ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 29, Number 4, Winter 1999

FOR $b \geq 3$ THERE EXIST INFINITELY MANY BASE b k-SMITH NUMBERS

BRAD WILSON

ABSTRACT. In [**5**] a Smith number is defined as a composite, the sum of whose digits equals the sum of the digits of the prime factors counted with multiplicity. In [**1**] it was shown there are infinitely many Smith numbers by giving a constructive algorithm. In [**2**] this result was extended to Smith numbers in bases $b \geq 8$ and in [**3**] to $b = 2$. In this paper we modify the argument in [**2**] to cover all bases $b \geq 3$.

1. Introduction, notation and definitions. Let $b \geq 3$ be a fixed base. All our references to integers will be to integers base b unless otherwise noted. Let x be a natural number, and let $x = p_1 p_2 \cdots p_r$ be its factorization into not necessarily distinct primes. Let $N(x)$ denote the number of digits of x base b, $S(x)$ the sum of the base b digits of x and $S_p(x)$ the sum of the base b digits of the prime factors of x counted with multiplicity, i.e., $S_p(x) = \sum_{i=1}^{r} S(p_i)$. Note that

$$S_p(xy) = S_p(x) + S_p(y). \tag{1}$$

Let k be a natural number.

Definition. A *base b k-Smith number* is a composite x so that

$$S_p(x) = kS(x).$$

2. Preliminary results. We now cite a number of useful lemmas from [**2**].

Lemma 1. *If $m > 1$ there exists a t so that $S_p(t) = m$.*

In view of (1) this lemma says that, given natural numbers x and y so that $S_p(x) < y - 1$, we can find t so that $S_p(xt) = y$. In particular, we

Received by the editors on February 5, 1997, and in revised form on January 9, 1998.

can take a finite collection of such t so that we can manipulate $S_p(xt)$ to whatever congruence class we wish modulo $S_p(b)$:

Corollary. *There exists a finite set T of integers such that $U = \{S_p(t) : t \in T\}$ is $\{2, 3, \ldots, S_p(b) + 1\}$.*

The final result we need from [**2**] is the following lemma:

Lemma 2. *If n, t, v are natural numbers so that $t \leq b^n - 1$, then*

$$S(t(b^n - 1)b^v) = S(b^n - 1) = (b - 1)n.$$

This says that we can multiply $b^n - 1$ by a variety of numbers without affecting the digital sum. In view of these lemmas, the basic strategy to show the existence of infinitely many base b k-Smith numbers is to start with a number of the form $b^n - 1$ satisfying $S_p(b^n - 1) < S(b^n - 1) - 1$. Lemma 1 and its corollary say, for n large enough so that $b^n - 1 \geq t$ for all $t \in T$, we can find a $t \in T$ so that

$$S_p(t(b^n - 1)) \equiv kS(t(b^n - 1)) \pmod{S_p(b)}.$$

This means

$$S_p(t(b^n - 1)) + vS_p(b) = kS(t(b^n - 1))$$

for some nonnegative integer v, and so Lemma 2 and (1) give

$$S_p(t(b^n - 1)b^v) = kS(t(b^n - 1)b^v).$$

Thus, the crux of constructing infinitely many base b k-Smith numbers is showing that there are infinitely many n so that $S_p(b^n - 1) < S(b^n - 1) - 1$.

3. Main theorem.

Main theorem. *There exist infinitely many base b k-Smith numbers.*

Proof. By the previous section it suffices to show there are infinitely many n satisfying $S_p(b^n-1) < S(b^n-1)-1$.

It is easy to show that $f(x) = (b-1)\log_b(x + ((b^2-1)/b^2)) - x$ is positive for all $x \in [1, b-2]$. Let ε be the smaller of 1 and the minimum of $f(x)$ on $[1, b-2]$.

For p a prime, $p \nmid b$, let $\mathrm{ind}\,(p^m)$ denote the smallest k so that $p^m|(b^k-1)$. It is well-known [**6**] that $p^m|(b^l-1)$ if and only if $\mathrm{ind}\,(p^m)|l$. Let $v_p(b-1)$ be the largest power of p dividing $b-1$, and let

$$S = \{\mathrm{ind}\,(p) : p < b^2, p \nmid (b-1), p \nmid b\}$$

and

$$T = \{\mathrm{ind}\,(p^{v_p(b-1)+1}) : p < b, p|(b-1)\}.$$

Since $S \cup T \subset \mathbf{N}$ is finite and $1 \notin S \cup T$ we know

$$U = \mathbf{N} - \bigcup_{x \in S \cup T} x\mathbf{N}$$

has infinitely many elements. For $u \in U$ we note $p \nmid ((b^u-1)/(b-1))$ for $p < b^2$. Thus if $u \in U - \{1\}$ there is a prime q so that $q|((b^u-1)/(b-1))$, $x \nmid \mathrm{ind}\,(q)$ and $x \nmid q$ for all $x \in S \cup T$.

For q as in the last paragraph, there is no single or double digit prime divisor of $(b^{\mathrm{ind}\,(q)q^k} - 1/b - 1)$ for any $k \geq 0$. We now claim that $n = \mathrm{ind}\,(q)q^k$ works for any $k > (b/\varepsilon)$.

To see this, factor $b^n - 1 = (b-1)p_1p_2\cdots p_r$. Let $\beta_i = N(p_i) - 1$ and $\beta = \sum_{i=1}^r \beta_i$. Then

$$S_p(b^n-1) = S_p(b-1) + \sum_{i=1}^r S(p_i) \leq (b-1) + \sum_{i=1}^r S(p_i). \tag{2}$$

Since $(b-1) \nmid S(p_i)$ we see $S(p_i) \leq (b-1)N(p_i) - 1 = (b-1)\beta_i + (b-2)$. Let

$$A_j = \{p_i : S(p_i) = (b-1)\beta_i + j\}$$

for $j = 1, 2, \ldots, b-2$ and

$$A_0 = \{p_i : S(p_i) < (b-1)\beta_i\}.$$

Let n_j be the number of elements in A_j for $j = 0, 1, \dots, b-2$. Then (2) becomes

$$S_p(b^n - 1) \leq (b-1) + (b-1)\beta + \sum_{j=1}^{b-2} j n_j - n_0. \tag{3}$$

By our choice of n all p_i satisfy $p_i > b^2$, i.e., we were careful in choosing n to make sure the $\operatorname{ind}(p) \nmid n$ for $p < b^2$, $p \nmid (b-1)$ and $\operatorname{ind}(p^{v_p(b-1)+1}) \nmid n$ for $p|(b-1)$). For $S(p_i) = (b-1)\beta_i + c_i$ we have

$$p_i \geq (c_i + 1)b^{\beta_i} - 1 \geq \left(c_i + \frac{b^2-1}{b^2}\right) b^{\beta_i}$$

if $c_i > 0$ and

$$p_i > b^{\beta_i}$$

if $c_i < 0$. Then

$$b^n - 1 = (b-1)p_1 p_2 \cdots p_r \geq (b-1) \cdot \prod_{j=1}^{b-2} \left(j + \frac{b^2-1}{b^2}\right)^{n_j} b^{\beta}. \tag{4}$$

Writing $b^n - 1$ as ab^{n-1} for $1 \leq a < b$ and taking logarithms in (4) gives

$$\log_b a + N(b^n - 1) - 1 \geq \log_b(b-1) + \beta + \sum_{j=1}^{b-2} n_j \log_b \left(j + \frac{b^2-1}{b^2}\right). \tag{5}$$

Multiplying both sides by $b-1$ yields

$$\begin{aligned}(b-1)N(b^n-1) \geq (b-1)\log_b(b-1) + (b-1)\beta + (b-1)(1 - \log_b a) \\ + (b-1)\sum_{j=1}^{b-2} n_j \log_b \left(j + \frac{b^2-1}{b^2}\right).\end{aligned}$$

Since $(b-1)\log_b(j + (b^2-1)/b^2) = f(j) + j \geq j + \varepsilon$ we get

$$(b-1)N(b^n-1) > (b-1)\log_b(b-1) + (b-1)\beta + \sum_{j=1}^{b-2}((j+\varepsilon)n_j). \tag{6}$$

If $S(q) > (b-1)(N(q)-1)$, then there exists $j \geq 1$ so that $n_j \geq k$. Since $k > b/\varepsilon$ (6) becomes

$$(7) \quad (b-1)N(b^n-1) > (b-1)\log_b(b-1) + (b-1)\beta + \sum_{j=1}^{b-2} jn_j + b.$$

Taken together, (3) and (7) give

$$(b-1)N(b^n-1) - 1 > S_p(b^n-1).$$

If $S(q) < (b-1)(N(q)-1)$, then $n_0 \geq k \geq b$ so (3) and (6) again give

$$(b-1)N(b^n-1) - 1 > S_p(b^n-1)$$

so there exist infinitely many n so that $S(b^n-1) - 1 > S_p(b^n-1)$, which was what was to be shown. □

REFERENCES

1. W. McDaniel, *The existence of infinitely many k-Smith numbers*, Fibonacci Quart. **25** (1987), 76–80.

2. ———, *Difference of the digital sums of an integer base b and its prime factors*, J. Number Theory **31** (1989), 91–98.

3. ———, *Constancy of the number of* 1*'s in a binary integer under factorization into prime factors*, Math. and Comp. Ed. **25** (1991), 285–287.

4. S. Oltikar and K. Wayland, *Construction of Smith numbers*, Math. Mag. **56** (1983), 36–37.

5. A. Wilansky, *Smith numbers*, Two Year Coll. Math. J. **13** (1982), 21.

6. S. Yates, *The mystique of repunits*, Math. Mag. **51** (1978), 22–28.

2030 State Street, Apt. 19, Santa Barbara, CA 93105
E-mail address: bwilson@warren-selborg.com