259 (arithmetic) Let us represent a natural number as a string of naturals, each in the range $0,..b$ for some natural base $b>1$, in reverse order. For example, if $b=10$, then $9;2;7$ represents 729. Write programs for each of the following.

(a) Find a string representing a given natural in a given base.

(b) Given a base and two strings representing naturals, find a string representing their sum.

(c) Given a base and two strings representing naturals, find a string representing their difference. You may assume the first string represents a number greater than or equal to the number represented by the second string. What is the result if this is not so?

(d) Given a base and two strings representing naturals, find a string representing their product.

(e) Given a base and two strings representing natural numbers, find strings representing their quotient and remainder.

After trying the question, scroll down to the solution.

(a) Find a string representing a given natural in a given base.

§ I will find the string that has no trailing zeros (but I won't prove that fact). Let the given natural be the initial value of natural variable n. Let S be a string variable, which will be the answer. The problem (except for timing) is P, and we define P and Q as follows.

$P \;=\; (\Sigma i\colon 0,..{\leftrightarrow}S'\cdot\; S'_i \times b^i) = n \;\wedge\; (\forall i\colon 0,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$

$Q \;=\; (\forall i\colon 0,..{\leftrightarrow}S\cdot\; S'_i{=}S_i) \wedge (\Sigma i\colon {\leftrightarrow}S,..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}S}) = n \wedge (\forall i\colon {\leftrightarrow}S,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$

We refine as follows.

$P \;\Leftarrow\;$ S:= *nil*. Q

$Q \;\Leftarrow\;$ **if** $n{=}0$ **then** *ok* **else** S:= S; *mod n b*. n:= *div n b*. Q **fi**

We prove as follows. First refinement, starting with the right side:

S:= *nil*. Q — expand Q then substitute

$=\quad (\forall i\colon 0,..{\leftrightarrow}nil\cdot\; S'_i{=}nil_i)$
$\wedge\; (\Sigma i\colon {\leftrightarrow}nil,..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}nil}) = n$
$\wedge\; (\forall i\colon {\leftrightarrow}nil,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$ — ${\leftrightarrow}nil{=}0$ four times

$=\quad (\forall i\colon 0,..0\cdot\; S'_i{=}nil_i) \;\wedge\; (\Sigma i\colon 0,..{\leftrightarrow}S'\cdot\; S'_i \times b^i) = n \;\wedge\; (\forall i\colon 0,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$
— empty domain in universal quantification

$=\quad P$

Last refinement, first case:

$n{=}0 \;\wedge\; ok \;\Rightarrow\; Q$ — expand Q and *ok*

$=\quad n{=}0 \;\wedge\; n'{=}n \;\wedge\; S'{=}S$
$\Rightarrow (\forall i\colon 0,..{\leftrightarrow}S\cdot\; S'_i{=}S_i) \wedge (\Sigma i\colon {\leftrightarrow}S,..{\leftrightarrow}S'\cdot\; S'_i{\times}b^{i-{\leftrightarrow}S}){=}n \wedge (\forall i\colon {\leftrightarrow}S,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$
— use antecedent as context in consequent

$=\quad n{=}0 \;\wedge\; n'{=}n \;\wedge\; S'{=}S$
$\Rightarrow\; (\forall i\colon 0,..{\leftrightarrow}S\cdot\; S_i{=}S_i) \wedge (\Sigma i\colon {\leftrightarrow}S,..{\leftrightarrow}S\cdot\; S_i{\times}b^{i-{\leftrightarrow}S}){=}0 \wedge (\forall i\colon {\leftrightarrow}S,..{\leftrightarrow}S\cdot\; 0 \le S_i < b)$
— identity, empty domain in sum, empty domain in universal quantification

$=\quad \top$

Last refinement, last case, right side:

$n{>}0 \;\wedge\; (S$:= S; *mod n b*. n:= *div n b*. $Q)$ — expand Q and substitution law twice

$=\quad n{>}0 \;\wedge\; (\forall i\colon 0,..{\leftrightarrow}(S;\, mod\ n\ b)\cdot\; S'_i{=}(S;\, mod\ n\ b)_i)$
$\wedge\; (\Sigma i\colon {\leftrightarrow}(S;\, mod\ n\ b),..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}(S;\, mod\ n\ b)}) = div\ n\ b$
$\wedge\; (\forall i\colon {\leftrightarrow}(S;\, mod\ n\ b),..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$ — simplify

$=\quad n{>}0 \;\wedge\; (\forall i\colon 0,..{\leftrightarrow}S{+}1\cdot\; S'_i{=}(S;\, mod\ n\ b)_i)$
$\wedge\; (\Sigma i\colon {\leftrightarrow}S{+}1,..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}S-1}) = div\ n\ b$
$\wedge\; (\forall i\colon {\leftrightarrow}S{+}1,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$ — split first domain

$=\quad n{>}0 \;\wedge\; (\forall i\colon 0,..{\leftrightarrow}S\cdot\; S'_i = S_i) \;\wedge\; S'_{{\leftrightarrow}S}{=}mod\ n\ b$
$\wedge\; (\Sigma i\colon {\leftrightarrow}S{+}1,..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}S-1}) = div\ n\ b$
$\wedge\; (\forall i\colon {\leftrightarrow}S{+}1,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$

An axiom about *mod* says $0 \le mod\ n\ b < b$ so $0 \le S'_{{\leftrightarrow}S} < b$ and we can extend the domain of the last quantification.

The other axiom about *mod* says $n = div\ n\ b \times b + mod\ n\ b$ and so $n = (\Sigma i\colon {\leftrightarrow}S{+}1,..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}S-1}){\times}b + S'_{{\leftrightarrow}S} = (\Sigma i\colon {\leftrightarrow}S,..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}S})$

$=\quad n{>}0 \;\wedge\; (\forall i\colon 0,..{\leftrightarrow}S\cdot\; S'_i = S_i)$
$\wedge\; (\Sigma i\colon {\leftrightarrow}S,..{\leftrightarrow}S'\cdot\; S'_i \times b^{i-{\leftrightarrow}S}) = n$
$\wedge\; (\forall i\colon {\leftrightarrow}S,..{\leftrightarrow}S'\cdot\; 0{\le}S'_i{<}b)$ — specialize

$\Longrightarrow\quad Q$

Now for the timing. Let T = **if** $n{=}0$ **then** $t'{=}t$ **else** $t' \le t + 1 + log\ n\ /\ log\ b$ **fi** . The refinements are

$T \;\Leftarrow\;$ S:= *nil*. T

$T \;\Leftarrow\;$ **if** $n{=}0$ **then** *ok* **else** S:= S; *mod n b*. n:= *div n b*. t:= t+1. T **fi**

Proof of first refinement: substitution law.

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

$n{=}0 \wedge ok$ expand ok and specialize

$\Longrightarrow$ $n{=}0 \wedge t'{=}t$ generalize

$\Longrightarrow$ $n{=}0 \wedge t'{=}t \vee n{\neq}0 \wedge t' \le t + 1 + log\ n / log\ b$

$=$ T

Last refinement, last case, right side:

$n{>}0 \wedge (S{:=}\ S;\ mod\ n\ b.\ n{:=}\ div\ n\ b.\ t{:=}\ t{+}1.\ T)$ expand T, then substitution law 3 times

$=$ $n{>}0 \wedge$ **if** $div\ n\ b = 0$ **then** $t'{=}t{+}1$ **else** $t' \le t + 2 + log(div\ n\ b) / log\ b$ **fi**

$=$ $n{>}0 \wedge$ **if** $0{\le}n{<}b$ **then** $t'{=}t{+}1$ **else** $t' \le t + 2 + log(div\ n\ b) / log\ b$ **fi** context

$=$ $n{>}0 \wedge$ **if** $1{\le}n{<}b$ **then** $t'{=}t{+}1$ **else** $t' \le t + 2 + log(div\ n\ b) / log\ b$ **fi**

increase $div\ n\ b$ to n/b

$\Longrightarrow$ $n{>}0 \wedge$ **if** $1{\le}n{<}b$ **then** $t'{=}t{+}1$ **else** $t' \le t + 2 + log(n/b) / log\ b$ **fi**

$=$ $n{>}0 \wedge$ **if** $1{\le}n{<}b$ **then** $t'{=}t{+}1$ **else** $t' \le t + 2 + (log\ n - log\ b) / log\ b$ **fi**

$=$ $n{>}0 \wedge$ **if** $1{\le}n{<}b$ **then** $t'{=}t{+}1$ **else** $t' \le t + 1 + log\ n / log\ b$ **fi**

In the **then**-part, we have $1{\le}n$ so $0 \le log\ n$ so we can add it and weaken

$\Longrightarrow$ $n{>}0 \wedge$ **if** $1{\le}n{<}b$ **then** $t' \le t + 1 + log\ n / log\ b$ **else** $t' \le t + 1 + log\ n / log\ b$ **fi**

case-idempotent law

$=$ $n{>}0 \wedge t' \le t + 1 + log\ n / log\ b$ generalize

$\Longrightarrow$ $n{=}0 \wedge t'{=}t \vee n{>}0 \wedge t' \le t + 1 + log\ n / log\ b$

$=$ T

(b) Given a base and two strings representing natural numbers, find a string representing their sum.

§ Let constants A and B be the two given strings. I assume that $\leftrightarrow A{=}\leftrightarrow B$, which can be achieved by padding the shorter string with trailing zeros (leading zeros in the number). Let variable S be a string variable whose final value represents the sum, and let c: 0,1 be a variable (the carry). Let m be a natural variable. The problem is P, and we define P and Q as follows.

$P \ = \ (\forall i{:}\ 0,..{\leftrightarrow}S'{\cdot}\ 0{\le}S'_i{<}b)$

$\wedge\ (\Sigma i{:}\ 0,..{\leftrightarrow}A{\cdot}\ A_i \times b^i) + (\Sigma i{:}\ 0,..{\leftrightarrow}B{\cdot}\ B_i \times b^i) \ = \ (\Sigma i{:}\ 0,..{\leftrightarrow}S'{\cdot}\ S'_i \times b^i)$

$Q \ = \ (\forall i{:}\ 0,..{\leftrightarrow}S{\cdot}\ S'_i = S_i) \ \wedge \ (\forall i{:}\ {\leftrightarrow}S,..{\leftrightarrow}S'{\cdot}\ 0{\le}S'_i{<}b)$

$\wedge\ (\Sigma i{:}\ {\leftrightarrow}S,..{\leftrightarrow}A{\cdot}\ A_i{\times}b^i) + (\Sigma i{:}\ {\leftrightarrow}S,..{\leftrightarrow}B{\cdot}\ B_i{\times}b^i) + c{\times}b^{{\leftrightarrow}S} \ = \ (\Sigma i{:}\ {\leftrightarrow}S,..{\leftrightarrow}S'{\cdot}\ S'_i{\times}b^i)$

We refine as follows.

$P \ \Longleftarrow \ S{:=}\ nil.\ c{:=}\ 0.\ Q$

$Q \ \Longleftarrow$ **if** $\leftrightarrow S{=}\leftrightarrow A$ **then** $S{:=}\ S;\ c$

else $m{:=}\ mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b.\ c{:=}\ div\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b.$

$S{:=}\ S;\ m.\ Q$ **fi**

We prove as follows. First refinement, starting with the right side:

$S{:=}\ nil.\ c{:=}\ 0.\ Q$ expand Q and substitution law twice

$=$ $(\forall i{:}\ 0,..0{\cdot}\ S'_i{=}nil_i) \ \wedge \ (\forall i{:}\ 0,..{\leftrightarrow}S'{\cdot}\ 0{\le}S'_i{<}b)$

$\wedge\ (\Sigma i{:}\ 0,..{\leftrightarrow}A{\cdot}\ A_i \times b^i) + (\Sigma i{:}\ 0,..{\leftrightarrow}B{\cdot}\ B_i \times b^i) + 0{\times}b^0 \ = \ (\Sigma i{:}\ 0,..{\leftrightarrow}S'{\cdot}\ S'_i \times b^i)$

empty domain in universal quant; base law of mult and identity of addition

$=$ P

Last refinement, first case:

$\leftrightarrow S{=}\leftrightarrow A \ \wedge \ (S{:=}\ S;\ c) \ \Rightarrow \ Q$ expand assignment and Q

$=$ $\leftrightarrow S{=}\leftrightarrow A \ \wedge \ S'{=}S;c \ \wedge \ c'{=}c$

$\Rightarrow$ $(\forall i{:}\ 0,..{\leftrightarrow}S{\cdot}\ S'_i = S_i) \ \wedge \ (\forall i{:}\ {\leftrightarrow}S,..{\leftrightarrow}S'{\cdot}\ 0{\le}S'_i{<}b)$

$\wedge\ (\Sigma i{:}\ {\leftrightarrow}S,..{\leftrightarrow}A{\cdot}\ A_i{\times}b^i) + (\Sigma i{:}\ {\leftrightarrow}S,..{\leftrightarrow}B{\cdot}\ B_i{\times}b^i) + c{\times}b^{{\leftrightarrow}S} = (\Sigma i{:}\ {\leftrightarrow}S,..{\leftrightarrow}S'{\cdot}\ S'_i{\times}b^i)$

use antecedent plus $\leftrightarrow A{=}\leftrightarrow B$ as context in consequent

$=$ $\leftrightarrow S{=}\leftrightarrow A \ \wedge \ S'{=}S;c \ \wedge \ c'{=}c$

$\Rightarrow$ $(\forall i{:}\ 0,..{\leftrightarrow}S{\cdot}\ (S;c)_i = S_i) \ \wedge \ (\forall i{:}\ {\leftrightarrow}S,..{\leftrightarrow}S{+}1{\cdot}\ 0{\le}(S;c)_i{<}b)$

$\wedge\ (\Sigma i{:}\ {\leftrightarrow}A,..{\leftrightarrow}A{\cdot}\ A_i \times b^i) + (\Sigma i{:}\ {\leftrightarrow}B,..{\leftrightarrow}B{\cdot}\ B_i \times b^i) + c{\times}b^{{\leftrightarrow}S}$

$= \quad (\Sigma i{:}\ \leftrightarrow S,..\leftrightarrow S{+}1 \cdot (S;c)_i \times b^i)$

string and quantifier axioms

$= \quad \leftrightarrow S{=}\leftrightarrow A \ \wedge\ S'{=}S;c \ \wedge\ c'{=}c \ \Rightarrow\ \top \ \wedge\ 0{\le}c{<}b \ \wedge\ 0{+}0{+}c{\times}b^{\leftrightarrow S}{=}c{\times}b^{\leftrightarrow S}$

given information, identity, base

$= \quad \top$

Last refinement, last case, starting with right side:

$\leftrightarrow S{\neq}\leftrightarrow A \ \wedge\ (m{:=}\ mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b.\ \ c{:=}\ div\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b.$
$\qquad S{:=}\ S;\ m.\ \ Q)$

expand Q, then use substitution law 3 times, simplifying $\leftrightarrow(S;m)$ to $\leftrightarrow S{+}1$

$= \quad \leftrightarrow S{\neq}\leftrightarrow A \ \wedge\ (\forall i{:}\ 0,..\leftrightarrow S{+}1 \cdot\ S'_i{=}(S;\ mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b)_i)$
$\wedge\ (\forall i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ 0{\le}S'_i{<}b)$
$\wedge \qquad (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow A \cdot\ A_i \times b^i) + (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow B \cdot\ B_i \times b^i)$
$\quad + (div\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b){\times}b^{\leftrightarrow S+1}$
$\quad = (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ S'_i \times b^i)$

split domain of first quantifier

$= \quad \leftrightarrow S{\neq}\leftrightarrow A \ \wedge\ (\forall i{:}\ 0,..\leftrightarrow S \cdot\ S'_i = S_i) \ \wedge\ S'_{\leftrightarrow S} = mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b$
$\wedge\ (\forall i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ 0{\le}S'_i{<}b)$
$\wedge \qquad (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow A \cdot\ A_i \times b^i) + (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow B \cdot\ B_i \times b^i)$
$\quad + (div\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b){\times}b^{\leftrightarrow S+1}$
$\quad = (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ S'_i \times b^i)$

using $S'_{\leftrightarrow S} = mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b$ as context,
and a property of mod, increase domain of second quantifier

$= \quad \leftrightarrow S{\neq}\leftrightarrow A \ \wedge\ (\forall i{:}\ 0,..\leftrightarrow S \cdot\ S'_i{=}S_i) \ \wedge\ S'_{\leftrightarrow S} = mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b$
$\wedge\ (\forall i{:}\ \leftrightarrow S,..\leftrightarrow S' \cdot\ 0{\le}S'_i{<}b)$
$\wedge \qquad (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow A \cdot\ A_i \times b^i) + (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow B \cdot\ B_i \times b^i)$
$\quad + (div\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b){\times}b^{\leftrightarrow S+1}$
$\quad = (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ S'_i \times b^i)$ Use $(div\ a\ b){\times}b = a - mod\ a\ b$.

$= \quad \leftrightarrow S{\neq}\leftrightarrow A \ \wedge\ (\forall i{:}\ 0,..\leftrightarrow S \cdot\ S'_i{=}S_i) \ \wedge\ S'_{\leftrightarrow S} = mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b$
$\wedge\ (\forall i{:}\ \leftrightarrow S,..\leftrightarrow S' \cdot\ 0{\le}S'_i{<}b)$
$\wedge \qquad (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow A \cdot\ A_i \times b^i) + (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow B \cdot\ B_i \times b^i)$
$\quad + (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c - mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b){\times}b^{\leftrightarrow S}$
$\quad = (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ S'_i \times b^i)$ use context $S'_{\leftrightarrow S} = mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b$

$= \quad \leftrightarrow S{\neq}\leftrightarrow A \ \wedge\ (\forall i{:}\ 0,..\leftrightarrow S \cdot\ S'_i{=}S_i) \ \wedge\ S'_{\leftrightarrow S} = mod\ (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c)\ b$
$\wedge\ (\forall i{:}\ \leftrightarrow S,..\leftrightarrow S' \cdot\ 0{\le}S'_i{<}b)$
$\wedge \qquad (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow A \cdot\ A_i \times b^i) + (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow B \cdot\ B_i \times b^i)$
$\quad + (A_{\leftrightarrow S} + B_{\leftrightarrow S} + c - S'_{\leftrightarrow S}){\times}b^{\leftrightarrow S}$
$\quad = (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ S'_i \times b^i)$ drop 2 conjuncts, and distribute $\times b^{\leftrightarrow S}$

$\Rightarrow \quad (\forall i{:}\ 0,..\leftrightarrow S \cdot\ S'_i = S_i) \ \wedge\ (\forall i{:}\ \leftrightarrow S,..\leftrightarrow S' \cdot\ 0{\le}S'_i{<}b)$
$\wedge \qquad (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow A \cdot\ A_i \times b^i) + (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow B \cdot\ B_i \times b^i)$
$\quad + A_{\leftrightarrow S}{\times}b^{\leftrightarrow S} + B_{\leftrightarrow S}{\times}b^{\leftrightarrow S} + c{\times}b^{\leftrightarrow S} - S'_{\leftrightarrow S}{\times}b^{\leftrightarrow S}$
$\quad = (\Sigma i{:}\ \leftrightarrow S{+}1,..\leftrightarrow S' \cdot\ S'_i \times b^i)$ use 3 of the terms to increase domains

$= \quad (\forall i{:}\ 0,..\leftrightarrow S \cdot\ S'_i = S_i) \ \wedge\ (\forall i{:}\ \leftrightarrow S,..\leftrightarrow S' \cdot\ 0{\le}S'_i{<}b)$
$\wedge\ (\Sigma i{:}\ \leftrightarrow S,..\leftrightarrow A \cdot\ A_i{\times}b^i) + (\Sigma i{:}\ \leftrightarrow S,..\leftrightarrow B \cdot\ B_i{\times}b^i) + c{\times}b^{\leftrightarrow S} \ =\ (\Sigma i{:}\ \leftrightarrow S,..\leftrightarrow S' \cdot\ S'_i{\times}b^i)$

$= \quad Q$

(c) Given a base and two strings representing natural numbers, find a string representing their difference. You may assume the first string represents a number greater than or equal to the number represented by the second string. What is the result if this is not so?

no solution given

(d) Given a base and two strings representing natural numbers, find a string representing their product.

no solution given

(e) Given a base and two strings representing natural numbers, find strings representing their quotient and remainder.

no solution given