259 (arithmetic) Let us represent a natural number as a list 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 the list representing a given natural in a given base.

(b) Given a base and two lists representing naturals, find the list representing their sum.

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

(d) Given a base and two lists representing naturals, find the list representing their product.

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

After trying the question, scroll down to the solution.

(a) Find the list representing a given natural in a given base.

§ The question says "the" list, but actually there are many; I will find the list 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 L be a list variable, which will be the answer. The problem (except for timing) is P, and we define P and Q as follows.

$P \;=\; (\Sigma i\colon 0,..\#L'\cdot L'i \times b^i) = n \;\wedge\; (\forall i\colon 0,..\#L'\cdot 0 \le L'i < b)$

$Q \;=\; (\forall i\colon 0,..\#L\cdot L'i = Li) \;\wedge\; (\Sigma i\colon \#L,..\#L'\cdot L'i \times b^{i-\#L}) = n \;\wedge\; (\forall i\colon \#L,..\#L'\cdot 0 \le L'i < b)$

We refine as follows.

$P \;\Leftarrow\; L := [nil].\; Q$

$Q \;\Leftarrow\;$ **if** $n=0$ **then** ok **else** $L := L ;; [mod\ n\ b].\; n := div\ n\ b.\; Q$ **fi**

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

$L := [nil].\; Q$ — expand Q then substitute

$=\;\; (\forall i\colon 0,..\#[nil]\cdot L'i = [nil]i)$
$\wedge\; (\Sigma i\colon \#[nil],..\#L'\cdot L'i \times b^{i-\#[nil]}) = n$
$\wedge\; (\forall i\colon \#[nil],..\#L'\cdot 0 \le L'i < b)$ — $\#[nil]=0$ four times

$=\;\; (\forall i\colon 0,..0\cdot L'i = [nil]i) \;\wedge\; (\Sigma i\colon 0,..\#L'\cdot L'i \times b^i) = n \;\wedge\; (\forall i\colon 0,..\#L'\cdot 0 \le L'i < b)$
empty domain in universal quantification

$=\;\; P$

Last refinement, first case:

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

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

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

$=\;\; \top$

Last refinement, last case, right side:

$n>0 \;\wedge\; (L := L ;; [mod\ n\ b].\; n := div\ n\ b.\; Q)$ expand Q and substitution law twice

$=\;\; n>0 \;\wedge\; (\forall i\colon 0,..\#(L ;; [mod\ n\ b])\cdot L'i = (L ;; [mod\ n\ b])i)$
$\wedge\; (\Sigma i\colon \#(L ;; [mod\ n\ b]),..\#L'\cdot L'i \times b^{i-\#(L + [mod\ n\ b])}) = div\ n\ b$
$\wedge\; (\forall i\colon \#(L ;; [mod\ n\ b]),..\#L'\cdot 0 \le L'i < b)$ — simplify

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

$=\;\; n>0 \;\wedge\; (\forall i\colon 0,..\#L\cdot L'i = L\ i) \;\wedge\; L'(\#L) = mod\ n\ b$
$\wedge\; (\Sigma i\colon \#L+1,..\#L'\cdot L'i \times b^{i-\#L-1}) = div\ n\ b$
$\wedge\; (\forall i\colon \#L+1,..\#L'\cdot 0 \le L'i < b)$

An axiom about mod says $0 \le mod\ n\ b < b$ so $0 \le L'(\#L) < b$ 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
$n \;=\; (\Sigma i\colon \#L+1,..\#L'\cdot L'i \times b^{i-\#L-1}) \times b \;+\; L'(\#L) \;=\; (\Sigma i\colon \#L,..\#L'\cdot L'i \times b^{i-\#L})$

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

$\Rightarrow\;\; Q$

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

$T \;\Leftarrow\; L := [nil].\; T$

$T \;\Leftarrow\;$ **if** $n=0$ **then** ok **else** $L := L ;; [mod\ n\ b].\; n := div\ n\ b.\; t := t+1.\; T$ **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

$\Rightarrow$ $n=0 \wedge t'=t$ generalize

$\Rightarrow$ $n=0 \wedge t'=t \vee n\ne 0 \wedge t' \le t + 1 + log\ n / log\ b$

$=$ T

Last refinement, last case, right side:

$n>0 \wedge (L:= L ;; [mod\ n\ b].\ n:= div\ n\ b.\ t:= t+1.\ T)$ 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

$\Rightarrow$ $n>0 \wedge$ **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

$\Rightarrow$ $n>0 \wedge$ **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

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

$=$ T

(b) Given a base and two lists representing natural numbers, find the list representing their sum.

§ The question says "the" list, but actually there are many; I will find one of them. Let constants A and B be the two given lists. I assume that $\#A=\#B$, which can be achieved by padding the shorter list with trailing zeros (leading zeros in the number). Let variable S be a list 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.

$P =$ $(\forall i: 0,..\#S'\cdot 0\le S'i<b)$
$\wedge (\Sigma i: 0,..\#A\cdot A\ i \times b^i) + (\Sigma i: 0,..\#B\cdot B\ i \times b^i) = (\Sigma i: 0,..\#S'\cdot S'i \times b^i)$

$Q =$ $(\forall i: 0,..\#S\cdot S'i = S\ i) \wedge (\forall i: \#S,..\#S'\cdot 0\le S'i<b)$
$\wedge (\Sigma i: \#S,..\#A\cdot A\ i \times b^i) + (\Sigma i: \#S,..\#B\cdot B\ i \times b^i) + c\times b^{\#S} = (\Sigma i: \#S,..\#S'\cdot S'i \times b^i)$

We refine as follows.

$P \Leftarrow S:= [nil].\ c:= 0.\ Q$

$Q \Leftarrow$ **if** $\#S=\#A$ **then** $S:= S ;; [c]$
else $m:= mod\ (A(\#S) + B(\#S) + c)\ b.\ c:= div\ (A(\#S) + B(\#S) + c)\ b.$
$S:= S ;; [m].\ Q$ **fi**

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

$S:= [nil].\ c:= 0.\ Q$ expand Q and substitution law twice

$=$ $(\forall i: 0,..0\cdot S'i=[nil]i) \wedge (\forall i: 0,..\#S'\cdot 0\le S'i<b)$
$\wedge (\Sigma i: 0,..\#A\cdot A\ i \times b^i) + (\Sigma i: 0,..\#B\cdot B\ i \times b^i) + 0\times b^0 = (\Sigma i: 0,..\#S'\cdot S'i \times b^i)$

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

$=$ P

Last refinement, first case:

$\#S=\#A \wedge (S:= S ;; [c]) \Rightarrow Q$ expand assignment and Q

$=$ $\#S=\#A \wedge S'=S;;[c] \wedge c'=c$
$\Rightarrow$ $(\forall i: 0,..\#S\cdot S'i = S\ i) \wedge (\forall i: \#S,..\#S'\cdot 0\le S'i<b)$
$\wedge (\Sigma i: \#S,..\#A\cdot A\ i \times b^i) + (\Sigma i: \#S,..\#B\cdot B\ i \times b^i) + c\times b^{\#S} = (\Sigma i: \#S,..\#S'\cdot S'i \times b^i)$

use antecedent plus $\#A=\#B$ as context in consequent

$=$ $\#S=\#A \wedge S'=S;;[c] \wedge c'=c$
$\Rightarrow$ $(\forall i: 0,..\#S\cdot (S;;[c])i = S\ i) \wedge (\forall i: \#S,..\#S+1\cdot 0\le(S;;[c])i<b)$

$\land\quad (\Sigma i\colon \#A,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#B,..\#B\cdot\ B\ i \times b^i) + c{\times}b^{\#S}$
$\quad = (\Sigma i\colon \#S,..\#S{+}1\cdot (S;;[c])i \times b^i)$

list and quantifier axioms

$=\quad \#S{=}\#A\ \land\ S'{=}S;;[c]\ \land\ c'{=}c\ \Rightarrow\ \top\ \land\ 0{\le}c{<}b\ \land\ 0{+}0{+}c{\times}b^{\#S}{=}c{\times}b^{\#S}$

given information, identity, base

$=\quad \top$

Last refinement, last case, starting with right side:

$\#S{\ne}\#A\ \land\ (\ m{:=}\ mod\ (A(\#S) + B(\#S) + c)\ b.\ \ c{:=}\ div\ (A(\#S) + B(\#S) + c)\ b.$
$\quad S{:=}\ S\ ;;\ [m].\ \ Q)$

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

$=\quad \#S{\ne}\#A\ \land\ (\forall i\colon 0,..\#S{+}1\cdot\ S'i{=}(S\ ;;\ [mod\ (A(\#S) + B(\#S) + c)\ b])i)$
$\land\ (\forall i\colon \#S{+}1,..\#S'\cdot\ 0{\le}S'i{<}b)$
$\land\quad (\Sigma i\colon \#S{+}1,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#S{+}1,..\#B\cdot\ B\ i \times b^i)$
$\quad + (div\ (A(\#S) + B(\#S) + c)\ b){\times}b^{\#S+1}$
$\quad = (\Sigma i\colon \#S{+}1,..\#S'\cdot\ S'i \times b^i)$

split domain of first quantifier

$=\quad \#S{\ne}\#A\ \land\ (\forall i\colon 0,..\#S\cdot\ S'i = S\ i)\ \land\ S'(\#S) = mod\ (A(\#S) + B(\#S) + c)\ b$
$\land\ (\forall i\colon \#S{+}1,..\#S'\cdot\ 0{\le}S'i{<}b)$
$\land\quad (\Sigma i\colon \#S{+}1,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#S{+}1,..\#B\cdot\ B\ i \times b^i)$
$\quad + (div\ (A(\#S) + B(\#S) + c)\ b){\times}b^{\#S+1}$
$\quad = (\Sigma i\colon \#S{+}1,..\#S'\cdot\ S'i \times b^i)$

using $S'(\#S) = mod\ (A(\#S) + B(\#S) + c)\ b$ as context,
and a property of mod, increase domain of second quantifier

$=\quad \#S{\ne}\#A\ \land\ (\forall i\colon 0,..\#S\cdot\ S'i{=}S\ i)\ \land\ S'(\#S) = mod\ (A(\#S) + B(\#S) + c)\ b$
$\land\ (\forall i\colon \#S,..\#S'\cdot\ 0{\le}S'i{<}b)$
$\land\quad (\Sigma i\colon \#S{+}1,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#S{+}1,..\#B\cdot\ B\ i \times b^i)$
$\quad + (div\ (A(\#S) + B(\#S) + c)\ b){\times}b^{\#S+1}$
$\quad = (\Sigma i\colon \#S{+}1,..\#S'\cdot\ S'i \times b^i)$ Use $(div\ a\ b){\times}b = a - mod\ a\ b$.

$=\quad \#S{\ne}\#A\ \land\ (\forall i\colon 0,..\#S\cdot\ S'i{=}Si)\ \land\ S'(\#S) = mod\ (A(\#S) + B(\#S) + c)\ b$
$\land\ (\forall i\colon \#S,..\#S'\cdot\ 0{\le}S'i{<}b)$
$\land\quad (\Sigma i\colon \#S{+}1,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#S{+}1,..\#B\cdot\ B\ i \times b^i)$
$\quad + (A(\#S) + B(\#S) + c - mod\ (A(\#S) + B(\#S) + c)\ b){\times}b^{\#S}$
$\quad = (\Sigma i\colon \#S{+}1,..\#S'\cdot\ S'i \times b^i)$ use context $S'(\#S) = mod\ (A(\#S) + B(\#S) + c)\ b$

$=\quad \#S{\ne}\#A\ \land\ (\forall i\colon 0,..\#S\cdot\ S'i{=}Si)\ \land\ S'(\#S) = mod\ (A(\#S) + B(\#S) + c)\ b$
$\land\ (\forall i\colon \#S,..\#S'\cdot\ 0{\le}S'i{<}b)$
$\land\quad (\Sigma i\colon \#S{+}1,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#S{+}1,..\#B\cdot\ B\ i \times b^i)$
$\quad + (A(\#S) + B(\#S) + c - S'(\#S)){\times}b^{\#S}$
$\quad = (\Sigma i\colon \#S{+}1,..\#S'\cdot\ S'i \times b^i)$ drop 2 conjuncts, and distribute ${\times}b^{\#S}$

$\Rightarrow\quad (\forall i\colon 0,..\#S\cdot\ S'i = S\ i)\ \land\ (\forall i\colon \#S,..\#S'\cdot\ 0{\le}S'i{<}b)$
$\land\quad (\Sigma i\colon \#S{+}1,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#S{+}1,..\#B\cdot\ B\ i \times b^i)$
$\quad + A(\#S){\times}b^{\#S} + B(\#S){\times}b^{\#S} + c{\times}b^{\#S} - S'(\#S){\times}b^{\#S}$
$\quad = (\Sigma i\colon \#S{+}1,..\#S'\cdot\ S'i \times b^i)$ use 3 of the terms to increase domains

$=\quad (\forall i\colon 0,..\#S\cdot\ S'i = S\ i)\ \land\ (\forall i\colon \#S,..\#S'\cdot\ 0{\le}S'i{<}b)$
$\land\ (\Sigma i\colon \#S,..\#A\cdot\ A\ i \times b^i) + (\Sigma i\colon \#S,..\#B\cdot\ B\ i \times b^i) + c{\times}b^{\#S} = (\Sigma i\colon \#S,..\#S'\cdot\ S'i \times b^i)$

$=\quad Q$

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

no solution given

(d) Given a base and two lists representing natural numbers, find the list representing their product.

no solution given

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

no solution given