*

**next**

assume  $a \text{ dvd } b$   
 then obtain  $k$  where  $b = a * k$  by (*auto simp add: dvd-def*)  
 hence  $b^n = a^n * k^n$  by (*simp only: power-mult-distrib*)  
 thus  $a^n \text{ dvd } b^n$  by *auto*

qed

Theorem: if  $n > 0$  and  $\text{gcd}(a,b) = 1$  and  $ab = c^n$  then  $\exists k : a = k^n$ . Proof uses induction on the number of prime factors of  $c$ .

**theorem** *nat-relprime-power-divisors*:

assumes  $npos: n \neq 0$  and  $abcn: a*b = c^n$  and  $relprime: \text{gcd}(a,b) = 1$   
 shows  $\exists k. a = k^n$

**proof** –

from  $npos$  obtain  $m$  where  $mn: n = \text{Suc } m$   
 by (*frule-tac n=n in not0-implies-Suc, auto*)  
 show ?thesis  
**proof** (*case-tac c=0*)  
 assume  $c=0$  with  $abcn npos mn$  have  $a*b = 0$  by (*auto simp only: power-0-Suc*)  
 hence  $a=0 \vee b=0$  by *auto*  
 moreover  
 { assume  $a=0$  with  $mn npos$  have  $a = 0^n$  by (*auto simp only: power-0-Suc*)  
 hence ?thesis by *blast* }  
 moreover  
 { assume  $b=0$  with  $relprime$  have  $a = 1^n$  by (*auto simp only: gcd-0 power-one*)  
 hence ?thesis by *blast* }  
 ultimately show ?thesis by *blast*

**next**

assume  $c \neq 0$  then obtain  $xs$  where  $xs: \text{primel } xs \wedge \text{prod } xs = c$   
 by (*frule-tac a=c in factor-exists-general, auto*)

moreover have

!! $a b. (\text{primel } xs \wedge a*b = (\text{prod } xs)^n \wedge \text{gcd}(a,b)=1) \implies \exists k. a = k^n$

**proof** (*induct xs*)

case *Nil* hence  $ass: a*b=1^n$  by *simp*

```

hence  $a*b=1$  by (simp only: power-one)
hence  $b=1$  by simp
with ass show  $\exists k. a = k^n$  by auto
next
case (Cons p ps)
hence ass: primel ps  $\wedge$  prime p  $\wedge$   $a*b=p^n*(\text{prod } ps)^n \wedge \text{gcd}(a,b)=1$ 
  and IH: !!a b. primel ps  $\wedge$   $a*b = (\text{prod } ps)^n \wedge \text{gcd}(a,b)=1 \implies \exists k. a = k^n$ 
  by (auto simp add: primel-def power-mult-distrib)
hence pnab: p^n dvd a*b and pn0: p^n ≠ 0 by (auto simp add: prime-def)
moreover
{ assume pa: p dvd a
  have  $\neg p \text{ dvd } b$ 
  proof (rule ccontr, simp)
    assume  $p \text{ dvd } b$ 
    with pa have  $p \text{ dvd } \text{gcd}(a,b)$  by (simp add: gcd-greatest-iff)
    with ass show False by (auto simp add: prime-def)
  }
qed
with ass pnab have  $p^n \text{ dvd } a$  by (simp add: prime-power-dvd-cancel-right)
then obtain A where  $A: a = p^n * A$  by (auto simp add: dvd-def)
with ass pn0 have  $A*b = (\text{prod } ps)^n$  by auto
moreover have  $\text{gcd}(A,b)=1$ 
proof -
  let  $?g = \text{gcd}(A,b)$ 
  have  $?g \text{ dvd } A \wedge ?g \text{ dvd } b$  by (simp add: gcd-greatest)
  with A have  $?g \text{ dvd } a \wedge ?g \text{ dvd } b$  by (simp add: dvd-mult)
  hence  $?g \text{ dvd } \text{gcd}(a,b)$  by (simp only: gcd-greatest)
  with ass show  $?g = 1$  by auto
qed
moreover from IH ass have
   $A*b = (\text{prod } ps)^n \wedge \text{gcd}(A,b)=1 \implies \exists k. A = k^n$  by auto
ultimately have  $\exists k. A = k^n$  by auto
then obtain k where  $A = k^n$  by auto
with A have  $a = (p*k)^n$  by (auto simp add: power-mult-distrib)
hence  $\exists k. a = k^n$  by blast }
moreover
{ assume  $\neg p \text{ dvd } a$ 
  moreover from ass pnab have  $p^n \text{ dvd } b*a \wedge \text{prime } p$ 
    by (auto simp only: mult-ac)
  ultimately have  $p^n \text{ dvd } b$  by (simp add: prime-power-dvd-cancel-right)
  then obtain B where  $B: b = p^n * B$  by (auto simp add: dvd-def)
  with ass pn0 have  $a*B = (\text{prod } ps)^n$  by auto
  moreover have  $\text{gcd}(a,B)=1$ 
  proof -
    let  $?g = \text{gcd}(a,B)$ 
    have  $?g \text{ dvd } a \wedge ?g \text{ dvd } B$  by (simp add: gcd-greatest)
    with B have  $?g \text{ dvd } a \wedge ?g \text{ dvd } b$  by (simp add: dvd-mult)
    hence  $?g \text{ dvd } \text{gcd}(a,b)$  by (simp only: gcd-greatest)
    with ass show  $?g = 1$  by auto
  }
qed
moreover from IH ass have
   $a*B = (\text{prod } ps)^n \wedge \text{gcd}(a,B)=1 \implies \exists k. a = k^n$  by auto
ultimately have  $\exists k. a = k^n$  by auto }

```

```

    ultimately show  $\exists k. a = k^n$  by auto
  qed
  moreover from abcn relprime have  $\text{gcd}(a,b)=1 \wedge a*b=c^n$  by simp
  ultimately show ?thesis by auto
  qed
  qed

```

## 2.4 Powers of integers

Now turn to the case of integers. This lemma is based on its equivalent for the natural numbers.

**corollary** *int-relprime-power-divisors*:

assumes *abcn*:  $a*b = c^n$  and *n*:  $n > 1$  and *relprime*:  $\text{zgcd}(a,b) = 1$   
 shows  $\exists k. |a| = k^n$

**proof** –

```

  let ?a1 = nat|a|
  let ?b1 = nat|b|
  let ?c1 = nat|c|
  from relprime have absrelprime:  $\text{gcd}(\text{?a1}, \text{?b1})=1$  by (auto simp only: zgcd-def)
  have  $|a*b| = |a|*|b|$  by (simp add: abs-mult)
  with abcn have  $|c|^n = |a|*|b|$  by (simp add: power-abs)
  hence  $\text{int}(\text{?c1}^n) = \text{int}(\text{?a1}*\text{?b1})$  by (simp only: int-nat-abs-eq-abs int-mult int-power)
  hence  $\text{?a1}*\text{?b1} = \text{?c1}^n$  by (simp only: int-int-eq)
  with absrelprime and n have  $\exists k. \text{?a1} = k^n$  by (simp only: nat-relprime-power-divisors)
  then obtain k::nat where alpha:  $\text{?a1} = k^n$  by auto
  moreover have  $\text{int } \text{?a1} = |a|$  by (simp add: int-nat-eq)
  ultimately have  $|a| = \text{int}(k^n)$  by simp
  hence  $|a| = \text{int}(k)^n$  by (simp only: int-power)
  thus ?thesis by auto

```

qed

**corollary** *int-triple-relprime-power-divisors*:

$\llbracket a*b*c = d^n; n > 1; \text{zgcd}(a,b)=1; \text{zgcd}(b,c)=1; \text{zgcd}(c,a)=1 \rrbracket$   
 $\implies \exists k l m. |a| = k^n \wedge |b| = l^n \wedge |c| = m^n$

**proof** –

```

  assume abcd:  $a*b*c = d^n$  and n1:  $n > 1$ 
  and ab:  $\text{zgcd}(a,b)=1$  and bc:  $\text{zgcd}(b,c)=1$  and ca:  $\text{zgcd}(c,a)=1$ 
  hence ba:  $\text{zgcd}(b,a)=1$  and cb:  $\text{zgcd}(c,b)=1$  and ac:  $\text{zgcd}(a,c)=1$ 
  by (auto simp only: zgcd-commute)
  from ba ca have  $\text{zgcd}(b*c,a)=1$  by (simp only: zgcd-zmult-cancel)
  with abcd have  $a*(b*c) = d^n \wedge \text{zgcd}(a,b*c)=1$  by (simp add: zgcd-commute)
  with n1 have k:  $\exists k. |a| = k^n$  by (auto dest: int-relprime-power-divisors)
  from ab cb have  $\text{zgcd}(a*c,b)=1$  by (simp only: zgcd-zmult-cancel)
  with abcd have  $b*(a*c) = d^n \wedge \text{zgcd}(b,a*c)=1$ 
  by (simp add: zgcd-commute mult-ac)
  with n1 have l:  $\exists l. |b| = l^n$  by (auto dest: int-relprime-power-divisors)
  from ac bc have  $\text{zgcd}(a*b,c)=1$  by (simp only: zgcd-zmult-cancel)
  with abcd have  $c*(a*b) = d^n \wedge \text{zgcd}(c,a*b)=1$ 
  by (simp add: zgcd-commute mult-ac)
  with n1 have m:  $\exists m. |c| = m^n$  by (auto dest: int-relprime-power-divisors)
  from k l m show ?thesis by auto

```

qed

**lemma** *neg-odd-power*:  $\llbracket x \in zOdd; x \geq 0 \rrbracket \implies (-a::int)^{\wedge(nat\ x)} = -(a^{\wedge(nat\ x)})$

**proof** –

assume  $x \in zOdd$  and  $0 \leq x$

hence  $-(a^{\wedge(nat\ x)}) = (-1)^{\wedge(nat\ x)} * a^{\wedge(nat\ x)}$  by (*simp add: neg-one-odd-power*)

also have  $\dots = (-1*a)^{\wedge(nat\ x)}$  by (*simp only: power-mult-distrib*)

finally show *?thesis* by *simp*

qed

**lemma** *neg-even-power*:  $\llbracket x \in zEven; x \geq 0 \rrbracket \implies (-a::int)^{\wedge(nat\ x)} = a^{\wedge(nat\ x)}$

**proof** –

assume  $x \in zEven$  and  $x \geq 0$

hence  $a^{\wedge(nat\ x)} = (-1)^{\wedge(nat\ x)} * a^{\wedge(nat\ x)}$  by (*simp add: neg-one-even-power*)

also have  $\dots = (-1*a)^{\wedge(nat\ x)}$  by (*simp only: power-mult-distrib*)

finally show *?thesis* by *simp*

qed

**corollary** *int-relprime-odd-power-divisors*:

$\llbracket a*b = c^{\wedge(nat\ x)}; nat\ x > 1; x \in zOdd; zgcd(a,b) = 1 \rrbracket \implies \exists k. a = k^{\wedge(nat\ x)}$

**proof** –

assume  $a*b = c^{\wedge(nat\ x)}$  and  $x1: nat\ x > 1$  and *odd*:  $x \in zOdd$  and  $zgcd(a,b)=1$

hence  $\exists k. |a| = k^{\wedge(nat\ x)}$  by (*simp only: int-relprime-power-divisors*)

then obtain  $k$  where  $k: |a| = k^{\wedge(nat\ x)}$  by *blast*

{ assume  $a \neq k^{\wedge(nat\ x)}$

with  $k$  have  $a = -(k^{\wedge(nat\ x)})$  by *arith*

with  $x1$  *odd* have  $a = (-k)^{\wedge(nat\ x)}$  by (*simp add: neg-odd-power*) }

thus *?thesis* by *blast*

qed

**corollary** *int-triple-relprime-odd-power-divisors*:

$\llbracket a*b*c = d^{\wedge(nat\ x)}; nat\ x > 1; x \in zOdd; zgcd(a,b)=1; zgcd(b,c)=1; zgcd(c,a)=1 \rrbracket$

$\implies \exists k\ l\ m. a = k^{\wedge(nat\ x)} \wedge b = l^{\wedge(nat\ x)} \wedge c = m^{\wedge(nat\ x)}$

**proof** –

assume *abcd*:  $a*b*c = d^{\wedge(nat\ x)}$  and  $x1: nat\ x > 1$  and *odd*:  $x \in zOdd$

and *ab*:  $zgcd(a,b)=1$  and *bc*:  $zgcd(b,c)=1$  and *ca*:  $zgcd(c,a)=1$

hence *ba*:  $zgcd(b,a)=1$  and *cb*:  $zgcd(c,b)=1$  and *ac*:  $zgcd(a,c)=1$

by (*auto simp only: zgcd-commute*)

{ from *ba ca* have  $zgcd(b*c,a)=1$  by (*simp only: zgcd-zmult-cancel*)

with *abcd* have  $a*(b*c) = d^{\wedge(nat\ x)} \wedge zgcd(a,b*c)=1$

by (*simp add: zgcd-commute*)

with  $x1$  *odd* have  $\exists k. a = k^{\wedge(nat\ x)}$

by (*auto dest: int-relprime-odd-power-divisors*) }

moreover

{ from *ab cb* have  $zgcd(a*c,b)=1$  by (*simp only: zgcd-zmult-cancel*)

with *abcd* have  $b*(a*c) = d^{\wedge(nat\ x)} \wedge zgcd(b,a*c)=1$

by (*simp add: zgcd-commute mult-ac*)

with  $x1$  *odd* have  $\exists l. b = l^{\wedge(nat\ x)}$

by (*auto dest: int-relprime-odd-power-divisors*) }

moreover

{ from *ac bc* have  $zgcd(a*b,c)=1$  by (*simp only: zgcd-zmult-cancel*)

with *abcd* have  $c*(a*b) = d^{\wedge(nat\ x)} \wedge zgcd(c,a*b)=1$

```

    by (simp add: zgcd-commute mult-ac)
  with x1 odd have m:  $\exists m. c = m^{\wedge}(\text{nat } x)$ 
    by (auto dest: int-relprime-odd-power-divisors) }
  ultimately show ?thesis by auto
qed

```

```

lemma zgcd-1-power-left-distrib:  $\text{zgcd}(a,b)=1 \implies \text{zgcd}(a^{\wedge}n,b)=1$ 
  by (induct n, auto simp add: zgcd-zmult-cancel)

```

```

lemma zgcd-1-power-distrib:  $\text{zgcd}(a,b) = 1 \implies \text{zgcd}(a^{\wedge}n,b^{\wedge}n)=1$ 
proof -
  assume zgcd(a,b)=1
  hence zgcd(a^{\wedge}n,b)=1 by (rule zgcd-1-power-left-distrib)
  hence zgcd(b,a^{\wedge}n)=1 by (simp only: zgcd-commute)
  hence zgcd(b^{\wedge}n,a^{\wedge}n)=1 by (rule zgcd-1-power-left-distrib)
  thus zgcd(a^{\wedge}n,b^{\wedge}n)=1 by (simp only: zgcd-commute)
qed

```

```

lemma zgcd-power-distrib:  $\text{zgcd}(a,b)^{\wedge}n = \text{zgcd}(a^{\wedge}n,b^{\wedge}n)$ 

```

```

proof cases
  assume a=0  $\wedge$  b=0
  thus ?thesis by (auto simp add: power-0-left)
next
  let ?g = zgcd(a,b)
  assume  $\neg (a=0 \wedge b=0)$ 
  hence ab0:  $a \neq 0 \vee b \neq 0$  by simp
  hence non0:  $\text{zgcd}(a,b) \neq 0 \wedge \text{zgcd}(a^{\wedge}n,b^{\wedge}n) \neq 0$ 
    by (auto simp add: zgcd-def gcd-zero power-eq-0-iff)
  moreover have  $\text{zgcd}(a,b) \geq 0 \wedge \text{zgcd}(a^{\wedge}n,b^{\wedge}n) \geq 0$  by (simp add: zgcd-geq-zero)
  ultimately have  $\text{zgcd}(a,b)^{\wedge}n > 0 \wedge \text{zgcd}(a^{\wedge}n,b^{\wedge}n) > 0$ 
    by (auto simp add: zero-less-power)
  moreover from ab0 obtain c d where abcd:  $a = ?g*c \wedge b = ?g*d \wedge \text{zgcd}(c,d)=1$ 
    by (frule-tac a=a in make-zrelprime, auto)
  moreover have  $(?g*c)^{\wedge}n = ?g^{\wedge}n * c^{\wedge}n \wedge (?g*d)^{\wedge}n = ?g^{\wedge}n * d^{\wedge}n$ 
    by (simp add: power-mult-distrib)
  ultimately have gabcdn:  $\text{zgcd}(a^{\wedge}n,b^{\wedge}n) = ?g^{\wedge}n * \text{zgcd}(c^{\wedge}n,d^{\wedge}n)$ 
    by (auto simp add: zgcd-zmult-distrib2)
  moreover from abcd have  $\text{zgcd}(c^{\wedge}n,d^{\wedge}n) = 1$  by (simp only: zgcd-1-power-distrib)
  ultimately show ?thesis by auto
qed

```

```

lemma zprime-zdvd-zmult-general:  $\llbracket \text{zprime } p; p \text{ dvd } m*n \rrbracket \implies p \text{ dvd } m \vee p \text{ dvd } n$ 
  apply (case-tac  $m \geq 0$ , simp only: zprime-zdvd-zmult)
  apply (subgoal-tac  $-m \geq 0 \wedge p \text{ dvd } (-m)*n$ , subgoal-tac  $p \text{ dvd } -m \vee p \text{ dvd } n$ )
  prefer 2
  apply (rule-tac  $m=-m$  in zprime-zdvd-zmult, auto)
done

```

```

lemma zprime-zdvd-power:  $\llbracket \text{zprime } p; p \text{ dvd } a^{\wedge}n \rrbracket \implies p \text{ dvd } a$ 
  apply (induct n, auto)
  prefer 2
  apply (frule-tac  $m=a$  and  $n=a^{\wedge}n$  in zprime-zdvd-zmult-general)

```

**apply** (*auto*, *simp add: zprime-def zdvd-not-zless*)  
**done**

**lemma** *zpower-zdvd-mono*:  $n \neq 0 \implies (a^{\hat{n}} \text{ dvd } b^{\hat{n}}) = (a \text{ dvd } (b::\text{int}))$

**proof**

**assume**  $n \neq 0$

**then obtain**  $m$  **where**  $mn: n = \text{Suc } m$

**by** (*frule-tac n=n in not0-implies-Suc, auto*)

**assume**  $a^{\hat{n}} \text{ dvd } b^{\hat{n}}$

**then obtain**  $k$  **where**  $k: b^{\hat{n}} = a^{\hat{n}} * k$  **by** (*auto simp add: dvd-def*)

**moreover have**  $\text{zgcd}(a^{\hat{n}*1}, a^{\hat{n}*k}) = |a^{\hat{n}}| * \text{zgcd}(1, k)$

**by** (*rule-tac k=a^{\hat{n}} in zgcd-zmult-distrib2-abs*)

**ultimately have**  $\text{zgcd}(a^{\hat{n}}, b^{\hat{n}}) = |a^{\hat{n}}|$

**by** (*auto simp add: zgcd-commute zgcd-1*)

**hence**  $\text{zgcd}(a, b)^{\hat{n}} = |a|^{\hat{n}} \wedge \text{zgcd}(a, b) \geq 0 \wedge |a| \geq 0$

**by** (*simp add: zgcd-power-distrib power-abs zgcd-geq-zero*)

**with**  $mn$  **have**  $|a| = \text{zgcd}(a, b)$  **by** (*rule-tac n=m in power-inject-base, auto*)

**moreover have**  $\text{zgcd}(a, b) \text{ dvd } b$  **by** (*rule-tac m=a in zgcd-zdvd2*)

**ultimately have**  $|a| \text{ dvd } b$  **by** *simp*

**thus**  $a \text{ dvd } b$  **by** (*simp add: zdvd-abs1*)

**next**

**assume**  $a \text{ dvd } b$

**then obtain**  $k$  **where**  $k: b = a * k$  **by** (*auto simp add: dvd-def*)

**hence**  $b^{\hat{n}} = a^{\hat{n}} * k^{\hat{n}}$  **by** (*simp only: power-mult-distrib*)

**thus**  $a^{\hat{n}} \text{ dvd } b^{\hat{n}}$  **by** *auto*

**qed**

**lemma** *zprime-power-zdvd-cancel-right*:

$\llbracket \text{zprime } p; \neg p \text{ dvd } b; p^{\hat{n}} \text{ dvd } a*b \rrbracket \implies p^{\hat{n}} \text{ dvd } a$

**proof** –

**assume**  $p: \text{zprime } p$  **and**  $pb: \neg p \text{ dvd } b$

**hence**  $p1: p > 1$  **by** (*simp add: zprime-def*)

**have**  $!!a. p^{\hat{n}} \text{ dvd } a*b \longrightarrow p^{\hat{n}} \text{ dvd } a$

**proof** (*induct n*)

**case**  $0$  **thus** *?case* **by** *auto*

**next**

**case** (*Suc n*) **hence** *IH*:  $!!a. p^{\hat{n}} \text{ dvd } a*b \longrightarrow p^{\hat{n}} \text{ dvd } a$  **..**

**fix**  $a$  **show**  $p^{\widehat{\text{Suc } n}} \text{ dvd } a*b \longrightarrow p^{\widehat{\text{Suc } n}} \text{ dvd } a$

**proof** (*auto*)

**assume**  $ppnab: p*p^{\hat{n}} \text{ dvd } a*b$

**hence**  $p \text{ dvd } a*b$  **by** (*auto simp add: dvd-def mult-assoc*)

**with**  $p$  **have**  $p \text{ dvd } a \vee p \text{ dvd } b$  **by** (*rule zprime-zdvd-zmult-general*)

**with**  $pb$  **have**  $p \text{ dvd } a$  **by** *simp*

**then obtain**  $k$  **where**  $apk: a = p*k$  **by** (*auto simp add: dvd-def*)

**with**  $ppnab$  **have**  $p*p^{\hat{n}} \text{ dvd } p*(k*b)$  **by** (*auto simp add: mult-ac*)

**with**  $p1$  **have**  $p^{\hat{n}} \text{ dvd } k*b$  **by** (*auto dest: zdvd-mult-cancel*)

**with** *IH* **have**  $p^{\hat{n}} \text{ dvd } k$  **..**

**with**  $apk$  **show**  $p*p^{\hat{n}} \text{ dvd } a$  **by** (*simp add: zdvd-zmult-mono*)

**qed**

**qed**

**thus**  $p^{\hat{n}} \text{ dvd } a*b \implies p^{\hat{n}} \text{ dvd } a$  **..**

**qed**

```

lemma zprime-power-zdvd-cancel-left:
  [[ zprime p; ¬ p dvd a; p ^ n dvd a*b ]] ==> p ^ n dvd b
  apply (subgoal-tac p ^ n dvd b*a)
  apply (auto dest: zprime-power-zdvd-cancel-right)
  apply (simp add: mult-ac)
done

```

## 2.5 Facts about small powers of integers

```

lemma zadd-power2: ((a::int)+b) ^ 2 = a ^ 2 + 2*a*b + b ^ 2
  by (simp add: nat-number ring-simps)

```

```

lemma zdiff-power2: ((a::int)-b) ^ 2 = a ^ 2 - 2*a*b + b ^ 2
  by (simp add: nat-number ring-simps)

```

```

lemma zspecial-product: ((a::int) + b) * (a - b) = a ^ 2 - b ^ 2
  by (simp add: nat-number ring-simps)

```

```

lemma abs-power2-distrib: |a ^ 2| = |a::int| ^ 2
  by (simp add: power2-eq-square abs-mult)

```

```

lemma power2-eq-iff-abs-eq: ((a::int) ^ 2 = b ^ 2) = (|a| = |b|)

```

**proof**

```

  assume a ^ 2 = b ^ 2
  hence (a+b)*(a-b) = 0 by (simp add: zspecial-product)
  hence a=b ∨ a=-b by auto
  thus |a| = |b| by auto

```

**next**

```

  assume |a| = |b|
  hence |a| ^ 2 = |b| ^ 2 by simp
  thus a ^ 2 = b ^ 2 by (simp only: power2-abs)

```

**qed**

```

lemma power2-eq1-iff: (a::int) ^ 2 = 1 ==> |a|=1
  by (auto simp add: zmult-eq-1-iff power2-eq-square abs-mult)

```

```

lemma zadd-power3: ((a::int)+b) ^ 3 = a ^ 3 + 3*a ^ 2*b + 3*a*b ^ 2 + b ^ 3
  by (simp add: nat-number ring-simps)

```

```

lemma zdiff-power3: ((a::int)-b) ^ 3 = a ^ 3 - 3*a ^ 2*b + 3*a*b ^ 2 - b ^ 3
  by (simp add: nat-number ring-simps)

```

```

lemma power3-minus: (-a::int) ^ 3 = -(a ^ 3)

```

**proof** –

```

  have (3::int) ∈ zOdd ∧ (3::int) ≥ 0 by (unfold zOdd-def, auto)
  hence (-a) ^ (nat 3) = -(a ^ (nat 3)) by (simp only: neg-odd-power)
  thus ?thesis by simp

```

**qed**

```

lemma abs-power3-distrib: |(x::int) ^ 3| = |x| ^ 3
  by (simp add: nat-number ring-simps abs-mult)

```

```

lemma cube-square:  $(a::int)*a^2 = a^3$ 
  by (simp add: nat-number ring-simps)

lemma quartic-square-square:  $(x^2)^2 = (x::int)^4$ 
  by (simp add: nat-number ring-simps)

lemma power2-ge-self:  $x^2 \geq (x::int)$ 
proof (cases)
  assume nonpos:  $x \leq 0$ 
  have  $0 \leq x^2$  by (rule zero-le-power2)
  with nonpos show ?thesis by (rule zle-trans)
next
  assume  $\neg x \leq 0$  hence x1:  $x \geq 1$  by simp
  thus ?thesis
  proof (cases)
    assume  $x = 1$ 
    thus ?thesis by simp
  next
    assume  $\neg x = 1$  with x1 have x2:  $1 < x$  by simp
    hence  $0 < x$  by simp
    with x2 have  $x*1 < x*x$  by (rule zmult-zless-mono2)
    thus ?thesis by (simp only: power2-eq-square)
  qed
qed
end

```

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

```

theory Fermat4
  imports InfDesc IntNatAux Parity
begin

```

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

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

```

lemma even-eq-two-dvd: even ( $r::nat$ ) =  $(2 \text{ dvd } r)$ 
  apply safe
  apply (simp only: even-nat-equiv-def2, arith)
  apply (auto simp add: even-def dvd-eq-mod-eq-0)
done

```

```

lemma nat-power2-add:  $((a::nat)+b)^2 = a^2 + b^2 + 2*a*b$ 
proof -
  have  $(a+b)^2 = (a+b)*(a+b)$  by (rule power2-eq-square)
  also have  $\dots = a^2 + 2*(a*b) + b^2$ 
    by (simp only: add-mult-distrib add-mult-distrib2 mult-commute power2-eq-square)
  finally show ?thesis by simp

```

qed

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

**proof** –

**assume** *a-ge-b*:  $a \geq b$

**hence** *a2-ge-b2*:  $a^2 \geq b^2$  **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-distrib*)

**also have**  $\dots = a*b + a^2 + (b^2 - b^2) - 2*a*b$

**by** (*simp add: diff-mult-distrib2 power2-eq-square*)

**also with** *a2-ge-b2* **have**  $\dots = a*b + (a^2 - b^2) + b^2 - 2*a*b$  **by** *simp*

**also with** *ab-ge-b2* **have**  $\dots = (a*b - b^2) + a^2 + b^2 - 2*a*b$  **by** *auto*

**also have**  $\dots = b*(a-b) + a^2 + b^2 - 2*a*b$

**by** (*simp only: diff-mult-distrib2 power2-eq-square mult-commute*)

**finally show** *?thesis* **by** *arith*

qed

**lemma** *nat-power-le-imp-le-base*:  $\llbracket n \neq 0; a^n \leq b^n \rrbracket \implies (a::nat) \leq b$

**proof** –

**assume**  $n \neq 0$  **and** *ab*:  $a^n \leq b^n$

**then obtain** *m* **where**  $n = \text{Suc } m$  **by** (*frule-tac n=n in not0-implies-Suc, auto*)

**with** *ab* **have**  $a \geq 0$  **and**  $a^{\text{Suc } m} \leq b^{\text{Suc } m}$  **and**  $b \geq 0$  **by** *auto*

**thus** *?thesis* **by** (*rule-tac n=m in power-le-imp-le-base*)

qed

**lemma** *nat-power-inject-base*:  $\llbracket n \neq 0; a^n = b^n \rrbracket \implies (a::nat) = b$

**proof** –

**assume**  $n \neq 0$  **and** *ab*:  $a^n = b^n$

**then obtain** *m* **where**  $n = \text{Suc } m$  **by** (*frule-tac n=n in not0-implies-Suc, auto*)

**with** *ab* **have**  $a^{\text{Suc } m} = b^{\text{Suc } m}$  **and**  $a \geq 0$  **and**  $b \geq 0$  **by** *auto*

**thus** *?thesis* **by** (*rule power-inject-base*)

qed

### 3.1 Parametrisation of Pythagorean triples (over $\mathbb{N}$ and $\mathbb{Z}$ )

**theorem** *nat-euclid-pyth-triples*:

**assumes** *abc*:  $a^2 + b^2 = c^2$  **and** *ab-relprime*:  $\text{gcd}(a,b)=1$  **and** *aodd*: *odd a*

**shows**  $\exists p\ q. a = p^2 - q^2 \wedge b = 2*p*q \wedge c = p^2 + q^2 \wedge \text{gcd}(p,q)=1$

**proof** –

**have** *two0*:  $(2::nat) \neq 0$  **by** *simp*

**from** *abc* **have** *a2cb*:  $a^2 = c^2 - b^2$  **by** *arith*

  — factor  $a^2$  in coprime factors  $(c-b)$  and  $(c+b)$ ; hence both are squares

**have** *a2factor*:  $a^2 = (c-b)*(c+b)$

**proof** –

**have**  $c*b - c*b = 0$  **by** *simp*

**with** *a2cb* **have**  $a^2 = c*c + c*b - c*b - b*b$  **by** (*simp add: power2-eq-square*)

**also have**  $\dots = c*(c+b) - b*(c+b)$

**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  $\neg a \neq 0$  hence  $a = 0$  by simp
  with aodd have 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 b2-le-c2:  $b^2 \leq c^2$  by (simp add: power-mono)
have bc-relprime:  $\gcd(b,c) = 1$ 
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 only: gcd-power-distrib)
  with cancelb2 have ?g^2 =  $\gcd(b^2, c^2 - b^2 + b^2)$  by simp
  hence ?g^2 =  $\gcd(b^2, c^2 - b^2)$  by simp
  with a2cb have ?g^2 dvd  $a^2$  by (simp only: gcd-dvd2)
  hence ?g dvd  $a \wedge ?g$  dvd  $b$  by (simp add: nat-power-dvd-mono gcd-dvd1)
  hence ?g dvd  $\gcd(a,b)$  by (simp only: gcd-greatest)
  with ab-relprime show ?thesis by auto
qed
have p2: prime 2 by (rule two-is-prime)
have factors-odd: odd (c-b)  $\wedge$  odd (c+b)
proof (auto simp only: ccontr)
  assume even (c-b) hence 2 dvd c-b by (simp only: even-eq-two-dvd)
  with a2factor have 2 dvd  $a^2$  by (simp only: dvd-mult2)
  with p2 have 2 dvd a by (rule prime-dvd-power)
  hence even a by (simp only: even-eq-two-dvd)
  with aodd show False by simp
next
  assume even (c+b) hence 2 dvd c+b by (simp only: even-eq-two-dvd)
  with a2factor have 2 dvd  $a^2$  by (simp only: dvd-mult)
  with p2 have 2 dvd a by (rule prime-dvd-power)
  hence even a by (simp only: even-eq-two-dvd)
  with aodd show False by simp
qed
have cb1:  $c-b + (c+b) = 2*c$ 
proof -
  have  $c-b + (c+b) = ((c-b)+b)+c$  by simp
  also with b-less-c have ... =  $(c+b-b)+c$  by (simp only: diff-add-assoc2)
  also have ... =  $c+c$  by simp
  finally show ?thesis by simp
qed
have cb2:  $2*b + (c-b) = c+b$ 
proof -

```

---

```

have  $2*b + (c-b) = b+b + (c - b)$  by auto
also have  $\dots = b + ((c-b)+b)$  by simp
also with b-less-c have  $\dots = b + (c+b-b)$  by (simp only: diff-add-assoc2)
finally show ?thesis by simp
qed
have factors-relprime: gcd(c-b,c+b) = 1
proof -
  let  $?g = gcd(c-b,c+b)$ 
  have  $cb1: c-b + (c+b) = 2*c$ 
  proof -
    have  $c-b + (c+b) = ((c-b)+b)+c$  by simp
    also with b-less-c have  $\dots = (c+b-b)+c$  by (simp only: diff-add-assoc2)
    also have  $\dots = c+c$  by simp
    finally show ?thesis by simp
  qed
have  $?g = gcd(c-b + (c+b),c+b)$  by simp
with cb1 have  $?g = gcd(2*c,c+b)$  by (rule-tac a=c-b + (c+b)) in back-subst
hence g2c: ?g dvd 2*c by (simp only: gcd-dvd1)
have  $gcd(c-b,2*b + (c-b)) = gcd(c-b,2*b)$  by simp
with cb2 have  $?g = gcd(c-b,2*b)$  by (rule-tac a=2*b + (c-b)) in back-subst
hence g2b: ?g dvd 2*b by (simp only: gcd-dvd2)
with g2c have  $?g dvd 2*gcd(b, c)$  by (simp only: gcd-greatest gcd-mult-distrib2)
with bc-relprime have  $?g dvd 2$  by simp
with p2 have  $g1or2: ?g = 2 \vee ?g = 1$  by (unfold prime-def, auto)
thus ?thesis
proof (auto)
  assume  $?g = 2$  hence  $2 dvd ?g$  by simp
  hence  $2 dvd c-b$  by (simp add: gcd-dvd1)
  with factors-odd show False by (simp add: even-eq-two-dvd)
qed
qed
from a2factor have  $(c-b)*(c+b) = a^2$  and  $(2::nat) > 1$  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 a2factor have  $(c+b)*(c-b) = a^2$  and  $(2::nat) > 1$  by auto
with factors-relprime have  $\exists k. c+b = k^2$ 
  by (simp only: nat-relprime-power-divisors gcd-commute)
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: odd r  $\wedge$  odd s
proof (auto dest: ccontr)
  assume even r hence  $2 dvd r$  by (simp only: even-eq-two-dvd)
  with r have  $2 dvd (c-b)$  by (simp only: power2-eq-square dvd-mult)
  hence even (c-b) by (simp only: even-eq-two-dvd)
  with factors-odd show False by simp
next
  assume even s hence  $2 dvd s$  by (simp only: even-eq-two-dvd)
  with s have  $2 dvd (c+b)$  by (simp only: power2-eq-square dvd-mult)
  hence even (c+b) by (simp only: even-eq-two-dvd)
  with factors-odd show 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 two0 have  $r \leq s$  by (rule-tac n=2 in nat-power-le-imp-le-base)
with  $m$  have  $m2: s = r + m$  by simp
have even m
proof (rule ccontr)
  assume odd m with rs-odd and m2 show False by auto
qed
hence  $2 \mid m$  by (simp only: even-eq-two-dvd)
then obtain  $q$  where  $m = 2*q$  by (auto simp add: dvd-def)
with  $m2$  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  $\dots = 2*r^2 + (2*q)^2 + 2*r*(2*q)$ 
    by (simp add: nat-power2-add)
  also have  $\dots = 2*r^2 + 2^2*q^2 + 2*2*q*r$  by (simp add: power-mult-distrib)
  also have  $\dots = 2*(r^2 + 2*q*r + q^2) + 2*q^2$  by (simp add: power2-eq-square)
  also with  $p$  have  $\dots = 2*p^2 + 2*q^2$  by (simp add: nat-power2-add)
  finally show ?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  $\dots = (2*q)^2 + 2*r*(2*q)$  by (simp add: nat-power2-add)
  also with  $p$  have  $\dots = 4*q*p$  by (simp add: power2-eq-square add-mult-distrib2)
  finally show ?thesis by auto
qed
moreover have  $a: a = p^2 - q^2$ 
proof -
  from  $p$  have  $p \geq q$  by simp
  hence p2-ge-q2: p^2 ≥ q^2 by (simp only: power-mono)
  from a2cb and b and c have a^2 = (p^2 + q^2)^2 - (2*p*q)^2 by simp
  also have  $\dots = (p^2)^2 + (q^2)^2 - 2*(p^2)*(q^2)$ 
    by (auto simp add: nat-power2-add power-mult-distrib mult-ac)
  also with p2-ge-q2 have  $\dots = (p^2 - q^2)^2$  by (simp only: nat-power2-diff)
  finally have  $a^2 = (p^2 - q^2)^2$  by simp
  with two0 show ?thesis by (rule-tac n=2 in nat-power-inject-base)
qed
moreover have  $\text{gcd}(p,q)=1$ 
proof -
  let  $?k = \text{gcd}(p,q)$ 
  have  $?k \mid p \wedge ?k \mid q$  by (simp add: gcd-dvd1 gcd-dvd2)
  with  $b$  and  $a$  have  $?k \mid a \wedge ?k \mid b$ 
    by (simp add: dvd-mult power2-eq-square dvd-diff)
  hence  $?k \mid \text{gcd}(a,b)$  by (simp only: gcd-greatest)
  with ab-relprime show ?thesis by auto
qed
ultimately show ?thesis by auto
qed

```

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

**corollary** *int-euclid-pyth-triples*:  $\llbracket \text{zgcd}(a,b) = 1; a \in \text{zOdd}; a^2 + b^2 = c^2 \rrbracket$

$\implies \exists p q. a = p^2 - q^2 \wedge b = 2*p*q \wedge |c| = p^2 + q^2 \wedge \text{zgcd}(p,q)=1$

**proof** –

**assume** *ab-rel*:  $\text{zgcd}(a,b) = 1$  **and** *aodd*:  $a \in \text{zOdd}$  **and** *abc*:  $a^2 + b^2 = c^2$

**let**  $?a = \text{nat}|a|$

**let**  $?b = \text{nat}|b|$

**let**  $?c = \text{nat}|c|$

**have** *ab2-pos*:  $a^2 \geq 0 \wedge b^2 \geq 0$  **by** (*simp add: zero-le-power2*)

**hence**  $\text{nat}(a^2) + \text{nat}(b^2) = \text{nat}(a^2 + b^2)$  **by** (*simp only: nat-add-distrib*)

**with** *abc* **have**  $\text{nat}(a^2) + \text{nat}(b^2) = \text{nat}(c^2)$

**by** (*auto simp add: power2-eq-square abs-power2-distrib*)

**hence**  $\text{nat}(|a|^2) + \text{nat}(|b|^2) = \text{nat}(|c|^2)$

**by** (*simp add: abs-power2-distrib*)

**hence** *new-abc*:  $?a^2 + ?b^2 = ?c^2$

**by** (*simp add: nat-mult-distrib power2-eq-square nat-add-distrib*)

**moreover from** *ab-rel* **have** *new-ab-rel*:  $\text{gcd}(?a,?b)=1$  **by** (*simp add: zgcd-def*)

**moreover have** *new-a-odd*:  $\text{odd } ?a$

**proof** –

**from** *aodd* **obtain**  $k$  **where**  $k: a = 2*k+1$  **by** (*unfold zOdd-def, auto*)

**show** *thesis*

**proof** (*cases*)

**assume** *apos*:  $a \geq 0$  **with**  $k$  **have**  $k \geq 0$  **by** *auto*

**with**  $k$  **and** *apos* **have**  $?a = 2*(\text{nat } k)+1$  **by** *arith*

**thus** *thesis* **by** *simp*

**next**

**assume**  $\neg a \geq 0$  **hence** *aneg*:  $a < 0$  **by** *simp*

**with**  $k$  **have**  $k2: 2*(-1-k) \geq 0$  **by** *simp*

**have** *aux2*:  $(2::\text{int}) \geq 0$  **by** *simp*

**have** *aux1*:  $(1::\text{int}) \geq 0$  **by** *simp*

**from**  $k$  **and** *aneg* **have**  $|a| = 2*(-1-k) + 1$  **by** *simp*

**with**  $k2$  *aux1* **have**  $?a = \text{nat } (2*(-1-k)) + \text{nat } 1$

**by** (*simp only: nat-add-distrib*)

**with** *aux2* **have**  $?a = (\text{nat } 2)*\text{nat}(-1-k) + \text{nat } 1$

**by** (*simp only: nat-mult-distrib*)

**thus** *thesis* **by** *simp*

**qed**

**qed**

**ultimately have**

$\exists p q. ?a = p^2 - q^2 \wedge ?b = 2*p*q \wedge ?c = p^2 + q^2 \wedge \text{gcd}(p,q) = 1$

**by** (*rule-tac a=?a and b=?b and c=?c in nat-euclid-pyth-triples*)

**then obtain**  $m$  **and**  $n$  **where** *mn*:

$?a = m^2 - n^2 \wedge ?b = 2*m*n \wedge ?c = m^2 + n^2 \wedge \text{gcd}(m,n) = 1$  **by** *auto*

**have**  $n^2 \leq m^2$

**proof** (*rule ccontr*)

**assume**  $\neg n^2 \leq m^2$  **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**  $\text{int } ?a = \text{int}(m^2 - n^2)$  **and**  $\text{int } ?b = \text{int}(2*m*n)$

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

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

**and**  $|c| = \text{int}(m^2) + \text{int}(n^2)$  **by** (*auto simp only: int-nat-abs-eq-abs zdiff-int*)

---

```

hence absabc:  $|a| = (int\ m)^2 - (int\ n)^2 \wedge |b| = 2*(int\ m)*int\ n$ 
   $\wedge |c| = (int\ m)^2 + (int\ n)^2$  by (simp add: power2-eq-square int-mult)
from mn have mn-rel:  $zgcd(int\ m,int\ n)=1$  by (simp add: zgcd-def)
show  $\exists\ p\ q. a = p^2 - q^2 \wedge b = 2*p*q \wedge |c| = p^2 + q^2 \wedge zgcd(p,q)=1$ 
  (is  $\exists\ p\ q. ?Q\ p\ q$ )
proof (cases)
  assume apos:  $a \geq 0$  then obtain p where  $p: p = int\ m$  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  $\neg\ b \geq 0$  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  $\neg\ a \geq 0$  hence aneg:  $a < 0$  by simp
  then obtain p where  $p: p = int\ n$  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: zgcd-commute)
    thus ?thesis by (rule exI)
  next
    assume  $\neg\ b \geq 0$  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: zgcd-commute mult-ac)
    thus ?thesis by (rule exI)
  qed
thus ?thesis by (simp only: exI)
qed
qed

```

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

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

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

**lemma** *smaller-fermat4*:

**assumes** *abc*:  $a^4 + b^4 = c^2$  **and** *abc0*:  $a*b*c \neq 0$  **and** *aodd*:  $a \in zOdd$   
**and** *ab-relprime*:  $zgcd(a,b)=1$

**shows**

$\exists\ p\ q\ r. (p^4 + q^4 = r^2 \wedge p*q*r \neq 0 \wedge p \in zOdd \wedge zgcd(p,q) = 1 \wedge r^2 < c^2)$

**proof** –

— put equation in shape of a pythagorean triple and obtain  $u$  and  $v$   
**from** *ab-relprime* **have**  $a^2 b^2 \text{relprime}$ :  $\text{zgcd}(a^2, b^2) = 1$   
**by** (*simp only: zgcd-1-power-distrib*)  
**moreover from** *aodd* **have**  $a^2 \in \text{zOdd}$  **by** (*simp only: power-preserves-odd*)  
**moreover from** *abc* **have**  $(a^2)^2 + (b^2)^2 = c^2$  **by** (*simp only: quartic-square-square*)  
**ultimately obtain**  $u$  **and**  $v$  **where** *uvabc*:  
 $a^2 = u^2 - v^2 \wedge b^2 = 2 * u * v \wedge |c| = u^2 + v^2 \wedge \text{zgcd}(u, v) = 1$   
**by** (*frule-tac a=a^2 in int-euclid-pyth-triples, auto*)  
**with** *abc0* **have** *uv0*:  $u \neq 0 \wedge v \neq 0$  **by** *auto*  
**have** *av-relprime*:  $\text{zgcd}(a, v) = 1$   
**proof** —  
**from** *uvabc* **have**  $\text{zgcd}(v, a^2) \text{dvd} \text{zgcd}(b^2, a^2)$  **by** (*simp only: zgcd-zdvd-zgcd-zmult*)  
**with** *a2b2relprime* **have**  $\text{zgcd}(a^2, v) \text{dvd} (1::\text{int})$  **by** (*simp only: zgcd-commute*)  
**moreover have**  $\text{zgcd}(a, v) \text{dvd} \text{zgcd}(a^2, v)$   
**by** (*simp only: zgcd-zdvd-zgcd-zmult power2-eq-square*)  
**ultimately have**  $\text{zgcd}(a, v) \text{dvd} 1$  **by** (*rule-tac m=zgcd(a,v) in zdvd-trans*)  
**hence**  $|\text{zgcd}(a, v)| = 1$  **by** *auto*  
**thus** *?thesis* **by** (*simp add: zgcd-geq-zero*)  
**qed**  
— make again a pythagorean triple and obtain  $k$  and  $l$   
**from** *uvabc* **have**  $a^2 + v^2 = u^2$  **by** *simp*  
**with** *av-relprime* **and** *aodd* **obtain**  $k$   $l$  **where**  
 $klavu$ :  $a = k^2 - l^2 \wedge v = 2 * k * l \wedge |u| = k^2 + l^2$  **and** *kl-rel*:  $\text{zgcd}(k, l) = 1$   
**by** (*frule-tac a=a in int-euclid-pyth-triples, auto*)  
— prove  $b = 2m$  and  $kl(k^2 + l^2) = m^2$ , for coprime  $k, l$  and  $k^2 + l^2$   
**from** *uvabc* **have**  $b^2 \in \text{zEven}$  **by** (*unfold zEven-def, auto*)  
**hence**  $b \in \text{zEven}$  **by** (*simp only: power-preserves-even*)  
**then obtain**  $m$  **where** *bm*:  $b = 2 * m$  **by** (*auto simp only: zEven-def*)  
**have**  $|k * l * |k^2 + l^2| = m^2$   
**proof** —  
**from** *bm* **have**  $4 * m^2 = b^2$  **by** (*simp only: power2-eq-square mult-ac*)  
**also have**  $\dots = |b^2|$  **by** *simp*  
**also with** *uvabc* **have**  $\dots = 2 * |v * |u||$  **by** (*simp add: abs-mult*)  
**also with** *klavu* **have**  $\dots = 2 * |2 * k * l * |k^2 + l^2||$  **by** *simp*  
**also have**  $\dots = 4 * |k * l * |k^2 + l^2||$  **by** (*auto simp add: abs-mult*)  
**finally show** *?thesis* **by** *simp*  
**qed**  
**moreover have**  $(2::\text{nat}) > 1$  **by** *auto*  
**moreover from** *kl-rel* **have**  $\text{zgcd}(|k|, |l|) = 1$  **by** (*unfold zgcd-def, auto*)  
**moreover have**  $\text{zgcd}(|l|, |k^2 + l^2|) = 1$   
**proof** —  
**from** *kl-rel* **have**  $\text{zgcd}(k * k, l) = 1$  **by** (*simp only: zgcd-zgcd-zmult*)  
**hence**  $\text{zgcd}(k * k + l * l, l) = 1$  **by** *simp*  
**hence**  $\text{zgcd}(l, k^2 + l^2) = 1$  **by** (*simp only: power2-eq-square zgcd-commute*)  
**thus** *?thesis* **by** (*unfold zgcd-def, auto*)  
**qed**  
**moreover have**  $\text{zgcd}(|k^2 + l^2|, |k|) = 1$   
**proof** —  
**from** *kl-rel* **have**  $\text{zgcd}(l, k) = 1$  **by** (*simp only: zgcd-commute*)  
**hence**  $\text{zgcd}(l * l, k) = 1$  **by** (*simp only: zgcd-zgcd-zmult*)  
**hence**  $\text{zgcd}(l * l + k * k, k) = 1$  **by** *simp*  
**hence**  $\text{zgcd}(k^2 + l^2, k) = 1$  **by** (*simp only: add-ac power2-eq-square*)

```

thus ?thesis by (unfold zgcd-def, auto)
qed
ultimately have
   $\exists x y z. ||k|| = x^2 \wedge ||l|| = y^2 \wedge ||k^2+l^2|| = z^2$ 
by (rule int-triple-relprime-power-divisors)
then obtain  $\alpha \beta \gamma$  where albega:
   $|k| = \alpha^2 \wedge |l| = \beta^2 \wedge |k^2+l^2| = \gamma^2$ 
by auto
— show this is a new solution
have  $k^2 = \alpha^4$ 
proof —
  from albega have  $|k|^2 = (\alpha^2)^2$  by simp
  thus ?thesis by (simp add: quartic-square-square abs-power2-distrib)
qed
moreover have  $l^2 = \beta^4$ 
proof —
  from albega have  $|l|^2 = (\beta^2)^2$  by simp
  thus ?thesis by (simp add: quartic-square-square abs-power2-distrib)
qed
moreover have gamma2:  $k^2 + l^2 = \gamma^2$ 
proof —
  have  $k^2 \geq 0 \wedge l^2 \geq 0$  by (simp add: zero-le-power2)
  with albega show ?thesis by auto
qed
ultimately have newabc:  $\alpha^4 + \beta^4 = \gamma^2$  by auto
from uv0 klavu albega have albega0:  $\alpha * \beta * \gamma \neq 0$  by auto
— show the coprimality
have alphabetarelprime:  $\text{zgcd}(\alpha, \beta) = 1$ 
proof (rule classical)
  let ?g =  $\text{zgcd}(\alpha, \beta)$ 
  assume gnot1: ?g  $\neq 1$ 
  have ?g > 1
  proof —
    have ?g  $\neq 0$ 
    proof
      assume ?g=0
      hence nat | $\alpha$ |=0 by (unfold zgcd-def, auto simp add: gcd-zero)
      hence  $\alpha=0$  by arith
      with albega0 show False by simp
    qed
    hence ?g > 0 by (auto simp only: zgcd-geq-zero less-int-def)
    with gnot1 show ?thesis by simp
  qed
moreover have ?g dvd  $\text{zgcd}(k, l)$ 
proof —
  have ?g dvd  $\alpha \wedge$  ?g dvd  $\beta$  by auto
  with albega have ?g dvd  $|k| \wedge$  ?g dvd  $|l|$ 
  by (simp add: zdvd-zmult power2-eq-square zmult-commute)
  hence ?g dvd  $k \wedge$  ?g dvd  $l$  by (simp add: zdvd-abs2)
  thus ?thesis by (simp add: zgcd-greatest-iff)
qed
ultimately have  $\text{zgcd}(k, l) \neq 1$  by auto

```

```

with kl-rel show ?thesis by auto
qed
— choose p and q in the right way
have  $\exists p q. p^4 + q^4 = \gamma^2 \wedge p * q * \gamma \neq 0 \wedge p \in zOdd \wedge zgcd(p,q)=1$ 
proof —
  have  $\alpha \in zOdd \vee \beta \in zOdd$ 
  proof (rule ccontr)
    assume  $\neg (\alpha \in zOdd \vee \beta \in zOdd)$ 
    hence  $\alpha \in zEven \wedge \beta \in zEven$  by (auto simp add: not-odd-impl-even)
    then have  $2 \text{ dvd } \alpha \wedge 2 \text{ dvd } \beta$  by (auto simp add: zEven-def)
    then have  $2 \text{ dvd } zgcd(\alpha,\beta)$  by (simp add: zgcd-greatest-iff)
    with alphabeta-relprime show False by auto
  qed
  moreover
  { assume  $\alpha \in zOdd$ 
    with newabc albega0 alphabeta-relprime obtain p q where
       $p=\alpha \wedge q=\beta \wedge p^4 + q^4 = \gamma^2 \wedge p * q * \gamma \neq 0 \wedge p \in zOdd \wedge zgcd(p,q)=1$ 
      by auto
    hence ?thesis by auto }
  moreover
  { assume  $\beta \in zOdd$ 
    with newabc albega0 alphabeta-relprime obtain p q where
       $q=\alpha \wedge p=\beta \wedge p^4 + q^4 = \gamma^2 \wedge p * q * \gamma \neq 0 \wedge p \in zOdd \wedge zgcd(p,q)=1$ 
      by (auto simp add: add-ac zgcd-commute)
    hence ?thesis by auto }
  ultimately show ?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  $\dots \leq |u|^2$  by (rule power2-ge-self)
  also have  $\dots \leq u^2$  by (simp add: abs-power2-distrib)
  also have  $\dots < u^2 + v^2$ 
  proof —
    from wv0 have  $v2non0: 0 \neq v^2$ 
    by (auto simp add: power2-eq-square zero-le-power2)
    have  $0 \leq v^2$  by (rule zero-le-power2)
    with v2non0 have  $0 < v^2$  by (auto simp add: less-int-def)
    thus ?thesis by auto
  qed
  also with uvabc have  $\dots \leq |c|$  by auto
  also have  $\dots \leq |c|^2$  by (rule power2-ge-self)
  also have  $\dots \leq c^2$  by (simp add: abs-power2-distrib)
  finally show ?thesis by simp
qed
ultimately show ?thesis by auto
qed

```

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

lemma no-rewritten-fermat4:

fixes  $c::int$

shows  $\neg (\exists a b. (a^4 + b^4 = c^2 \wedge a*b*c \neq 0 \wedge a \in zOdd \wedge zgcd(a,b)=1))$   
(is ?Q c)  
**proof** (rule-tac  $x=c$  and  $V = \lambda c. nat(c^2)$  in val-infinite-descent)  
**fix**  $x$   
**assume**  $x2zero: nat(x^2)=0$   
**have**  $x^2 \geq 0$  **by** (rule zero-le-power2)  
**with**  $x2zero$  **have**  $int(nat(x^2)) = 0$  **by** auto  
**hence**  $x = 0$  **by** auto  
**thus** ?Q  $x$  **by** auto  
**next**  
**fix**  $x$   
**assume**  $x2pos: 0 < nat(x^2)$  and  $\neg ?Q x$   
**then obtain**  $a b$  **where**  $a^4 + b^4 = x^2$  and  $a*b*x \neq 0$   
and  $a \in zOdd$  and  $zgcd(a,b)=1$  **by** auto  
**hence**  $\exists p q r. (p^4 + q^4 = r^2 \wedge p*q*r \neq 0 \wedge p \in zOdd$   
 $\wedge zgcd(p,q)=1 \wedge r^2 < x^2)$  **by** (rule smaller-fermat4)  
**then obtain**  $p q r$  **where**  $pqr: p^4 + q^4 = r^2 \wedge p*q*r \neq 0 \wedge p \in zOdd$   
 $\wedge zgcd(p,q)=1 \wedge r^2 < x^2$  **by** auto  
**have**  $r^2 \geq 0$  and  $x^2 \geq 0$  **by** (auto simp only: zero-le-power2)  
**hence**  $int(nat(r^2)) = r^2 \wedge int(nat(x^2)) = x^2$  **by** auto  
**with**  $pqr$  **have**  $int(nat(r^2)) < int(nat(x^2))$  **by** auto  
**hence**  $nat(r^2) < nat(x^2)$  **by** (simp only: zless-int)  
**with**  $pqr$  **show**  $\exists y. nat(y^2) < nat(x^2) \wedge \neg ?Q y$  **by** auto  
**qed**

The theorem. Puts equation in requested shape.

**theorem** *fermat4*:

**assumes**  $ass: (x::int)^4 + y^4 = z^4$

**shows**  $x*y*z=0$

**proof** (rule ccontr)

**let** ?g =  $zgcd(x,y)$

**let** ?c =  $(z \text{ div } ?g)^2$

**assume**  $xyz0: x*y*z \neq 0$

— divide out the g.c.d.

**hence**  $x \neq 0 \vee y \neq 0$  **by** simp

**then obtain**  $a b$  **where**  $ab: x = ?g*a \wedge y = ?g*b \wedge zgcd(a,b)=1$

**by** (frule-tac  $a=x$  in make-zrelprime, auto)

**moreover have**  $abc: a^4 + b^4 = ?c^2 \wedge a*b*?c \neq 0$

**proof** —

**have**  $zgab: z^4 = ?g^4 * (a^4 + b^4)$

**proof** —

**from**  $ab$   $ass$  **have**  $z^4 = (?g*a)^4 + (?g*b)^4$  **by** simp

**thus** ?thesis **by** (simp only: power-mult-distrib zadd-zmult-distrib2)

**qed**

**have**  $cgz: z^2 = ?c * ?g^2$

**proof** —

**from**  $zgab$  **have**  $?g^4 \text{ dvd } z^4$  **by** simp

**hence**  $?g \text{ dvd } z$  **by** (simp only: zpower-zdvd-mono)

**hence**  $(z \text{ div } ?g)*?g = z$  **by** (simp only: mult-ac zdvd-mult-div-cancel)

**with**  $ab$  **show** ?thesis **by** (auto simp only: power2-eq-square mult-ac)

**qed**

**with**  $xyz0$  **have**  $c0: ?c \neq 0$  **by** (auto simp add: power2-eq-square)

**from**  $xyz0$  **have**  $g0: ?g \neq 0$  **by** (*simp add: zgcd-def gcd-zero*)  
**have**  $a^4 + b^4 = ?c^2$   
**proof** –  
**have**  $?c^2 * ?g^4 = (a^4 + b^4) * ?g^4$   
**proof** –  
**have**  $?c^2 * ?g^4 = (?c * ?g^2)^2$   
**by** (*simp only: quartic-square-square power-mult-distrib*)  
**also with**  $cgz$  **have**  $\dots = (z^2)^2$  **by** *simp*  
**also have**  $\dots = z^4$  **by** (*rule quartic-square-square*)  
**also with**  $zgab$  **have**  $\dots = ?g^4 * (a^4 + b^4)$  **by** *simp*  
**finally show** *?thesis* **by** *simp*  
**qed**  
**with**  $g0$  **show** *?thesis* **by** *auto*  
**qed**  
**moreover from**  $ab xyz0 c0$  **have**  $a * b * ?c \neq 0$  **by** *auto*  
**ultimately show** *?thesis* **by** *simp*  
**qed**  
— choose the parity right  
**have**  $\exists p q. p^4 + q^4 = ?c^2 \wedge p * q * ?c \neq 0 \wedge p \in zOdd \wedge zgcd(p, q) = 1$   
**proof** –  
**have**  $a \in zOdd \vee b \in zOdd$   
**proof** (*rule ccontr*)  
**assume**  $\neg(a \in zOdd \vee b \in zOdd)$   
**hence**  $a \in zEven \wedge b \in zEven$  **by** (*auto simp add: not-odd-impl-even*)  
**hence**  $2 \text{ dvd } a \wedge 2 \text{ dvd } b$  **by** (*auto simp add: zEven-def*)  
**hence**  $2 \text{ dvd } zgcd(a, b)$  **by** (*simp add: zgcd-greatest-iff*)  
**with**  $ab$  **show** *False* **by** *auto*  
**qed**  
**moreover**  
{ **assume**  $a \in zOdd$   
**then obtain**  $p q$  **where**  $p = a$  **and**  $q = b$  **and**  $p \in zOdd$  **by** *simp*  
**with**  $ab abc$  **have** *?thesis* **by** *auto* }  
**moreover**  
{ **assume**  $b \in zOdd$   
**then obtain**  $p q$  **where**  $p = b$  **and**  $q = a$  **and**  $p \in zOdd$  **by** *simp*  
**with**  $ab abc$  **have**  
 $p^4 + q^4 = ?c^2 \wedge p * q * ?c \neq 0 \wedge p \in zOdd \wedge zgcd(p, q) = 1$   
**by** (*auto simp add: zgcd-commute zmult-commute*)  
**hence** *?thesis* **by** *auto* }  
**ultimately show** *?thesis* **by** *auto*  
**qed**  
— show contradiction using the earlier result  
**thus** *False* **by** (*auto simp only: no-rewritten-fermat4*)  
**qed**

**corollary** *fermat-mult4*:  
**assumes**  $xyz: (x::int)^n + y^n = z^n$  **and**  $n: 4 \text{ dvd } n$   
**shows**  $x * y * z = 0$   
**proof** –  
**from**  $n$  **obtain**  $m$  **where**  $n = m * 4$  **by** (*auto simp only: mult-ac dvd-def*)  
**with**  $xyz$  **have**  $(x^m)^4 + (y^m)^4 = (z^m)^4$  **by** (*simp only: power-mult*)  
**hence**  $(x^m) * (y^m) * (z^m) = 0$  **by** (*rule fermat4*)

```

thus ?thesis by auto
qed

end

```

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

```

theory QuadForm
imports
  ~~/src/HOL/NumberTheory/Quadratic-Reciprocity
  IntNatAux InfDesc
begin

```

Shows some properties of the quadratic form  $x^2 + Ny^2$ , such as how to multiply and divide them. The second part focuses on the case  $N = 3$  and is used in the proof of the case  $n = 3$  of Fermat's last theorem. The last part – not used for FLT3 – shows which primes can be written as  $x^2 + 3y^2$ .

### 4.1 Definitions and auxiliary results

```

constdefs
  is-qn :: int ⇒ int ⇒ bool
  is-qn A N == ∃ x y. A = x2 + N*y2

  is-cube-form :: int ⇒ int ⇒ bool
  is-cube-form a b == ∃ p q. a = p3 - 9*p*q2 ∧ b = 3*p2*q - 3*q3

lemma abs-eq-impl-unitfactor: |a::int| = |b| ⇒ ∃ u. a = u*b ∧ |u|=1
proof -
  assume |a| = |b|
  hence a = 1*b ∨ a = (-1)*b by arith
  then obtain u where a = u*b ∧ (u=1 ∨ u=-1) by blast
  thus ?thesis by auto
qed

```

```

lemma zprime-3: zprime 3
proof (auto simp add: zprime-def)
  fix m::int assume m0: m ≥ 0 and mdvd3: m dvd 3 and mn3: m ≠ 3
  hence m ≤ 3 by (auto simp only: zdvd-imp-le)
  with mn3 have m < 3 by simp
  moreover from mdvd3 have m ≠ 0 by auto
  moreover with m0 have m > 0 by simp
  ultimately have m = 1 ∨ m = 2 by auto
  moreover from mdvd3 have m = 2 ⇒ False by arith
  ultimately show m = 1 by auto
qed

```

### 4.2 Basic facts if $N \geq 1$

```

lemma qfN-pos: [ N ≥ 1; is-qn A N ] ⇒ A ≥ 0
proof -

```

```

assume  $N: N \geq 1$  and  $is\_qfN\ A\ N$ 
then obtain  $a\ b$  where  $ab: A = a^2 + N*b^2$  by (auto simp add: is-qfN-def)
have  $N*b^2 \geq 0$ 
proof (cases)
  assume  $b = 0$  thus ?thesis by auto
next
  assume  $\neg b = 0$  hence  $b^2 > 0$  by (simp add: zero-less-power2)
  moreover from  $N$  have  $N > 0$  by simp
  ultimately have  $N*b^2 > N*0$  by (auto simp only: zmult-zless-mono2)
  thus ?thesis by auto
qed
with  $ab$  have  $A \geq a^2$  by auto
moreover have  $a^2 \geq 0$  by (rule zero-le-power2)
ultimately show ?thesis by arith
qed

```

**lemma** *qfN-zero*:  $\llbracket (N::int) \geq 1; a^2 + N*b^2 = 0 \rrbracket \implies (a = 0 \wedge b = 0)$

```

proof -
  assume  $N: N \geq 1$  and  $abN: a^2 + N*b^2 = 0$ 
  show ?thesis
  proof (rule ccontr, auto)
    assume  $a \neq 0$  hence  $a^2 > 0$  by (simp add: zero-less-power2)
    moreover have  $N*b^2 \geq 0$ 
    proof (cases)
      assume  $b = 0$  thus ?thesis by auto
    next
      assume  $\neg b = 0$  hence  $b^2 > 0$  by (simp add: zero-less-power2)
      moreover from  $N$  have  $N > 0$  by simp
      ultimately have  $N*b^2 > N*0$  by (auto simp only: zmult-zless-mono2)
      thus ?thesis by auto
    qed
    ultimately have  $a^2 + N*b^2 > 0$  by arith
    with  $abN$  show False by auto
  next
    assume  $b \neq 0$  hence  $b^2 > 0$  by (simp add: zero-less-power2)
    moreover from  $N$  have  $N > 0$  by simp
    ultimately have  $N*b^2 > N*0$  by (auto simp only: zmult-zless-mono2)
    hence  $N*b^2 > 0$  by simp
    moreover have  $a^2 \geq 0$  by (rule zero-le-power2)
    ultimately have  $a^2 + N*b^2 > 0$  by arith
    with  $abN$  show False by auto
  qed
qed

```

### 4.3 Multiplication and division

```

lemma qfN-mult1:  $((a::int)^2 + N*b^2)*(c^2 + N*d^2)$ 
   $= (a*c + N*b*d)^2 + N*(a*d - b*c)^2$ 
by (simp add: nat-number ring-simps)

```

```

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

```

by (*simp add: nat-number ring-simps*)

**corollary** *is-qn-mult*:  $is-qn\ A\ N \implies is-qn\ B\ N \implies is-qn\ (A*B)\ N$   
by (*unfold is-qn-def, auto, auto simp only: qn-mult1*)

**corollary** *is-qn-power*:  $(n::nat) > 0 \implies is-qn\ A\ N \implies is-qn\ (A^n)\ N$   
by (*induct n, auto, case-tac n=0, auto simp add: is-qn-mult*)

**lemma** *qn-div-prime*:

**assumes** *ass*:  $zprime\ (p^2+N*q^2) \wedge (p^2+N*q^2)\ dvd\ (a^2+N*b^2)$

**shows**  $\exists\ u\ v.\ a^2+N*b^2 = (u^2+N*v^2)*(p^2+N*q^2)$

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

**proof** –

**let**  $?P = p^2+N*q^2$

**let**  $?A = a^2+N*b^2$

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

**have**  $\exists\ e.\ ?P\ dvd\ b*p + e*a*q \wedge |e| = 1$

**proof** –

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

**proof** –

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

**by** (*simp add: nat-number ring-simps*)

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

**finally show** *?thesis* **by** *simp*

**qed**

**with** *ass* **have**  $?P\ dvd\ (b*p + a*q) \vee ?P\ dvd\ (b*p - a*q)$

**by** (*simp only: zprime-zdvd-zmult-general*)

**moreover**

{ **assume**  $?P\ dvd\ b*p + a*q$

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

**moreover**

{ **assume**  $?P\ dvd\ b*p - a*q$

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

**ultimately show** *?thesis* **by** *blast*

**qed**

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

**by** (*auto simp only: dvd-def*)

**have**  $?P\ dvd\ a*p - e*N*b*q$

**proof** (*cases*)

**assume**  $e1: e = 1$

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

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

**by** (*simp only: qn-mult2 add-commute zmult-1*)

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

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

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

**by** (*simp add: mult-ac zdiff-zmult-distrib*)

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

**thus** *?thesis* **by** (*simp only: zpower-zdvd-mono*)

**next**

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

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

**also with  $e1$  have**  $\dots = (a*p - e*N*b*q)^2 + N*(-(b*p + e*a*q))^2$   
**by** (*simp add: qfN-mult1*)  
**also have**  $\dots = (a*p - e*N*b*q)^2 + N*(b*p + e*a*q)^2$   
**by** (*simp only: power2-minus*)  
**also with  $v$  have**  $\dots = (a*p - e*N*b*q)^2 + N*v^2*?P^2$   
**by** (*simp only: power-mult-distrib mult-ac*)  
**finally have**  $(a*p - e*N*b*q)^2 = ?P^2*(U - N*v^2)$   
**by** (*simp add: mult-ac zdiff-zmult-distrib*)  
**hence**  $?P^2 \text{ dvd } (a*p - e*N*b*q)^2$  **by** (*rule dvdI*)  
**thus** *?thesis* **by** (*simp only: zpower-zdvd-mono*)  
**qed**  
**then obtain  $u$  where**  $u: a*p - e*N*b*q = ?P*u$  **by** (*auto simp only: dvd-def*)  
**from  $e$  have**  $e2-1: e*e = 1$  **by** *auto*  
**have**  $a: a = p*u + e*N*q*v$   
**proof** –  
**have**  $(p*u + e*N*q*v)*?P = p*(?P*u) + (e*N*q)*(?P*v)$   
**by** (*simp only: zadd-zmult-distrib mult-ac*)  
**also with  $v u$  have**  $\dots = p*(a*p - e*N*b*q) + (e*N*q)*(b*p + e*a*q)$   
**by** *simp*  
**also have**  $\dots = a*(p^2 + e*e*N*q^2)$   
**by** (*simp add: power2-eq-square zadd-zmult-distrib2 mult-ac zdiff-zmult-distrib2*)  
**also with  $e2-1$  have**  $\dots = a*?P$  **by** *simp*  
**finally have**  $(a - (p*u + e*N*q*v))*?P = 0$  **by** *auto*  
**moreover from** *ass* **have**  $?P \neq 0$  **by** (*unfold zprime-def, auto*)  
**ultimately show** *?thesis* **by** *simp*  
**qed**  
**moreover have**  $b: b = p*v - e*q*u$   
**proof** –  
**have**  $(p*v - e*q*u)*?P = p*(?P*v) - (e*q)*(?P*u)$   
**by** (*simp only: zdiff-zmult-distrib mult-ac*)  
**also with  $v u$  have**  $\dots = p*(b*p + e*a*q) - e*q*(a*p - e*N*b*q)$  **by** *simp*  
**also have**  $\dots = b*(p^2 + e*e*N*q^2)$   
**by** (*simp add: power2-eq-square zadd-zmult-distrib2 mult-ac zdiff-zmult-distrib2*)  
**also with  $e2-1$  have**  $\dots = b*?P$  **by** *simp*  
**finally have**  $(b - (p*v - e*q*u))*?P = 0$  **by** *auto*  
**moreover from** *ass* **have**  $?P \neq 0$  **by** (*unfold zprime-def, auto*)  
**ultimately show** *?thesis* **by** *simp*  
**qed**  
**moreover have**  $?A = (u^2 + N*v^2)*?P$   
**proof** (*cases*)  
**assume**  $e=1$   
**with  $a$  and  $b$  show** *?thesis* **by** (*simp add: qfN-mult1 zmult-1 mult-ac*)  
**next**  
**assume**  $\neg e=1$  **with  $e$  have**  $e=-1$  **by** *simp*  
**with  $a$  and  $b$  show** *?thesis* **by** (*simp add: qfN-mult2 zmult-1 mult-ac*)  
**qed**  
**moreover from**  $e$  **have**  $|e| = 1$  **..**  
**ultimately show** *?thesis* **by** *blast*  
**qed**  
**corollary** *qfN-div-prime-weak*:  
 $\llbracket \text{zprime } (p^2 + N*q^2); (p^2 + N*q^2) \text{ dvd } (a^2 + N*b^2) \rrbracket$

$\implies \exists u v. a^2 + N * b^2 = (u^2 + N * v^2) * (p^2 + N * q^2)$   
**apply** (*subgoal-tac*  $\exists u v. a^2 + N * b^2 = (u^2 + N * v^2) * (p^2 + N * q^2)$   
 $\wedge (\exists e. a = p * u + e * N * q * v \wedge b = p * v - e * q * u \wedge |e| = 1)$ , *blast*)  
**apply** (*rule qfN-div-prime, auto*)  
**done**

**corollary** *qfN-div-prime-general*:  $\llbracket \text{zprime } P; P \text{ dvd } A; \text{is-qfN } A \ N; \text{is-qfN } P \ N \rrbracket$   
 $\implies \exists Q. A = Q * P \wedge \text{is-qfN } Q \ N$   
**apply** (*subgoal-tac*  $\exists u v. A = (u^2 + N * v^2) * P$ )  
**apply** (*unfold is-qfN-def, auto*)  
**apply** (*simp only: qfN-div-prime-weak*)  
**done**

**lemma** *qfN-power-div-prime*:

**assumes** *ass*:  $\text{zprime } P \wedge P \in \text{zOdd} \wedge P \text{ dvd } A \wedge P^n = p^2 + N * q^2$   
 $\wedge A^n = a^2 + N * b^2 \wedge \text{zgcd}(a, b) = 1 \wedge \text{zgcd}(p, N * q) = 1 \wedge n > 0$   
**shows**  $\exists u v. a^2 + N * b^2 = (u^2 + N * v^2) * (p^2 + N * q^2) \wedge \text{zgcd}(u, v) = 1$   
 $\wedge (\exists e. a = p * u + e * N * q * v \wedge b = p * v - e * q * u \wedge |e| = 1)$

**proof** –

**from** *ass* **have**  $P \text{ dvd } A \wedge n > 0$  **by** *simp*  
**hence**  $P^n \text{ dvd } A^n$  **by** (*simp add: zpower-zdvd-mono*)  
**then obtain**  $U$  **where**  $U: A^n = U * P^n$  **by** (*auto simp only: dvd-def mult-ac*)  
**have**  $\exists e. P^n \text{ dvd } b * p + e * a * q \wedge |e| = 1$

**proof** –

**have**  $P^n \text{ dvd } (b * p + a * q) * (b * p - a * q)$   
**proof** –  
**have**  $(b * p + a * q) * (b * p - a * q) = (b * p)^2 - (a * q)^2$  **by** (*rule zspecial-product*)  
**also have**  $\dots = b^2 * p^2 + b^2 * N * q^2 - b^2 * N * q^2 - a^2 * q^2$   
**by** (*simp add: power-mult-distrib*)  
**also with** *ass* **have**  $\dots = b^2 * P^n - q^2 * A^n$   
**by** (*simp only: mult-ac zadd-zmult-distrib zadd-zmult-distrib2*)  
**also with**  $U$  **have**  $\dots = (b^2 - q^2 * U) * P^n$  **by** (*simp only: zdiff-zmult-distrib*)  
**finally show** *?thesis* **by** (*simp add: mult-ac*)

**qed**

**have**  $P^n \text{ dvd } (b * p + a * q) \vee P^n \text{ dvd } (b * p - a * q)$

**proof** –

**have**  $P \text{ dvd } P^n$

**proof** –

**from** *ass* **have**  $\exists m. n = \text{Suc } m$  **by** (*simp add: not0-implies-Suc*)  
**then obtain**  $m$  **where**  $n = \text{Suc } m$  **by** *auto*  
**hence**  $P^n = P * (P^m)$  **by** *auto*  
**thus** *?thesis* **by** *auto*

**qed**

**have**  $\neg P \text{ dvd } b * p + a * q \vee \neg P \text{ dvd } b * p - a * q$

**proof** (*rule ccontr, simp*)

**assume**  $P \text{ dvd } b * p + a * q \wedge P \text{ dvd } b * p - a * q$

**hence**  $P \text{ dvd } (b * p + a * q) + (b * p - a * q) \wedge P \text{ dvd } (b * p + a * q) - (b * p - a * q)$

**by** (*simp only: zdvd-zadd, simp only: zdvd-zdiff*)

**hence**  $P \text{ dvd } 2 * (b * p) \wedge P \text{ dvd } 2 * (a * q)$  **by** (*simp only: mult-2, auto*)

**with** *ass* **have**  $(P \text{ dvd } 2 \vee P \text{ dvd } b * p) \wedge (P \text{ dvd } 2 \vee P \text{ dvd } a * q)$

**by** (*simp add: zprime-zdvd-zmult-general*)

**hence**  $P \text{ dvd } 2 \vee (P \text{ dvd } b * p \wedge P \text{ dvd } a * q)$  **by** *auto*

```

moreover have  $\neg P \text{ dvd } 2$ 
proof (rule ccontr, simp)
  assume  $p \text{ dvd } 2$ 
  have  $P \leq 2$ 
  proof (rule ccontr)
    assume  $\neg P \leq 2$  hence  $P > 2$  by simp
    with  $p \text{ dvd } 2$  show False by (simp add: z dvd-not-zless)
  qed
moreover from ass have  $P > 1$  by (simp only: zprime-def)
ultimately have  $P = 2$  by auto
with ass have  $2 \in \text{zOdd}$  by simp
moreover have  $2 \in \text{zEven}$  by (simp add: zEven-def)
ultimately show False by (simp add: odd-iff-not-even)
qed
ultimately have  $P \text{ dvd } b * p \wedge P \text{ dvd } a * q$  by auto
with ass have  $(P \text{ dvd } b \vee P \text{ dvd } p) \wedge (P \text{ dvd } a \vee P \text{ dvd } q)$ 
by (auto simp only: zprime-z dvd-zmult-general)
moreover have  $\neg P \text{ dvd } p \wedge \neg P \text{ dvd } q$ 
proof (auto dest: ccontr)
  assume  $P \text{ dvd } p$ 
  hence  $P \text{ dvd } p^2$  by (simp only: z dvd-zmult power2-eq-square)
  with  $P \text{ dvd } P^n$  have  $P \text{ dvd } P^{n-p} p^2$  by (simp only: z dvd-zdiff)
  with ass have  $P \text{ dvd } N * (q * q)$  by (simp add: power2-eq-square)
  with ass have  $P \text{ dvd } N \vee P \text{ dvd } q$  by (auto dest: zprime-z dvd-zmult-general)
  hence  $P \text{ dvd } N * q$  by (auto simp add: z dvd-zmult z dvd-zmult2)
  with  $P \text{ dvd } p$  have  $P \text{ dvd } \text{zgcd}(p, N * q)$  by (simp add: zgcd-greatest-iff)
  with ass show False by (auto simp add: zprime-def)
next
  assume  $P \text{ dvd } q$ 
  hence  $P \text{ dvd } N * q$  by (simp add: z dvd-zmult)
  hence  $P \text{ dvd } N * q * q$  by (simp add: z dvd-zmult2)
  hence  $P \text{ dvd } N * q^2$  by (simp add: power2-eq-square mult-ac)
  with  $P \text{ dvd } P^n$  have  $P \text{ dvd } P^{n-N} N * q^2$  by (simp only: z dvd-zdiff)
  with ass have  $P \text{ dvd } p * p$  by (simp add: power2-eq-square)
  with ass have  $P \text{ dvd } p$  by (auto dest: zprime-z dvd-zmult-general)
  with  $P \text{ dvd } N * q$  have  $P \text{ dvd } \text{zgcd}(p, N * q)$  by (simp add: zgcd-greatest-iff)
  with ass show False by (auto simp add: zprime-def)
qed
ultimately have  $P \text{ dvd } a \wedge P \text{ dvd } b$  by auto
hence  $P \text{ dvd } \text{zgcd}(a, b)$  by (simp add: zgcd-greatest-iff)
with ass show False by (auto simp add: zprime-def)
qed
moreover
{ assume  $\neg P \text{ dvd } b * p + a * q$ 
  with  $P^n \text{ dvd-prod}$  and ass have  $P^n \text{ dvd } b * p - a * q$ 
  by (rule-tac  $a = b * p + a * q$  in zprime-power-z dvd-cancel-left, simp) }
moreover
{ assume  $\neg P \text{ dvd } b * p - a * q$ 
  with  $P^n \text{ dvd-prod}$  and ass have  $P^n \text{ dvd } b * p + a * q$ 
  by (rule-tac  $a = b * p + a * q$  in zprime-power-z dvd-cancel-right, simp) }
ultimately show ?thesis by auto
qed

```

**moreover**  
 { assume  $P^n \text{ dvd } b*p + a*q$   
 hence  $P^n \text{ dvd } b*p + 1*a*q \wedge |1| = (1::int)$  by *simp* }  
**moreover**  
 { assume  $P^n \text{ dvd } b*p - a*q$   
 hence  $P^n \text{ dvd } b*p + (-1)*a*q \wedge |-1| = (1::int)$  by *simp* }  
**ultimately show** *?thesis* by *blast*  
**qed**  
**then obtain**  $v \in e$  where  $v: b*p + e*a*q = P^n*v$  and  $e: |e| = 1$   
 by (*auto simp only: dvd-def*)  
**have**  $P^n \text{ dvd } a*p - e*N*b*q$   
**proof** (*cases*)  
 assume  $e1: e = 1$   
**from**  $U$  **have**  $(P^n)^2*U = A^n*P^n$  by (*simp add: power2-eq-square mult-ac*)  
**also with**  $e1$  **ass have**  $\dots = (a*p - e*N*b*q)^2 + N*(b*p + e*a*q)^2$   
 by (*simp only: qfN-mult2 add-commute zmult-1*)  
**also with**  $v$  **have**  $\dots = (a*p - e*N*b*q)^2 + (P^n)^2*(N*v^2)$   
 by (*simp only: power-mult-distrib mult-ac*)  
**finally have**  $(a*p - e*N*b*q)^2 = (P^n)^2*U - (P^n)^2*N*v^2$  by *simp*  
**also have**  $\dots = (P^n)^2 * (U - N*v^2)$  by (*simp only: zdiff-zmult-distrib2*)  
**finally have**  $(P^n)^2 \text{ dvd } (a*p - e*N*b*q)^2$  by (*rule dvdI*)  
**thus** *?thesis* by (*simp only: zpower-zdvd-mono*)  
**next**  
 assume  $\neg e=1$  with  $e$  **have**  $e1: e=-1$  by *auto*  
**from**  $U$  **have**  $(P^n)^2 * U = A^n * P^n$  by (*simp add: power2-eq-square*)  
**also with**  $e1$  **ass have**  $\dots = (a*p - e*N*b*q)^2 + N*(-(b*p + e*a*q))^2$   
 by (*simp add: qfN-mult1*)  
**also have**  $\dots = (a*p - e*N*b*q)^2 + N*(b*p + e*a*q)^2$   
 by (*simp only: power2-minus*)  
**also with**  $v$  **and** **ass have**  $\dots = (a*p - e*N*b*q)^2 + N*v^2*(P^n)^2$   
 by (*simp only: power-mult-distrib mult-ac*)  
**finally have**  $(a*p - e*N*b*q)^2 = (P^n)^2*U - (P^n)^2*N*v^2$  by *simp*  
**also have**  $\dots = (P^n)^2 * (U - N*v^2)$  by (*simp only: zdiff-zmult-distrib2*)  
**finally have**  $(P^n)^2 \text{ dvd } (a*p - e*N*b*q)^2$  by (*rule dvdI*)  
**thus** *?thesis* by (*simp only: zpower-zdvd-mono*)  
**qed**  
**then obtain**  $u$  where  $u: a*p - e*N*b*q = P^n*u$  by (*auto simp only: dvd-def*)  
**from**  $e$  **have**  $e2-1: e*e = 1$  by *auto*  
**have**  $a: a = p*u + e*N*q*v$   
**proof** -  
**from** *ass* **have**  $(p*u + e*N*q*v)*P^n = p*(P^n*u) + (e*N*q)*(P^n*v)$   
 by (*simp only: zadd-zmult-distrib mult-ac*)  
**also with**  $v$  **and**  $u$  **have**  $\dots = p*(a*p - e*N*b*q) + (e*N*q)*(b*p + e*a*q)$   
 by *simp*  
**also have**  $\dots = a*(p^2 + e*e*N*q^2)$   
 by (*simp add: power2-eq-square zadd-zmult-distrib2 mult-ac zdiff-zmult-distrib2*)  
**also with**  $e2-1$  **and** *ass* **have**  $\dots = a*P^n$  by *simp*  
**finally have**  $(a - (p*u + e*N*q*v))*P^n = 0$  by *auto*  
**moreover from** *ass* **have**  $P^n \neq 0$   
 by (*unfold zprime-def, auto simp add: power-eq-0-iff*)  
**ultimately show** *?thesis* by *auto*  
**qed**

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

proof –

from *ass* have  $(p*v - e*q*u)*P^n = p*(P^n*v) - (e*q)*(P^n*u)$

by (*simp only: zdiff-zmult-distrib mult-ac*)

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

also have  $\dots = b*(p^2 + e*e*N*q^2)$

by (*simp add: power2-eq-square zadd-zmult-distrib2 mult-ac zdiff-zmult-distrib2*)

also with  $e2-1$  and *ass* have  $\dots = b * P^n$  by *simp*

finally have  $(b - (p*v - e*q*u))*P^n = 0$  by *auto*

moreover from *ass* have  $P^n \neq 0$

by (*unfold zprime-def, auto simp add: power-eq-0-iff*)

ultimately show *?thesis* by *auto*

qed

moreover have  $A^n = (u^2 + N*v^2)*P^n$

proof (*cases*)

assume  $e=1$

with  $a$  and  $b$  and *ass* show *?thesis* by (*simp add: qfN-mult1 zmult-1 mult-ac*)

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 zmult-1 mult-ac*)

qed

moreover have  $zgcd(u,v)=1$

proof –

let  $?g = zgcd(u,v)$

have  $?g \text{ dvd } u \wedge ?g \text{ dvd } v$  by *auto*

hence  $?g \text{ dvd } u*p + v*(e*N*q) \wedge ?g \text{ dvd } v*p - u*(e*q)$

by (*simp add: zdvd-zmult2 zdvd-zadd zdvd-zdiff*)

with  $a$  and  $b$  have  $?g \text{ dvd } a \wedge ?g \text{ dvd } b$  by (*auto simp only: mult-ac*)

hence  $?g \text{ dvd } zgcd(a,b)$  by (*simp add: zgcd-greatest-iff*)

with *ass* have  $?g = 1 \vee ?g = -1$  by *simp*

moreover have  $?g \geq 0$  by (*rule zgcd-geq-zero*)

ultimately show *?thesis* by *auto*

qed

moreover from  $e$  and *ass* have

$|e| = 1 \wedge A^n = a^2 + N*b^2 \wedge P^n = p^2 + N*q^2$  by *simp*

ultimately show *?thesis* by *auto*

qed

lemma *qfN-primedivisor-not*:

assumes *ass*:  $zprime P \wedge Q > 0 \wedge is-qfN (P*Q) N \wedge \neg is-qfN P N$

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

proof (*rule ccontr, auto*)

assume *ass2*:  $\forall R. R \text{ dvd } Q \longrightarrow zprime R \longrightarrow is-qfN R N$

have  $\exists ps. primel ps \wedge int (prod ps) = Q$

proof –

from *ass* have  $Q=1 \vee nat(Q) > Suc 0$  by *auto*

moreover

{ assume  $Q=1$  hence  $primel [] \wedge int (prod []) = Q$  by (*simp add: primel-def*)  
hence *?thesis* by *auto* }

moreover

{ assume  $nat(Q) > Suc 0$

then have  $\exists ps. primel ps \wedge prod ps = nat(Q)$  by (*simp only: factor-exists*)

```

    with ass have ?thesis by auto }
  ultimately show ?thesis by blast
qed
then obtain ps where ps: primel ps  $\wedge$  int(prod ps) = Q by auto
have ps-lemma: (primel ps  $\wedge$  is-qn (P*int(prod ps)) N
 $\wedge$  ( $\forall R. (zprime R \wedge R \text{ dvd } \text{int}(\text{prod } ps)) \longrightarrow \text{is-qn } R \text{ } N$ )  $\implies$  False
(is ?B ps  $\implies$  False)
proof (induct ps)
  case Nil hence is-qn P N by simp
  with ass show False by simp
next
  case (Cons p ps)
  hence ass3: ?B ps  $\implies$  False
    and IH: ?B (p#ps) by simp
  hence p: zprime (int p) and int p dvd int(prod(p#ps))
    by (auto simp add: primel-def prime-impl-zprime-int int-mult)
  moreover with IH have qn: is-qn (int p) N
    and int p dvd P*int(prod(p#ps)) and is-qn (P*int(prod(p#ps))) N
    by (auto simp add: zdvd-zmult)
  ultimately obtain S where S: P*int(prod(p#ps)) = S*(int p)  $\wedge$  is-qn S N
    by (auto dest: qn-div-prime-general)
  hence (int p)*(P*int(prod ps) - S) = 0 by (auto simp add: int-mult)
  with p S have is-qn (P*int(prod ps)) N by (auto simp add: zprime-def)
  moreover from IH have primel ps by (simp add: primel-def)
  moreover from IH have  $\forall R. zprime R \wedge R \text{ dvd } \text{int}(\text{prod } ps) \longrightarrow \text{is-qn } R \text{ } N$ 
    by (auto simp add: int-mult zdvd-zmult)
  ultimately have ?B ps by simp
  with ass3 show False by simp
qed
with ps ass2 ass show False by auto
qed

```

lemma *qn-oddprime-cube*:

```

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

```

proof –

```

let ?P = p^2+N*q^2
assume P: zprime ?P and Podd: ?P  $\in$  zOdd 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: nat-number ring-simps)
have zgcd(?b,?a)  $\neq$  1  $\implies$  ?P dvd p

```

proof –

```

let ?h = zgcd(?b,?a)
assume h1: ?h  $\neq$  1
have ?h  $\geq$  0 by (rule zgcd-geq-zero)
hence ?h = 0  $\vee$  ?h = 1  $\vee$  ?h > 1 by auto
with h1 have ?h = 0  $\vee$  ?h > 1 by auto
moreover
{ assume ?h = 0 hence nat|?b| = 0  $\wedge$  nat|?a| = 0
  by (unfold zgcd-def, auto simp add: gcd-zero)

```

hence  $?a = 0 \wedge ?b = 0$  by *arith*  
 with  $abP$  have  $?P^3 = 0$  by *auto*  
 with  $P$  have *False* by (*unfold zprime-def, auto*)  
 hence *?thesis* by *simp* }

moreover

{ assume  $?h > 1$  hence  $\exists g. \text{zprime } g \wedge g \text{ dvd } ?h$  by (*rule zprime-factor-exists*)  
 then obtain  $g$  where  $g: \text{zprime } g \wedge g \text{ dvd } ?h$  by *blast*  
 hence  $g \text{ dvd } ?b \wedge g \text{ dvd } ?a$  by (*simp add: zgcd-greatest-iff*)  
 with  $g$  have  $g1: g \text{ dvd } q \vee g \text{ dvd } 3*p^2 - N*q^2$   
   and  $g2: g \text{ dvd } p \vee g \text{ dvd } p^2 - 3*N*q^2$   
   by (*auto simp add: zprime-zdvd-zmult-general*)  
 from  $g$  have  $gpos: g \geq 0$  by (*auto simp only: zprime-def*)  
 have  $g \text{ dvd } ?P$   
 proof (*cases*)  
   assume  $g \text{ dvd } q$   
   hence  $gNq: g \text{ dvd } N*q^2$  by (*auto simp add: dvd-def power2-eq-square*)  
   show *?thesis*  
   proof (*cases*)  
     assume  $gp: g \text{ dvd } p$   
     hence  $g \text{ dvd } p^2$  by (*auto simp add: dvd-def power2-eq-square*)  
     with  $gNq$  show *?thesis* by (*auto simp add: zdvd-zadd*)  
   next  
     assume  $\neg g \text{ dvd } p$  with  $g2$  have  $g \text{ dvd } p^2 - 3*N*q^2$  by *auto*  
     moreover from  $gNq$  have  $g \text{ dvd } 4*(N*q^2)$  by (*rule zdvd-zmult*)  
     ultimately have  $g \text{ dvd } p^2 - 3*(N*q^2) + 4*(N*q^2)$   
     by (*simp only: zdvd-zadd mult-ac*)  
     moreover have  $p^2 - 3*(N*q^2) + 4*(N*q^2) = p^2 + N*q^2$  by *arith*  
     ultimately show *?thesis* by *simp*

qed

next

assume  $\neg g \text{ dvd } q$  with  $g1$  have  $gpq: g \text{ dvd } 3*p^2 - N*q^2$  by *simp*  
 show *?thesis*  
 proof (*cases*)  
   assume  $g \text{ dvd } p$   
   hence  $g \text{ dvd } 4*p^2$  by (*auto simp add: dvd-def power2-eq-square*)  
   with  $gpq$  have  $g \text{ dvd } 4*p^2 - (3*p^2 - N*q^2)$  by (*simp only: zdvd-zdiff*)  
   moreover have  $4*p^2 - (3*p^2 - N*q^2) = p^2 + N*q^2$  by *arith*  
   ultimately show *?thesis* by *simp*

next

assume  $\neg g \text{ dvd } p$  with  $g2$  have  $g \text{ dvd } p^2 - 3*N*q^2$  by *auto*  
 with  $gpq$  have  $g \text{ dvd } 3*p^2 - N*q^2 - (p^2 - 3*N*q^2)$   
   by (*simp only: zdvd-zdiff*)  
 moreover have  $3*p^2 - N*q^2 - (p^2 - 3*N*q^2) = 2*?P$  by *auto*  
 ultimately have  $g \text{ dvd } 2*?P$  by *simp*  
 with  $g$  have  $g \text{ dvd } 2 \vee g \text{ dvd } ?P$  by (*simp only: zprime-zdvd-zmult*)  
 moreover have  $\neg g \text{ dvd } 2$   
 proof (*rule ccontr, simp*)  
   assume  $gdvd2: g \text{ dvd } 2$   
   have  $g \leq 2$   
   proof (*rule ccontr*)  
     assume  $\neg g \leq 2$  hence  $g > 2$  by *simp*  
     moreover have  $(0::int) < 2$  by *auto*

```

    ultimately have  $\neg g \text{ dvd } 2$  by (auto simp only: zdvd-not-zless)
    with  $gdvd2$  show False by simp
  qed
  moreover from  $g$  have  $g \geq 2$  by (simp add: zprime-def)
  ultimately have  $g = 2$  by auto
  with  $g$  have  $2 \text{ dvd } ?a \wedge 2 \text{ dvd } ?b$  by (auto simp add: zgcd-greatest-iff)
  hence  $2 \text{ dvd } ?a^2 \wedge 2 \text{ dvd } N * ?b^2$ 
    by (auto simp only: power2-eq-square zdvd-zmult)
  with  $abP$  have  $2 \text{ dvd } ?P^3$  by (simp only: zdvd-zadd)
  hence  $?P^3 \in \text{zEven}$  by (auto simp add: dvd-def zEven-def)
  moreover have  $?P^3 \in \text{zOdd}$ 
  proof -
    from  $P\text{odd}$  have  $?P * ?P^2 \in \text{zOdd}$ 
      by (simp only: odd-times-odd power2-eq-square)
    thus ?thesis by (simp only: cube-square)
  qed
  ultimately show False by (auto simp only: odd-iff-not-even)
  qed
  ultimately show ?thesis by simp
  qed
  with  $P$   $gpos$  have  $g = 1 \vee g = ?P$  by (auto simp only: zprime-def)
  with  $g$  have  $g = ?P$  by (simp add: zprime-def)
  with  $g$  have  $Pab: ?P \text{ dvd } ?a \wedge ?P \text{ dvd } ?b$  by (auto simp add: zgcd-greatest-iff)
  have ?thesis
  proof -
    from  $Pab$   $P$  have  $?P \text{ dvd } p \vee ?P \text{ dvd } p^2 - 3 * N * q^2$ 
      by (auto simp add: zprime-zdvd-zmult-general)
    moreover
    { assume  $?P \text{ dvd } p^2 - 3 * N * q^2$ 
      moreover have  $?P \text{ dvd } 3 * (p^2 + N * q^2)$ 
        by (auto simp only: zdvd-refl zdvd-zmult)
      ultimately have  $?P \text{ dvd } p^2 - 3 * N * q^2 + 3 * (p^2 + N * q^2)$ 
        by (simp only: zdvd-zadd)
      hence  $?P \text{ dvd } 4 * p^2$  by auto
      with  $P$  have  $?P \text{ dvd } 4 \vee ?P \text{ dvd } p^2$ 
        by (simp only: zprime-zdvd-zmult-general)
      moreover have  $\neg ?P \text{ dvd } 4$ 
      proof (rule ccontr, simp)
        assume  $P\text{dvd}4: ?P \text{ dvd } 4$ 
        have  $?P \leq 4$ 
        proof (rule ccontr)
          assume  $\neg ?P \leq 4$  hence  $?P > 4$  by simp
          moreover have  $(0::\text{int}) < 4$  by auto
          ultimately have  $\neg ?P \text{ dvd } 4$  by (auto simp only: zdvd-not-zless)
          with  $P\text{dvd}4$  show False by simp
        qed
      qed
    }
    moreover from  $P$  have  $?P \geq 2$  by (auto simp add: zprime-def)
    moreover have  $?P \neq 2 \wedge ?P \neq 4$ 
    proof (rule ccontr, simp)
      assume  $?P = 2 \vee ?P = 4$  hence  $?P \in \text{zEven}$ 
        by (auto simp add: zEven-def)
    }
  }

```

```

    with Podd show False by (simp add: odd-iff-not-even)
  qed
  ultimately have ?P = 3 by auto
  with P dvd 4 have (3::int) dvd 4 by simp
  thus False by arith
  qed
  ultimately have ?P dvd p*p by (simp add: power2-eq-square)
  with P have ?thesis by (auto dest: zprime-zdvd-zmult-general) }
  ultimately show ?thesis by auto
  qed }
  ultimately show ?thesis by blast
  qed
  moreover have zgcd(N, ?a) ≠ 1 ⇒ ?P dvd p
  proof -
    let ?h = zgcd(N, ?a)
    assume h1: ?h ≠ 1
    have ?h ≥ 0 by (rule zgcd-geq-zero)
    hence ?h = 0 ∨ ?h = 1 ∨ ?h > 1 by auto
    with h1 have ?h = 0 ∨ ?h > 1 by auto
  moreover
  { assume ?h = 0 hence nat|N| = 0 ∧ nat|?a| = 0
    by (unfold zgcd-def, auto simp add: gcd-zero)
    hence N = 0 by arith
    with N1 have False by auto
    hence ?thesis by simp }
  moreover
  { assume ?h > 1 hence ∃ g. zprime g ∧ g dvd ?h by (rule zprime-factor-exists)
    then obtain g where g: zprime g ∧ g dvd ?h by blast
    hence gN: g dvd N and g dvd ?a by (auto simp add: zgcd-greatest-iff)
    hence g dvd p*p^2 - N*(3*p*q^2)
      by (auto simp only: zdiff-zmult-distrib2 mult-ac)
    with gN have g dvd p*p^2 - N*(3*p*q^2) + N*(3*p*q^2)
      by (simp only: zdvd-zadd zdvd-zmult2)
    hence g dvd p*p^2 by simp
    with g have g dvd p ∨ g dvd p*p
      by (simp add: zprime-zdvd-zmult-general power2-eq-square)
    with g have gp: g dvd p by (auto dest: zprime-zdvd-zmult-general)
    hence g dvd p^2 by (simp add: zdvd-zmult power2-eq-square)
    with gN have gP: g dvd ?P by (auto simp add: zdvd-zmult2 zdvd-zadd)
    from g have g ≥ 0 by (simp add: zprime-def)
    with gP P have g = 1 ∨ g = ?P by (auto simp only: zprime-def)
    with g have g = ?P by (auto simp only: zprime-def)
    with gp have ?thesis by simp }
  ultimately show ?thesis by auto
  qed
  moreover have ¬ ?P dvd p
  proof (rule ccontr, clarsimp)
    assume P dvd p: ?P dvd p
    have p^2 ≥ ?P^2
    proof (rule ccontr)
      assume ¬ p^2 ≥ ?P^2 hence pP: p^2 < ?P^2 by simp
      moreover with p0 have p^2 > 0 by (simp add: zero-less-power2)

```

ultimately have  $\neg ?P^2 \text{ dvd } p^2$  by (simp add: zdvd-not-zless)  
 with Pdvdp show False by (simp add: zpower-zdvd-mono)  
 qed  
 moreover with P have  $?P*1 < ?P*?P$   
 by (unfold zprime-def, auto simp only: zmult-zless-mono2)  
 ultimately have  $p^2 > ?P$  by (auto simp add: power2-eq-square)  
 hence neg:  $N*q^2 < 0$  by auto  
 show False  
 proof -  
 have is-qn ( $0^2 + N*q^2$ ) N by (auto simp only: is-qn-def)  
 with N1 have  $0^2 + N*q^2 \geq 0$  by (rule qn-pos)  
 with neg show False by simp  
 qed  
 qed  
 ultimately have  $\text{zgcd}(?b, ?a) = 1 \wedge \text{zgcd}(N, ?a) = 1$  by auto  
 hence  $\text{zgcd}(N*?b, ?a) = 1$  by (simp only: zgcd-zmult-cancel)  
 with abP show ?thesis by (auto simp only: zgcd-commute)  
 qed

#### 4.4 Uniqueness ( $N > 1$ )

lemma qfN-prime-unique:

$\llbracket \text{zprime } (a^2 + N*b^2); N > 1; a^2 + N*b^2 = c^2 + N*d^2 \rrbracket$   
 $\implies (|a| = |c| \wedge |b| = |d|)$

proof -

let  $?P = a^2 + N*b^2$

assume P: zprime ?P and N:  $N > 1$  and abcdN:  $?P = c^2 + N*d^2$

have mult:  $(a*d + b*c)*(a*d - b*c) = ?P*(d^2 - b^2)$

proof -

have  $(a*d + b*c)*(a*d - b*c) = (a^2 + N*b^2)*d^2 - b^2*(c^2 + N*d^2)$

by (simp add: nat-number ring-simps)

with abcdN show ?thesis by (simp add: ring-simps)

qed

have  $?P \text{ dvd } a*d + b*c \vee ?P \text{ dvd } a*d - b*c$

proof -

from mult have  $?P \text{ dvd } (a*d + b*c)*(a*d - b*c)$  by simp

with P show ?thesis by (simp add: zprime-zdvd-zmult-general)

qed

moreover

{ assume  $?P \text{ dvd } a*d + b*c$

then obtain Q where  $Q: a*d + b*c = ?P*Q$  by (auto simp add: dvd-def)

from abcdN have  $?P^2 = (a^2 + N*b^2) * (c^2 + N*d^2)$

by (simp add: power2-eq-square)

also have  $\dots = (a*c - N*b*d)^2 + N*(a*d + b*c)^2$  by (rule qfN-mult2)

also with Q have  $\dots = (a*c - N*b*d)^2 + N*Q^2*?P^2$

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

also have  $\dots \geq N*Q^2*?P^2$  by (simp add: zero-le-power2)

finally have pos:  $?P^2 \geq ?P^2*(Q^2*N)$  by (simp add: mult-ac)

have  $b^2 = d^2$

proof (rule ccontr)

assume  $b^2 \neq d^2$

with P mult Q have  $Q \neq 0$  by (unfold zprime-def, auto)

hence  $Q^2 > 0$  by (*simp add: zero-less-power2*)  
 moreover with  $N$  have  $Q^2 * N > Q^2 * 1$  by (*simp only: zmult-zless-mono2*)  
 ultimately have  $Q^2 * N > 1$  by *arith*  
 moreover with  $P$  have  $?P^2 > 0$  by (*simp add: zprime-def zero-less-power2*)  
 ultimately have  $?P^2 * 1 < ?P^2 * (Q^2 * N)$  by (*simp only: zmult-zless-mono2*)  
 with *pos* show *False* by *simp*  
 qed }  
 moreover  
 { assume  $?P \text{ dvd } a*d - b*c$   
 then obtain  $Q$  where  $Q: a*d - b*c = ?P * Q$  by (*auto simp add: dvd-def*)  
 from *abcdN* have  $?P^2 = (a^2 + N*b^2) * (c^2 + N*d^2)$   
 by (*simp add: power2-eq-square*)  
 also have  $\dots = (a*c + N*b*d)^2 + N*(a*d - b*c)^2$  by (*rule qfN-mult1*)  
 also with  $Q$  have  $\dots = (a*c + N*b*d)^2 + N*Q^2 * ?P^2$   
 by (*simp add: mult-ac power-mult-distrib*)  
 also have  $\dots \geq N*Q^2 * ?P^2$  by (*simp add: zero-le-power2*)  
 finally have *pos*:  $?P^2 \geq ?P^2 * (Q^2 * N)$  by (*simp add: mult-ac*)  
 have  $b^2 = d^2$   
 proof (*rule ccontr*)  
 assume  $b^2 \neq d^2$   
 with  $P$  mult  $Q$  have  $Q \neq 0$  by (*unfold zprime-def, auto*)  
 hence  $Q^2 > 0$  by (*simp add: zero-less-power2*)  
 moreover with  $N$  have  $Q^2 * N > Q^2 * 1$  by (*simp only: zmult-zless-mono2*)  
 ultimately have  $Q^2 * N > 1$  by *arith*  
 moreover with  $P$  have  $?P^2 > 0$  by (*simp add: zprime-def zero-less-power2*)  
 ultimately have  $?P^2 * 1 < ?P^2 * (Q^2 * N)$  by (*simp only: zmult-zless-mono2*)  
 with *pos* show *False* by *simp*  
 qed }  
 ultimately have *bd*:  $b^2 = d^2$  by *blast*  
 moreover with *abcdN* have  $a^2 = c^2$  by *auto*  
 ultimately show *?thesis* by (*auto simp only: power2-eq-iff-abs-eq*)  
 qed

lemma *qfN-square-prime*:

assumes *ass*:

*zprime*  $(p^2 + N*q^2) \wedge N > 1 \wedge (p^2 + N*q^2)^2 = r^2 + N*s^2 \wedge \text{zgcd}(r,s) = 1$   
 shows  $|r| = |p^2 - N*q^2| \wedge |s| = |2*p*q|$

proof –

let  $?P = p^2 + N*q^2$

let  $?A = r^2 + N*s^2$

from *ass* have *P1*:  $?P > 1$  by (*simp add: zprime-def*)

from *ass* have *APP*:  $?A = ?P * ?P$  by (*simp only: power2-eq-square*)

with *ass* have *zprime*  $?P \wedge ?P \text{ dvd } ?A$  by (*simp add: dvdI*)

then obtain  $u \ v \ e$  where *uve*:

$?A = (u^2 + N*v^2) * ?P \wedge r = p*u + e*N*q*v \wedge s = p*v - e*q*u \wedge |e| = 1$

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

with *APP P1 ass* have *zprime*  $(u^2 + N*v^2) \wedge N > 1 \wedge u^2 + N*v^2 = ?P$

by *auto*

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

then obtain  $f \ g$  where  $f: u = f*p \wedge |f| = 1$  and  $g: v = g*q \wedge |g| = 1$

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

with *uve* have  $r = f*p*p + (e*g)*N*q*q \wedge s = g*p*q - (e*f)*p*q$  by *simp*

**hence**  $rs: r = f*p^2 + (e*g)*N*q^2 \wedge s = (g - e*f)*p*q$   
**by** (*auto simp only: power2-eq-square zdiff-zmult-distrib*)  
**moreover** **have**  $s \neq 0$   
**proof** (*rule ccontr, simp*)  
**assume**  $s0: s=0$   
**hence**  $zgcd(r,s) = |r|$  **by** (*simp only: zgcd-0*)  
**with**  $ass$  **have**  $|r| = 1$  **by** *simp*  
**hence**  $r^2 = 1$  **by** (*auto simp add: abs-power2-distrib*)  
**with**  $s0$  **have**  $?A = 1$  **by** *simp*  
**moreover** **have**  $?P^2 > 1$   
**proof** –  
**from**  $P1$  **have**  $1 < ?P \wedge (0::int) \leq 1 \wedge (0::nat) < 2$  **by** *auto*  
**hence**  $?P^2 > 1^2$  **by** (*simp only: power-strict-mono*)  
**thus**  $?thesis$  **by** *auto*  
**qed**  
**moreover** **from**  $ass$  **have**  $?A = ?P^2$  **by** *simp*  
**ultimately** **show** *False* **by** *auto*  
**qed**  
**ultimately** **have**  $g \neq e*f$  **by** *auto*  
**moreover** **from**  $f g$  **we** **have**  $|g| = |e*f|$  **by** *auto*  
**ultimately** **have**  $g = -(e*f)$  **by** *arith*  
**with**  $rs$  **we** **have**  $r = f*(p^2 - N*q^2) \wedge s = -(e*f)*2*p*q$   
**by** (*auto simp add: power2-eq-square zdiff-zmult-distrib2*)  
**hence**  $|r| = |f| * |p^2 - N*q^2|$   
 $\wedge |s| = |e|*|f|*2*p*q$   
**by** (*auto simp add: abs-mult*)  
**with**  $f g$  **show**  $?thesis$  **by** (*auto simp only: zmult-1*)  
**qed**

**lemma** *qfN-cube-prime*:

**assumes**  $ass: zprime (p^2 + N*q^2) \wedge N > 1$   
 $\wedge (p^2 + N*q^2)^3 = a^2 + N*b^2 \wedge zgcd(a, b)=1$   
**shows**  $|a| = |p^3 - 3*N*p*q^2| \wedge |b| = |3*p^2*q - N*q^3|$   
**proof** –  
**let**  $?P = p^2 + N*q^2$   
**let**  $?A = a^2 + N*b^2$   
**from**  $ass$  **have**  $P1: ?P > 1$  **by** (*simp add: zprime-def*)  
**with**  $ass$  **have**  $APP: ?A = ?P*?P^2$  **by** (*auto simp only: cube-square*)  
**with**  $ass$  **have**  $zprime ?P \wedge ?P \text{ dvd } ?A$  **by** (*simp add: dvdI*)  
**then** **obtain**  $u v e$  **where**  $u v e$ :  
 $?A = (u^2 + N*v^2)*?P \wedge a = p*u + e*N*q*v \wedge b = p*v - e*q*u \wedge |e|=1$   
**by** (*frule-tac p=p in qfN-div-prime, auto*)  
**have**  $zgcd(u,v)=1$   
**proof** –  
**let**  $?g = zgcd(u,v)$   
**have**  $?g \text{ dvd } u \wedge ?g \text{ dvd } v$  **by** (*auto simp add: zgcd-greatest-iff*)  
**with**  $u v$  **have**  $?g \text{ dvd } a \wedge ?g \text{ dvd } b$   
**by** (*auto simp add: zdvd-zmult zdvd-zadd zdvd-zdiff*)  
**hence**  $?g \text{ dvd } zgcd(a,b)$  **by** (*auto simp add: zgcd-greatest-iff*)  
**with**  $ass$  **have**  $?g \text{ dvd } 1$  **by** *simp*  
**moreover** **have**  $?g \geq 0$  **by** (*rule zgcd-geq-zero*)  
**ultimately** **show**  $?thesis$  **by** *auto*

**qed**  
**with**  $P1$  *we APP ass* **have**  $zprime\ ?P \wedge N > 1 \wedge ?P^2 = u^2 + N*v^2$   
 $\wedge zgcd(u,v)=1$  **by** (*auto simp add: mult-ac*)  
**hence**  $|u| = |p^2 - N*q^2| \wedge |v| = |2*p*q|$  **by** (*rule qfN-square-prime*)  
**then obtain**  $f\ g$  **where**  $f: u = f*(p^2 - N*q^2) \wedge |f| = 1$   
**and**  $g: v = g*(2*p*q) \wedge |g| = 1$  **by** (*blast dest: abs-eq-impl-unitfactor*)  
**with** *we* **have**  $a = p*f*(p^2 - N*q^2) + e*N*q*g*2*p*q$   
 $\wedge b = p*g*2*p*q - e*q*f*(p^2 - N*q^2)$  **by** *auto*  
**hence**  $ab: a = f*p*p^2 + -f*N*p*q^2 + 2*e*g*N*p*q^2$   
 $\wedge b = 2*g*p^2*q - e*f*p^2*q + e*f*N*q*q^2$   
**by** (*auto simp add: mult-ac zdiff-zmult-distrib2 power2-eq-square*)  
**from**  $f$  **have**  $f2: f^2 = 1$  **by** (*auto simp add: abs-power2-distrib*)  
**from**  $g$  **have**  $g2: g^2 = 1$  **by** (*auto simp add: abs-power2-distrib*)  
**have**  $e \neq f*g$   
**proof** (*rule ccontr, simp*)  
**assume**  $efg: e = f*g$   
**with**  $ab\ g$  **have**  $a = f*p*p^2 + f*N*p*q^2$  **by** (*auto simp add: power2-eq-square*)  
**hence**  $a = (f*p)*?P$  **by** (*auto simp add: zadd-zmult-distrib2 mult-ac*)  
**hence**  $Pa: ?P \text{ dvd } a$  **by** *auto*  
**from**  $efg\ f\ ab$  **have**  $b = g*p^2*q + g*N*q*q^2$  **by** (*auto simp add: power2-eq-square*)  
**hence**  $b = (g*q)*?P$  **by** (*auto simp add: zadd-zmult-distrib2 mult-ac*)  
**hence**  $?P \text{ dvd } b$  **by** *auto*  
**with**  $Pa$  **have**  $?P \text{ dvd } zgcd(a,b)$  **by** (*simp add: zgcd-greatest-iff*)  
**with** *ass* **have**  $?P \text{ dvd } 1$  **by** *auto*  
**with**  $P1$  **show** *False* **by** *auto*  
**qed**  
**moreover from**  $f\ g$  *we* **have**  $|e| = |f*g|$  **by** *auto*  
**ultimately have**  $e = -(f*g)$  **by** *arith*  
**with**  $ab\ f\ g$  **have**  $a = f*p*p^2 - 3*f*N*p*q^2 \wedge b = 3*g*p^2*q - g*N*q*q^2$   
**by** (*auto simp add: power2-eq-square*)  
**hence**  $a = f*(p^3 - 3*N*p*q^2) \wedge b = g*(3*p^2*q - N*q^3)$   
**by** (*auto simp only: zdiff-zmult-distrib2 mult-ac cube-square*)  
**with**  $f\ g$  **show** *?thesis* **by** (*auto simp add: zmult-1 abs-mult*)  
**qed**

#### 4.5 The case $N = 3$

**lemma** *qf3-even*:  $a^2 + 3*b^2 \in zEven \implies \exists B. a^2 + 3*b^2 = 4*B \wedge is-qfN\ B\ 3$

**proof** –

**let**  $?A = a^2 + 3*b^2$   
**assume**  $even: ?A \in zEven$   
**have**  $(a \in zOdd \wedge b \in zOdd) \vee (a \in zEven \wedge b \in zEven)$   
**proof** (*rule ccontr, auto dest: not-odd-impl-even*)  
**assume**  $a \notin zOdd$  **and**  $b \notin zEven$   
**hence**  $a \in zEven \wedge b \in zOdd$  **by** (*auto simp only: odd-iff-not-even*)  
**hence**  $a^2 \in zEven \wedge b^2 \in zOdd$   
**by** (*auto simp only: power2-eq-square odd-times-odd even-times-either*)  
**moreover have**  $3 \in zOdd$  **by** (*unfold zOdd-def, auto*)  
**ultimately have**  $?A \in zOdd$  **by** (*auto simp add: odd-times-odd even-plus-odd*)  
**with**  $even$  **show** *False* **by** (*simp add: odd-iff-not-even*)  
**next**  
**assume**  $a \notin zEven$  **and**  $b \notin zOdd$

hence  $a \in zOdd \wedge b \in zEven$  **by** (*auto simp only: odd-iff-not-even*)  
 hence  $a^2 \in zOdd \wedge b^2 \in zEven$   
 by (*auto simp only: power2-eq-square odd-times-odd even-times-either*)  
 moreover hence  $b^2 * 3 \in zEven$  **by** (*simp only: even-times-either*)  
 ultimately have  $b^2 * 3 + a^2 \in zOdd$  **by** (*auto simp add: even-plus-odd*)  
 hence  $?A \in zOdd$  **by** (*simp only: mult-ac add-ac*)  
 with *even* show *False* **by** (*simp add: odd-iff-not-even*)  
**qed**  
 moreover  
 { assume  $a \in zEven \wedge b \in zEven$   
 then obtain  $c d$  where  $abcd: a = 2*c \wedge b = 2*d$  **by** (*unfold zEven-def, auto*)  
 hence  $?A = 4*(c^2 + 3*d^2)$  **by** (*simp add: power-mult-distrib*)  
 moreover have  $is-qn (c^2 + 3*d^2) 3$  **by** (*unfold is-qn-def, auto*)  
 ultimately have *?thesis* **by blast** }  
 moreover  
 { assume  $a \in zOdd \wedge b \in zOdd$   
 then obtain  $c d$  where  $abcd: a = 2*c + 1 \wedge b = 2*d + 1$   
 by (*unfold zOdd-def, auto*)  
 have  $c - d \in zOdd \vee c - d \in zEven$  **by** (*rule-tac x=c-d in even-odd-disj*)  
 moreover  
 { assume  $c - d \in zEven$   
 then obtain  $e$  where  $c - d = 2*e$  **by** (*auto simp add: zEven-def*)  
 with *abcd* have  $e1: a - b = 4*e$  **by arith**  
 hence  $e2: a + 3*b = 4*(e + b)$  **by auto**  
 have  $4*?A = (a + 3*b)^2 + 3*(a - b)^2$   
 by (*simp add: nat-number ring-simps*)  
 also with  $e1 e2$  have  $\dots = (4*(e + b))^2 + 3*(4*e)^2$  **by** (*simp(no-asm-simp)*)  
 finally have  $?A = 4*((e + b)^2 + 3*e^2)$  **by** (*simp add: nat-number ring-simps*)  
 moreover have  $is-qn ((e + b)^2 + 3*e^2) 3$  **by** (*unfold is-qn-def, auto*)  
 ultimately have *?thesis* **by blast** }  
 moreover  
 { assume  $c - d \in zOdd$   
 then obtain  $e$  where  $c - d = 2*e + 1$  **by** (*auto simp add: zOdd-def*)  
 with *abcd* have  $e1: a + b = 4*(e + d + 1)$  **by auto**  
 hence  $e2: a - 3*b = 4*(e + d - b + 1)$  **by auto**  
 have  $4*?A = (a - 3*b)^2 + 3*(a + b)^2$   
 by (*simp add: nat-number ring-simps*)  
 also with  $e1 e2$  have  $\dots = (4*(e + d - b + 1))^2 + 3*(4*(e + d + 1))^2$   
 by (*simp(no-asm-simp)*)  
 finally have  $?A = 4*((e + d - b + 1)^2 + 3*(e + d + 1)^2)$   
 by (*simp add: nat-number ring-simps*)  
 moreover have  $is-qn ((e + d - b + 1)^2 + 3*(e + d + 1)^2) 3$   
 by (*unfold is-qn-def, auto*)  
 ultimately have *?thesis* **by blast** }  
 ultimately have *?thesis* **by auto** }  
 ultimately show *?thesis* **by auto**  
**qed**

lemma *qf3-even-general*:  $\llbracket is-qn A 3; A \in zEven \rrbracket$   
 $\implies \exists B. A = 4*B \wedge is-qn B 3$

**proof** –

assume  $A \in zEven$  and  $is-qn A 3$

then obtain  $a b$  where  $A = a^2 + 3b^2$   
 and  $a^2 + 3b^2 \in zEven$  by (unfold is-qn-def, auto)  
 thus ?thesis by (auto simp add: qf3-even)  
 qed

lemma qf3-oddprimedivisor-not:

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

proof (rule ccontr, simp)

assume  $ass2: \forall R. R \text{ dvd } Q \longrightarrow R \in zOdd \longrightarrow zprime R \longrightarrow is-qn R \exists$   
 (is ?A Q)

obtain  $n::nat$  where  $n = nat Q$  by auto

with  $ass$  have  $n: Q = int n$  by auto

have  $(n > 0 \wedge is-qn (P*int n) \exists \wedge ?A(int n)) \implies False$  (is ?B n  $\implies False$ )

proof (induct n rule: less-induct)

case (less n)

hence IH:  $\forall m. m < n \wedge ?B m \implies False$

and  $Bn: ?B n$  by auto

show False

proof (cases)

assume  $odd: (int n) \in zOdd$

from  $Bn$   $ass$  have  $zprime P \wedge int n > 0 \wedge is-qn (P*int n) \exists \wedge \neg is-qn P \exists$   
 by simp

hence  $\exists R. zprime R \wedge R \text{ dvd } int n \wedge \neg is-qn R \exists$

by (rule qn-primedivisor-not)

then obtain  $R$  where  $R: zprime R \wedge R \text{ dvd } int n \wedge \neg is-qn R \exists$  by auto

moreover with  $odd$  have  $R \in zOdd$

proof -

from  $R$  obtain  $U$  where  $int n = R*U$  by (auto simp add: dvd-def)

with  $odd$  show ?thesis by (auto dest: odd-mult-odd-prop)

qed

moreover from  $Bn$  have ?A (int n) by simp

ultimately show False by auto

next

assume  $\neg (int n) \in zOdd$

hence  $even: int n \in zEven$  by (rule not-odd-impl-even)

hence  $(int n)*P \in zEven$  by (rule even-times-either)

with  $Bn$  have  $P*int n \in zEven \wedge is-qn (P*int n) \exists$  by (simp add: mult-ac)

hence  $\exists B. P*(int n) = 4*B \wedge is-qn B \exists$  by (simp only: qf3-even-general)

then obtain  $B$  where  $B: P*(int n) = 4*B \wedge is-qn B \exists$  by auto

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

moreover have  $\neg 2 \text{ dvd } P$

proof (rule ccontr, simp)

assume  $2 \text{ dvd } P$

with  $ass$  have  $P \in zOdd \wedge P \in zEven$  by (simp add: dvd-def zEven-def)

thus False by (simp only: even-odd-conj)

qed

moreover have  $zprime 2$  by (rule zprime-2)

ultimately have  $2^2 \text{ dvd } int n$

by (rule-tac p=2 in zprime-power-zdvd-cancel-right)

then obtain  $im::int$  where  $int n = 4*im$  by (auto simp add: dvd-def)

moreover obtain  $m::nat$  where  $m = nat im$  by auto

```

ultimately have  $m: n = 4 * m$  by arith
with  $B$  have  $is\text{-}qfN (P * int\ m) \exists$  by (auto simp add: int-mult)
moreover from  $m\ Bn$  have  $m > 0$  by auto
moreover from  $m\ Bn$  have  $?A (int\ m)$ 
  by (auto simp add: zdvd-zmult int-mult)
ultimately have  $Bm: ?B\ m$  by simp
from  $Bn\ m$  have  $m < n$  by arith
with  $IH\ Bm$  show  $False$  by auto
qed
qed
with  $ass\ ass2\ n$  show  $False$  by auto
qed

lemma  $qf3\text{-}oddprime\ divisor$ :
  [|  $zprime\ P; P \in zOdd; zgcd(a,b)=1; P\ dvd\ (a^2+3*b^2)$  |]
  ==>  $is\text{-}qfN\ P\ \exists$ 
proof -
  have  $lem: \forall a\ b. (zprime\ P \wedge P \in zOdd \wedge zgcd(a,b)=1 \wedge P\ dvd\ (a^2+3*b^2))$ 
     $\longrightarrow is\text{-}qfN\ P\ \exists$  (is  $?B\ P$ )
  proof (rule-tac  $x=P$  and  $V=\lambda P. nat|P|$  in  $val\text{-}infinite\text{-}descent$ )
    fix  $x$ 
    assume  $nat|x| = 0$ 
    hence  $x = 0$  by arith
    thus  $?B\ x$  by (simp add:  $zprime\text{-}def$ )
  next
    fix  $x$ 
    assume  $nat|x| > 0$  and  $\neg ?B\ x$ 
    then obtain  $a\ b$  where  $abx: zprime\ x \wedge x \in zOdd \wedge zgcd(a,b)=1$ 
       $\wedge x\ dvd\ (a^2+3*b^2) \wedge \neg is\text{-}qfN\ x\ \exists$  by auto
    then obtain  $M$  where  $M: a^2+3*b^2 = x * M$  by (auto simp add:  $dvd\text{-}def$ )
    let  $?A = a^2 + 3*b^2$ 
    from  $abx$  have  $x0: x > 0 \wedge x \in zOdd$  by (simp add:  $zprime\text{-}def$ )
    then obtain  $m$  where  $2*|a-m*x| < x$  by (auto dest:  $best\text{-}odd\text{-}division\text{-}abs$ )
    then obtain  $c$  where  $cm: c = a-m*x \wedge 2*|c| < x$  by auto
    from  $x0$  obtain  $n$  where  $2*|b-n*x| < x$  by (auto dest:  $best\text{-}odd\text{-}division\text{-}abs$ )
    then obtain  $d$  where  $dn: d = b-n*x \wedge 2*|d| < x$  by auto
    let  $?C = c^2+3*d^2$ 
    have  $C3: is\text{-}qfN\ ?C\ \exists$  by (unfold  $is\text{-}qfN\text{-}def$ , auto)
    have  $C0: ?C > 0$ 
  proof -
    have  $hlp: (\exists::int) \geq 1$  by simp
    with  $C3$  have  $?C \geq 0$  by (simp only:  $qfN\text{-}pos$ )
    hence  $?C = 0 \vee ?C > 0$  by auto
  moreover
  { assume  $?C = 0$ 
    with  $hlp$  have  $c=0 \wedge d=0$  by (rule  $qfN\text{-}zero$ )
    with  $cm\ dn$  have  $a = m*x \wedge b = n*x$  by simp
    hence  $x\ dvd\ a \wedge x\ dvd\ b$  by simp
    hence  $x\ dvd\ zgcd(a,b)$  by (simp add:  $zgcd\text{-}greatest\text{-}iff$ )
    with  $abx$  have  $False$  by (auto simp add:  $zprime\text{-}def$ ) }
  ultimately show  $?thesis$  by blast
qed

```

```

have x dvd ?C
proof
  have ?C = |c|^2 + 3*|d|^2 by (simp only: power2-abs)
  also with cm dn have ... = (a-m*x)^2 + 3*(b-n*x)^2 by simp
  also have ... =
    a^2 - 2*a*(m*x) + (m*x)^2 + 3*(b^2 - 2*b*(n*x) + (n*x)^2)
  by (simp only: zdiff-power2)
  also with abx M have ... =
    x*M - x*(2*a*m + 3*2*b*n) + x^2*(m^2 + 3*n^2)
  by (simp only: power-mult-distrib zadd-zmult-distrib2 mult-ac, auto)
  finally show ?C = x*(M - (2*a*m + 3*2*b*n) + x*(m^2 + 3*n^2))
  by (simp add: power2-eq-square zadd-zmult-distrib2 zdiff-zmult-distrib2)
qed
then obtain y where y: ?C = x*y by (auto simp add: dvd-def)
have yx: y < x
proof (rule ccontr)
  assume ¬ y < x hence xy: x-y ≤ 0 by simp
  have hlp: 2*|c| ≥ 0 ∧ 2*|d| ≥ 0 ∧ (3::nat) > 0 by simp
  from y have 4*x*y = 2^2*c^2 + 3*2^2*d^2 by simp
  hence 4*x*y = (2*|c|)^2 + 3*(2*|d|)^2
  by (auto simp add: power2-abs power-mult-distrib)
  with cm dn hlp have 4*x*y < x^2 + 3*(2*|d|)^2
  and (3::int) > 0 ∧ (2*|d|)^2 < x^2
  by (auto simp add: power-strict-mono)
  hence x*4*y < x^2 + 3*x^2 by (auto)
  also have ... = x*4*x by (simp add: power2-eq-square)
  finally have contr: (x-y)*(4*x) > 0 by (auto simp add: zdiff-zmult-distrib2)
  show False
proof (cases)
  assume x-y = 0 with contr show False by auto
next
  assume ¬ x-y = 0 with xy have x-y < 0 by simp
  moreover from x0 have 4*x > 0 by simp
  ultimately have 4*x*(x-y) < 4*x*0 by (simp only: zmult-zless-mono2)
  with contr show False by auto
qed
qed
have y0: y > 0
proof (rule ccontr)
  assume ¬ y > 0
  hence y ≤ 0 by simp
  moreover have y ≠ 0
  proof (rule ccontr)
    assume ¬ y ≠ 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*0 by (simp only: zmult-zless-mono2)
  with C0 y show False by simp
qed
let ?g = zgcd(c,d)
have c ≠ 0 ∨ d ≠ 0

```

```

proof (rule ccontr)
  assume  $\neg (c \neq 0 \vee d \neq 0)$  hence  $c=0 \wedge d=0$  by simp
  with C0 show False by simp
qed
then obtain e f where ef:  $c = ?g * e \wedge d = ?g * f \wedge \text{zgcd}(e, f) = 1$ 
  by (frule-tac a=c in make-zrelprime, auto)
have g2nonzero:  $?g^2 \neq 0$ 
proof (rule ccontr, clarsimp)
  assume ?g = 0
  hence  $\text{nat}|c|=0 \wedge \text{nat}|d|=0$ 
  by (unfold zgcd-def, auto simp add: gcd-zero)
  hence  $c=0 \wedge d=0$  by arith
  with C0 show False by simp
qed
let ?E =  $e^2 + 3 * f^2$ 
have E3: is-qn ?E 3 by (unfold is-qn-def, auto)
have CgE: ?C =  $?g^2 * ?E$ 
proof -
  have  $?g^2 * ?E = (?g * e)^2 + 3 * (?g * f)^2$ 
  by (simp add: zadd-zmult-distrib2 power-mult-distrib)
  with ef show ?thesis by simp
qed
hence  $?g^2 \text{ dvd } ?C$  by (simp add: dvd-def)
with y have g2dvdxy:  $?g^2 \text{ dvd } y * x$  by (simp add: mult-ac)
moreover have  $\text{zgcd}(x, ?g^2) = 1$ 
proof -
  let ?h =  $\text{zgcd}(?g, x)$ 
  have ?h dvd ?g and ?g dvd c by auto
  hence hc: ?h dvd c by (rule zdvd-trans)
  have ?h dvd ?g and ?g dvd d by auto
  hence hd: ?h dvd d by (rule zdvd-trans)
  have hx: ?h dvd x by simp
  hence ?h dvd m * x by (rule zdvd-zmult)
  with hc have ?h dvd c + m * x by (rule zdvd-zadd)
  with cm have ha: ?h dvd a by simp
  from hx have ?h dvd n * x by (rule zdvd-zmult)
  with hd have ?h dvd d + n * x by (rule zdvd-zadd)
  with dn have hb: ?h dvd b by simp
  with ha have ?h dvd  $\text{zgcd}(a, b)$  by (simp add: zgcd-greatest-iff)
  with abx have ?h dvd 1 by simp
  hence ?h = 1 by (simp add: zgcd-geq-zero)
  hence  $\text{zgcd}(?g^2, x) = 1$  by (rule zgcd-1-power-left-distrib)
  thus ?thesis by (simp only: zgcd-commute)
qed
ultimately have  $?g^2 \text{ dvd } y$  by (auto dest: zrelprime-zdvd-zmult)
then obtain w where w:  $y = ?g^2 * w$  by (auto simp add: dvd-def)
with CgE y g2nonzero have Ewx:  $?E = x * w$  by auto
have w0:  $w > 0$ 
proof (rule ccontr)
  assume  $\neg w > 0$  hence  $w \leq 0$  by auto
  hence  $w = 0 \vee w < 0$  by auto
  moreover

```

```

{ assume w=0 with w y0 have False by auto }
moreover
{ assume wneg: w < 0
  have ?g^2 ≥ 0 by (rule zero-le-power2)
  with g2nonzero have ?g^2 > 0 by arith
  with wneg have ?g^2*w < ?g^2*0 by (simp only: zmult-zless-mono2)
  with w y0 have False by auto }
ultimately show False by blast
qed
have w-le-y: w ≤ y
proof (rule ccontr)
  assume ¬ w ≤ y
  hence wy: w > y by simp
  have ?g^2 = 1 ∨ ?g^2 > 1
  proof -
    have ?g^2 ≥ 0 by (rule zero-le-power2)
    hence ?g^2 = 0 ∨ ?g^2 > 0 by auto
    with g2nonzero show ?thesis by arith
  qed
moreover
{ assume ?g^2 = 1 with w wy have False by simp }
moreover
{ assume g1: ?g^2 > 1
  with w0 have w*1 < w*?g^2 by (auto dest: zmult-zless-mono2)
  with w have w < y by (simp add: zmult-1 mult-ac)
  with wy have False by auto }
ultimately show False by blast
qed
from Ewx E3 abx w0 have
  zprime x ∧ x ∈ zOdd ∧ w > 0 ∧ is-qn (x*w) 3 ∧ ¬ is-qn x 3 by simp
then obtain z where z: zprime z ∧ z ∈ zOdd ∧ z dvd w ∧ ¬ is-qn z 3
  by (frule-tac P=x in qf3-oddprimedivisor-not, auto)
from Ewx have w dvd ?E by simp
with z have z dvd ?E by (auto dest: zdvd-trans)
with z ef have zprime z ∧ z ∈ zOdd ∧ zgcd(e,f)=1 ∧ z dvd ?E ∧ ¬ is-qn z 3
  by auto
moreover have nat|z| < nat|x|
proof -
  have z ≤ w
  proof (rule ccontr)
    assume ¬ z ≤ w hence w < z by auto
    with w0 have ¬ z dvd w by (rule zdvd-not-zless)
    with z show False by simp
  qed
  with w-le-y yx have z < x by simp
  with z have |z| < |x| by (simp add: zprime-def)
  thus ?thesis by auto
qed
ultimately show ∃ z. nat|z| < nat|x| ∧ ¬ ?B z by auto
qed
assume zprime P and P ∈ zOdd and zgcd(a,b)=1 and P dvd a^2+3*b^2
with lem show ?thesis by blast

```

qed

lemma *qf3-cube-prime-impl-cube-form*:

assumes *ab-relprime*:  $\text{zgcd}(a,b)=1$  and *abP*:  $P^3 = a^2 + 3*b^2$

and *P*: *zprime*  $P \wedge P \in \text{zOdd}$

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

proof –

from *abP* have *qfP3*: *is-qfN*  $(P^3)\ 3$  by (auto simp only: *is-qfN-def*)

have *PvdP3*:  $P \text{ dvd } P^3$  by (simp add: *nat-number*)

with *abP* *ab-relprime* *P* have *qfP*: *is-qfN*  $P\ 3$  by (simp only: *qf3-oddprimedivisor*)

then obtain  $p\ q$  where *pq*:  $P = p^2 + 3*q^2$  by (auto simp only: *is-qfN-def*)

with *P* *abP* *ab-relprime* have *zprime*  $(p^2 + 3*q^2) \wedge (3::\text{int}) > 1$

$\wedge (p^2 + 3*q^2)^3 = a^2 + 3*b^2 \wedge \text{zgcd}(a,b)=1$  by auto

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

by (rule *qfN-cube-prime*)

hence *a*:  $a = p^3 - 9*p*q^2 \vee a = -(p^3) + 9*p*q^2$  by *arith*

from *ab* have *b*:  $b = 3*p^2*q - 3*q^3 \vee b = -(3*p^2*q) + 3*q^3$  by *arith*

obtain  $r\ s$  where *r*:  $r = -p$  and *s*:  $s = -q$  by *simp*

show *?thesis*

proof (cases)

assume *a1*:  $a = p^3 - 9*p*q^2$

show *?thesis*

proof (cases)

assume *b1*:  $b = 3*p^2*q - 3*q^3$

with *a1* show *?thesis* by (unfold *is-cube-form-def*, auto)

next

assume  $\neg b = 3*p^2*q - 3*q^3$

with *b* have  $b = -3*p^2*q + 3*q^3$  by *simp*

with *s* have  $b = 3*p^2*s - 3*s^3$  by (simp add: *power3-minus*)

moreover from *a s* have  $a = p^3 - 9*p*s^2$  by (simp add: *power2-minus*)

ultimately show *?thesis* by (unfold *is-cube-form-def*, auto)

qed

next

assume  $\neg a = p^3 - 9*p*q^2$

with *a* have  $a = -(p^3) + 9*p*q^2$  by *simp*

with *r* have *ar*:  $a = r^3 - 9*r*q^2$  by (simp add: *power3-minus*)

show *?thesis*

proof (cases)

assume *b1*:  $b = 3*p^2*q - 3*q^3$

with *r* have  $b = 3*r^2*q - 3*q^3$  by (simp add: *power2-minus*)

with *ar* show *?thesis* by (unfold *is-cube-form-def*, auto)

next

assume  $\neg b = 3*p^2*q - 3*q^3$

with *b* have  $b = -3*p^2*q + 3*q^3$  by *simp*

with *r s* have  $b = 3*r^2*s - 3*s^3$

by (simp add: *power2-minus power3-minus*)

moreover from *ar s* have  $a = r^3 - 9*r*s^2$  by (simp add: *power2-minus*)

ultimately show *?thesis* by (unfold *is-cube-form-def*, auto)

qed

qed

qed

**lemma** *cube-form-mult*:  $\llbracket$  *is-cube-form*  $a$   $b$ ; *is-cube-form*  $c$   $d$ ;  $|e| = 1$   $\rrbracket$

$\implies$  *is-cube-form*  $(a*c + e*3*b*d)$   $(a*d - e*b*c)$

**proof** –

**assume**  $ab$ : *is-cube-form*  $a$   $b$  **and**  $c$ - $d$ : *is-cube-form*  $c$   $d$  **and**  $e$ :  $|e| = 1$

**from**  $ab$  **obtain**  $p$   $q$  **where**  $pq$ :  $a = p^3 - 9*p*q^2 \wedge b = 3*p^2*q - 3*q^3$

**by** (*auto simp only: is-cube-form-def*)

**from**  $c$ - $d$  **obtain**  $r$   $s$  **where**  $rs$ :  $c = r^3 - 9*r*s^2 \wedge d = 3*r^2*s - 3*s^3$

**by** (*auto simp only: is-cube-form-def*)

**let**  $?t = p*r + e*3*q*s$

**let**  $?u = p*s - e*r*q$

**have**  $e^2 = 1$

**proof** –

**from**  $e$  **have**  $e = 1 \vee e = -1$  **by** *simp*

**moreover**

{ **assume**  $e = 1$  **hence**  $?thesis$  **by** *auto* }

**moreover**

{ **assume**  $e = -1$  **hence**  $?thesis$  **by** (*simp add: power2-minus*) }

**ultimately show**  $?thesis$  **by** *blast*

**qed**

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

**hence**  $e^3$ :  $e*1 = e^3$  **by** (*simp only: cube-square*)

**have**  $a*c + e*3*b*d = ?t^3 - 9*?t*?u^2$

**proof** –

**have**  $?t^3 - 9*?t*?u^2 = p^3*r^3 + e*9*p^2*q*r^2*s + e^2*27*p*q^2*r*s^2$   
 $+ e^3*27*q^3*s^3 - 9*p*p^2*r*s^2 + e*18*p^2*q*r^2*s - e^2*9*p*q^2*(r*r^2)$   
 $- e*27*p^2*q*(s*s^2) + e^2*54*p*q^2*r*s^2 - e*e^2*27*(q*q^2)*r^2*s$

**by** (*simp add: nat-number ring-simps*)

**also with**  $e^2$   $e^3$  **have** ... =

$p^3*r^3 + e*27*p^2*q*r^2*s + 81*p*q^2*r*s^2 + e*27*q^3*s^3$   
 $- 9*p^3*r*s^2 - 9*p*q^2*r^3 - e*27*p^2*q*s^3 - e*27*q^3*r^2*s$

**by** (*simp add: cube-square zmult-1*)

**also with**  $pq$   $rs$  **have** ... =  $a*c + e*3*b*d$

**by** (*simp only: zdiff-zmult-distrib zdiff-zmult-distrib2 mult-ac*)

**finally show**  $?thesis$  **by** *auto*

**qed**

**moreover have**  $a*d - e*b*c = 3*?t^2*?u - 3*?u^3$

**proof** –

**have**  $3*?t^2*?u - 3*?u^3 =$

$3*(p*p^2)*r^2*s - e*3*p^2*q*(r*r^2) + e*18*p^2*q*r*s^2$   
 $- e^2*18*p*q^2*r^2*s + e^2*27*p*q^2*(s*s^2) - e*e^2*27*(q*q^2)*r*s^2$   
 $- 3*p^3*s^3 + e*9*p^2*q*r*s^2 - e^2*9*p*q^2*r^2*s + e^3*3*r^3*q^3$

**by** (*simp add: nat-number ring-simps*)

**also with**  $e^2$   $e^3$  **have** ... =  $3*p^3*r^2*s - e*3*p^2*q*r^3 + e*18*p^2*q*r*s^2$

$- 18*p*q^2*r^2*s + 27*p*q^2*s^3 - e*27*q^3*r*s^2 - 3*p^3*s^3$   
 $+ e*9*p^2*q*r*s^2 - 9*p*q^2*r^2*s + e*3*r^3*q^3$

**by** (*simp add: cube-square zmult-1*)

**also with**  $pq$   $rs$  **have** ... =  $a*d - e*b*c$

**by** (*simp only: zdiff-zmult-distrib zdiff-zmult-distrib2 mult-ac*)

**finally show**  $?thesis$  **by** *auto*

**qed**

**ultimately show**  $?thesis$  **by** (*auto simp only: is-cube-form-def*)

**qed**

**lemma** *qf3-cube-primelist-impl-cube-form*:  $\llbracket \text{primel } ps; \text{int } (\text{prod } ps) \in z\text{Odd} \rrbracket \implies$   
 $(!! a b. \text{zgcd}(a,b)=1 \implies a^2 + 3*b^2 = (\text{int}(\text{prod } ps))^3 \implies \text{is-cube-form } a b)$

**proof** (*induct ps*)  
**case Nil** **hence** *ab1*:  $a^2 + 3*b^2 = 1$  **by** *simp*  
**have** *b0*:  $b=0$   
**proof** (*rule ccontr*)  
**assume**  $b \neq 0$   
**hence**  $b^2 > 0$  **by** (*simp add: zero-less-power2*)  
**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** *False* **by** *auto*  
**qed**

**with** *ab1* **have** *a1*:  $(a=1 \vee a=-1)$  **by** (*auto simp add: power2-eq-square zmult-eq-1-iff*)  
**then obtain**  $p$  **and**  $q$  **where**  $p=a$  **and**  $q=(0::\text{int})$  **by** *simp*  
**with** *a1* **and** *b0* **have**  $a = p^3 - 9*p*q^2 \wedge b = 3*p^2*q - 3*q^3$  **by** *auto*  
**thus** *is-cube-form a b* **by** (*auto simp only: is-cube-form-def*)

**next**  
**case** (*Cons p ps*) **hence** *ass*:  $\text{zgcd}(a,b)=1 \wedge \text{int}(\text{prod } (p\#ps)) \in z\text{Odd}$   
 $\wedge a^2+3*b^2 = \text{int}(\text{prod } (p\#ps))^3 \wedge \text{primel } ps \wedge \text{zprime } (\text{int } p)$   
**and** *IH*:  $!! u v. \text{zgcd}(u,v)=1 \wedge u^2+3*v^2 = \text{int}(\text{prod } ps)^3$   
 $\wedge \text{int}(\text{prod } ps) \in z\text{Odd} \implies \text{is-cube-form } u v$   
**by** (*auto simp add: primel-def prime-impl-zprime-int*)  
**let**  $?w = \text{int } (\text{prod } (p\#ps))$   
**let**  $?X = \text{int } (\text{prod } ps)$   
**let**  $?p = \text{int } p$   
**have** *ge3-1*:  $(3::\text{int}) \geq 1$  **by** *auto*  
**have** *pw*:  $?w = ?p * ?X \wedge ?p \in z\text{Odd} \wedge ?X \in z\text{Odd}$   
**proof** (*safe*)  
**have**  $\text{prod } (p\#ps) = p * \text{prod } ps$  **by** *simp*  
**thus** *wpx*:  $?w = ?p * ?X$  **by** (*auto simp only: zmult-int*)  
**with** *ass* **show**  $?p \in z\text{Odd}$  **by** (*auto dest: odd-mult-odd-prop*)  
**from** *wpx* **have**  $?w = ?X * ?p$  **by** *simp*  
**with** *ass* **show**  $?X \in z\text{Odd}$  **by** (*auto dest: odd-mult-odd-prop*)  
**qed**

**have** *is-qfN ?p 3*  
**proof** –  
**from** *ass* **have**  $a^2+3*b^2 = (?p*?X)^3$  **by** (*simp add: zmult-int*)  
**hence**  $?p \text{ dvd } a^2+3*b^2$  **by** (*simp add: nat-number ring-simps*)  
**moreover from** *ass* **have**  $\text{zprime } ?p$  **and**  $\text{zgcd}(a,b)=1$  **by** *simp*  
**moreover from** *pw* **have**  $?p \in z\text{Odd}$  **by** *simp*  
**ultimately show** *?thesis* **by** (*simp only: qf3-oddprimedivisor*)  
**qed**

**then obtain**  $\alpha \beta$  **where** *alphabet*:  $?p = \alpha^2 + 3*\beta^2$   
**by** (*auto simp add: is-qfN-def*)  
**have**  $\alpha \neq 0$   
**proof** (*rule ccontr, simp*)  
**assume**  $\alpha = 0$  **with** *alphabet* **have**  $3 \text{ dvd } ?p$  **by** *auto*  
**with** *pw* **have** *w3*:  $3 \text{ dvd } ?w$  **by** (*simp only: zdvd-zmult2*)  
**then obtain**  $v$  **where**  $?w = 3*v$  **by** (*auto simp add: dvd-def*)  
**with** *ass* **have**  $27*v^3 = a^2 + 3*b^2$  **by** (*simp add: power-mult-distrib*)

hence  $a^2 = 3*(9*v^3 - b^2)$  by *auto*  
 hence  $3 \text{ dvd } a^2$  by (*unfold dvd-def, blast*)  
 moreover have  $zprime\ 3$  by (*rule zprime-3*)  
 ultimately have  $a3: 3 \text{ dvd } a$  by (*rule-tac p=3 in zprime-zdvd-power*)  
 then obtain  $c$  where  $c: a = 3*c$  by (*auto simp add: dvd-def*)  
 with  $vab$  have  $27*v^3 = 9*c^2 + 3*b^2$  by (*simp add: power-mult-distrib*)  
 hence  $b^2 = 3*(3*v^3 - c^2)$  by *auto*  
 hence  $3 \text{ dvd } b^2$  by (*unfold dvd-def, blast*)  
 moreover have  $zprime\ 3$  by (*rule zprime-3*)  
 ultimately have  $3 \text{ dvd } b$  by (*rule-tac p=3 in zprime-zdvd-power*)  
 with  $a3$  have  $3 \text{ dvd } zgcd(a,b)$  by (*simp add: zgcd-greatest-iff*)  
 with *ass* show *False* by *simp*  
 qed  
 moreover from *alphabet* *pw* *ass* have  
 $zprime\ (\alpha^2 + 3*\beta^2) \wedge \alpha^2 + 3*\beta^2 \in zOdd \wedge (3::int) \geq 1$  by *auto*  
 ultimately obtain  $c\ d$  where *cdp*:  
 $(\alpha^2 + 3*\beta^2)^3 = c^2 + 3*d^2 \wedge zgcd(c, 3*d) = 1$   
 by (*blast dest: qfN-oddprime-cube*)  
 with *ass* *pw* *alphabet* have  $\exists u\ v. a^2 + 3*b^2 = (u^2 + 3*v^2)*(c^2 + 3*d^2)$   
 $\wedge zgcd(u,v) = 1 \wedge (\exists e. a = c*u + e*3*d*v \wedge b = c*v - e*d*u \wedge |e| = 1)$   
 by (*rule-tac A=?w and n=3 in qfN-power-div-prime, auto*)  
 then obtain  $u\ v\ e$  where *uve*:  $a^2 + 3*b^2 = (u^2 + 3*v^2)*(c^2 + 3*d^2)$   
 $\wedge zgcd(u,v) = 1 \wedge a = c*u + e*3*d*v \wedge b = c*v - e*d*u \wedge |e| = 1$  by *blast*  
 moreover have *is-cube-form*  $u\ v$   
 proof -  
 have  $uvX: u^2 + 3*v^2 = ?X^3$   
 proof -  
 from *ass* have  $p0: ?p \neq 0$  by (*simp add: zprime-def*)  
 from *pw* have  $?p^3 * ?X^3 = ?w^3$  by (*simp add: power-mult-distrib*)  
 also with *ass* have  $\dots = a^2 + 3*b^2$  by *simp*  
 also with *uve* have  $\dots = (u^2 + 3*v^2)*(c^2 + 3*d^2)$  by *auto*  
 also with *cdp* *alphabet* have  $\dots = ?p^3 * (u^2 + 3*v^2)$  by (*simp only: mult-ac*)  
 finally have  $?p^3*(u^2 + 3*v^2 - ?X^3) = 0$  by *auto*  
 with  $p0$  show *?thesis* by *auto*  
 qed  
 with *pw* *IH* *uve* show *?thesis* by *simp*  
 qed  
 moreover have *is-cube-form*  $c\ d$   
 proof -  
 have  $zgcd(c,d) = 1$   
 proof (*simp only: zgcd1-iff-no-common-primedivisor, clarify*)  
 fix  $h::int$  assume  $h \text{ dvd } c$  and  $h \text{ dvd } d$  and  $h: zprime\ h$   
 hence  $h \text{ dvd } c*u + d*(e*3*v) \wedge h \text{ dvd } c*v - d*(e*u)$   
 by (*simp add: zdvd-zmult2 zdvd-zadd zdvd-zdiff*)  
 with *uve* have  $h \text{ dvd } a \wedge h \text{ dvd } b$  by (*auto simp only: mult-ac*)  
 with *ass*  $h$  show *False* by (*auto simp add: zgcd1-iff-no-common-primedivisor*)  
 qed  
 with *pw* *cdp* *ass* *alphabet* show *?thesis*  
 by (*rule-tac P=?p in qf3-cube-prime-impl-cube-form, auto*)  
 qed  
 ultimately show *is-cube-form*  $a\ b$  by (*simp only: cube-form-mult*)  
 qed

```

lemma qf3-cube-impl-cube-form:
  assumes ass:  $\text{zgcd}(a,b)=1 \wedge a^2 + 3*b^2 = w^3 \wedge w \in \text{zOdd}$ 
  shows is-cube-form a b
proof -
  have  $\exists ps. \text{primel } ps \wedge \text{int } (\text{prod } ps) = w$ 
proof -
  have wpos:  $w \geq 1$ 
proof -
  have  $b^2 \geq 0$  by (rule zero-le-power2)
  hence  $3*b^2 \geq 0$  by arith
  moreover have  $a^2 \geq 0$  by (rule zero-le-power2)
  ultimately have  $a^2 + 3*b^2 \geq 0$  by arith
  with ass have w3pos:  $w^3 \geq 0$  by simp
  have  $w \geq 0$ 
proof (rule ccontr)
  assume  $\neg w \geq 0$  hence  $-w > 0$  by auto
  hence  $(-1 * w)^3 > 0$  by (auto simp only: zero-less-power)
  hence  $(-1)^3 * (w^3) > 0$  by (simp only: power-mult-distrib)
  hence  $w^3 < 0$  by (simp add: neg-one-odd-power)
  with w3pos show False by auto
qed
moreover have  $w \neq 0$ 
proof (rule ccontr)
  assume  $\neg w \neq 0$  with ass have  $0 \in \text{zOdd}$  by simp
  moreover have  $0 \in \text{zEven}$  by (simp add: zEven-def)
  ultimately show False by (auto simp add: odd-iff-not-even)
qed
ultimately show ?thesis by (auto)
qed
hence  $w=1 \vee \text{Suc } 0 < \text{nat } w$  by auto
moreover
{ assume  $w=1$ 
  hence  $\text{primel } [] \wedge \text{int } (\text{prod } []) = w$  by (auto simp add: primel-def)
  hence ?thesis by (simp only: exI) }
moreover
{ assume  $\text{Suc } 0 < \text{nat } w$ 
  hence  $\exists l. \text{primel } l \wedge \text{prod } l = \text{nat } w$  by (rule factor-exists)
  then obtain ps where  $\text{primel } ps \wedge \text{prod } ps = \text{nat } w$  by auto
  with wpos have ?thesis by auto }
ultimately show ?thesis by blast
qed
with ass show ?thesis by (auto dest: qf3-cube-primelist-impl-cube-form)
qed

```

## 4.6 Existence ( $N = 3$ )

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

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

**lemma** *Legendre-zmult*:  $\llbracket p > 2; \text{zprime } p \rrbracket$   
 $\implies (\text{Legendre } (a*b) \ p) = (\text{Legendre } a \ p) * (\text{Legendre } b \ p)$   
**proof** –  
 assume  $p2: p > 2$  and  $prp: \text{zprime } p$   
 let  $?p12 = \text{nat}(((p) - 1) \text{ div } 2)$   
 let  $?Labp = \text{Legendre } (a*b) \ p$   
 let  $?Lap = \text{Legendre } a \ p$   
 let  $?Lbp = \text{Legendre } b \ p$   
 from  $p2 \ prp$  have  $[?Labp = (a*b)^{?p12}] \pmod p$   
 by (*simp only: Euler-Criterion*)  
 hence  $[a^{?p12} * b^{?p12} = ?Labp] \pmod p$   
 by (*simp only: power-mult-distrib zcong-sym*)  
 moreover from  $p2 \ prp$  have  $[?Lap * ?Lbp = a^{?p12} * b^{?p12}] \pmod p$   
 by (*simp only: Euler-Criterion zcong-zmult*)  
 ultimately have  $[?Lap * ?Lbp = ?Labp] \pmod p$   
 by (*rule-tac b=a^{?p12} \* b^{?p12} in zcong-trans*)  
 then obtain  $k$  where  $k: ?Labp = (?Lap * ?Lbp) + p * k$   
 by (*auto simp add: zcong-iff-lin*)  
 have  $k=0$   
**proof** (*rule ccontr*)  
 assume  $k \neq 0$  hence  $|k| = 1 \vee |k| > 1$  by *arith*  
 moreover  
 { assume  $|k|=1$   
 with  $p2$  have  $|k|*p > 2$  by *auto* }  
 moreover  
 { assume  $k1: |k| > 1$   
 with  $p2$  have  $|k|*2 < |k|*p$   
 by (*simp only: zmult-zless-mono2*)  
 with  $k1$  have  $|k|*p > 2$  by *auto* }  
 ultimately have  $|k|*p > 2$  by *auto*  
 moreover from  $p2$  have  $|p| = p$  by *auto*  
 ultimately have  $|k*p| > 2$  by (*auto simp only: abs-mult*)  
 moreover from  $k$  have  $?Labp - ?Lap * ?Lbp = k*p$  by *auto*  
 ultimately have  $|?Labp - ?Lap * ?Lbp| > 2$  by *auto*  
 moreover have  $?Labp = 1 \vee ?Labp = 0 \vee ?Labp = -1$   
 by (*simp add: Legendre-def*)  
 moreover have  $?Lap * ?Lbp = 1 \vee ?Lap * ?Lbp = 0 \vee ?Lap * ?Lbp = -1$   
 by (*auto simp add: Legendre-def*)  
 ultimately show *False* by *auto*  
**qed**  
 with  $k$  show *?thesis* by *auto*  
**qed**

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

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

**proof** –  
 let  $?p = 6*m+1$   
 let  $?L = \text{Legendre } (-3) \ ?p$   
 let  $?L1 = \text{Legendre } (-1) \ ?p$   
 let  $?L3 = \text{Legendre } 3 \ ?p$   
 assume  $p: \text{zprime } ?p$

---

```

have neg1cube:  $(-1::int)^3 = -1$  by (simp add: power3-minus)
have m1:  $m \geq 1$ 
proof (rule ccontr)
  assume  $\neg m \geq 1$  hence  $m \leq 0$  by simp
  with p show False by (auto simp add: zprime-def)
qed
hence pn3:  $?p \neq 3$  and p2:  $?p > 2$  by auto
with p have ?L = (Legendre  $(-1)$  ?p) * (Legendre 3 ?p)
  by (frule-tac a=-1 and b=3 in Legendre-zmult, auto)
moreover have [Legendre  $(-1)$  ?p =  $(-1)^{\text{nat } m}$ ] (mod ?p)
proof -
  from p p2 have [?L1 =  $(-1)^{\text{nat}((?p) - 1 \text{ div } 2)}$ ] (mod ?p)
    by (simp only: Euler-Criterion)
  moreover have  $\text{nat}((?p) - 1 \text{ div } 2) = 3 * \text{nat } m$ 
  proof -
    have  $(?p) - 1 \text{ div } 2 = 3 * m$  by auto
    hence  $\text{nat}((?p) - 1 \text{ div } 2) = \text{nat}(3 * m)$  by simp
    moreover have  $(3::int) \geq 0$  by simp
    ultimately show ?thesis by (simp add: nat-mult-distrib)
  qed
  moreover with neg1cube have  $(-1::int)^{(3 * \text{nat } m)} = (-1)^{\text{nat } m}$ 
    by (simp only: power-mult)
  ultimately show ?thesis by auto
qed
moreover have ?L3 =  $(-1)^{\text{nat } m}$ 
proof -
  have ?L3 * (Legendre ?p 3) =  $(-1)^{\text{nat } m}$ 
  proof -
    have  $3 \in zOdd \wedge ?p \in zOdd$  by (unfold zOdd-def, auto)
    with p pn3 have ?L3 * (Legendre ?p 3) =  $(-1::int)^{(3 * \text{nat } m)}$ 
      by (simp add: zprime-3 Quadratic-Reciprocity nat-mult-distrib)
    with neg1cube show ?thesis by (simp add: power-mult)
  qed
  moreover have Legendre ?p 3 = 1
  proof -
    have  $[1^2 = ?p] \pmod 3$  by (unfold zcong-def dvd-def, auto)
    hence QuadRes 3 ?p by (unfold QuadRes-def, blast)
    moreover have  $\neg [?p = 0] \pmod 3$ 
    proof (rule ccontr, simp)
      assume  $[?p = 0] \pmod 3$ 
      hence  $3 \text{ dvd } ?p$  by (simp add: zcong-def)
      moreover have  $3 \text{ dvd } 6 * m$  by (auto simp add: dvd-def)
      ultimately have  $3 \text{ dvd } ?p - 6 * m$  by (simp only: zdvd-zdiff)
      hence  $(3::int) \text{ dvd } 1$  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 =  $(-1)^{\text{nat } m} * (-1)^{\text{nat } m}$ ] (mod ?p)
  by (auto dest: zcong-scalar)

```

```

hence [ $?L = (-1)^{((nat\ m)+(nat\ m))} \pmod{?p}$ ] by (simp only: power-add)
moreover have  $(nat\ m)+(nat\ m) = 2*(nat\ m)$  by auto
ultimately have [ $?L = (-1)^{2*(nat\ m)} \pmod{?p}$ ] by simp
hence [ $?L = ((-1)^2)^{(nat\ m)} \pmod{?p}$ ] by (simp only: power-mult)
hence [ $1 = ?L \pmod{?p}$ ] by (auto simp add: zcong-sym)
hence  $?p\ dvd\ 1 - ?L$  by (simp only: zcong-def)
moreover have  $?L = -1 \vee ?L = 0 \vee ?L = 1$  by (simp add: Legendre-def)
ultimately have  $?p\ dvd\ 2 \vee ?p\ dvd\ 1 \vee ?L = 1$  by auto
moreover
{ assume  $?p\ dvd\ 2 \vee ?p\ dvd\ 1$ 
  with  $p2$  have False by (auto simp add: zdvd-not-zless) }
ultimately show ?thesis by auto
qed

```

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

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

**proof** –

```

let  $?p = 6*m+1$ 
assume  $p$ :  $zprime\ ?p$ 
hence Legendre  $(-3)\ ?p = 1$  by (rule Legendre-1mod6)
moreover
{ assume  $\neg\ QuadRes\ ?p\ (-3)$ 
  hence Legendre  $(-3)\ ?p \neq 1$  by (unfold Legendre-def, auto) }
ultimately have QuadRes  $?p\ (-3)$  by auto
then obtain  $s$  where  $s$ :  $[s^2 = -3] \pmod{?p}$  by (auto simp add: QuadRes-def)
hence  $?p\ dvd\ s^2 - (-3::int)$  by (unfold zcong-def, simp)
moreover have  $s^2 - (-3::int) = s^2 + 3$  by arith
ultimately have  $?p\ dvd\ s^2 + 3*1^2$  by auto
moreover have  $zgcd(s,1) = 1$  by (unfold zgcd-def, auto)
moreover have  $?p \in zOdd$ 
proof –
  have  $?p = 2*(3*m)+1$  by simp
  thus ?thesis by (unfold zOdd-def, blast)
qed
moreover from  $p$  have  $zprime\ ?p$  by simp
ultimately have is-qfN  $?p\ 3$  by (simp only: qf3-oddprimedivisor)
thus ?thesis by (unfold is-qfN-def, auto)
qed

```

end

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

```

theory Fermat3
  imports QuadForm
begin

```

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

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

**lemma** *factor-sum-cubes*:  $(x::int)^3 + y^3 = (x+y)*(x^2 - x*y + y^2)$

by (*simp add: nat-number ring-simps*)

**lemma** *two-not-abs-cube*:  $|x^3| = (2::int) \implies False$

**proof** –

assume  $|x^3| = 2$

hence *x32*:  $|x|^3 = 2$  by (*simp only: abs-power3-distrib*)

have  $|x| \geq 0$  by *simp*

moreover

{ assume  $|x| = 0 \vee |x| = 1 \vee |x| = 2$

with *x32* have *False* by (*auto simp add: power-0-left*) }

moreover

{ assume  $|x| > 2$

moreover have  $(0::int) \leq 2$  and  $(0::nat) < 3$  by *auto*

ultimately have  $|x|^3 > 2^3$  by (*simp only: power-strict-mono*)

with *x32* 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  $\gcd(v, w) = 1$  and  $x$  even, by constructing a solution with a smaller  $|x^3|$ .

**lemma** *no-rewritten-fermat3*:

$\neg (\exists v w. v^3 + w^3 = x^3 \wedge v * w * x \neq 0 \wedge x \in zEven \wedge zgcd(v, w) = 1)$  (**is** ?*Q* *x*)

**proof** (*rule-tac x=x and V= $\lambda x. nat|x^3|$  in val-infinite-descent*)

**fix** *x*

assume  $nat|x^3| = 0$  hence  $x^3 = 0$  by *arith*

hence  $x = 0$  by *auto*

thus ?*Q* *x* by *auto*

**next**

**fix** *x*

assume *x3pos*:  $0 < nat|x^3|$  and  $\neg ?Q x$

then obtain *v w* where *vwx*:

$v^3 + w^3 = x^3 \wedge v * w * x \neq 0 \wedge x \in zEven \wedge zgcd(v, w) = 1$  (**is** ?*P* *v w x*)

by *auto*

have  $\exists \alpha \beta \gamma. ?P \alpha \beta \gamma \wedge nat|\gamma^3| < nat|x^3|$

**proof** –

– obtain coprime *p* and *q* such that  $v = p + q$  and  $w = p - q$

have *vwOdd*:  $v \in zOdd \wedge w \in zOdd$

**proof** (*rule ccontr, case-tac v  $\in zOdd$ , simp-all*)

assume  $v \notin zOdd$  hence *ve*:  $v \in zEven$  by (*rule not-odd-impl-even*)

hence  $v^3 \in zEven$  by (*simp only: power-preserves-even*)

moreover from *vwx* have  $x^3 \in zEven$  by (*simp only: power-preserves-even*)

ultimately have  $(x^3 - v^3) \in zEven$  by (*simp only: even-minus-even*)

moreover from *vwx* have  $x^3 - v^3 = w^3$  by *simp*

ultimately have  $w^3 \in zEven$  by *simp*

hence  $w \in zEven$  by (*simp only: power-preserves-even*)

with *ve* have  $2 \text{ dvd } v \wedge 2 \text{ dvd } w$  by (*auto simp add: zEven-def*)

hence  $2 \text{ dvd } zgcd(v, w)$  by (*simp add: zgcd-greatest-iff*)

with *vwx* show *False* by *simp*

**next**

assume *vo*:  $v \in zOdd$  and  $w \notin zOdd$

hence  $w \in zEven$  by (*simp add: not-odd-impl-even*)

**with**  $vo$  **have**  $v^3 \in zOdd$  **and**  $w^3 \in zEven$   
**by** (*auto simp only: power-preserves-even power-preserves-odd*)  
**hence**  $w^3 + v^3 \in zOdd$  **by** (*simp only: even-plus-odd*)  
**with**  $vwx$  **have**  $x^3 \in zOdd$  **by** (*simp add: zadd-commute*)  
**hence**  $x \in zOdd$  **by** (*simp only: power-preserves-odd*)  
**with**  $vwx$  **show** *False* **by** (*auto simp add: odd-iff-not-even*)  
**qed**  
**hence**  $v+w \in zEven \wedge v-w \in zEven$  **by** (*simp add: odd-minus-odd odd-plus-odd*)  
**then obtain**  $p$   $q$  **where**  $pq: v+w = 2*p \wedge v-w = 2*q$   
**by** (*auto simp add: zEven-def*)  
**hence**  $vw: v = p+q \wedge w = p-q$  **by** *auto*  
— show that  $x^3 = (2p)(p^2 + 3q^2)$  and that these factors are  
— either coprime (first case), or have 3 as g.c.d. (second case)  
**have**  $vwpq: v^3 + w^3 = (2*p)*(p^2 + 3*q^2)$   
**proof** —  
**have**  $2*(v^3 + w^3) = 2*(v+w)*(v^2 - v*w + w^2)$   
**by** (*simp only: factor-sum-cubes*)  
**also from**  $pq$  **have**  $\dots = 4*p*(v^2 - v*w + w^2)$  **by** *auto*  
**also have**  $\dots = p*((v+w)^2 + 3*(v-w)^2)$   
**by** (*simp add: nat-number ring-simps*)  
**also with**  $pq$  **have**  $\dots = p*((2*p)^2 + 3*(2*q)^2)$  **by** *simp*  
**also have**  $\dots = 2*(2*p)*(p^2 + 3*q^2)$  **by** (*simp add: power-mult-distrib*)  
**finally show** *?thesis* **by** *simp*  
**qed**  
**let**  $?g = zgcd(2*p, p^2 + 3*q^2)$   
**have**  $g1: ?g \geq 1$   
**proof** (*rule ccontr*)  
**assume**  $\neg ?g \geq 1$  **hence**  $?g < 0 \vee ?g = 0$  **by** *auto*  
**moreover have**  $?g \geq 0$  **by** (*rule zgcd-geq-zero*)  
**ultimately have**  $?g = 0$  **by** *simp*  
**hence**  $nat|2*p| = 0$  **by** (*unfold zgcd-def, simp add: gcd-zero*)  
**hence**  $p = 0$  **by** *arith*  
**with**  $vwpq$   $vwx$   $x3pos$  **show** *False* **by** *auto*  
**qed**  
**have**  $gOdd: \neg 2 \text{ dvd } ?g$   
**proof** (*rule ccontr, simp*)  
**assume**  $2 \text{ dvd } ?g$   
**hence**  $2 \text{ dvd } p^2 + 3*q^2$  **by** (*simp only: zgcd-greatest-iff*)  
**then obtain**  $k$  **where**  $k: p^2 + 3*q^2 = 2*k$  **by** (*auto simp add: dvd-def*)  
**hence**  $2*(k - 2*q^2) = p^2 - q^2$  **by** *auto*  
**with**  $vw$  **have**  $v*w = 2*(k - 2*q^2)$  **by** (*simp add: zspecial-product*)  
**hence**  $v*w \in zEven$  **by** (*auto simp only: zEven-def*)  
**hence**  $v \in zEven \vee w \in zEven$  **by** (*simp add: even-product*)  
**with**  $vwOdd$  **show** *False* **by** (*auto simp add: odd-iff-not-even*)  
**qed**  
— first case:  $p$  is not a multiple of 3; hence  $2p$  and  $p^2 + 3q^2$   
— are coprime; hence both are cubes  
**{ assume**  $p3: \neg 3 \text{ dvd } p$   
**have**  $g3: \neg 3 \text{ dvd } ?g$   
**proof** (*rule ccontr, simp*)  
**assume**  $3 \text{ dvd } ?g$  **hence**  $3 \text{ dvd } 2*p$  **by** (*simp add: zgcd-greatest-iff*)  
**hence**  $(3::int) \text{ dvd } 2 \vee 3 \text{ dvd } p$

```

    by (auto simp only: zprime-3 zprime-zdvd-zmult-general)
  with p3 show False by arith
qed
have pq-relprime: zgcd(p,q)=1
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix z assume z: zprime z and zp: z dvd p and zq: z dvd q
  hence z dvd p+q ∧ z dvd p−q by (auto simp only: zdvd-zadd zdvd-zdiff)
  with vw have z dvd v ∧ z dvd w by simp
  with z vwx show False
  by (auto simp add: zgcd1-iff-no-common-primedivisor)
qed
have factors-relprime: ?g = 1
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix z assume z: zprime z and z2p: z dvd 2*p and zpq: z dvd p^2+3*q^2
  hence zg: z dvd ?g by (simp add: zgcd-greatest-iff)
  with gOdd have z ≠ 2 by auto
  with z have zg2: z > 2 by (auto simp add: zprime-def)
  from z z2p have z dvd 2 ∨ z dvd p by (simp only: zprime-zdvd-zmult-general)
  moreover
  { assume z dvd 2
    hence z ≤ 2 by (auto simp add: zdvd-imp-le)
    with zg2 have False by simp }
  ultimately have zp: z dvd p by auto
  hence z dvd p^2 by (auto simp add: power2-eq-square zdvd-zmult2)
  with zpq have z dvd p^2+3*q^2−p^2 by (simp only: zdvd-zdiff)
  hence z dvd 3*q^2 by auto
  with z have z dvd 3 ∨ z dvd q^2 by (simp only: zprime-zdvd-zmult-general)
  moreover
  { assume z dvd 3
    hence z ≤ 3 by (auto simp add: zdvd-imp-le)
    with zg2 have z = 3 by auto
    with zg3 have False by auto }
  ultimately have z dvd q^2 by auto
  with z have z dvd q by (rule zprime-zdvd-power)
  with zp z pq-relprime show False
  by (auto simp add: zgcd1-iff-no-common-primedivisor)
qed
moreover from vwx vwpq have pqx: (2*p)*(p^2 + 3*q^2) = x^3 by auto
moreover have triv3: 3 = nat 3 ∧ nat 3 > 1 ∧ 3 ∈ zOdd
  by (unfold zOdd-def, auto)
ultimately have ∃ c. 2*p = c^3
  by (simp only: int-relprime-odd-power-divisors)
then obtain c where c: c^3 = 2*p by auto
from pqx factors-relprime have zgcd(p^2 + 3*q^2, 2*p) = 1
  and (p^2 + 3*q^2)*(2*p) = x^3 by (auto simp add: zgcd-commute mult-ac)
with triv3 have ∃ d. p^2 + 3*q^2 = d^3
  by (simp only: int-relprime-odd-power-divisors)
then obtain d where d: p^2 + 3*q^2 = d^3 by auto
have d ∈ zOdd
proof (rule ccontr)
  assume d ∉ zOdd hence d ∈ zEven by (rule not-odd-impl-even)
  hence d^3 ∈ zEven by (simp only: power-preserves-even)

```

hence  $2 \text{ dvd } d^3$  by (simp add: zEven-def dvd-def)  
 moreover have  $2 \text{ dvd } 2*p$  by (rule zdvd-triv-left)  
 ultimately have  $2 \text{ dvd } \text{zgcd}(2*p, d^3)$  by (simp add: zgcd-greatest-iff)  
 with  $d$  factors-relprime show False by auto  
 qed  
 with  $d$  pq-relprime have  $\text{zgcd}(p,q)=1 \wedge p^2 + 3*q^2 = d^3 \wedge d \in \text{zOdd}$   
 by simp  
 hence is-cube-form  $p$   $q$  by (rule qf3-cube-impl-cube-form)  
 then obtain  $a$   $b$  where  $p = a^3 - 9*a*b^2 \wedge q = 3*a^2*b - 3*b^3$   
 by (unfold is-cube-form-def, auto)  
 hence  $ab: p = a*(a+3*b)*(a-3*b) \wedge q = b*(a+b)*(a-b)*3$   
 by (simp add: nat-number ring-simps)  
 with  $c$  have  $abc: (2*a)*(a+3*b)*(a-3*b) = c^3$  by auto  
 have  $ab$ -relprime:  $\text{zgcd}(a,b)=1$   
 proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)  
 fix  $z$  assume  $z: \text{zprime } z$  and  $za: z \text{ dvd } a$  and  $zb: z \text{ dvd } b$   
 with  $ab$  have  $z \text{ dvd } p \wedge z \text{ dvd } q$  by (simp add: zdvd-zmult2)  
 with  $z$  pq-relprime show  
 False by (auto simp add: zgcd1-iff-no-common-primedivisor)  
 qed  
 have  $ab1: \text{zgcd}(2*a, a+3*b) = 1$   
 proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)  
 fix  $z$  assume  $z: \text{zprime } z$  and  $z \text{ dvd } 2*a$  and  $zab: z \text{ dvd } a+3*b$   
 hence  $z \text{ dvd } 2 \vee z \text{ dvd } a$  by (simp add: zprime-zdvd-zmult)  
 moreover have  $zn2: \neg z \text{ dvd } 2$   
 proof (rule ccontr, simp)  
 assume  $z2: z \text{ dvd } 2$   
 hence  $z \leq 2$  by (simp only: zdvd-imp-le)  
 with  $z$  have  $z = 2$  by (unfold zprime-def, auto)  
 with  $zab$  have  $ab2: 2 \text{ dvd } a+3*b$  by simp  
 moreover have  $2 \text{ dvd } 2*b$  by (rule zdvd-triv-left)  
 ultimately have  $2 \text{ dvd } a+3*b - 2*b$  by (rule zdvd-zdiff)  
 hence  $2 \text{ dvd } a+b$  by arith  
 hence  $2 \text{ dvd } (a+b)*((a-b)*b*3)$  by (rule zdvd-zmult2)  
 with  $ab$  have  $q\text{Even}: 2 \text{ dvd } q$  by (simp only: mult-ac)  
 from  $ab2$  have  $2 \text{ dvd } (a+3*b)*((a-3*b)*a)$  by (rule zdvd-zmult2)  
 with  $ab$  have  $2 \text{ dvd } p$  by (simp only: mult-ac)  
 with  $q\text{Even}$  have  $2 \text{ dvd } \text{zgcd}(p,q)$  by (simp add: zgcd-greatest-iff)  
 with  $pq$ -relprime show False by auto  
 qed  
 ultimately have  $za: z \text{ dvd } a$  by auto  
 with  $zab$  have  $z \text{ dvd } a+3*b - a$  by (simp only: zdvd-zdiff)  
 hence  $z \text{ dvd } 3*b$  by simp  
 with  $z$  have  $z \text{ dvd } 3 \vee z \text{ dvd } b$  by (simp only: zprime-zdvd-zmult-general)  
 moreover  
 { assume  $z \text{ dvd } 3$   
 with  $z$  have  $z \leq 3$  by (auto simp add: zdvd-imp-le)  
 moreover from  $zn2$  have  $z \neq 2$  by auto  
 moreover from  $z$  have  $z > 1$  by (simp add: zprime-def)  
 ultimately have  $z=3$  by auto  
 with  $za$  have  $3 \text{ dvd } a$  by simp  
 with  $ab$  have  $3 \text{ dvd } p$  by (auto simp add: zdvd-zmult2)

```

    with p3 have False by auto }
  ultimately have z dvd b by auto
  with za z ab-relprime show False
  by (auto simp add: zgcd1-iff-no-common-primedivisor)
qed
have ab2: zgcd(a+3*b, a- 3*b) = 1
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix z assume z: zprime z and zab1: z dvd a+3*b and zab2: z dvd a- 3*b
  hence z dvd (a+3*b)+(a- 3*b) by (simp only: zdvd-zadd)
  hence z dvd 2*a by simp
  with zab1 z ab1 show False
  by (auto simp add: zgcd1-iff-no-common-primedivisor)
qed
have zgcd(a- 3*b, 2*a) = 1
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix z assume z: zprime z and z2a: z dvd 2*a and zab: z dvd a- 3*b
  hence z dvd 2*a-(a- 3*b) by (simp only: zdvd-zdiff)
  moreover have 2*a-(a- 3*b) = a+3*b by simp
  ultimately have z dvd a+3*b by simp
  with z2a z ab1 show False
  by (auto simp add: zgcd1-iff-no-common-primedivisor)
qed
with abc ab1 ab2 triv3 have  $\exists k l m. 2*a=k^3 \wedge a+3*b=l^3 \wedge a- 3*b=m^3$ 
  by (simp only: int-triple-relprime-odd-power-divisors)
then obtain  $\alpha \beta \gamma$  where albega:
   $2*a = \gamma^3 \wedge a - 3*b = \alpha^3 \wedge a+3*b = \beta^3$  by auto
— show this is a (smaller) solution
hence  $\alpha^3 + \beta^3 = \gamma^3$  by auto
moreover have  $\alpha*\beta*\gamma \neq 0$ 
proof (rule ccontr, safe)
  assume  $\alpha * \beta * \gamma = 0$ 
  with albega ab have p=0 by (auto simp add: power-0-left)
  with vwpq vwx show False by auto
qed
moreover have  $\gamma \in zEven$ 
proof —
  have  $2*a \in zEven$  by (simp add: zEven-def)
  with albega have  $\gamma^3 \in zEven$  by simp
  thus ?thesis by (simp only: power-preserves-even)
qed
moreover have zgcd( $\alpha, \beta$ )=1
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix z assume z: zprime z and za: z dvd  $\alpha$  and zb: z dvd  $\beta$ 
  hence z dvd  $\alpha * \alpha^2 \wedge z dvd \beta * \beta^2$  by (simp add: zdvd-zmult2)
  hence z dvd  $\alpha^3 \wedge z dvd \beta^3$  by (auto simp only: power-Suc)
  with albega have z dvd  $a - 3*b \wedge z dvd a+3*b$  by auto
  with ab2 z show False
  by (auto simp add: zgcd1-iff-no-common-primedivisor)
qed
moreover have  $nat|\gamma^3| < nat|x^3|$ 
proof —
  let ?A =  $p^2 + 3*q^2$ 

```

**from**  $vwx$   $vwpq$  **have**  $x^3 = 2*p*?A$  **by** *auto*  
**also with**  $ab$  **have**  $\dots = 2*a*((a+3*b)*(a-3*b)*?A)$  **by** *auto*  
**also with**  $albega$  **have**  $\dots = \gamma^3 * ((a+3*b)*(a-3*b)*?A)$  **by** *auto*  
**finally have**  $eq: |x^3| = |\gamma^3| * |(a+3*b)*(a-3*b)*?A|$   
**by** (*auto simp add: abs-mult*)  
**with**  $x3pos$  **have**  $|(a+3*b)*(a-3*b)*?A| > 0$  **by** *auto*  
**hence**  $eqpos: |(a+3*b)*(a-3*b)| > 0$  **by** *auto*  
**moreover have**  $Ag1: |?A| > 1$   
**proof** –  
**have**  $Aqf3: is-qn ?A 3$  **by** (*auto simp add: is-qn-def*)  
**moreover have**  $triv3b: (3::int) \geq 1$  **by** *simp*  
**ultimately have**  $?A \geq 0$  **by** (*simp only: qn-pos*)  
**hence**  $?A > 1 \vee ?A = 0 \vee ?A = 1$  **by** *auto*  
**moreover**  
**{ assume**  $?A = 0$  **with**  $triv3b$  **have**  $p = 0 \wedge q = 0$  **by** (*rule qn-zero*)  
**with**  $vwpq$   $vwx$  **have** *False* **by** *auto* **}**  
**moreover**  
**{ assume**  $A1: ?A = 1$   
**have**  $q=0$   
**proof** (*rule ccontr*)  
**assume**  $q \neq 0$   
**hence**  $q^2 > 0$  **by** (*simp add: zero-less-power2*)  
**hence**  $3*q^2 > 1$  **by** *arith*  
**moreover have**  $p^2 \geq 0$  **by** (*rule zero-le-power2*)  
**ultimately have**  $?A > 1$  **by** *arith*  
**with**  $A1$  **show** *False* **by** *simp*  
**qed**  
**with**  $A1$  **have**  $p21: p^2 = 1$  **by** *simp*  
**hence**  $|p| = 1$  **by** (*rule power2-eq1-iff*)  
**with**  $vwpq$   $vwx$   $A1$  **have**  $|x^3| = 2$  **by** *auto*  
**hence** *False* **by** (*rule two-not-abs-cube*) **}**  
**ultimately show**  $?thesis$  **by** *auto*  
**qed**  
**ultimately have**  
 $| (a+3*b)*(a-3*b) | * 1 < | (a+3*b)*(a-3*b) | * |?A|$   
**by** (*simp only: zmult-zless-mono2*)  
**with**  $eqpos$  **have**  $| (a+3*b)*(a-3*b) | * |?A| > 1$  **by** *arith*  
**hence**  $| (a+3*b)*(a-3*b) * ?A | > 1$  **by** (*auto simp add: abs-mult*)  
**moreover have**  $|\gamma^3| > 0$   
**proof** –  
**from**  $eq$  **have**  $|\gamma^3| = 0 \implies |x^3| = 0$  **by** *auto*  
**with**  $x3pos$  **show**  $?thesis$  **by** *auto*  
**qed**  
**ultimately have**  $|\gamma^3| * 1 < |\gamma^3| * | (a+3*b)*(a-3*b) * ?A |$   
**by** (*rule zmult-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  $x^3 = (18r)(q^2 + 3r^2)$  and these  
– factors are coprime; hence both are cubes

```

{ assume p3: 3 dvd p
  then obtain r where r: p = 3*r by (auto simp add: dvd-def)
  moreover have 3 dvd 3*(3*r^2 + q^2) by (rule zdvd-triv-left)
  ultimately have pq3: 3 dvd p^2+3*q^2 by (simp add: power-mult-distrib)
  moreover from p3 have 3 dvd 2*p by (rule zdvd-zmult)
  ultimately have g3: 3 dvd ?g by (simp add: zgcd-greatest-iff)
  have qr-relprime: zgcd(q,r) = 1
  proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
    fix z assume z: zprime z and zq: z dvd q and z dvd r
    with r have z dvd p by (simp add: zdvd-zmult)
    with zq have z dvd p+q ∧ z dvd p-q by (simp add: zdvd-zadd zdvd-zdiff)
    with vw have z dvd zgcd(v, w) by (simp add: zgcd-greatest-iff)
    with vwx z show False by (auto simp add: zprime-def)
  qed
  have factors-relprime: zgcd(18*r, q^2 + 3*r^2) = 1
  proof -
    from g3 obtain k where k: ?g = 3*k by (auto simp add: dvd-def)
    have k = 1
    proof (rule ccontr)
      assume k ≠ 1
      with g1 k have k > 1 by auto
      then obtain h where h: zprime h ∧ h dvd k
        by (frule-tac a=k in zprime-factor-exists, blast)
      with k have hg: 3*h dvd ?g by (auto simp add: zdvd-zmult-mono)
      hence 3*h dvd p^2 + 3*q^2 and hp: 3*h dvd 2*p
        by (auto simp only: zgcd-greatest-iff)
      then obtain s where s: p^2 + 3*q^2 = (3*h)*s
        by (auto simp add: dvd-def)
      with r have rqh: 3*r^2+q^2 = h*s by (simp add: power-mult-distrib)
      from hp r have 3*h dvd 3*(2*r) by simp
      moreover have (3::int) ≠ 0 by simp
      ultimately have h dvd 2*r by (rule zdvd-mult-cancel)
      with h have h dvd 2 ∨ h dvd r by (simp only: zprime-zdvd-zmult-general)
      moreover have ¬ h dvd 2
      proof (rule ccontr, simp)
        assume h dvd 2
        with h have h=2 by (auto simp add: zdvd-not-zless zprime-def)
        with hg have 2*3 dvd ?g by auto
        hence 2 dvd ?g by (rule zdvd-zmultD2)
        with gOdd show False by simp
      qed
      ultimately have hr: h dvd r by simp
      then obtain t where r = h*t by (auto simp add: dvd-def)
      hence t: r^2 = h*(h*t^2) by (auto simp add: power2-eq-square)
      with rqh have h*s = h*(3*h*t^2) + q^2 by simp
      hence q^2 = h*(s - 3*h*t^2) by (simp add: zdiff-zmult-distrib2)
      hence h dvd q^2 by simp
      with h have h dvd q by (auto dest: zprime-zdvd-power)
      with hr have h dvd zgcd(q,r) by (simp add: zgcd-greatest-iff)
      with h qr-relprime show False by (unfold zprime-def, auto)
    qed
    with k r have 3 = zgcd(2*(3*r), (3*r)^2 + 3*q^2) by auto
  }

```

**also have**  $\dots = \text{zgcd}(3*(2*r), 3*(3*r^2 + q^2))$   
**by** (*simp add: power-mult-distrib*)  
**also have**  $\dots = 3 * \text{zgcd}(2*r, 3*r^2 + q^2)$   
**by** (*simp only: zgcd-zmult-distrib2*)  
**finally have**  $\text{zgcd}(2*r, 3*r^2 + q^2) = 1$  **by** *auto*  
**moreover have**  $\text{zgcd}(3*3, 3*r^2 + q^2) = 1$   
**proof** (*simp only: zgcd1-iff-no-common-primedivisor, clarify*)  
**fix**  $h::\text{int}$  **assume**  $h \text{ dvd } 3*3$  **and**  $h: \text{zprime } h$  **and**  $\text{hrq}: h \text{ dvd } 3*r^2 + q^2$   
**hence**  $h \text{ dvd } 3 \vee h \text{ dvd } 3$  **by** (*simp only: zprime-zdvd-zmult-general*)  
**hence**  $h3: h \text{ dvd } 3$  **by** *simp*  
**have**  $h \leq 3$   
**proof** (*rule ccontr*)  
**assume**  $\neg h \leq 3$  **hence**  $h > 3$  **by** *simp*  
**with**  $h3$  **show** *False* **by** (*auto simp add: zdvd-not-zless*)  
**qed**  
**with**  $h$  **have**  $h = 2 \vee h = 3$  **by** (*unfold zprime-def, auto*)  
**with**  $h h3$  **have**  $h = 3 \vee (2::\text{int}) \text{ dvd } 3$  **by** *auto*  
**hence**  $h=3$  **by** *arith*  
**with**  $\text{hrq}$  **obtain**  $s$  **where**  $3*r^2 + q^2 = 3*s$  **by** (*auto simp add: dvd-def*)  
**hence**  $q^2 = 3*(s - r^2)$  **by** *auto*  
**hence**  $3 \text{ dvd } q^2$  **and**  $\text{zprime } 3$  **by** (*auto simp only: zdvd-triv-left zprime-3*)  
**hence**  $3 \text{ dvd } q$  **by** (*rule-tac p=3 in zprime-zdvd-power*)  
**with**  $p3$  **have**  $3 \text{ dvd } p+q \wedge 3 \text{ dvd } p-q$  **by** (*simp add: zdvd-zdiff zdvd-zadd*)  
**with**  $vw$  **have**  $3 \text{ dvd } \text{zgcd}(v,w)$  **by** (*simp add: zgcd-greatest-iff*)  
**with**  $vw x$  **show** *False* **by** *auto*  
**qed**  
**ultimately have**  $\text{zgcd}((3*3)*(2*r), 3*r^2 + q^2) = 1$   
**by** (*simp only: zgcd-zmult-cancel*)  
**thus** *?thesis* **by** (*auto simp add: mult-ac add-ac*)  
**qed**  
**moreover have**  $\text{rqx}: (18*r)*(q^2 + 3*r^2) = x^3$   
**proof** –  
**from**  $vw x \text{ vwpq}$  **have**  $x^3 = 2*p*(p^2 + 3*q^2)$  **by** *auto*  
**also with**  $r$  **have**  $\dots = 2*(3*r)*(9*r^2 + 3*q^2)$   
**by** (*auto simp add: power2-eq-square*)  
**finally show** *?thesis* **by** *auto*  
**qed**  
**moreover have**  $\text{triv3}: 3 = \text{nat } 3 \wedge \text{nat } 3 > 1 \wedge 3 \in \text{zOdd}$   
**by** (*unfold zOdd-def, auto*)  
**ultimately have**  $\exists c. 18*r = c^3$   
**by** (*simp only: int-relprime-odd-power-divisors*)  
**then obtain**  $c1$  **where**  $c1^3 = 3*(6*r)$  **by** *auto*  
**hence**  $3 \text{ dvd } c1^3$  **and**  $\text{zprime } 3$  **by** (*auto simp only: zdvd-triv-left zprime-3*)  
**hence**  $3 \text{ dvd } c1$  **by** (*rule-tac p=3 in zprime-zdvd-power*)  
**with**  $c1$  **obtain**  $c$  **where**  $3*c^3 = 2*r$   
**by** (*auto simp add: power-mult-distrib dvd-def*)  
**from**  $\text{rqx}$  **factors-relprime** **have**  $\text{zgcd}(q^2 + 3*r^2, 18*r) = 1$   
**and**  $(q^2 + 3*r^2)*(18*r) = x^3$  **by** (*auto simp add: zgcd-commute mult-ac*)  
**with**  $\text{triv3}$  **have**  $\exists d. q^2 + 3*r^2 = d^3$   
**by** (*simp only: int-relprime-odd-power-divisors*)  
**then obtain**  $d$  **where**  $q^2 + 3*r^2 = d^3$  **by** *auto*  
**have**  $d \in \text{zOdd}$

```

proof (rule ccontr)
  assume  $d \notin zOdd$  hence  $d \in zEven$  by (rule not-odd-impl-even)
  hence  $d^3 \in zEven$  by (simp only: power-preserves-even)
  hence  $2 \text{ dvd } d^3$  by (simp add: zEven-def dvd-def)
  moreover have  $2 \text{ dvd } 2*(9*r)$  by (rule zdvd-triv-left)
  ultimately have  $2 \text{ dvd } zgcd(2*(9*r), d^3)$  by (simp add: zgcd-greatest-iff)
  with  $d$  factors-relprime show False by auto
qed
with  $d$  qr-relprime have  $zgcd(q,r)=1 \wedge q^2 + 3*r^2 = d^3 \wedge d \in zOdd$ 
by simp
hence is-cube-form  $q$   $r$  by (rule qf3-cube-impl-cube-form)
then obtain  $a$   $b$  where  $q = a^3 - 9*a*b^2 \wedge r = 3*a^2*b - 3*b^3$ 
by (unfold is-cube-form-def, auto)
hence  $ab: q = a*(a+3*b)*(a-3*b) \wedge r = b*(a+b)*(a-b)*3$ 
by (simp add: nat-number ring-simps)
with  $c$  have  $abc: (2*b)*(a+b)*(a-b) = c^3$  by auto
have  $ab\text{-relprime}: zgcd(a,b)=1$ 
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix  $z$  assume  $z: zprime\ z$  and  $za: z \text{ dvd } a$  and  $zb: z \text{ dvd } b$ 
  with  $ab$  have  $z \text{ dvd } q \wedge z \text{ dvd } r$  by (simp add: zdvd-zmult2)
  with  $z$  qr-relprime show False
  by (auto simp add: zgcd1-iff-no-common-primedivisor)
qed
have  $ab1: zgcd(2*b, a+b) = 1$ 
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix  $z$  assume  $z: zprime\ z$  and  $z \text{ dvd } 2*b$  and  $zab: z \text{ dvd } a+b$ 
  hence  $z \text{ dvd } 2 \vee z \text{ dvd } b$  by (simp add: zprime-zdvd-zmult)
  moreover
  { assume  $z2: z \text{ dvd } 2$ 
    hence  $z \leq 2$  by (simp only: zdvd-imp-le)
    with  $z$  have  $z = 2$  by (unfold zprime-def, auto)
    with  $zab$  have  $ab2: 2 \text{ dvd } a+b$  by simp
    moreover have  $2 \text{ dvd } 2*b$  by (rule zdvd-triv-left)
    ultimately have  $2 \text{ dvd } a+b+2*b$  by (rule zdvd-zadd)
    hence  $2 \text{ dvd } a+3*b$  by arith
    hence  $2 \text{ dvd } (a+3*b)*((a-3*b)*a)$  by (rule zdvd-zmult2)
    with  $ab$  have  $qEven: 2 \text{ dvd } q$  by (simp only: mult-ac)
    from  $ab2$  have  $2 \text{ dvd } (a+b)*((a-b)*3*b)$  by (rule zdvd-zmult2)
    with  $ab$  have  $2 \text{ dvd } r$  by (simp only: mult-ac)
    with  $qEven$  have  $2 \text{ dvd } zgcd(q,r)$  by (simp add: zgcd-greatest-iff)
    with  $qr\text{-relprime}$  have False by auto }
  moreover
  { assume  $zb: z \text{ dvd } b$ 
    with  $zab$  have  $z \text{ dvd } a+b-b$  by (simp only: zdvd-zdiff)
    hence  $z \text{ dvd } a$  by simp
    with  $zb$   $ab\text{-relprime}$   $z$  have False
    by (auto simp add: zgcd1-iff-no-common-primedivisor) }
  ultimately show False by auto
qed
have  $ab2: zgcd(a+b, a-b) = 1$ 
proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)
  fix  $z$  assume  $z: zprime\ z$  and  $zab1: z \text{ dvd } a+b$  and  $zab2: z \text{ dvd } a-b$ 

```

hence  $z \text{ dvd } (a+b)-(a-b)$  by (simp only: zdvd-zdiff)  
 hence  $z \text{ dvd } 2*b$  by simp  
 with  $zab1 \ z \ ab1$  show False  
 by (auto simp add: zgcd1-iff-no-common-primedivisor)  
 qed  
 have  $zgcd(a-b, 2*b) = 1$   
 proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)  
 fix  $z$  assume  $z$ :  $zprime \ z$  and  $z2b$ :  $z \text{ dvd } 2*b$  and  $zab$ :  $z \text{ dvd } a-b$   
 hence  $z \text{ dvd } a-b+2*b$  by (simp only: zdvd-zadd)  
 moreover have  $a-b+2*b = a+b$  by simp  
 ultimately have  $z \text{ dvd } a+b$  by simp  
 with  $z2b \ z \ ab1$  show False  
 by (auto simp add: zgcd1-iff-no-common-primedivisor)  
 qed  
 with  $abc \ ab1 \ ab2 \ triv3$  have  $\exists \ k \ l \ m. 2*b = k^3 \wedge a+b = l^3 \wedge a-b = m^3$   
 by (simp only: int-triple-relprime-odd-power-divisors)  
 then obtain  $\alpha1 \ \beta \ \gamma$  where  $a1$ :  $2*b = \gamma^3 \wedge a-b = \alpha1^3 \wedge a+b = \beta^3$   
 by auto  
 then obtain  $\alpha$  where  $\alpha = -\alpha1$  by auto  
 — show this is a (smaller) solution  
 with  $triv3 \ a1$  have  $a2$ :  $\alpha^3 = b-a$  by (auto simp only: neg-odd-power)  
 with  $a1$  have  $\alpha^3 + \beta^3 = \gamma^3$  by auto  
 moreover have  $\alpha*\beta*\gamma \neq 0$   
 proof (rule ccontr, safe)  
 assume  $\alpha * \beta * \gamma = 0$   
 with  $a1 \ a2 \ ab$  have  $r=0$  by (auto simp add: power-0-left)  
 with  $r \ vwpq \ vwx$  show False by auto  
 qed  
 moreover have  $\gamma \in zEven$   
 proof —  
 have  $2*b \in zEven$  by (simp add: zEven-def)  
 with  $a1$  have  $\gamma^3 \in zEven$  by simp  
 thus ?thesis by (simp only: power-preserves-even)  
 qed  
 moreover have  $zgcd(\alpha, \beta)=1$   
 proof (simp only: zgcd1-iff-no-common-primedivisor, clarify)  
 fix  $z$  assume  $z$ :  $zprime \ z$  and  $za$ :  $z \text{ dvd } \alpha$  and  $zb$ :  $z \text{ dvd } \beta$   
 hence  $z \text{ dvd } \alpha * \alpha^2 \wedge z \text{ dvd } \beta * \beta^2$  by (simp add: zdvd-zmult2)  
 hence  $z \text{ dvd } \alpha^3 \wedge z \text{ dvd } \beta^3$  by (auto simp only: power-Suc)  
 with  $a1 \ a2$  have  $z \text{ dvd } b-a \wedge z \text{ dvd } a+b$  by auto  
 hence  $z \text{ dvd } -(b-a) \wedge z \text{ dvd } a+b$  by (auto simp only: zdvd-zminus-iff)  
 with  $ab2 \ z$  show False  
 by (auto simp add: zgcd1-iff-no-common-primedivisor)  
 qed  
 moreover have  $nat|\gamma^3| < nat|x^3|$   
 proof —  
 let  $?A = p^2 + 3*q^2$   
 from  $vwx \ vwpq$  have  $x^3 = 2*p*?A$  by auto  
 also with  $r$  have  $\dots = 6*r*?A$  by auto  
 also with  $ab$  have  $\dots = 2*b*(9*(a+b)*(a-b)*?A)$  by auto  
 also with  $a1$  have  $\dots = \gamma^3 * (9*(a+b)*(a-b)*?A)$  by auto  
 finally have eq:  $|x^3| = |\gamma^3| * |9*(a+b)*(a-b)*?A|$

by (auto simp add: abs-mult)  
 with  $x3pos$  have  $|9*(a+b)*(a-b)*?A| > 0$  by auto  
 hence  $|(a+b)*(a-b)*?A| \geq 1$  by arith  
 hence  $|9*(a+b)*(a-b)*?A| > 1$  by arith  
 moreover have  $|\gamma^3| > 0$   
 proof -  
 from eq have  $|\gamma^3| = 0 \implies |x^3|=0$  by auto  
 with  $x3pos$  show ?thesis by auto  
 qed  
 ultimately have  $|\gamma^3| * 1 < |\gamma^3| * |9*(a+b)*(a-b)*?A|$   
 by (rule zmult-zless-mono2)  
 with eq have  $|x^3| > |\gamma^3|$  by auto  
 thus ?thesis by arith  
 qed  
 ultimately have ?thesis by auto }  
 ultimately show ?thesis by auto  
 qed  
 thus  $\exists y. \text{nat}|y^3| < \text{nat}|x^3| \wedge \neg ?Q y$  by auto  
 qed

The theorem. Puts equation in requested shape.

**theorem** *fermat3*:

assumes *ass*:  $(x::\text{int})^3 + y^3 = z^3$

shows  $x*y*z=0$

**proof** (rule ccontr)

let  $?g = \text{zgcd}(x,y)$

let  $?c = z \text{ div } ?g$

assume *xyz0*:  $x*y*z \neq 0$

— divide out the g.c.d.

hence  $x \neq 0 \vee y \neq 0$  by simp

then obtain  $a b$  where  $ab$ :  $x = ?g*a \wedge y = ?g*b \wedge \text{zgcd}(a,b)=1$

by (frule-tac  $a=x$  in make-zrelprime, auto)

moreover have *abc*:  $?c*?g = z \wedge a^3 + b^3 = ?c^3 \wedge a*b*?c \neq 0$

**proof** -

from *xyz0* have *g0*:  $?g \neq 0$  by (simp add: zgcd-def gcd-zero)

have *zgab*:  $z^3 = ?g^3 * (a^3 + b^3)$

**proof** -

from *ab* and *ass* have  $z^3 = (?g*a)^3 + (?g*b)^3$  by simp

thus ?thesis by (simp only: power-mult-distrib zadd-zmult-distrib2)

qed

have *cgz*:  $?c * ?g = z$

**proof** -

from *zgab* have  $?g^3 \text{ dvd } z^3$  by simp

hence  $?g \text{ dvd } z$  by (simp only: zpower-zdvd-mono)

thus ?thesis by (simp only: mult-ac zdvd-mult-div-cancel)

qed

moreover have  $a^3 + b^3 = ?c^3$

**proof** -

have  $?c^3 * ?g^3 = (a^3 + b^3) * ?g^3$

**proof** -

have  $?c^3 * ?g^3 = (?c*?g)^3$  by (simp only: power-mult-distrib)

also with *cgz* have  $\dots = z^3$  by simp

also with  $zgab$  have  $\dots = ?g^3*(a^3+b^3)$  by *simp*  
 finally show *?thesis* by *simp*  
 qed  
 with  $g0$  show *?thesis* by *auto*  
 qed  
 moreover from  $ab$  and  $xyz0$  and  $cgz$  have  $a*b*?c \neq 0$  by *auto*  
 ultimately show *?thesis* by *simp*  
 qed  
 — make both sides even  
 have  $\exists u v w. u^3 + v^3 = w^3 \wedge u*v*w \neq 0 \wedge w \in zEven \wedge zgcd(u,v)=1$   
 proof —  
 let  $?Q u v w = u^3 + v^3 = w^3 \wedge u*v*w \neq 0 \wedge w \in zEven \wedge zgcd(u,v)=1$   
 have  $a \in zEven \vee b \in zEven \vee ?c \in zEven$   
 proof (rule *ccontr*)  
 assume  $\neg(a \in zEven \vee b \in zEven \vee ?c \in zEven)$   
 hence *aodd*:  $a \in zOdd$  and  $b \in zOdd \wedge ?c \in zOdd$   
 by (auto simp add: *odd-iff-not-even*)  
 hence  $?c^3 - b^3 \in zEven$  by (simp only: *power-preserves-odd odd-minus-odd*)  
 moreover from *abc* have  $?c^3 - b^3 = a^3$  by *simp*  
 ultimately have  $a^3 \in zEven$  by *auto*  
 hence  $a \in zEven$  by (simp only: *power-preserves-even*)  
 with *aodd* show *False* by (simp add: *odd-iff-not-even*)  
 qed  
 moreover  
 { assume  $a \in zEven$   
 then obtain  $u v w$  where *uvwabc*:  $u = -b \wedge v = ?c \wedge w = a \wedge w \in zEven$   
 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  $\dots = (-1)^3*b^3 + ?c^3$  by (simp only: *power-mult-distrib*)  
 also have  $\dots = -(b^3) + ?c^3$  by (auto simp add: *neg-one-odd-power*)  
 also with *abc* and *uvwabc* have  $\dots = w^3$  by *auto*  
 finally show *?thesis* by *simp*  
 qed  
 moreover have  $zgcd(u,v)=1$   
 proof (simp only: *zgcd1-iff-no-common-primedivisor*, *clarify*)  
 fix  $h::int$  assume *hu*:  $h \text{ dvd } u$  and  $h \text{ dvd } v$  and  $h$ : *zprime*  $h$   
 with *uvwabc* have  $h \text{ dvd } ?c*?c^2$  by (simp only: *zdvd-zmult2*)  
 with *abc* have  $h \text{ dvd } a^3 + b^3$  by (simp only: *cube-square*)  
 moreover from *hu uvwabc* have  $h \text{ dvd } b*b^2$  by (simp add: *zdvd-zmult2*)  
 ultimately have  $h \text{ dvd } a^3 + b^3 - b^3$  by (simp only: *cube-square zdvd-zdiff*)  
 with  $h$  *hu uvwabc* have  $h \text{ dvd } a \wedge h \text{ dvd } b$  by (auto dest: *zprime-zdvd-power*)  
 with  $h$  *ab* show *False* by (auto simp add: *zgcd1-iff-no-common-primedivisor*)  
 qed  
 ultimately have  $?Q u v w$  by *simp*  
 hence *?thesis* by *auto* }  
 moreover  
 { assume  $b \in zEven$   
 then obtain  $u v w$  where *uvwabc*:  $u = -a \wedge v = ?c \wedge w = b \wedge w \in zEven$   
 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  $\dots = (-1)^3*a^3 + ?c^3$  by (*simp only: power-mult-distrib*)**  
**also have  $\dots = -(a^3) + ?c^3$  by (*auto simp add: neg-one-odd-power*)**  
**also with  $abc$  and  $uvwabc$  have  $\dots = w^3$  by *auto***  
**finally show *?thesis* by *simp***  
**qed**  
**moreover have  $zgcd(u,v)=1$**   
**proof (*simp only: zgcd1-iff-no-common-primedivisor, clarify*)**  
**fix  $h::int$  assume  $hu: h \text{ dvd } u$  and  $h \text{ dvd } v$  and  $h: zprime\ h$**   
**with  $uvwabc$  have  $h \text{ dvd } ?c*?c^2$  by (*simp only: zdvd-zmult2*)**  
**with  $abc$  have  $h \text{ dvd } a^3+b^3$  by (*simp only: cube-square*)**  
**moreover from  $hu\ uvwabc$  have  $h \text{ dvd } a*a^2$  by (*simp add: zdvd-zmult2*)**  
**ultimately have  $h \text{ dvd } a^3+b^3-a^3$  by (*simp only: cube-square zdvd-zdiff*)**  
**with  $h\ hu\ uvwabc$  have  $h \text{ dvd } a \wedge h \text{ dvd } b$  by (*auto dest: zprime-zdvd-power*)**  
**with  $h\ ab$  show *False* by (*auto simp add: zgcd1-iff-no-common-primedivisor*)**  
**qed**  
**ultimately have  $?Q\ u\ v\ w$  by *simp***  
**hence *?thesis* by *auto* }**  
**moreover**  
**{ assume  $?c \in zEven$**   
**then obtain  $u\ v\ w$  where  $uvwabc: u = a \wedge v = b \wedge w = ?c \wedge w \in zEven$**   
**by *auto***  
**with  $abc\ ab$  have *?thesis* by *auto* }**  
**ultimately show *?thesis* by *auto***  
**qed**  
**hence  $\exists w. \exists u\ v. u^3 + v^3 = w^3 \wedge u*v*w \neq 0 \wedge w \in zEven \wedge zgcd(u,v)=1$**   
**by *auto***  
**— show contradiction using the earlier result**  
**thus *False* by (*auto simp only: no-rewritten-fermat3*)**  
**qed**  
**corollary *fermat-mult3*:**  
**assumes  $xyz: (x::int)^n + y^n = z^n$  and  $n: 3 \text{ dvd } n$**   
**shows  $x*y*z=0$**   
**proof –**  
**from  $n$  obtain  $m$  where  $n = m*3$  by (*auto simp only: mult-ac dvd-def*)**  
**with  $xyz$  have  $(x^m)^3 + (y^m)^3 = (z^m)^3$  by (*simp only: power-mult*)**  
**hence  $(x^m)*(y^m)*(z^m) = 0$  by (*rule fermat3*)**  
**thus *?thesis* by *auto***  
**qed**  
**end**