224 (Fermat's last program) Given natural c , write a program to find the number of unordered pairs of naturals a and b such that $a^2 + b^2 = c^2$ in time proportional to c . (An unordered pair is really a bunch of size 1 or 2 . If we have counted the pair a and b , we don't want to count the pair b and a .) Your program may use addition, subtraction, multiplication, division, and comparisons, but not exponentiation or square root.

After trying the question, scroll down to the solution.

§ Define $f\ l\ r\ =\ $ (the number of a and b such that $l{\le}a{\le}b{\le}r\ \land\ a^2{+}b^2{=}c^2$) . Formally,

$$f\ =\ \langle l, r\colon nat\cdot\ \Sigma a, b\colon 0,..c{+}1\cdot\ \textbf{if}\ l{\le}a{\le}b{\le}r\ \land\ a^2{+}b^2{=}c^2\ \textbf{then}\ 1\ \textbf{else}\ 0\rangle$$

Let's record the answer as the final value of natural variable n .

$$n' = f\ 0\ c\ \ \Leftarrow\ \ l{:=}\ 0.\ \ r{:=}\ c.\ \ n{:=}\ 0.\ \ n' = n + f\ l\ r$$

$$\begin{array}{ll} n' = n + f\ l\ r\ \ \Leftarrow & \textbf{if}\ l{>}r\ \textbf{then}\ ok \\ & \textbf{else if}\ l{\times}l + r{\times}r > c{\times}c\ \textbf{then}\ r{:=}\ r{-}1.\ \ n' = n + f\ l\ r \\ & \quad \textbf{else if}\ l{\times}l + r{\times}r < c{\times}c\ \textbf{then}\ l{:=}\ l{+}1.\ \ n' = n + f\ l\ r \\ & \quad\quad \textbf{else}\ n{:=}\ n{+}1.\ \ l{:=}\ l{+}1.\ \ r{:=}\ r{-}1.\ \ n' = n + f\ l\ r\ \textbf{fi fi fi} \end{array}$$

For timing, we must prove

$$t' \le t{+}c\ \ \Leftarrow\ \ l{:=}\ 0.\ \ r{:=}\ c.\ \ n{:=}\ 0.\ \ l{\le}r \Rightarrow t' \le t{+}r{-}l$$

$$\begin{array}{l} l{\le}r \Rightarrow t' \le t{+}r{-}l\ \ \Leftarrow \\ \quad \textbf{if}\ l{>}r\ \textbf{then}\ ok \\ \quad \textbf{else if}\ l{\times}l + r{\times}r > c{\times}c\ \textbf{then}\ r{:=}\ r{-}1.\ \ t{:=}\ t{+}1.\ \ l{\le}r \Rightarrow t' \le t{+}r{-}l \\ \quad\quad \textbf{else if}\ l{\times}l + r{\times}r < c{\times}c\ \textbf{then}\ l{:=}\ l{+}1.\ \ t{:=}\ t{+}1.\ \ l{\le}r \Rightarrow t' \le t{+}r{-}l \\ \quad\quad\quad \textbf{else}\ n{:=}\ n{+}1.\ \ l{:=}\ l{+}1.\ \ r{:=}\ r{-}1.\ \ t{:=}\ t{+}1.\ \ l{\le}r \Rightarrow t' \le t{+}r{-}l\ \textbf{fi fi fi} \end{array}$$

Instead of c^2 we could use any natural q (even if q is not a square) in time proportional to $q^{1/2}$. To do so, we need

$$r{:=}\ ceil\ (q^{1/2})\ \ \Leftarrow\ \ r{:=}\ 0.\ \ r{<}q^{1/2}{+}1 \Rightarrow q^{1/2}{\le}r'{<}q^{1/2}{+}1$$

$$\begin{array}{l} r{<}q^{1/2}{+}1 \Rightarrow q^{1/2}{\le}r'{<}q^{1/2}{+}1\ \ \Leftarrow \\ \quad \textbf{if}\ r{\times}r \ge q\ \textbf{then}\ ok\ \textbf{else}\ r{:=}\ r{+}1.\ \ r{<}q^{1/2}{+}1 \Rightarrow q^{1/2}{\le}r'{<}q^{1/2}{+}1\ \textbf{fi} \end{array}$$