

Chapter 31 : Decomposition in the sum of two squares.

We are given $N : \text{nat}$ and asked to determine the number of ways N can be expressed as the sum of two squares, in other words we want to establish the following

Post: $r = \langle + x, y : 0 \leq x \leq y : g.x.y \rangle$

where

$$* (0) \quad g.x.y = 1 \quad \Leftarrow \quad x^2 + y^2 = N$$

$$* (1) \quad g.x.y = 0 \quad \Leftarrow \quad x^2 + y^2 \neq N$$

We will begin by modelling the domain.

$$* (2) \quad C.0 = \langle + x, y : 0 \leq x \leq y : g.x.y \rangle$$

We would like to get an expression in which the range is bounded above as well as below. To that end we calculate.

$$\begin{aligned} & C.0 \\ = & \quad \{(0)\} \\ & \langle + x, y : 0 \leq x \leq y : g.x.y \rangle \\ = & \quad \{\text{Algebra}\} \\ & \langle + x, y : 0 \leq x \leq y \leq b : g.x.y \rangle + \langle + x, y : 0 \leq x \leq y \wedge y > b : g.x.y \rangle \\ = & \quad \{\text{seeking to eliminate 2nd quantifier, assume } b^2 \geq N\} \\ & \langle + x, y : 0 \leq x \leq y \leq b : g.x.y \rangle + 0 \\ = & \quad \{\text{Name and conquer}\} \\ & D.0.b \end{aligned}$$

$$- (3) \quad b^2 \geq N \Rightarrow D.0.b = C.0$$

Now we can parameterise D as follows

$$* (4) \quad D.a.b = \langle + x, y : a \leq x \leq y \leq b : g.x.y \rangle$$

Let us now explore D

Consider

$$\begin{aligned} & D.a.b \\ = & \quad \{(1)\} \\ & \langle + x, y : a \leq x \leq y \leq b : g.x.y \rangle \\ = & \quad \{\text{split off } x = a \text{ term}\} \\ & \langle + x, y : a+1 \leq x \leq y \leq b : g.x.y \rangle + \langle + y : a \leq y \leq b : g.a.y \rangle \\ = & \quad \{(1), (7)\} \\ & D.(a+1).b + E.b \end{aligned}$$

$$- (5) \quad D.a.b = D.(a+1).b + E.b$$

Symmetrically, we also consider

$$\begin{aligned}
& D.a.b \\
= & \{(1)\} \\
& \langle +x, y : a \leq x \leq y \leq b : g.x.y \rangle \\
= & \{\text{split off } y = b \text{ term}\} \\
& \langle +x, y : a \leq x \leq y \leq b-1 : g.x.y \rangle + \langle +x : a \leq x \leq b : g.x.b \rangle \\
= & \{(1), (8)\} \\
& D.a.(b-1) + F.a
\end{aligned}$$

$$- (6) D.a.b = D.a.(b-1) + F.a$$

$$* (7) E.b = \langle +y : a \leq y \leq b : g.a.y \rangle$$

$$* (8) F.a = \langle +x : a \leq x \leq b : g.x.b \rangle$$

$$- (9) a > b \Rightarrow D.a.b = 0$$

Now we examine E and F and see if we can evaluate them.

$$- (10) E.b = 0 \Leftarrow a^2 + b^2 < N^1$$

$$- (11) E.b = 1 \Leftarrow a^2 + b^2 = N$$

$$- (12) E.b = ? \Leftarrow a^2 + b^2 > N$$

$$- (13) F.a = ? \Leftarrow a^2 + b^2 < N$$

$$- (14) F.a = 1 \Leftarrow a^2 + b^2 = N$$

$$- (15) F.a = 0 \Leftarrow a^2 + b^2 > N^2$$

And this would seem to complete our model. We begin to calculate the solution.

Invariants.

$$P0 : r + D.a.b = C.0$$

$$P1 : 0 \leq a$$

Termination and Guard.

We note that $P0 \wedge P1 \wedge a > b \Rightarrow \text{Post}$

So we will choose $a \leq b$ as our guard.

¹ $a^2 + y^2$ increasing in y

² $x^2 + b^2$ increasing in x

Establish the invariants

$$r, a, b := 0, 0, \alpha \{ \alpha^2 \geq N \}$$

This can be achieved by a linear search giving us the program outline as follows.

```

r, a, b := 0, 0, 0
;do  $b^2 < N \rightarrow b := b+1$  od
{ $P_0 \wedge P_1$ }

```

Loop body.

```

P0
=      {defn.}
r + D.a.b = C.0
=      {(5)}
r + D.(a+1).b + E.b = C.0
=      {case analysis,  $a^2 + b^2 < N$  (10)}
r + D.(a+1).b + 0 = C.0
=      {WP}
(a := a + 1).P0

```

This gives us

$$\text{if } a^2 + b^2 < N \rightarrow a := a + 1$$

```

P0
=      {defn.}
r + D.a.b = C.0
=      {(5)}
r + D.(a+1).b + E.b = C.0
=      {case analysis,  $a^2 + b^2 = N$  (11)}
r + D.(a+1).b + 1 = C.0
=      {WP}
(r, a := r+1, a+1).P0

```

This gives us

$$\text{if } a^2 + b^2 = N \rightarrow r, a := r+1, a+1$$

Symmetrically we explore using (4)

$$\begin{aligned}
& P0 \\
= & \quad \{\text{defn.}\} \\
& r + D.a.b = C.0 \\
= & \quad \{(6)\} \\
& r + D.(a+1).b + F.a = C.0 \\
= & \quad \{\text{case analysis, } a^2 + b^2 = N \text{ (14)}\} \\
& r + D.a.(b-1) + 1 = C.0 \\
= & \quad \{\text{WP}\} \\
& (r, b := r+1, b-1).P0
\end{aligned}$$

This gives us

$$\text{if } a^2 + b^2 = N \rightarrow r, b := r+1, b-1$$

$$\begin{aligned}
& P0 \\
= & \quad \{\text{defn.}\} \\
& r + D.a.b = C.0 \\
= & \quad \{(6)\} \\
& r + D.a.(b-1) + F.a = C.0 \\
= & \quad \{\text{case analysis, } a^2 + b^2 > N \text{ (15)}\} \\
& r + D.a.(b-1) + 0 = C.0 \\
= & \quad \{\text{WP}\} \\
& (b := b-1).P0
\end{aligned}$$

This gives us

$$\text{if } a^2 + b^2 > N \rightarrow b := b-1$$

Finished Algorithm.

$r, a, b := 0, 0, 0$

$\text{;do } b^2 < N \rightarrow b := b+1 \text{ od}$

$\text{;do } a \leq b \rightarrow$

$\text{if } a^2 + b^2 < N \rightarrow a := a + 1$
 $\square a^2 + b^2 = N \rightarrow r, a := r+1, a+1$
 $\square a^2 + b^2 = N \rightarrow r, b := r+1, b-1$
 $\square a^2 + b^2 > N \rightarrow b := b-1$
 fi

od

