Alternative Carries for Base-b Addition

Jacob Beckel

Winona State University

April 27, 2016

Introduction

- Number Bases and Modular Arithmetic
- Carries with 2 digits
- Carries with n digits
- Carries with ∞ digits

Number Bases

- What is a number base?
- In base-10,

$$345 = 3 \cdot 100 + 4 \cdot 10 + 5 = 3 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0.$$

- Consider the base-7 representation $n = 345_7$. Then,

$$n = 3 \cdot 7^2 + 4 \cdot 7^1 + 5 \cdot 7^0 = 180.$$

Number Bases cont.

Definition

Division Algorithm: Given $m, n \in \mathbb{Z}$ *and* $n > 0$, *there exists unique* $q, r \in \mathbb{Z}$ *such that* $m = q \cdot n + r$ *where* $0 \leq r < n$.

Example: To convert the base-10 number 438 to base-7, we use the division algorithm to make groups of 7 and keep track of the left-overs.

$$438 = 62 \cdot 7 + 4$$

$$62 = 8 \cdot 7 + 6$$

$$8 = 1 \cdot 7 + 1$$

$$1 = 0 \cdot 7 + 1$$

Using the remainders from bottom to top, we can write 438 as 1164_7.

Number Bases cont.

Compute $125_7 + 624_7$.

Write the numbers as you would when adding in base-10, except carry groups of 7.

- $$\begin{array}{r} 1\,2\,5_7 \\ +\;\; 6\,2\,4_7 \\ \hline \end{array}$$

- $$\begin{array}{r} {\scriptstyle 1}\;\;\; \\ 1\,2\,5_7 \\ +\,6\,2\,4_7 \\ \hline 2_7 \end{array}$$

Number Bases cont.

- $$\begin{array}{r} {}^{1} \\ 125_7 \\ +\ 624_7 \\ \hline 52_7 \end{array}$$

- $$\begin{array}{r} {}^{1}\ \ {}^{1} \\ 125_7 \\ +\ \ 624_7 \\ \hline 1052_7 \end{array}$$

Modular Arithmetic

Definition

$a \mod b$: *For* $a, b \in \mathbb{Z}$ *where* $b > 0$, *we will let* $a \mod b$ *denote the remainder of* a *when divided by* b. *Also,* $\mathbb{Z}_b = \{0, 1, ..., b-1\}$.

- For example, $45891 \mod 10$ is 1 since $45891 = 4589 \cdot 10 + 1$.

Modular Arithmetic cont.

- To model the last k digits of a number, simply work $(\mod 10^k)$.
  Example: $45891 \mod 10^3$ is 891 since $45891 = 45 \cdot 10^3 + 891$.
- $\mathbb{Z}_b$ models the ones digit in addition of base-b integers.
  Example: Compute $32456_7 \mod 7^2$.

$$32456_7 = 3 \cdot 7^4 + 2 \cdot 7^3 + 4 \cdot 7^2 + 5 \cdot 7^1 + 6$$

$$= (3 \cdot 7^2 + 2 \cdot 7^1 + 4) \cdot 7^2 + 5 \cdot 7^1 + 6$$

So, $32456_7 \mod 7^2 = 5 \cdot 7^1 + 6 = 56_7$.

Alternate Carries: 2-digit

Daniel Isaksen's model for 2-Digit Addition

Definition

Let $\mathbb{Z}_b^2 = \{[d_1][d_0] : d_i \in \mathbb{Z}_b\}$ *be the set of 2-digit base-b representations with* d_1 *representing the b digit and* d_0 *representing the ones digit.*

Definition

For $[c_1][c_0], [d_1][d_0] \in \mathbb{Z}_b^2$*, let*

$$[c_1][c_0] + [d_1][d_0] = [c_1 + d_1 + z_b(c_0 + d_0)][c_0 + d_0],$$

where

$$z_b(c_0 + d_0) = \left\lfloor \frac{c_0 + d_0}{b} \right\rfloor$$

is the carry that counts how many groups of size b are in $c_0 + d_0$*.*

Alternate Carries: 2-digit cont.

Compute $26_7 + 33_7$ using this model.

$$[2][6]_7 + [3][3]_7 = [2 + 3 + z_7(6 + 3)][6 + 3]$$

$$z_7(6 + 3) = \left\lfloor \frac{6 + 3}{7} \right\rfloor = 1$$

$$[2][6]_7 + [3][3]_7 = [2 + 3 + 1][2]_7 = [6][2]_7$$

So, $26_7 + 33_7 = 62_7$.

Alternate Carries: 2-digit cont.

Definition

For $[c_1][c_0], [d_1][d_0] \in \mathbb{Z}_b^2$, *let*
$[c_1][c_0] +_k [d_1][d_0] = [c_1 + d_1 + kz_b(c_0 + d_0)][c_0 + d_0]$.

Consider $26_7 + 33_7$, this time with carries $k = 5$. Then,

$$[2][6]_7 +_5 [3][3]_7 = [2 + 3 + 5 \cdot 1][6 + 3]_7 = [3][2]_7.$$

Alternate Carries: 2-digit cont.

- $$\begin{array}{r} 1 \\ 2\,6_7 \\ +_1\; 3\,3_7 \\ \hline 6\,2_7 \end{array}$$

- $$\begin{array}{r} 5 \\ 2\,6_7 \\ +_5\; 3\,3_7 \\ \hline 3\,2_7 \end{array}$$

Alternate Carries: 2-digit cont.

Theorem (Isaksen)

$\mathbb{Z}_b^2$ with $+_k$ is a group, denoted as $(\mathbb{Z}_b^2, k)$.

- Example:

$$\begin{array}{rr} & \overset{5}{} \\ & 2\,3_7 \\ +_5 & 0\,4_7 \\ \hline & 0\,0_7 \end{array}$$

- Example: In particular, $(\mathbb{Z}_b^2, 0) \cong \mathbb{Z}_b \times \mathbb{Z}_b$ and $(\mathbb{Z}_b^2, 1) \cong \mathbb{Z}_{b^2}$.

Alternate Carries: 2-digit cont.

Theorem

For $k < b$, if $gcd(b, k) = 1$, then $(\mathbb{Z}_b^2, k) \cong (\mathbb{Z}_b^2, 1)$.

Alternate Carries: 2-digit cont.

The Isomorphism that maps $(\mathbb{Z}_b^2, 1) \rightarrow (\mathbb{Z}_b^2, k)$ is defined as

$$\phi([d_1][d_0]) \rightarrow [kd_1][d_0].$$

$$\begin{array}{r} {}^{1} \\ 6\,6_7 \\ +_1\;2\,3_7 \\ \hline 2\,2_7 \end{array} \qquad\qquad \begin{array}{r} {}^{5} \\ 2\,6_7 \\ +_5\;3\,3_7 \\ \hline 3\,2_7 \end{array}$$

Then, $32_7 = [3][2] \rightarrow [3 \cdot 3][2] = [2][2] = 22_7$.

Alternate Carries: n-digit

Definition

Let $\mathbb{Z}_b^n = \{[d_n][d_{n-1}]...[d_1][d_0] : d_i \in \mathbb{Z}_b\}$. *Define* $+_k$ *on* $\mathbb{Z}_b^n$ *by*

$$[c_n][c_{n-1}]...[c_1][c_0] +_k [d_n][d_{n-1}]...[d_1][d_0] = [e_n][e_{n-1}]...[e_1][e_0]$$

where

$$f_i = c_i + d_i + kz(f_{i-1}),$$

$f_{-1} = 0$, *and* $e_i = f_i \mod b$.

Alternate Carries: n-digit cont.

Compute $3161_7 +_5 1146_7$ with carries of 5.

- $$\begin{array}{rr} & 3\,1\,6\,1_7 \\ +_5 & 1\,1\,4\,6_7 \\ \hline \end{array}$$

- $$\begin{array}{rr} & {}^{5} \\ & 3\,1\,6\,1_7 \\ +_5 & 1\,1\,4\,6_7 \\ \hline & 0_7 \end{array}$$

Alternate Carries: n-digit cont.

- $$\begin{array}{r} {\scriptstyle 10\ 5} \\ 3\,1\,6\,1_7 \\ +_5\ 1\,1\,4\,6_7 \\ \hline 1\,0_7 \end{array}$$

- $$\begin{array}{r} {\scriptstyle 5\ \ 10\ 5} \\ 3\,1\,6\,1_7 \\ +_5\ 1\,1\,4\,6_7 \\ \hline 2\ 5\,1\,0_7 \end{array}$$

Alternate Carries: n-digit cont.

Theorem

For $k < b$, if $gcd(b,k) = 1$, then $(\mathbb{Z}_b^n, k) \cong (\mathbb{Z}_b^n, 1) \cong \mathbb{Z}_{b^n}$ when b is the base and k is the carry.

The Isomorphism that maps $(\mathbb{Z}_b^n, 1) \to (\mathbb{Z}_b^n, k)$ is defined as

$$\phi([d_2][d_1][d_0]) \to [k^2 d_2 + k \left\lfloor \frac{kd_1}{b} \right\rfloor][kd_1][d_0].$$

Alternate Carries: n-digit cont.

For $b = 7$ and $k = 5$,

$$234_7 \in (\mathbb{Z}_7^3, 1)$$
$$= [2][3][4] \to [5^2 \cdot 2 + 5 \left\lfloor \frac{5 \cdot 3}{7} \right\rfloor][5 \cdot 3][4] = [1][1][4]$$
$$= 114_7 \in (\mathbb{Z}_7^3, 5).$$

Alternate Carries: ∞-digit

Definition

Let $\mathbb{Z}_b^\infty = \{...[d_n][d_{n-1}]...[d_1][d_0] : d_i \in \mathbb{Z}_b\}$.

Theorem

For $k < b$, *if* $gcd(b,k) = 1$, *then* $(\mathbb{Z}_b^\infty, k) \cong (\mathbb{Z}_b^\infty, 1) \cong \mathbb{N}[\frac{b}{k}]$ *where* b *is the base and* k *is the carry.*

Let the Isomorphism ϕ map

$$\phi([d_n][d_{n-1}]...[d_1][d_0]_{\frac{b}{k}}) \to d_n(\frac{b}{k})^n + d_{n-1}(\frac{b}{k})^{n-1} + ... + d_1(\frac{b}{k})^1 + d_0(\frac{b}{k})^0.$$

Alternate Carries: ∞-digit cont.

Example: Compute $46_7 + 32_7$ with carries of 5.

$$\begin{array}{r} 4\,6_7 \\ +_5 \quad 2\,2_7 \\ \hline \end{array}$$

$$\begin{array}{r} {\scriptstyle 5\ 5\ \ } \\ 4\,6_7 \\ +_5 \quad 2\,2_7 \\ \hline 5\,4\,1_7 \end{array}$$

Alternate Carries: ∞-digit cont.

$$[4(\frac{7}{5}) + 6] + [2(\frac{7}{5}) + 2]$$

$$6(\frac{7}{5}) + 8$$

$$6(\frac{7}{5}) + 7 + 1$$

$$6(\frac{7}{5}) + 5(\frac{7}{5}) + 1$$

$$11(\frac{7}{5}) + 1$$

Alternate Carries: ∞-digit cont.

$$(7+4)(\frac{7}{5})+1$$

$$(5(\frac{7}{5})+4)(\frac{7}{5})+1$$

$$5(\frac{7}{5})(\frac{7}{5})+4(\frac{7}{5})+1$$

$$5(\frac{7}{5})^2+4(\frac{7}{5})+1$$

$$\Rightarrow 541_7.$$

Some Notes on ∞-digit Carries

- $(\mathbb{Z}_b^\infty, k)$ with only finite elements can no longer be called a group.
- $(\mathbb{Z}_b^\infty, k)$ with possibly infinite digits to the left is a group. p-adic conversion?