Chapter 31 : Decomposition in the sum of two squares.

We are given N : 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: $r = \langle + x,y : 0 \le x \le y : g.x.y \rangle$
where
* (0) $g.x.y \quad = \quad 1 \quad \Leftarrow \quad x^2 + y^2 = N$
* (1) $g.x.y \quad = \quad 0 \quad \Leftarrow \quad x^2 + y^2 \ne N$

We will begin by modelling the domain.
`
* (2) $C.0 = \langle + x, y : 0 \le x \le y : g.x.y \rangle$

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

$C.0$
= {(2)}
$\langle + x, y : 0 \le x \le y : g.x.y \rangle$
= {Algebra}
$\langle + x, y : 0 \le x \le y \le b : g.x.y \rangle + \langle + x, y : 0 \le x \le y \ \wedge y > b : g.x.y \rangle$
= {seeking to eliminate 2nd quantifier, assume $b^2 \ge N$ }
$\langle + x, y : 0 \le x \le y \le b : g.x.y \rangle + 0$
= {Name and conquer}
$D.0.b$

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

Now we can parameterise D as follows

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

Let us now explore D

Consider

$D.a.b$
= {(4)}
$\langle + x, y : a \le x \le y \le b : g.x.y \rangle$
= {split off x = a term}
$\langle + x, y : a+1 \le x \le y \le b : g.x.y \rangle + \langle + y : a \le y \le b: g.a.y \rangle$
= {(4), (7)}
$D.(a+1).b + E.b$

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

Symmetrically, we also consider

$$
\begin{array}{ll}
 & D.a.b \\
= & \quad \{(4)\} \\
 & \langle + x, y : a \le x \le y \le b : g.x.y \rangle \\
= & \quad \{\text{split off } y = b \text{ term}\} \\
 & \langle + x, y : a \le x \le y \le b\text{-}1 : g.x.y \rangle + \langle + x : a \le x \le b : g.x.b \rangle \\
= & \quad \{(4), (8)\} \\
 & D.a.(b\text{-}1) + F.a
\end{array}
$$

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

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

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

- (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 : $0 \le a$

Termination and Guard.

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

So we will choose $a \le b$ 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, α $\{\alpha^2 \geq N\}$

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
$\{P0 \wedge P1\}$

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

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

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

Symmetrically we explore using (4)

P0

= {defn.}

r + D.a.b = C.0

= {(6)}

r + D.a.(b-1) +F.a = C.0

= {case analysis, $a^2 + b^2 = N$ (14)}

r + D.a.(b-1) + 1 = C.0

= {WP}

(r, b := r+1, b-1).P0

This gives us

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

P0

= {defn.}

r + D.a.b = C.0

= {(6)}

r + D.a.(b-1) + F.a = C.0

= {case analysis, $a^2 + b^2 > N$ (15)}

r + D.a.(b-1) + 0 = C.0

= {WP}

(b := b-1).P0

This gives us

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

Finished Algorithm.

```
r, a, b := 0, 0, 0

;do b² < N → b := b+1 od

;do a ≤ b →
        if a² + b² < N → a := a + 1
        [] a² + b² = N → r, a := r+1, a+1
        [] a² + b² = N → r, b := r+1, b-1
        [] a² + b² > N → b := b-1
        fi
od
```