HISTORY OF MATHEMATICS
MATHEMATICAL TOPIC I
BASES

PAUL L. BAILEY

1. Introduction

Consider the difference between the words *number* and *numeral*, as they are used by mathematicians.

Webster's New World dictionary defines number as *a symbol or word, or a group of either of these, showing how many or which one in a series.* This is clearly not what we mean when we refer to rational or real numbers. Yet, the alternate definitions are even further from our usage. Perhaps closer would be *an idea corresponding to a quantity.* Let's take that for now (although it certainly seems to exclude complex numbers).

Webster's does a better job with the second word, defining numeral as *a figure, letter, or word, or a group of any of these, expressing a number.* So if a number is an idea, a numeral is an expression of an idea.

Our standard way of writing numbers depends on the choice of 10 as a base; this is called the *decimal system.* For example, the number eight thousand six hundred forty two divided by twenty five is written in decimal as

$$\frac{8642}{25} = 345.68 = 3(10^2) + 4(10^1) + 5(10^0) + 6(10^{-1}) + 8(10^{-2}).$$

However, the choice of ten is arbitrary, and other cultures have made other choices.

In this note, we explore how to express numbers in differing bases, and discover an interesting fact about radix expansions in alternate bases.

Date: September 9, 2008.

2. Integer Expansion Algorithm

The property of the integers which is pivotal is understanding bases is the way an integer breaks down into a quotient and remainder when it is divided by another integer. We state the result we use.

Proposition 1. Division Algorithm
Let $m, n \in \mathbb{Z}$. There exist unique integers $q, r \in \mathbb{Z}$ such that

$$n = mq + r \qquad \textit{and} \qquad 0 \leq r < m.$$

We call q the *quotient* and r the *remainder*.

Recall that a polynomial is a function of the form

$$f(x) = \sum_{i=0}^{k} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k,$$

where the coefficients a_i are selected from some prespecified set. We will use the division algorithm to show how to express an integer n as a polynomial in b, where b is the base. That is, for $b, n \in \mathbb{Z}$ with with $b \geq 2$, we find f as above with and $0 \leq a_i < b$ such that $f(b) = n$.

Lets first consider how we compute $f(b)$. The naive way to evaluate the polynomial f at a given value for x involves evaluating each monomial separately and adding the values together. This requires k additions and $\sum_{i=1}^{k} i = \frac{k(k+1)}{k}$ multiplications.

However, we may factor the polynomial thusly:

$$f(x) = a_0 + x(a_1 + x(a_2 + \cdots + x(a_{k-1} + x(a_k)) \ldots)).$$

Evaluating this at the same x requires k additions and k multiplications.

Proposition 2. Integer Expansion Algorithm
Let $b, n \in \mathbb{Z}$ with $b \geq 2$. Then there exists a unique polynomial

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

with integer coefficients such that

(1) *$f(b) = n$;*
(2) *$0 \leq a_i < b$, with $a_k > 0$.*

We call the coefficients a_i the *base b digits* of the number n. We may compute these as follows. Let $n \in \mathbb{Z}$; for simplicity assume n is positive. The division algorithm states that $n = bq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < b$. That $0 \leq r < b$ states that r is a digit in base b.

Set $q_0 = n$, $q_1 = q$, and $r_0 = r$ so that the above equation becomes

$$q_0 = bq_1 + r_0.$$

Then inductively compute

$$q_i = bq_{i+1} + r_i.$$

Since the q_i's are positive and decreasing, this process eventually ends, say at the k^{th} stage, so that

$$q_k = bq_{k+1} + r_k \qquad \text{with} \qquad q_{k+1} = 0;$$

at this point, $r_k = q_k$. If we plug this back into the previous equation $q_{k-1} = bq_k + r_{k-1}$, we see that $q_{k-1} = br_k + r_{k-1}$, which we rewrite as $q_{k-1} = r_{k-1} + br_k$. If we then take this and plug it back into its predecessor and rearrange, we obtain $q_{k-2} = bq_{k-1} + r_{k-2} = r_{k-2} + b(r_{k-1} + br_k)$. Next, and in the same manner, we find that $q_{k-3} = r_{k-3} + b(r_{k-2} + b(r_{k-1} + br_k))$. Continuing this process, we eventually arrive at

$$n = q_0 = r_0 + b(r_1 + b(r_2 + b \ldots (r_{k-1} + br_k) \ldots)).$$

Rewritten in standard polynomial form, using summation notation, this becomes

$$n = \sum_{i=0}^{k} r_i b^i.$$

In shortened notation, the base b numeral representing the number n is written

$$n = (r_k r_{k-1} \ldots r_1 r_0)_b.$$

That is, the digits of n written in base b are the remainders upon successive division by b.

3. Radix Expansion Algorithm

The expression of a real number in base b is called its *base b radix expansion.* We show how to find this for a real number between 0 and 1; combine this with the integer expansion algorithm to find the base b expansion of any real number.

Definition 1. A *power series* is a function of the form

$$f(x) = \sum_{i=0}^{\infty} a_i x^i,$$

where $a_i \in \mathbb{C}$.

For example, $|x| < 1$ and $a_i = 1$ for all i, then the power series is a convergent geometric series.

Proposition 3. Radix Expansion Algorithm
Let $z \in \mathbb{R}$ with $0 < z < 1$ and $b \in \mathbb{Z}$ with $b \geq 2$. Then there exists a unique power series

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

with integer coefficients such that

1. *$f(\frac{1}{b}) = z$;*
2. *$0 \leq a_i < b$ for all i;*
3. *if $a_i = b - 1$ then there exists $j > i$ such that $a_i \neq b - 1$.*

Note that since $a_i \leq b - 1$ for all i, then $f(\frac{1}{b}) \leq \sum_{i=0}^{\infty} (\frac{b-1}{b})^i$, which is a geometric series and therefore is convergent. Thus $f(\frac{1}{b})$ also converges.

Let $z \in (0, 1)$. Then $0 \leq bz_0 < b$. Multiply z_0 by b and take the integer part; call this p_1. Set

$$z_1 = bz_0 - p_1 \text{ with } p_1 \in \mathbb{Z}, 0 \leq p_1 < b, \text{ and } 0 \leq z_1 < 1.$$

Repeat this: $z_2 = bz_1 - p_2$, $z_3 = bz_2 - p_3$, and so forth. Inductively, take z_i and produce p_{i+1} and z_{i+1} such that

$$z_{i+1} = bz_i - p_{i+1} \text{ with } p_{i+1} \in \mathbb{Z}, 0 \leq p_{i+1} < b, \text{ and } 0 \leq z_{i+1} < 1.$$

The base b radix expansion of z is the series

$$z = \sum_{i=0}^{\infty} p_i \frac{1}{b^i}.$$

For the valiant reader, we explain why the series above converges to z. To do this, we show that the difference between the z and the partial sums of the series becomes as small as we want as we add additional terms. Such proofs often begin with the phrase "let $\epsilon > 0$"; this means that ϵ is arbitrarily small, and we show that the difference eventually becomes less than ϵ.

Let $\epsilon > 0$ and select $k \in \mathbb{N}$ so large that $\frac{1}{b^k} < \epsilon$. Then $\frac{z_{k+1}}{b^{k+1}} < \epsilon$. Solve each equation $z_{i+1} = bz_i - p_{i+1}$ for z_i to obtain

$$z_i = b^{-1}(p_{i+1} + z_{i+1}).$$

Rewind all this by substituting each such equation into the previous one:

$$z_k = b^{-1}p_{k+1} + b^{-1}z_{k+1};$$

$$z_{k-1} = b^{-1}(p_k + b^{-1}p_{k+1}) + b^{-2}z_{k+1};$$

$$z_{k-2} = b^{-1}(p_{k-1} + b^{-1}(p_k + b^{-1}p_{k+1})) + b^{-3}z_{k+1};$$

and so forth, until eventually

$$z = z_0 = b^{-1}(p_1 + b^{-1}(p_2 + b^{-1}(\dots b^{-1}(p_k + b^{-1}p_{k+1})\dots))) + b^{-(k+1)}z_{k+1}.$$

Thus

$$z - \sum_{i=0}^{k} p_i \frac{1}{b^i} = \frac{z_{k+1}}{b^{k+1}} < \epsilon,$$

which shows the convergence we desire.

4. Rational Expansion Property

Let $z \in \mathbb{Q}$, and for simplicity assume that $0 < z < 1$. Then $z = \frac{m}{n}$ for some $m, n \in \mathbb{N}$ with $m < n$ such that $\gcd(m, n) = 1$; this last condition guarantees that n is as small as possible.

We may obtain the base b radix expansion for z,

$$z = \sum_{i=0}^{\infty} p_i \frac{1}{b^i},$$

by repeated use of the division algorithm; this is the normal process of division, in base b, dividing n into m. Since $m < n$, we must first multiply m by b; then the quotient will be p_1 and the remainder will be an integer which is less than n:

$$bm = np_1 + r_1.$$

Next we multiply r_1 by b and divide, to get

$$br_1 = np_2 + r_2.$$

Inductively find p_i and r_i such that

$$br_i = np_{i+1} + r_{i+1}.$$

Now at each stage, $r_i < n$, so eventually two of remainders will be the same; let k be the smallest integer such that

$$r_k = r_i$$

for some $i < k$. Then $p_{i+j} = p_{k+j}$ for $j = 1, \ldots, k - i$, and this pattern continues to repeat. We call this a radix expansion whose repeating part starts after the i^{th} place and has length $k - i$.

On the other hand, if $z = \sum_{i=0}^{\infty} p_i \frac{1}{b^i}$ is a radix expansion whose repeating part starts after the i^{th} place of length $k - i$, then $(b^k - b^i)z$ is an integer, and

$$z = \frac{(b^k - b^i)z}{b^k - b^i}$$

expresses z as a rational number.

Together, we see that

Proposition 4. Rational Expansion Property *Let $z \in \mathbb{R}$, with $0 < z < 1$. Then the base b radix expansion of z repeats if and only if $b \in \mathbb{Q}$. Moreover, if $z = \frac{m}{n}$, then the sum of the lengths of the nonrepeating and the repeating parts of the radix expansion of z is less than or equal to n.*

If the repeating part of the base b radix expansion of z consists of a single repeating zero, we say that it *terminates.*

5. Regular Numbers

Definition 2. Let $n \in \mathbb{Z}$ with $n \geq 2$. We say that n is *base b regular* if the base b radix expansion of its reciprocal terminates.

Proposition 5. *Let $n \in \mathbb{Z}$ with $n \geq 2$. Then n is base b regular if and only if n is a product of powers of the prime divisors of b.*

Proof. We prove both directions of the implication.

($\Rightarrow$) Suppose that n is base b regular and that p is a prime divisor of n. We show that b is a prime of divisor of b, so that all primes in n are in b, and n must be the product of prime divisors of b.

Since n is base b regular, $\frac{1}{n}$ has a finite base b radix expansion, say of length i. Then $\frac{b^i}{n}$ is an integer, and n divides b^i. That is, b^i is a multiple of n, so every prime divisor of n must also be a prime divisor of b^i, and therefore of b itself.

($\Leftarrow$) Suppose that n is a product of powers of the prime divisors of b. Then for some $k \in \mathbb{N}$, we have $n \mid b^k$, say $nm = b^k$. Then

$$\frac{1}{n} = \frac{m}{b^k},$$

which clearly has a finite base b radix expansion. □

Department of Mathematics & Computer Science, Southern Arkansas University
E-mail address: plbailey@saumag.edu