163 (cube test) Write a program to determine if a given natural number is a cube without using exponentiation.

After trying the question, scroll down to the solution.

§ The solution will be a linear search (although binary search would be faster). Let n be the given natural number. Let c be a binary variable whose final value will indicate whether n is a cube. Let k be a natural variable.

$$c'=(n\colon nat^3) \quad \Longleftarrow \quad k{:=}\,0.\ \ c'=(k^3 \le n : nat^3)$$

$$\begin{array}{ll} c'=(k^3 \le n : nat^3) \ \Longleftarrow & \textbf{if } k{\times}k{\times}k{=}n \textbf{ then } c{:=}\top \\ & \textbf{else if } k{\times}k{\times}k{>}n \textbf{ then } c{:=}\bot \\ & \quad \textbf{else } k{:=}\,k{+}1.\ \ c'=(k^3 \le n : nat^3) \textbf{ fi fi} \end{array}$$

Proof of the first refinement, starting with the right side:

$k{:=}\,0.\ \ c'=(k^3 \le n : nat^3)$ — substitution law

$=\ \ c'=(0^3 \le n : nat^3)$ — n is natural

$=\ \ c'=(n\colon nat^3)$

Proof of last refinement by cases: first case:

$c'=(k^3 \le n : nat^3) \ \Leftarrow\ k^3{=}n \wedge (c{:=}\top)$ — expand assignment

$=\ \ k^3{=}n \wedge c' \wedge k'{=}k \ \Rightarrow\ c'=(k^3 \le n : nat^3)$ — context

$=\ \ k^3{=}n \wedge c' \wedge k'{=}k \ \Rightarrow\ \top=(k^3 \le k^3 : nat^3)$ — reflexive, and $k\colon nat$

$=\ \ k^3{=}n \wedge c' \wedge k'{=}k \ \Rightarrow\ \top{=}\top$ — reflexive

$=\ \ k^3{=}n \wedge c' \wedge k'{=}k \ \Rightarrow\ \top$ — base

$=\ \ \top$

Last refinement middle case:

$c'=(k^3 \le n : nat^3) \ \Leftarrow\ k^3{>}n \wedge (c{:=}\bot)$ — expand assignment

$=\ \ k^3{>}n \wedge c'{=}\bot \wedge k'{=}k \ \Rightarrow\ c'=(k^3 \le n : nat^3)$ — context

$=\ \ k^3{>}n \wedge c'{=}\bot \wedge k'{=}k \ \Rightarrow\ c'{=}\bot$ — specialization

$=\ \ \top$

Last refinement last case:

$c'=(k^3 \le n : nat^3) \ \Leftarrow\ k^3{<}n \wedge (k{:=}\,k{+}1.\ \ c'=(k^3 \le n : nat^3))$ — substitution

$=\ \ c'=(k^3 \le n : nat^3) \ \Leftarrow\ k^3{<}n \wedge c'=((k{+}1)^3 \le n : nat^3)$ — context

$=\ \ ((k{+}1)^3 \le n : nat^3)=(n : nat^3) \ \Leftarrow\ k^3{<}n \wedge c'=((k{+}1)^3 \le n : nat^3)$

drop part of antecedent

$\Longleftarrow\ \ ((k{+}1)^3 \le n : nat^3)=(n : nat^3) \ \Leftarrow\ k^3{<}n$ — case idempotent law

$=\ \ \textbf{if } n\colon nat \textbf{ then } ((k{+}1)^3 \le n : nat^3)=(n : nat^3) \ \Leftarrow\ k^3{<}n$ — context

$\quad\ \ \textbf{else } ((k{+}1)^3 \le n : nat^3)=(n : nat^3) \ \Leftarrow\ k^3{<}n \textbf{ fi}$ — context

$=\ \ \textbf{if } n\colon nat^3 \textbf{ then } (k{+}1)^3 \le n \ \Leftarrow\ k^3 < n : nat^3$

$\quad\ \ \textbf{else } \bot{=}\bot \ \Leftarrow\ k^3{<}n \textbf{ fi}$ — reflexive, base, one-case

$=\ \ n\colon nat^3 \Rightarrow ((k{+}1)^3 \le n \ \Leftarrow\ k^3 < n)$ — portation

$=\ \ k^3 < n : nat^3 \ \Rightarrow (k{+}1)^3 \le n$

$=\ \ k < n^{1/3} : nat \ \Rightarrow k{+}1 \le n^{1/3}$ — arithmetic

$=\ \ \top$

The execution time is exactly $ceil\ (n^{1/3})$. But $ceil$ is an awkward function, so I will prove

$$t' \le t{+}n^{1/3} \quad \Longleftarrow \quad k{:=}\,0.\ \ k{\le}n^{1/3} \Rightarrow t' \le t{+}n^{1/3}{-}k$$

$$\begin{array}{l} k{\le}n^{1/3} \Rightarrow t' \le t{+}n^{1/3}{-}k \ \ \Longleftarrow \\ \qquad \textbf{if } k{\times}k{\times}k{=}n \textbf{ then } c{:=}\top \\ \qquad \textbf{else if } k{\times}k{\times}k{>}n \textbf{ then } c{:=}\bot \\ \qquad\quad \textbf{else } k{:=}\,k{+}1.\ \ t{:=}\,t{+}1.\ \ k{\le}n^{1/3} \Rightarrow t' \le t{+}n^{1/3}{-}k \textbf{ fi fi} \end{array}$$

Proof of the first refinement, starting with the right side:

$k{:=}\,0.\ \ k{\le}n^{1/3} \Rightarrow t' \le t{+}n^{1/3}{-}k$ — substitution law

$=\ \ 0{\le}n^{1/3} \Rightarrow t' \le t{+}n^{1/3}$ — n is natural, so antecedent is $\top$

$=\ \ \top \Rightarrow t' \le t{+}n^{1/3}$ — identity

$=\ \ t' \le t{+}n^{1/3}$

Proof of last refinement by cases: first case:

$(k \le n^{1/3} \Rightarrow t' \le t+n^{1/3}-k) \;\Leftarrow\; k^3=n \wedge (c{:=}\top)$ — portation

$= \; k^3=n \wedge (c{:=}\top) \wedge k \le n^{1/3} \;\Rightarrow\; t' \le t+n^{1/3}-k$ — expand assignment

$= \; k^3=n \wedge c'=\top \wedge k'=k \wedge t'=t \wedge k \le n^{1/3} \;\Rightarrow\; t' \le t+n^{1/3}-k$ — context

$= \; k^3=n \wedge c'=\top \wedge k'=k \wedge t'=t \wedge k \le n^{1/3} \;\Rightarrow\; t \le t+(k^3)^{1/3}-k$ — simplify consequent

$= \; k^3=n \wedge c'=\top \wedge k'=k \wedge t'=t \wedge k \le n^{1/3} \;\Rightarrow\; 0 \le 0$ — direction

$= \; k^3=n \wedge c'=\top \wedge k'=k \wedge t'=t \wedge k \le n^{1/3} \;\Rightarrow\; \top$ — base

$= \; \top$

Last refinement middle case:

$(k \le n^{1/3} \Rightarrow t' \le t+n^{1/3}-k) \;\Leftarrow\; k^3>n \wedge (c{:=}\bot)$ — portation

$= \; k \le n^{1/3} \wedge k^3>n \wedge (c{:=}\bot) \;\Rightarrow\; t' \le t+n^{1/3}-k$ — cube $k \le n^{1/3}$

$= \; k^3 \le n \wedge k^3>n \wedge (c{:=}\bot) \;\Rightarrow\; t' \le t+n^{1/3}-k$ — exclusivity

$= \; \bot \wedge (c{:=}\bot) \;\Rightarrow\; t' \le t+n^{1/3}-k$ — base

$= \; \bot \;\Rightarrow\; t' \le t+n^{1/3}-k$ — base

$= \; \top$

Last refinement last case:

$(k \le n^{1/3} \;\Rightarrow\; t' \le t+n^{1/3}-k)$ — drop antecedent in this line

$\Leftarrow \; k^3<n \wedge (k{:=}k+1.\; t{:=}t+1.\; k \le n^{1/3} \Rightarrow t' \le t+n^{1/3}-k)$ — and substitution twice

$\Longleftarrow \; t' \le t+n^{1/3}-k$

$\Leftarrow \; k^3<n \wedge (k+1 \le n^{1/3} \Rightarrow t' \le t+1+n^{1/3}-(k+1))$ — simplify this line

$= \; t' \le t+n^{1/3}-k$

$\Leftarrow \; k^3<n \wedge (k+1 \le n^{1/3} \Rightarrow t' \le t+n^{1/3}-k)$ — discharge this line

$= \; t' \le t+n^{1/3}-k$

$\Leftarrow \; k^3<n \;\wedge\; t' \le t+n^{1/3}-k$ — specialize

$= \; \top$