The Radicans

James B. Wilson

March 28, 2002

1 Primitive Radicans

The computer revolution has brought awareness to the use of various bases in representing integers. The standard for most number systems is decimal, which is base 10, or has radix 10.[1] The radix for binary is 2; for octal, 8; and hexidecimal, 16.

An interesting case occurs when the radix 1 is considered. This construct is in fact the simplest representation of integers and is commonly known as a *tally* and is typically drawn in groups of 5 where the fifth stroke strikes through the previous 4. The trouble with a tally is best seen with a little development of the radices.

Definition 1.1 *Given an integer $r > 1$, r is the* radix *of a non-negative integer n, when n is expressed as the sequence $a_0, \ldots, a_k$ where $0 \leq a_i < r$ and*

$$n = a_k r^k + \cdots + a_2 r^2 + a_1 r + a_0.$$

The integers expressed with respect to the radix r will be denoted $\mathbb{N}_r$ and called a primitive radican *of r. The individual coefficients a_i are called r-*dits*, or simply* radits *when the r clear from the context.*

Using induction and the division algorithum it is routine to show that this representation is unique for any integer. The restriction that r be greater than 1 is required since $0 \leq a_i < 1$ forces $a_i = 0$ and clearly a sum of zeros will never equal a non-zero integer. Likewise radix 0 or negative cause similar problems. All hope is not lost though.

The difficulty when $r = 1$ is that with only one radit available for radix 1, it is impossible to distinguish between the element that should play the role of 0 from the object that shoul play the role of 1. In effect this is the trivial ring where multiplication is exactly addition. However the non-negative integers are fully expressed in a tally so they should not be immediately excluded. In fact the formal construction of the integers is similar to a tally, and so rightfully the natural numbers in their abstract sense are defined as the tally.

[1] The use of the term *base* is more common than *radix*. However due to the use of the the terms basis and bases later, *base* will be avoided in favor of *radix*. A number is expressed in base 10, or 2, etc, while the radix of a string of numbers is 10, or 2, etc.

Definition 1.2 $\mathbb{N}_1 = \mathbb{N}$

Now $\mathbb{N}_r$ is defined for all radices in $\mathbb{Z}^+$. Next the $\mathbb{N}$ will be replaced with arbitrary subsets of numbers. This will allow for a generalization of the structures in question. Later infinity will extend the primitive radicans by one more set.

Before moving on it is important to note several techniques exist to extend the radix representation of a positive integer to its negative: simply fix a new symbol (the minus sign) in front of the number, or for the case of more complex systems, such as the p-adic integers, use infinite sequences. Most of these methods can be extended to the following construction but for simplicity negative integers are ignored.

2 Radicans

Definition 2.1 *An r-radican is any semigroup, isomorphic to a semigroup of non-negative integers, expressed according to the radix r. That is, any semigroup that can be embedded in a primitive radican.*

A subradican of a radican is any subsemigroup expressed in the same radix.

Definition 2.2 *A* morphism $\gamma : A_r \to B_s$ *is a function* $\gamma : A_r \to B_s$ *where*

$$\gamma(a_0, \ldots, a_k) = (\gamma(a_0), \ldots, \gamma(a_k)).$$

[PENDING: determine if morphisms should be some type of homomorphism as well.]

In a sense a morphism is a change of radix. Notice that a morphism is fully determined by how it maps the r-dits to the s-dits.

Proposition 2.3 *Let $\mathcal{O}$ of all radicans be objects and define $Mor(A_r, B_s)$ to be all morphisms from the objects A_r to B_s. The collection $\mathfrak{R} = \langle \mathcal{O}, Mor(A_r, B_s) \rangle$, is a concrete category and is called the* Radican Category.

Proposition 2.4 $\mathbb{N}_1$ *is a zero – universal(initial) and co-universal(terminal) – in $\mathfrak{R}$.*

3 Universal Radicans

Applications typically demand the choice of a radix, but the theory in use rarely requires a specific radix. The properties of the integers are true in any radix. When the theorems allow, variables are substituted for specific numbers and as such no radix is required. The basic properties then at play behind every radix are those of an integral domain. Any theorem that makes use of these properties can be safely transplanted into any radix. Before exploiting this idea it will help to illustrate the concept with an example.

Example 3.1 *Every radix has a 0 and a 1 radit, so in each radix the expression* $1111 = 11 \cdot 101$ *is well formed. Of course for different radices this expression refers to different integers, for instance in radix 2 the expression equates to (expressed now in decimal):* $15 = 3 \cdot 5$*; radix 4:* $85 = 5 \cdot 17$*; and in radix 10 the expression does not change but would be read as* one-thousand-one-hundred-eleven equals eleven times one-hundred-one.

Likewise every radix r *has an element* $r-1$ *akin to the digit 9 in decimal, in that* $9+1=10$*, the situatation when* $r=2$ *will be explained in a moment. So give* $r-1$ *a special label* $\mathfrak{9}$.[2] *Now using this simple the expression* $1001 = 11 \cdot \mathfrak{9}1$ *also is admitted in every radix. Again the context determines which integers are being refered to so once again in decimal: radix 2 specificies* $9 = 3 \cdot 3$*; radix 4 states* $65 = 5 \cdot 13$*; and finally radix 10 states* $1,001 = 11 \cdot 91$*. Notice when the radix was* 2 *the symbol* $\mathfrak{9}$ *was read as* 1*, since* 1 *is both the* one *and the* nine *in radix 2.*

The symbols $0, 1$ and $\mathfrak{9}$ can be admited to any radix. However even with $\mathfrak{9}$ there is little room left to accomdate $\mathbb{N}_2$. Extending the character set no longer allows for the simple tranformation of sentences into any given radix. The following definition sums up the condition.

Definition 3.2 *A string of characters from the set* $\mathfrak{U} = \{0, 1, \mathfrak{9}\}$ *is called a universal formula/string. The set of all universal formulas is denoted by* $\mathbb{N}_\infty$.

Proposition 3.3 $\mathbb{N}_\infty$ *is a primitive radican. (Largely definitional.)*

Definition 3.4 *The universal mapping* Υ_r *from* $\mathbb{N}_\infty$ *to* $\mathbb{N}_r$ *is given by:*

$$\Upsilon_r(0) = 0 \qquad \Upsilon_r(1) = 1 \qquad \Upsilon_r(\mathfrak{9}) = (r-1).$$

Proposition 3.5 $\mathbb{N}_\infty$ *is universal(initial) in* $\mathfrak{R}$.

Proposition 3.6 $\mathbb{N}_\infty$ *is free in* $\mathfrak{R}$.

4 The Universal Numbers

A universal number is any universal string. The use of the $\mathfrak{9}$ allows the representation of a string to be expressed appropariately as a string of non-negative integers less than the radix. However the function of $\mathfrak{9}$ in the radix is akin to -1 as follows.

Example 4.1 *In a string* $(a_0, \ldots, a_i = \mathfrak{9}, \ldots, a_n)$*,* $\mathfrak{9} = (r-1)$*, so the* i^{th} *instance of* $\mathfrak{9}$ *equals* $(r-1)r^{i-1} = r^i - r^{i-1}$ *so the string is equivalent to* $(a_0, \ldots, -1, a_{i+1}+1, \ldots, a_n)$.

[2] The double nine ($\mathfrak{9}$) is intended to recall the digit 9 as a mneumonic device. It should not be taken to mean the digit 9 except when the radix is 10.

In this manner the use of $\mathbb{9}$ may be replaced by -1. However the resulting transformation creates two problems: first negative numbers are not in the radix character set; second, if $a_{i+1} \neq 0$ then $a_{i+1} + 1$ is no longer defined universally. For this reason special care must be taken when using -1 in place of $\mathbb{9}$.

In any case, the use of the universal character set is defined easily with the following addition and multiplication relations.

$+$	0	1	$\mathbb{9}$
0	0	1	$\mathbb{9}$
1	1	$\varnothing$	10
$\mathbb{9}$	$\mathbb{9}$	10	$\varnothing$

$\cdot$	0	1	$\mathbb{9}$
0	0	0	0
1	0	1	$\mathbb{9}$
$\mathbb{9}$	0	$\mathbb{9}$	$\varnothing$

Definition 4.2 *Given a universal formula $\alpha = (a_1, \ldots, a_n)$ and a radix r, $\alpha(r) = \sum_{i=1}^{n} a_i r^{i-1}$.*

Definition 4.3 *Given the universal formulas α, β and γ, define multiplication as $\alpha\beta = \gamma$ if $\alpha(r)\beta(r) = \gamma(r)$ for all radices r. Likewise define addition as $\alpha + \beta = \gamma$ when $\alpha(r) + \beta(r) = \gamma(r)$.*

Notice not all universal formulas can be multiplied or summed, but the condition when they may is well-defined. Since the multiplication and addition are direct results of multiplication and addition in integral domains, the properties are identical where ever the product and sums are defined.

Note that radix multiplication is polynomial multiplication within an equivalence class. Therefore a product that is out of range will be reformated to be in the normal form required by the radix range. This occurs exclusively when a number divisible by 10 appears as a coefficient.

Definition 4.4 *Given universal formals α and β, β is a* universal factor *of α if $\beta(r)|\alpha(r)$ for all radices r. If 1 and α are the only universal factors of α, then α is a* universal prime.

Example 4.5 *Let $\alpha = (1, 1, 1, 1)$ and $\beta = (1, 1)$. Given any radix $r > 1$ it follows:*

$$\alpha(r) = r^3 + r^2 + r + 1 = (r + 1)r^2 + (r + 1) = (r + 1)(r^2 + 1) = \beta(r)(r^2 + 1)$$

so $\beta(r)|\alpha(r)$. Therefore β is a universal factor of α. By the same argument $\gamma = (1, 0, 1)$ is a universal factor of α.

Now let $\alpha = (1, 0, 0, 1)$, $\beta = (1, 1)$ and $\gamma = (\mathbb{9}, 1)$. Again given any radix r,

$$\begin{aligned} \beta(r)\gamma(r) &= (r + 1)((r - 1)r + 1) = ((r + 1)(r - 1))r + (r + 1)1 \\ &= (r^2 - 1)r + r + 1 = r^3 - r + r + 1 = r^3 + 1 = \alpha(r) \end{aligned}$$

and so β and γ are universal factors of α.

Finally $\beta = (1, 1)$ is a universal prime since $(1, 0)$ does not divide β ever so β is divisible only by 1 and itself. By the same empirical argument $(1, 0)$ and $(\mathbb{9}, 1)$ are universal primes.

Division and multiplication of universal numbers can be done in radix 10 as standard decimals, provided at each step only 0, 1, or 9 appear as digits.

Example 4.6 $1111/11$ *and* $1001/11$ *can be computed by standard division.*

$$\begin{array}{rr|l} & 101 & \\ \hline 11 &)1111 & \\ & \underline{-11} & \\ & 11 & \\ & \underline{-11} & \\ & 0 & \end{array} \qquad \begin{array}{rr|l} & 91 & \\ \hline 11 &)1001 & \\ & \underline{-99} & \\ & 11 & \\ & \underline{-11} & \\ & 0 & \end{array}$$

Now reading each 9 *as* $\mathbb{9}$ *it follows* $11 \cdot 101 = 1111$ *and* $11 \cdot \mathbb{9}1 = 1001$.

Lemma 4.7 *If* α *is a universal factor of* γ *then there exists a universal factor* β *of* γ *such that* $\alpha\beta = \gamma$.

Proof: Let $\alpha = (a_1, \ldots, a_l)$, $\beta = (b_1, \ldots, b_m)$ and $\gamma = (g_1, \ldots, g_n)$. Suppose α and γ are universal and that $\alpha\beta = \gamma$ so that α is a universal factor of $'g$. Note that the coefficients are all non-negative since such is the requirement for any radix representation of a positive integer.

The product of polynomials perscribes that each $g_i = \sum_{i-1=j+k} a_j b_k$. By assumption each g_i and each a_j is either $0, 1$ or $\mathbb{9}$. Therefore if $g_i = 0$ then $\sum_{i-1=j+k} a_j b_k = 0$. Since all coefficients are non-negative it follows the sum is 0 only when either each $a_j b_k = 0$ or they sum to a number divisible by 10. However 10 is only defined by $1 + \mathbb{9}$ so each b_k is either 0, 1, or $\mathbb{9}$. Therefore β is universal, and so it is a universal factor of α. $\square$

Proposition 4.8 *Every universal formula can be factored into universal primes.*

Proof: Given a universal formula γ it is either a universal prime or it has a proper universal factor. If it has a proper universal factor α then by Lemma-**??** there exists another universal factor β that together factors γ into $\alpha\beta$. Repeat this process recursively on α and β until γ is expressed as a product of universal primes. $\square$

Proposition 4.9 *The universal factorization of a universal number into universal primes is unique.*

Proof: Apply the fundamental theorem of arithmetic. NOTE: this isn't that easy. There is a plausible case that universal primes may be derived from multiple primes and thus may not be unique. Requires the converse of the previous proposition!! $\square$

By dividing by all universal formulas between 1 and α will succeed in testing whether α is a universal prime, however the process is tedious and inefficient. A considerably simpler approach concerns the use of the Fundamental Theorem of Arithmetic.

Theorem 4.10 *If a universal formula is a prime number with respect to some radix, greater than 1, then it is a universal prime.*

Proof: Since a universal factorization is an integer factorization, it follows any prime number written as a universal number can be factored only trivially and thus it can only be universally factored trivially. Therefore the universal representation of any prime is a universal prime. □

Conjecture 4.11 *A universal prime is a prime number in some radix.*

Nothing is known about the converse of this statement. It is however the case that given some universal primes (perhaps all), not all radices, will admit the number as a prime. For instance, $111 = 7$ in radix 2, and is prime, and therefore 111 is a universal prime. However $111 = 3 \cdot 37$ in radix 10 so it is not prime.

Knowing the converse of this statement could be increadibly useful. It would provide an equivalent definition for prime numbers. Also a proof for Conjecture-4.11 would replace the uncertainty in Corollary-5.4 with the statement that for every prime p there exists an r where $r^p - 1/r - 1$ is prime. Thus this would provide an infinite class of prime numbers.

It is clear that every positive integer n is the image of a universal prime, for instance 11 in radix $n-1$. Therefore every prime is an image of a universal prime. However the stricter assumption that every universal prime have an image that is prime is more involved. Presuming it is so, a new process to search for prime numbers can be created. First locate a universal prime. This is simple since certain infinite families of universal primes are known, for instance, strings for 1's of prime length. Next take the image of the universal prime over various radices until one returns a prime. There is no esitmation as to the efficiency of this process, however it now doubt has certain optimizations.

So the questions are: are their any universal primes whose image is never prime? Or are their any universal numbers at all whose image is never prime? Are their any numbers that can't be made the image of a given universal prime? We know already the images of 11 span the integers greater than 1. Likewise with 1, all positive integers. However 6 cannot be had from 111 in any radix since any radix over 1 is out of range and in the tally 6 is not 111.

Before proceeding a tool will be established. What are all the possilbe universal representations of a number?

Proposition 4.12 *Every positive integer n is represented universally in the following radices:*

- *1, 2, 3, n-1, n, n+1*
- *If $n = m^k$ then radix m^i, where $0 < i < k$.*

Proof: First observe the number will be finite. This is because the length of any universal number whose image is n in a radix r must be less than or equal to n as in the case of the tally.

Radices 1, 2 and 3 use only the symbols $0, 1, \mathbb{9}$ so they represent n universally. Radix $n-1$ represents n as 11, radix n as 10, and radix $n+1$ as $\mathbb{9}$ so each is universal.

Finally suppose $n = m^k$. Then in radix m^i, n is $10\cdots0$ of length m^{k-i}. $\square$ Other universal forms may be found emperically. Note however the radices 1, 2, 3, $n-1$, n, and $n+1$ are particularly useful because they require no knowledge of factors of n and can be computed directly. Notice infact in radix 3 the factorization of a number is always a prime universal factorization.

5 The General Mersenne Numbers

The structure of universal formulas tends to be regular, enough so that certain factors are immediately appearent and others require simple checks. Surprisingly one class of universal numbers appears repeatedly as a factor of universal numbers, the string of all 1's. Fortunately the factorization of this class of universal formulas is fully determined.

Definition 5.1 *A universal formula of all* 1*'s and length* n *is called a* General Mersenne Number *of length* n *or simply an* n*-mersenne and is denoted* $\vec{1}_n$.

Lemma 5.2 *Every* n*-mersenne has an* m*-mersenne factor if and only if* $m|n$.

Proof: Let m and n be positive integers. $m|n$ if and only if $\vec{1}_n$ can be partitioned into n/m copies of $\vec{1}_m$. Therefore

$$\vec{1}_n(r) = \sum_{i=1}^{n/m} \vec{1}_m(r) r^{m(i-1)} = \vec{1}_m(r) \sum_{i=1}^{n/m} r^{m(i-1)}.$$

So $\vec{1}_m$ is a universal factor of $\vec{1}_n$ if and only if $m|n$. $\square$

The interesting property of General Mersenne Numbers is that their factorization is completely determined by their length. The length is always less than the magnitude of the number when placed in a specific radix, and since universal factors are also factors in the usual sense once expressed according to a radix, this offers a short cut to factoring potentially large numbers by using the length instead of the number itself. Of course there is no guarantee that the universal factorization is the complete factorization, but it will reduce the magnitude of the factors for easier computation.

Proposition 5.3 *A* p*-mersenne is a universal prime if and only if* p *is prime.*

Proof: When p is prime Lemma-5.2 proves no proper mersenne divides the p-mersenne. [PENDING: make a case that these are always factors of a factorable mersenne.]

Suppose now α is a universal prime.[PENDING: write it up in all its glory.] $\square$

Corollary 5.4 *Let p be a prime and $r > 1$. $\frac{r^p-1}{r-1}$ may be prime.*

Proof: $r^p = (1, 0, \ldots, 0)(r)$ of length $p+1$ so $r^p - 1 = (\mathbb{9}, \ldots \mathbb{9})(r)$ is of length p and so $\frac{r^p-1}{r-1} = (1, \ldots, 1)(r) = \alpha(r)$ is of prime length. Therefore by Theorem-5.3 it follows α is a universal prime and so it may have a prime image under some radix. $\square$

Corollary 5.5 (Classic Mersenne Numbers) $2^p - 1$ *may be prime.*

Proof: Let $r = 2$ and apply Corollary-5.4 $\square$

Proposition 5.6 *The following factors are all examples of the prolific mersenne factors.*

- $(1, 0, \ldots, 0, 1)_{2n+4} = \vec{1}_2(\mathbb{9}0(1010 \cdots 01)_{2n} + 1)$ *where* $n \geq 0$.
- $(1, 0, 1, 1, \ldots, 1, 1, 0, 1)_{n+2} = \vec{1}_n \cdot \mathbb{9}1$ *where* $n > 1$.
- $(1, 1, 0, 1, 1, \ldots, 1, 1, 0, 0, 1)_{n+3} = \vec{1}_n \cdot \mathbb{99}1$, $n > 2$.

Proof: Induction. $\square$

Corollary 5.7 (Mersenne Factor Tip) *Given a universal formula, α, expressed with all 0's and 1's, if α is not a universal prime then it will likely have $\vec{1}_m$ as a factor where m is the sum total of all the 1's in α.*

6 Compressed Factorization

The task of factoring large numbers is difficult. However most computational systems rarely deal with raw large numbers but invariably compress the information and swap the the details in the compressed format. The goal is to explore certain factorization techniques that can be applied to the compressed representations of large numbers. To do this we require a lossless compression scheme. The scheme we adopt is a run length compression scheme.

Given an integer expressed according to a specified radix (base) b, we may compress the representation of the number by describing the number interms of sequences of repeating digits.

Proposition 6.1 *In any radix b, a number beginning with 1 and ending with 1 and zeros in between is prime only if it has prime length plus 1. That is, $b^n + 1$ is prime only if n is composite.*

Proof: Let $m = b^n + 1$. $\square$

Corollary 6.2 (Fermat Criterion) $2^{2^n} + 1$ *may be prime.*

7 Radix Free Relations

We already know that $11 \cdot 101 = 1111$ in any radix and any number of generalizations of this method. Consequently we know $22 \cdot 101 = 2222$ and $11 \cdot 202 = 2222$ and in general $k(11 \cdot 101) = k \cdot 1111$. While k may not be in expressed in the given radix, for instance $55 \cdot 101 = 5555$ in radix 2 is not expressed correctly, but the relation still holds; that is, $5 \cdot (11 \cdot 11) = (101 \cdot 11) \cdot 101) = 1111 \cdot 101 = 1001011 = 101 \cdot 1111 = 5 \cdot 1111$. This generalization recalls the notion of a set of generators, the minimal relations being true in any radix, and the scalings being true once expressed according to a given radix.

So we build a category in which to place our universal - radix free - relations. Given that the relations must translate into any radix it follows a limited number of symbols may be used. Since the smallest radix is 2 it follows at most 3 symbols may be used: 0 - meaning the null digit in the radix, 1, meaning the first non-null digit, and $\mathbb{9}$ - the larget digit. In the case of radix 2, $1 = \mathbb{9}$.[3]

[3]The double nine ($\mathbb{9}$) is meant to invoke the intuition of 9 in radix 10. It is however a universal 9 so that $1 + \mathbb{9} = 10$ in whatever radix the context requires.