ITERATED EXPONENTS IN NUMBER THEORY

DANIEL B. SHAPIRO AND S. DAVID SHAPIRO

Dedicated to the memory of Prof. Arnold Ross

Introduction

What is the units digit of a number like $7^{8^{9^{10}}}$? Problems of this nature often appear on contests, and we consider various generalizations in this article. For instance we show that if $a_1, a_2, a_3, \dots$ is a sequence of positive integers and k is given, then the sequence $a_1,\ a_1^{a_2},\ a_1^{a_2^{a_3}}, \dots$ becomes constant when reduced $\pmod{k}$. We also consider the sequence $1^1,\ 2^2,\ 3^3, \dots \pmod{k}$, showing that this sequence, and related ones like $n^{n^n} \pmod{k}$, are eventually periodic. With further work we are able determine their minimal periods. Using those ideas we prove that if u is relatively prime to k then the congruences $x^x \equiv u \pmod{k}$ and $y^{y^y} \equiv u \pmod{k}$ have solutions. Finally, we lift these ideas to the ring of p-adic integers and pose some open questions.

The methods used here are part of elementary number theory and we have attempted to present the ideas in as elementary a way as possible. The results proved here were originally obtained in 1985, but not published previously.

Many papers have been written about limits of the form $x^{x^{x^{\cdot^{\cdot^{\cdot}}}}}$, where x is a real or complex number. In fact, such convergence questions go back to Bernoulli, Goldbach and Euler. Results and references to the literature appear in Anderson (2004), Knoebel (1981), and Baker and Rippon (1985). However, relatively little work has been done on the arithmetic aspects of such numbers when x is an integer. Early work in this direction was done by Maurer (1901) and Cunningham (1907). Fifty years later some related papers appeared in Polish journals by Sierpiński (1950), Hampel (1955) and Schinzel-Sierpiński (1959). More recently Blakley-Borosh (1983) and Dawson (1994) published further results about the periodic behavior of these sequences modulo k. In this article we unify and extend these arithmetic results. In the first sections below we have repeated some of the results of Blakley-Borosh and Dawson in order to have a self-contained presentation and to clarify the notations.

1. Reducing iterated exponents modulo k.

The symbol $\mathbf{Z}$ stands for the set of integers and $\mathbf{Z}^+$ is the subset of positive integers. We assume the reader is familiar with some elementary number theory.

Definition 1.1. If a, b are positive integers, define $a \uparrow b = a^b$. These arrows are always associated to the right if no parentheses are present: $a \uparrow b \uparrow c = a \uparrow (b \uparrow c)$. The related "E" notation is defined in analogy with "Σ" for sums:

$$\mathop{\mathrm{E}}_{j=1}^{s} a_j \;=\; a_1 {\uparrow} a_2 {\uparrow} \ldots {\uparrow} a_s \;=\; a_1^{a_2^{\cdot^{\cdot^{\cdot^{a_s}}}}} .$$

Recursively we can define: $\mathop{\mathrm{E}}_{j=1}^{s} a_j = a_1 {\uparrow} \left(\mathop{\mathrm{E}}_{j=2}^{s} a_j \right)$, if $s > 1$.

The goal of this section is to investigate conditions on integer sequences $\{a_j\}$ and $\{b_j\}$ which imply that

$$a_1 {\uparrow} a_2 {\uparrow} \ldots {\uparrow} a_s \equiv b_1 {\uparrow} b_2 {\uparrow} \ldots {\uparrow} b_s \pmod{k}.$$

To begin let's refine the usual definition of the *order* of an element (mod k) by allowing non-units.

Definition 1.2. Given n and k, the sequence $1, n, n^2, n^3, \ldots$ (mod k) is eventually periodic. The *order*, $o_k(n) = o(n \bmod k)$, is the length of that periodic cycle. The *tail length* $\rho_k(n)$ is the number of terms in the sequence before the repeating cycle begins. (The notations ρ and o are suggested by the shapes of those letters.)

For example the powers of 2 (mod 40) are 1, 2, 4, 8, 16, 32, 24, 8, 16, 32, … . The terms (1, 2, 4) form an initial "tail" so that $\rho_{40}(2) = 3$. The repeating portion or "cycle" is (8, 16, 32, 24), so that $o_{40}(2) = 4$.

Lemma 1.3. *Given positive integers n and k:*
(a) *$\rho_k(n)$ and $o_k(n)$ depend only on n modulo k.*
(b) *If $r \neq s$ then:*
$$n^r \equiv n^s \pmod{k} \iff r \equiv s \pmod{o_k(n)} \quad \text{and} \quad r, s \geq \rho_k(n).$$

Proof. These statements follow from the Definition. For instance, for (b), any repetition in the sequence $\{n^r \pmod{k}\}$ must occur within the repeating cycle. □

When n is invertible (mod k), the sequence $1, n, n^2, n^3, \ldots$ (mod k) is purely periodic. Then the cycle length is the first exponent which yields 1. That is, $\rho_k(n) = 0$ and $o_k(n) = \min\{d : d > 0 \text{ and } n^d \equiv 1 \pmod{k}\}$.

Lemma 1.4. *Given $k, n \in \mathbf{Z}^+$, factor $k = k'(n)k''(n)$, where $k'(n)$ and n are coprime, and every prime factor of $k''(n)$ also divides n.*
(1) *$o_k(n) = o_{k'(n)}(n)$.*
(2) *$\rho_k(n) = \min\{r \in \mathbf{Z} : r \geq 0 \text{ and } k''(n) \,|\, n^r\}$.*

Proof. The values $n^r \pmod{k'}$ are purely periodic while $n^r \equiv 0 \pmod{k''}$ for all large r. This yields the expression for $\rho_k(n)$. The Chinese Remainder Theorem implies that the length of the (eventual) cycle (mod k) equals the length of the cycle (mod k'). □

Suppose $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$, where the p_i are distinct primes and every $r_i > 0$. Arrange the prime factors of k so that $k = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t} \cdots p_u^{m_u}$, where $m_i \geq 0$. Then $k''(n) = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ and $\rho_k(n) = \max\limits_{1 \leq i \leq t} \{\lceil \frac{m_i}{r_i} \rceil\}$.
(Here, $\lceil x \rceil$ is the smallest integer $\geq x$.)

Euler proved that $c^{\varphi(k)} \equiv 1 \pmod{k}$ for every c coprime to k. Here the Euler function $\varphi(k)$ is the number of elements in the group of units $\mathbf{U}_k = (\mathbf{Z}/k\mathbf{Z})^*$. Equivalently, $\varphi(k)$ is the number of integers c coprime to k with $0 \leq c < k$. For our purposes, the *smallest* exponent for $\mathbf{U}_k$ is a more important value.

Definition 1.5. For $k \in \mathbf{Z}^+$ define $\lambda(k)$ to be the smallest positive integer e such that $n^e \equiv 1 \pmod{k}$ for every n coprime to k.

Define $R(k) = \max\{\rho_k(n) :\ 0 \le n < k\}$.

This $\lambda(k)$ is the "exponent" of the abelian group $\mathbf{U}_k$. Carmichael (1910) showed how to compute $\lambda(k)$ from the prime factorization of k.

Proposition 1.6. Suppose $k = p_1^{m_1} p_2^{m_2} \dots p_t^{m_t}$ in prime factorization.
(0) $R(k) = \max\{m_i\}$.
(1) $\lambda(k)$ is the maximal order of an element in $\mathbf{U}_k$. If $d\,|\,k$ then $\lambda(d)\,|\,\lambda(k)$.
(2) If a, b are coprime, then $\lambda(ab) = \mathrm{lcm}\{\lambda(a), \lambda(b)\}$.
Generally: $\lambda\big(\mathrm{lcm}\{a,b\}\big)$ divides $\mathrm{lcm}\{\lambda(a), \lambda(b)\}$.
(3) If p is an odd prime, $\lambda(p^m) = p^{m-1}(p-1)$.
(4) $\lambda(2) = 1,\ \lambda(4) = 2,$ and $\lambda(2^m) = 2^{m-2}$ whenever $m \ge 3$.

Proof. These results follow from the ideas used to determine which of the groups $\mathbf{U}_n$ are cyclic. Key steps in an elementary proof are:
(i) If $x, y \in \mathbf{U}_m$, there exists $z \in \mathbf{U}_m$ with $o_k(z) = \mathrm{lcm}\{o_k(x), o_k(y)\}$.
(ii) If p is an odd prime, there is an element of order p^{m-1} in $\mathbf{U}_{p^m}$.
(iii) There is an element of order 2^{m-2} in $\mathbf{U}_{2^m}$ whenever $m \ge 3$.
Further information appears in many references, like [Carmichael: 1910], [Vinogradov: 1954] pp. 106-107, or [H. Shapiro: 1983] Theorems 6.2.2 and 6.3.1.

For part (2), when a, b are coprime apply the Chinese Remainder Theorem. For the general case, factor $\mathrm{lcm}\{a,b\} = a'b'$ where $a'\,|\,a,\ b'\,|\,b$ and a', b' are coprime. Then $\lambda(\mathrm{lcm}\{a,b\}) = \lambda(a'b') = \mathrm{lcm}\{\lambda(a'), \lambda(b')\}$ divides $\mathrm{lcm}\{\lambda(a), \lambda(b)\}$. □

As a corollary we see that $\lambda(k)$ and $R(k)$ are the o and ρ for everything in $\mathbf{Z}/k\mathbf{Z}$, taken simultaneously.

Corollary 1.7. Let k be a positive integer.
(1) For every $n \in \mathbf{Z}$, $o_k(n)\,|\,\lambda(k)$ and $\rho_k(n) \le R(k)$.
(2) Let a, b be nonnegative integers. Then:

$$n^a \equiv n^b \ (\mathrm{mod}\, k) \ \text{ for every } n \iff \begin{cases} \text{either} & a = b, \\ \quad\text{or} & a \equiv b \pmod{\lambda(k)} \ \text{ and } \ a, b \ge R(k). \end{cases}$$

Proof. (1) $o_k(n) = o_{k'}(n)$ which divides $\lambda(k')$. Since $k'\,|\,k$ we apply (1.6)(2) above.
(2) Apply Lemma 1.3. □

Consequently, the mod k reduction of, say, $a_1^{a_2^{a_3}} = a_1 \uparrow a_2 \uparrow a_3$ should depend only on the residues of $a_1 \pmod{k}$, of $a_2 \pmod{\lambda(k)}$ and of $a_3 \pmod{\lambda(\lambda(k))}$. For example, since $\lambda(\lambda(8)) = 1$, this *ought* to imply that the value of $a_1 \uparrow a_2 \uparrow x$ (mod 8) is *independent* of the choice of x. However $2^{2^1} \not\equiv 2^{2^2} \pmod{8}$. This happens because the value $2^{2^1} = 4$ lies in the "tail" rather than the "cycle". The next few results detail the inequalities needed to avoid this problem.

Lemma 1.8. Suppose $a_r \equiv b_r \pmod{\lambda^{r-1}(k)}$ for $r = 1, 2, \dots, s$. Then

$$\mathop{\mathrm{E}}_{i=1}^{s} a_i \ \equiv\ \mathop{\mathrm{E}}_{i=1}^{s} b_i \pmod{k},$$

provided $\mathop{\mathrm{E}}_{i=r+1}^{s} a_i$ and $\mathop{\mathrm{E}}_{i=r+1}^{s} b_i$ are $\ge R(\lambda^{r-1}(k))$ whenever $1 \le r < s$.

Proof. Induction on s using Corollary 1.7. □

Proposition 1.9. Suppose $a_r \equiv b_r \pmod{\lambda^{r-1}(k)}$ for $r = 1, \ldots, s$. Suppose further that $a_r, b_r \geq 2$ for $1 < r \leq s$; and $a_s, b_s \geq R(\lambda^{s-2}(k))$. Then

$$\mathop{\mathrm{E}}_{i=1}^{s} a_i \equiv \mathop{\mathrm{E}}_{i=1}^{s} b_i \pmod{k}.$$

Proof. It suffices to verify the inequalities in (1.8). The case $r = s-1$ is assumed. The other inequalities follow by repetition of the following claim.
Claim: If $a \geq 2$ and $a \geq R(\lambda(k))$ then $2^a \geq R(k)$.
This is clear when $\rho(k) \leq 4$ since $2^a \geq 2^2 = 4$. If $\rho(k) > 4$ the definitions imply that $R(\lambda(k)) \geq R(k) - 2$. Since $2^{x-2} \geq x$ whenever $x \geq 4$ we find that $2^a \geq 2^{R(k)-2} \geq R(k)$. □

Definition 1.10. For $k \in \mathbf{Z}^+$ the *height* of k is $h(k) = \min\{s : \lambda^s(k) = 1\}$.

Checking small cases we find: $h(k) = 0 \iff k = 1$, $h(k) = 1 \iff k = 2$, and $h(k) = 2 \iff k = 3, 4, 6, 8, 12$ or 24.

Corollary 1.11. If $a_j \in \mathbf{Z}^+$, then the towers $a_1 \uparrow a_2 \uparrow \cdots \uparrow a_{h(k)} \uparrow c$ reduce to the same value in $\mathbf{Z}/k\mathbf{Z}$, for every $c > 1$. Consequently, $a_1 \uparrow a_2 \uparrow \cdots \uparrow a_s \uparrow x \pmod{k}$ is independent of the value of $x \in \mathbf{Z}^+$, provided $s > h(k)$.

Proof. If $a_j = 1$ for some $j \leq h(k)$, the result is trivial, so assume all $a_j \geq 2$. Compare two such towers differing only in the top entries $a_{h(k)+1} = c$ by checking the conditions in (1.9) when $s = h(k) + 1$. They all hold provided $c \geq 2$. The second statement follows using $c = a_{h(k)+1} \uparrow \cdots \uparrow a_s \uparrow x$. □

Therefore, for any any sequence $\{a_j\}$ in $\mathbf{Z}^+$ and $k \in \mathbf{Z}^+$, the sequence of "partial powers" $\mathrm{E}_{i=1}^{s} a_i$ becomes stable (mod k) as s increases; all terms with $s > h(k)$ are congruent (mod k).

2. The sequences $n \uparrow\uparrow t$ (mod k).

Define the double-arrow $n \uparrow\uparrow t$ to be $\mathrm{E}_{i=1}^{t}(n)$, an exponential ladder of t n's. Then $n \uparrow\uparrow 0 = 1$, $n \uparrow\uparrow 1 = n$, $n \uparrow\uparrow 2 = n^n$, etc. This is part of the arrow notation as defined in Knuth (1976).

For a fixed modulus k, Hampel (1955) showed that the sequence $1^1, 2^2, 3^3, \ldots$ (mod k) is eventually periodic and determined its minimal period. In this section we generalize that result, showing for any $t \geq 0$, the sequence $1 \uparrow\uparrow t$, $2 \uparrow\uparrow t$, $3 \uparrow\uparrow t, \ldots$ is eventually periodic (mod k), and computing its minimal period, $L_t(k)$.

For fixed k and n, the sequence n, n^n, n^{n^n}, $n \uparrow\uparrow 4, \ldots$ eventually becomes constant (mod k). In fact, Corollary 1.11 implies:

$$n \uparrow\uparrow t \equiv n \uparrow\uparrow (t+1) \pmod{k} \quad \text{whenever } t > h(k).$$

The "stable value" $\overline{\alpha}_k(n)$ of this sequence $n \uparrow\uparrow t$ (mod k) is a well defined element of $\mathbf{Z}/k\mathbf{Z}$. However, it's best to define a positive integer representing this value, since we will also use it as an exponent.

Definition 2.1. For $k, n \in \mathbf{Z}^+$ let $\alpha_k(n) = n \uparrow\uparrow (1 + h(k))$. This is defined recursively by: $\alpha_1(n) = n$ and $\alpha_k(n) = n \uparrow \alpha_{\lambda(k)}(n)$ for every $k \geq 2$.

Then $\alpha_k(n) \equiv n\!\uparrow\!\uparrow\! t \pmod{k}$ for every $t > h(k)$, and we may consider this value in $\mathbf{Z}/k\mathbf{Z}$ as the "infinite tower" of exponents:

$$\alpha_k(n) \;\equiv\; n^{n^{n^{\cdot^{\cdot^{\cdot}}}}} \pmod{k}.$$

Corollary 2.2. If $k, n \in \mathbf{Z}^+$ then $x = \alpha_k(n)$ satisfies $x \equiv n^x \pmod{k}$.

Proof. With $t = 1 + h(k)$, Corollary 1.11 implies $x = n\!\uparrow\!\uparrow\! t \equiv n\!\uparrow\!\uparrow\!(t+1) \equiv n\!\uparrow\!(n\!\uparrow\!\uparrow\! t) = n^x \pmod{k}$. □

Let's examine a few numerical cases. Table 1 lists the sequences $\alpha_k(n)$ reduced to their least nonnegative residues modulo k, for the first few values of k and n.

$k \setminus^n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	(1	0)	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3	(1	1	0	1	2	0)	1	1	0	1	2	0	1	1	0	1	2	0	1	1	0	1	2
4	(1	0	3	0)	1	0	3	0	1	0	3	0	1	0	3	0	1	0	3	0	1	0	3
5	(1	1	2	1	0	1	3	1	4	0	1	1	3	1	0	1	2	1	4	0)	1	1	2
6	(1	4	3	4	5	0)	1	4	3	4	5	0	1	4	3	4	5	0	1	4	3	4	5
7	(1	2	6	4	3	1	0	1	1	4	2	1	6	0	1	2	5	1	5	1	0	1	4
8	(1	0	3	0	5	0	7	0)	1	0	3	0	5	0	7	0	1	0	3	0	5	0	7
9	(1	7	0	4	2	0	7	1	0	1	5	0	4	4	0	7	8	0)	1	7	0	4	2

TABLE 1. The (k,n)-entry is $\alpha_k(n) \pmod{k}$.

Here k indexes the rows and n indexes the columns. Parentheses indicate the first repeating block of each sequence.

As one example let's calculate the residue of $\alpha_7(5) \pmod{7}$. First check that $h(7) = 3$ (since $\lambda(7) = 6$, $\lambda^2(7) = 2$ and $\lambda^3(7) = 1$). By definition, $\alpha_7(5) = 5\!\uparrow\!\uparrow\! 4 = 5^{5^{5^5}}$, a number of more than $2 \cdot 10^{17}$ digits. To reduce it modulo 7 we first compute that $5\!\uparrow\!\uparrow\! 3 \equiv 5^{5^5} \equiv (-1)^{5^5} \equiv -1 \equiv 5 \pmod{6}$. Conclude from (1.7) that $\alpha_7(5) \equiv 5^5 \equiv 3 \pmod{7}$. Further values for $k = 7$ appear in Table 2 below. These calculations suggest that the sequence $\alpha_k(n) \pmod{k}$ is always periodic (with no tail). The minimal periods $L(k)$ are: $L(1) = 1$, $L(2) = 2$, $L(3) = 6$, $L(4) = 4$, $L(5) = 20$, $L(6) = 6$, $L(7) = 42$, $L(8) = 8$, $L(9) = 18$. Our goal is to find a simple formula for these periods.

Proposition 1.9 shows that the sequences $\{n\!\uparrow\!\uparrow\! t \pmod{k}\}$ are eventually periodic and provides natural candidates for their periods.

Lemma 2.3. Suppose $k > 0$ is given and let $L = \operatorname{lcm}\{k, \lambda(k), \lambda^2(k), \ldots, \lambda^{t-1}(k)\}$, the least common multiple.

If $t \geq 2$ and integers a, b satisfy $a, b \geq R(\lambda^{t-2}(k))$ then:

$$a \equiv b \pmod{L} \quad \text{implies} \quad a\!\uparrow\!\uparrow\! t \equiv b\!\uparrow\!\uparrow\! t \pmod{k}.$$

Proof. If $a \equiv 1$ or $b \equiv 1 \pmod{k}$ the conclusion is trivial, so we may assume $a, b \geq 2$. By hypothesis, $a \equiv b \pmod{\lambda^{r-1}(k)}$ for $r = 1, 2, \ldots, t$. The implication now follows from Proposition 1.9. □

Definition 2.4. For $k, t \in \mathbf{Z}^+$, let $L_t(k)$ be the minimal period of the eventually periodic sequence $\{n\!\uparrow\!\uparrow\! t \pmod{k}\}$.

Let $L(k)$ be the minimal period of the periodic sequence $\{\alpha_k(n) \pmod{k}\}$.

Observe that (1.11) implies $L_t(k) = L(k)$ whenever $t \geq h(k)$. Also $L_1(k) = k$ for all k. Moreover, by (2.3), $L_t(k)$ divides $\operatorname{lcm}\{k, \lambda(k), \lambda^2(k), \ldots, \lambda^{t-1}(k)\}$, since any period is a multiple of the minimal period.

Theorem 2.5. $L_t(k) = \operatorname{lcm}\{k, \lambda(k), \lambda^2(k), \dots, \lambda^{t-1}(k)\}$.

The proof of this theorem is preceded by several lemmas. Our strategy is to compute $L_t(k)$ when k is a prime power, then to glue these formulas together using the next lemma.

Lemma 2.6. (i) If $d \,|\, k$ then $L_t(d) \,|\, L_t(k)$.
(ii) $L_t\big(\operatorname{lcm}\{k_1, k_2\}\big) = \operatorname{lcm}\{L_t(k_1), L_t(k_2)\}$.
(iii) $\lambda^s(\operatorname{lcm}\{a, b\})$ divides $\operatorname{lcm}\{\lambda^s(a), \lambda^s(b)\}$.

Proof. (i) If $a \equiv b \pmod{L_t(k)}$ and a, b are large then $a \uparrow\uparrow t \equiv b \uparrow\uparrow t \pmod{k}$. Then if $d \mid k$, the sequence $\{n \uparrow\uparrow t \pmod{d}\}$ has $L_t(k)$ as a period. Hence the minimal period $L_t(d)$ divides $L_t(k)$.

(ii) Let $l = \operatorname{lcm}\{k_1, k_2\}$ and $m = \operatorname{lcm}\{L_t(k_1), L_t(k_2)\}$. Part (i) implies that $m \mid L_t(l)$. Conversely suppose $a \equiv b \pmod{m}$ and a, b are large. Then $a \equiv b \pmod{L_t(k_j)}$, implying $a \uparrow\uparrow t \equiv b \uparrow\uparrow t \pmod{k_j}$ for $j = 1, 2$. Then the congruence holds $\pmod{l}$, and the minimal period $L_t(l)$ divides m.

(iii) This property of λ follows by repeated application of (1.6)(2). □

Lemma 2.7. If p is prime then $p^m \,|\, L_t(p^m)$.

Proof. We may assume $t \geq 2$. It is easy to check that $p \mid L_t(p)$, since $n \uparrow\uparrow t \equiv 0 \pmod{p}$ iff $n \equiv 0 \pmod{p}$. Suppose $m > 1$. By induction $p^{m-1} \mid L_t(p^{m-1})$ so it also divides $L_t(p^m)$. Then $L_t(p^m) = p^{m-1}y$ for some y, and we want to prove $p \,|\, y$. By definition of L_t we have $(n + p^{m-1}y) \uparrow\uparrow t \equiv n \uparrow\uparrow t \pmod{p^m}$ whenever $n \geq R(\lambda^{t-2}(p^m))$. We use $n = 1 + p^m$, which does satisfy that inequality. Setting $r = (1 + p^m + p^{m-1}y) \uparrow\uparrow (t-1)$, the congruence becomes:

$$(1 + p^{m-1}y)^r \equiv (1 + p^m + p^{m-1}y) \uparrow\uparrow t \equiv (1 + p^m) \uparrow\uparrow t \equiv 1 \pmod{p^m}.$$

The binomial theorem then implies $1 + rp^{m-1}y \equiv 1 \pmod{p^m}$, so that $ry \equiv 0 \pmod{p}$. Since $r \equiv 1 \pmod{p}$, we get $p \,|\, y$ as claimed. □

Lemma 2.8. If p is prime and $t \geq 2$ then $L_{t-1}(p-1) \,|\, L_t(p)$.

Proof. For $\ell = L_t(p)$, we have $(n + \ell) \uparrow\uparrow t \equiv n \uparrow\uparrow t \pmod{p}$, for every large n. Since $p \,|\, \ell$ we find:

$$n \uparrow ((n + \ell) \uparrow\uparrow (t-1)) \equiv (n + \ell) \uparrow\uparrow t \equiv n \uparrow\uparrow t \equiv n \uparrow (n \uparrow\uparrow (t-1)) \pmod{p},$$

provided $n \geq R(\lambda^{t-2}(p))$. Suppose g is a generator of the group $\mathbf{U}_p$. Then for any large n with $n \equiv g \pmod{p}$, the previous congruence implies:

$$(n + \ell) \uparrow\uparrow (t-1) \equiv n \uparrow\uparrow (t-1) \pmod{p-1}. \tag{*}$$

Consequently, (*) holds for any large n of the form $n = g + px + wy$, where $w = L_{t-1}(p-1)$. Note that w and p are coprime, since w divides $\operatorname{lcm}\{p-1, \lambda(p-1), \dots\}$. Therefore, congruence (*) holds for all large integers n, so that the minimal period w must divide ℓ. □

Lemma 2.9. If p is prime, and $t \geq 2$, then:

$$\operatorname{lcm}\{p^m, \lambda(p^m), \dots, \lambda^{t-1}(p^m)\} = \operatorname{lcm}\{p^m, p-1, \lambda(p-1), \dots, \lambda^{t-2}(p-1)\}.$$

Proof. If $p = 2$ both sides equal 2^m. Suppose p is odd. Since $(p-1) \mid \lambda(p^m)$, (1.6)(1) implies $\lambda^{r-1}(p-1) \,|\, \lambda^r(p^m)$, and the right side divides the left. To prove: $\lambda^r(p^m)$ divides the right side, whenever $0 \leq r < t$. This is easy for $r = 0, 1$, so assume $r > 1$ and use induction. Since $\lambda^r(p^m) = \lambda^{r-1}(p^{m-1}(p-1))$ divides

$\operatorname{lcm}\{\lambda^{r-1}(p^m), \lambda^{r-1}(p-1)\}$, by (2.6)(iii), we may apply the induction hypothesis to complete the proof. □

Proof of Theorem 2.5. We prove this statement by induction on k. The formula for $k = 1$ is trivial, so we assume $k > 1$ and that the formula for $L_t(a)$ holds true for every $a < k$.

First suppose $k = p^m$ is a prime power. We want to prove that $L_t(p^m)$ equals the quantity in Lemma 2.9, which we call M here. As mentioned after (2.4), $L_t(p^m)$ divides M. By induction, $L_{t-1}(p-1) = \operatorname{lcm}\{p-1, \lambda(p-1), \dots, \lambda^{t-2}(p-1)\}$, so that $M = \operatorname{lcm}\{p^m, L_{t-1}(p-1)\}$. The fact that M divides $L_t(p^m)$ now follows from (2.7), (2.8) and (2.6)(i). Hence $L_t(p^m) = M$.

Proceeding by induction for arbitrary k, we may assume that $k > 1$ is not a prime power. Then there is a factorization $k = ab$ where a, b are coprime and $a, b < k$. As noted before, $L_t(k)$ divides $\operatorname{lcm}\{k, \lambda(k), \dots, \lambda^{t-1}(k)\}$. Since $k = ab$, (2.6)(iii) implies that this divides $\operatorname{lcm}\{a, b, \lambda(a), \lambda(b), \dots, \lambda^{t-1}(a), \lambda^{t-1}(b)\}$. Apply the induction hypothesis to see that this quantity equals $\operatorname{lcm}\{L_t(a), L_t(b)\}$, which equals $L_t(ab) = L_t(k)$ by (2.6)(ii), since a, b are coprime. Then all the terms in this divisor chain are equal and the Theorem follows. □

Corollary 2.10. (1) If p is prime then $L_t(p^m) = \operatorname{lcm}\{p^m, L_{t-1}(p-1)\}$.
(2) $L_t(k) = \operatorname{lcm}\{k, L_{t-1}(\lambda(k))\} = \operatorname{lcm}_{p|k}\{k, L_{t-1}(p-1)\}$.

Proof. By this notation we mean that if $k = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$ is the prime factorization of k then $L_t(k) = \operatorname{lcm}\{k, L_{t-1}(p_1 - 1), \dots, L_{t-1}(p_s - 1)\}$. These formulas follow from (2.9) and Theorem 2.5. □

Corollary 2.11. The period $L(k)$ of the sequence $\overline{\alpha}_k(0), \overline{\alpha}_k(1), \overline{\alpha}_k(2), , \dots$ in $\mathbf{Z}/k\mathbf{Z}$ has the following properties:

(1) $$L(k) = \operatorname{lcm}\{k, \lambda(k), \lambda^2(k), \dots\}. \\ = \operatorname{lcm}_{p|k}\{k, L(p-1)\}$$

(2) If $d \,|\, k$ then $L(d) \,|\, L(k)$. Moreover, $L\big(\operatorname{lcm}\{a, b\}\big) = \operatorname{lcm}\{L(a), L(b)\}$. $L(mn) = \operatorname{lcm}\{mn, L(m), L(n)\}$.
(3) The periods $k = L_1(k), L_2(k), L_3(k), \dots, L(k)$ form a divisor chain (i.e. each term divides the next).
(4) $L\big(\lambda(k)\big)$ divides $L(k)$.
(5) $L(L(k)) = L(k)$.
(6) $L(k) = k \iff \lambda(k) \,|\, k \iff$ for prime p, $p \,|\, k$ implies $(p-1) \,|\, k$.

Proof. (1) Use Theorems 2.5 and 2.10, noting that $L(k) = L_t(k)$ whenever $t \geq h(k)$. The other parts follow from (1). For instance, for (6) note that (1) implies: $L(k) = k$ if and only if every $\lambda^r(k) \,|\, k$. By (1.6)(1), that is equivalent to: $\lambda(k) \,|\, k$. The formula for $\lambda(k)$ in (1.6) implies that this occurs exactly when $(p-1) \,|\, k$ for every prime factor p of k. □

The sequence $\alpha_k(n) \pmod{k}$ was viewed as a mapping $\overline{\alpha}_k : \mathbf{Z}^+ \to \mathbf{Z}/k\mathbf{Z}$. Knowing the periodicity we re-interpret it (with some abuse of notation) as a map

$$\overline{\alpha}_k : \mathbf{Z}/L(k)\mathbf{Z} \to \mathbf{Z}/k\mathbf{Z}.$$

This observation explains how to make sense of $\overline{\alpha}_k(n)$ for negative values of n.

Proposition 2.12. (i) $\overline{\alpha}_k(0) = 0$ and $\overline{\alpha}_k(-1) = -1$.
(ii) If n is even then $\overline{\alpha}_k(-n) = \overline{\alpha}_k(n)$.
(iii) If $n \in \mathbf{U}_{L(k)}$ is a unit, then $\overline{\alpha}_k(-n) = -\overline{\alpha}_k(n^{-1})$.

Proof. Assume $k > 1$ so that $L = L(k)$ is even. (i) Note that $\overline{\alpha}_k(-1) = \overline{\alpha}_k(L-1) = (-1)^s$ in $\mathbf{Z}/k\mathbf{Z}$, where $s = a_{\lambda(k)}(L-1)$ is odd.

(ii) Induct on k. By the periodicity we may assume $0 \le n < L$. Then $\overline{\alpha}_k(-n) \equiv \alpha_k(L-n) \equiv (L-n)^s \equiv (-n)^s \pmod{k}$, where $s = \alpha_{\lambda(k)}(L-n)$. Since n and L are even, s is even and $\overline{\alpha}_k(-n) \equiv n^s \pmod{k}$. Since L is a multiple of $L(\lambda(k))$, we have $s \equiv \overline{\alpha}_{\lambda(k)}(-n) \pmod{\lambda(k)}$. Applying the induction hypothesis we find $s \equiv \alpha_{\lambda(k)}(n) \pmod{\lambda(k)}$ and therefore $\overline{\alpha}_k(-n) \equiv \overline{\alpha}_k(n) \pmod{k}$, as claimed.

(iii) Using a similar strategy (but with less detail), we have

$$\overline{\alpha}_k(n^{-1}) \equiv n^{-1}\!\uparrow\! s \equiv n\!\uparrow\!(-s) \pmod{k},$$

where $s \equiv \overline{\alpha}_{\lambda(k)}(n^{-1}) \pmod{\lambda(k)}$. By induction $s \equiv -\overline{\alpha}_{\lambda(k)}(-n) \pmod{\lambda(k)}$. Then since n is odd, $\overline{\alpha}_k(n^{-1}) \equiv n\!\uparrow\!\overline{\alpha}_{\lambda(k)}(-n) \equiv -\overline{\alpha}_k(-n) \pmod{k}$. □

It's interesting to look for patterns in tables of values of $\overline{\alpha}_k(n)$. For example, here are the values of $\overline{\alpha}_7(n)$ arranged in rows of seven. The period is $L(7) = 42$.

0	1	2	6	4	3	1
0	1	1	4	2	1	6
0	1	2	5	1	5	1
0	1	4	1	4	2	6
0	1	1	3	4	6	1
0	1	2	4	1	2	6

TABLE 2. $\overline{\alpha}_7(n)$ for $n = 0, 1, \dots, 41$.

A number of patterns of ±1's can be observed from such charts. The simplest ones are easily explained.

Proposition 2.13. Let p be an odd prime, and suppose $n \not\equiv 0 \pmod{p}$.
(i) If $n \equiv 1 \pmod{p}$ then $\alpha_p(n) \equiv 1 \pmod{p}$.
If $n \equiv -1 \pmod{p}$ then $\alpha_p(n) \equiv (-1)^n \pmod{p}$.
(ii) If $p \nmid n$ and each prime factor of $p-1$ divides n, then $\alpha_p(n) \equiv 1 \pmod{p}$.

Proof. $\alpha_p(n) = n^s$ where $s = \alpha_{p-1}(n) \equiv n^t \pmod{p-1}$, for some large t. (i) Easy. (ii) Since t is large, $(p-1) \,|\, n^t = s$ and the claim follows. □

This frequent occurrence of ±1's doesn't happen for every value of k. In the next section we will prove that when $L(k) = k$, the value 1 occurs only once in each period of $\alpha_k(n) \pmod{k}$. For example, since $L(7) = 42$ we know from Corollary 2.11(5) that $L(42) = 42$. Here is a table of the values of $\overline{\alpha}_{42}(n)$, arranged in rows of seven. Note that these values induce those of $\overline{\alpha}_7(n)$ after reduction (mod 7).

3. Values occurring in the sequences.

Which values in $\mathbf{Z}/k\mathbf{Z}$ are assumed by the sequence $\overline{\alpha}_k(n)$? That is, for which $a \in \mathbf{Z}^+$ does there exist n with $\alpha_k(n) \equiv a \pmod{k}$? For example, Table 1 shows

0	1	16	27	4	17	36
7	22	15	4	23	36	13
28	15	16	5	36	19	22
21	22	11	36	25	16	27
28	29	36	31	4	27	22
35	36	37	4	15	16	41

Table 3. $\overline{\alpha}_{42}(n)$ for $n = 0, 1, \ldots, 41$.

that the sequence $\alpha_k(n)$ assumes all the values in $\mathbf{Z}/k\mathbf{Z}$ when $k = 2, 3, 5, 7$. However, when $k = 4, 6, 8, 9$ some values are missed. An easy argument settles the question when k is a prime, or more generally when k and $\lambda(k)$ have no prime factors in common.

Lemma 3.1. Suppose k and $\lambda(k)$ are coprime. For any $t \geq 1$ and any $a \in \mathbf{Z}$, there exists n satisfying $n \uparrow\uparrow t \equiv a \pmod{k}$.

Proof. If $t = 1$ the claim is trivial, so assume $t \geq 2$. Note that $R(k) = 1$. By the Chinese Remainder Theorem there exists $n \in \mathbf{Z}^+$ such that $n \equiv a \pmod{k}$ and $n \equiv 1 \pmod{\lambda(k)}$. Then $n \uparrow\uparrow t = n \uparrow n^m$ where $m = n \uparrow\uparrow (t-2)$. Corollary 1.7 implies: $n \uparrow\uparrow t = n \uparrow n^m \equiv a \uparrow 1 \equiv a \pmod{k}$, . □

Define the map $E_t : \mathbf{Z}^+ \to \mathbf{Z}/k\mathbf{Z}$ by $E_t(n) = n \uparrow\uparrow t$. It is not always surjective, but we will show that every E_t is at least surjective on units.

Since E_t is eventually periodic with period $L = L_t(k)$, we can restrict to values $n \geq R(k)$ to get an induced map $\mathbf{Z}/L\mathbf{Z} \to \mathbf{Z}/k\mathbf{Z}$. Since $L \mid L(k)$ we can use the possibly larger domain $\mathbf{Z}/L(k)\mathbf{Z}$ for all values of t. Then E_t induces a map

$$\overline{E}_t : \mathbf{Z}/L(k)\mathbf{Z} \ \to \ \mathbf{Z}/k\mathbf{Z}, \text{ which restricts to a map } \quad \mathbf{U}_{L(k)} \to \mathbf{U}_k.$$

Here is a key observation: When c is an exponent coprime to $\lambda(k)$ then: $n^c \equiv 1 \pmod{k}$ implies $n \equiv 1 \pmod{k}$. Consequently,

$$\text{if } x, y \in \mathbf{U}_k \text{ then: } \ x^c \equiv y^c \pmod{k} \implies x \equiv y \pmod{k}.$$

Proposition 3.2. Suppose $\lambda(k) \mid k$ so that $k = L(k)$. Then for every t, the map $\overline{E}_t : \mathbf{U}_k \to \mathbf{U}_k$ is bijective.

Proof. Since $\mathbf{U}_k$ is a finite set it suffices to prove $\overline{E}_t$ is injective. The case $t = 1$ is trivial so assume $t \geq 2$. The initial cases $k = 1, 2$ are also easy, so we may assume $k > 2$ and use induction on k. From $\lambda(k) \mid k$ we know $\lambda(\lambda(k)) \mid \lambda(k)$ and the induction hypothesis implies $\overline{E}_t : \mathbf{U}_{\lambda(k)} \to \mathbf{U}_{\lambda(k)}$ is injective. Suppose $x, y \in \mathbf{U}_k$ and $E_t(x) \equiv E_t(y) \pmod{k}$. Then this congruence holds (mod $\lambda(k)$) so that $x \equiv y \pmod{\lambda(k)}$, by induction. Since $L_{t-1}(\lambda(k)) = \lambda(k)$ by (2.11) we find that $E_{t-1}(x) \equiv E_{t-1}(y) \pmod{\lambda(k)}$. Letting $c = E_{t-1}(x)$ we have $x^c \equiv E_t(x) \equiv E_t(y) \equiv y^c \pmod{k}$. From the key observation above we conclude that $x \equiv y \pmod{k}$. □

Corollary 3.3. For any k, the restriction $\overline{E}_t : \mathbf{U}_{L(k)} \to \mathbf{U}_k$ is surjective. In particular, the map $\overline{\alpha}_k : \mathbf{Z}^+ \to \mathbf{Z}/k\mathbf{Z}$ induces a surjective map $\overline{\alpha}_k : \mathbf{U}_{L(k)} \to \mathbf{U}_k$.

Proof. Let $a \in \mathbf{U}_k$. Since $k \mid L(k)$ we can choose $b \in \mathbf{U}_{L(k)}$ with $b \equiv a \pmod{k}$. Since $L(L(k)) = L(k)$ by (2.11), Proposition 3.2 provides $n \in \mathbf{U}_{L(k)}$ with $\overline{E}_t(n) \equiv b \pmod{L(k)}$. Reducing this congruence shows that $\overline{E}_t(n) \equiv a \pmod{k}$. The final statement follows since $\alpha_k(n) \equiv E_t(n) \pmod{k}$ whenever $t \geq h(k)$. □

Here is an alternative approach to the map $\overline{\alpha}_k$. If $c = \alpha_k(n)$ then by (2.2), $n^c \equiv c \pmod{k}$. We can solve for n to get $n \equiv c^{1/c} \pmod{k}$, provided that fractional exponent makes sense. Recall that for $c^s \pmod{k}$, the exponent s behaves modulo $\lambda(k)$. If s is a unit (mod $\lambda(k)$), choose $t \in \mathbf{Z}^+$ with $t \equiv s^{-1} \pmod{\lambda(k)}$. Then for $c \in \mathbf{U}_k$:

$x \equiv c^t \pmod{k}$ is the unique solution to $x^s \equiv c \pmod{k}$.

Therefore $c^{1/c} \pmod{k}$ makes sense whenever $c \in \mathbf{Z}^+$ is coprime to both k and $\lambda(k)$. Since $\operatorname{lcm}\{k, \lambda(k)\}$ divides $L(k)$, we obtain a well-defined map $\delta : \mathbf{U}_{L(k)} \to \mathbf{U}_k$ given by $\delta(x) = x^{1/x}$. This proves the following result, related to (3.2).

Proposition 3.4. Suppose $\lambda(k) \,|\, k$ so that $L(k) = k$. The map $\overline{\alpha}_k : \mathbf{U}_k \to \mathbf{U}_k$ is bijective with inverse map δ.

Proposition 3.2 can be improved by allowing certain non-units. We will state our best result along these lines.

Theorem 3.5. Define $W_k = \{n \in \mathbf{Z}/k\mathbf{Z} \ : \ \gcd(n, k, \lambda(k)) = 1\}$. Then for every t, the restriction $\overline{E}_t : W_{L(k)} \to W_k$ is surjective.

When $\lambda(k) \,|\, k$ the method used in Proposition 3.4 can extended to W_k. However the full theorem does not seem to follow easily from that case. Our proof of the theorem starts with the idea in Lemma 3.1 and uses induction, building up k one prime at a time. It is too long to include here.

We have not found any other useful conditions to ensure that a occurs as a value of $\overline{\alpha}_k(n)$. In the other direction there is one easy condition for the number a to be a missing value for the sequences (mod k).

Proposition 3.6. Suppose a, k, and t are given and $t \geq 2$, and suppose there exists large x with $E_t(x) \equiv a \pmod{k}$. If $p^d \,|\, k$ where p^d is a prime power, then either $p \nmid a$ or $p^d \,|\, a$.

Proof. Suppose $p \,|\, a$. Since $E_t(x) \equiv a \pmod{p^d}$ we see that $p \,|\, x$. Since x is large it follows that $a \equiv x \uparrow E_{t-1}(x) \equiv 0 \pmod{p^d}$. □

4. p-adic interpretations.

In this section we assume the reader has some knowledge of the ring $\mathbf{Z}_p$ of p-adic integers. However, to keep the presentation more elementary we include a review of some of the definitions and basic properties. More details appear in various texts like Borevich-Shafarevich (1966) or Koblitz (1977).

Let p be a fixed prime number. If $n \geq m$ there is a natural reduction map $\pi_{n,m} : \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^m\mathbf{Z}$. The ring $\mathbf{Z}_p$ of p-adic integers is the projective limit $\varprojlim(\mathbf{Z}/p^n\mathbf{Z})$ relative to these maps $\pi_{n,m}$. An element $c \in \mathbf{Z}_p$ is defined to be a sequence $(c_1, c_2, c_3, \dots)$ where $c_n \in \mathbf{Z}/p^n\mathbf{Z}$ satisfying the following "coherence" condition: if $n \geq m$ then $\pi_{n,m}(c_n) = c_m$. With component-wise addition and multiplication, $\mathbf{Z}_p$ becomes an integral domain. The ring of integers $\mathbf{Z}$ is embedded as a subring of $\mathbf{Z}_p$ by viewing $k \in \mathbf{Z}$ as a constant sequence $(k, k, \dots)$ in $\mathbf{Z}_p$. Then $u \in \mathbf{Z}_p$ is a p-adic unit (i.e. u is invertible) iff $u \not\equiv 0 \pmod{p}$, and every nonzero $c \in \mathbf{Z}_p$ factors uniquely as $c = p^m u$ for some $m \geq 0$ in $\mathbf{Z}$ and some p-adic unit $u \in \mathbf{Z}_p^*$. Let $\operatorname{ord}(c)$ be that exponent m.

Define the p-adic absolute value on $\mathbf{Z}_p$ by setting $|0|_p = 0$ and if $c \neq 0$:

$$|c|_p = p^{-\mathrm{ord}(c)}.$$

This absolute value satisfies several rules:

$$|a|_p \leq 1, \text{ with equality} \iff a \text{ is a unit in } \mathbf{Z}_p;$$
$$|ab|_p = |a|_p \cdot |b|_p \quad \text{and} \quad |a+b|_p \leq \max\{|a|_p, |b|_p\}.$$

That last inequality is stronger than the triangle inequality $|a+b|_p \leq |a|_p + |b|_p$. This absolute value makes $\mathbf{Z}_p$ into a complete metric space (every Cauchy sequence converges), with $\mathbf{Z}^+$ as a dense subset.

Elements of $\mathbf{Z}_p$ are often viewed as series: every $c \in \mathbf{Z}_p$ can be expressed as a "power series" $c = a_0 + a_1 p + a_2 p^2 + \dots$, where every $a_n \in \{0, 1, \dots, p-1\}$. Every such power series $\sum a_n p^n$ (with $0 \leq a_n < p$) converges relative to the metric above.

Lemma 4.1. For any positive integers $b_1, b_2, b_3 \dots$, the iterated exponential $\mathop{\mathrm{E}}\limits_{j=1}^{\infty} b_j = b_1 \uparrow b_2 \uparrow b_3 \uparrow \dots$ converges in $\mathbf{Z}_p$.

Proof. Let $c_n = b_1 \uparrow b_2 \uparrow \dots \uparrow b_n$. By Corollary 1.11, if $s, t > h(p^m)$ then $c_s \equiv c_t \pmod{p^m}$, that is, $|c_s - c_t|_p < p^{-m}$. Then $\{c_n\}$ is a Cauchy sequence so its limit exists in $\mathbf{Z}_p$. □

Definition 4.2. If $n \in \mathbf{Z}^+$ define $\alpha(n) = a^{(p)}(n) = \mathop{\mathrm{E}}\limits_{j=1}^{\infty}(n)$ in $\mathbf{Z}_p$. We could also write this as: $\alpha(n) = n \uparrow\uparrow \infty$.

Since $\alpha(n) = n \uparrow n \uparrow n \uparrow \cdots$, it is natural to expect that $n^{\alpha(n)} = \alpha(n)$ in $\mathbf{Z}_p$. This fails when $p \mid n$, because in that case $\alpha(n) = 0$ in $\mathbf{Z}_p$. Difficulties arise even when $n \not\equiv 0 \pmod{p}$ because it's not clear how to define n^x for a p-adic integer x. The function $f(x) = n^x$ is defined for x in $\mathbf{Z}$, but it might have no continuous extension to the larger ring $\mathbf{Z}_p$. The next lemma shows that when $n \equiv 1 \pmod{p}$ there is no obstruction to extending the domain of $f(x) = n^x$ from $\mathbf{Z}^+$ to $\mathbf{Z}_p$.

Lemma 4.3. Suppose $a \in \mathbf{Z}_p$ and $|a-1|_p < 1$. Equivalently, $a \equiv 1 \pmod{p}$. Suppose $x, y \in \mathbf{Z}_p$.
(1) For $m \geq 1$, $x \equiv y \pmod{p^m}$ implies $x^p \equiv y^p \pmod{p^{m+1}}$.
(2) If $s, t \in \mathbf{Z}^+$ and $s \equiv t \pmod{p^m}$ then $a^s \equiv a^t \pmod{p^{m+1}}$.
(3) If $x \in \mathbf{Z}_p$, express $x = \lim\limits_{n\to\infty} x_n$ where $x_n \in \mathbf{Z}^+$, and define $a^x = \lim a^{x_n}$.
Then a^x is well defined, independent of the choice of the sequence $\{x_n\}$. Moreover, $f(x) = a^x$ defines a continuous function $\mathbf{Z}_p \to \mathbf{Z}_p$ satisfying:
(4) $a^{x+y} = a^x a^y$.
$a^x \equiv 1 \pmod{p}$ and $(a^x)^y = a^{xy}$.
$|a^x - a^y|_p \leq \frac{1}{p}|x-y|_p$.
(5) If $a, b \in \mathbf{Z}_p$ and $a \equiv b \equiv 1 \pmod{p}$ then $(ab)^x = a^x b^x$.

Proof Sketch. (1) Express $y = x + p^m t$ and use the binomial theorem. (2) By (1) we know $a^{p^m} \equiv 1 \pmod{p^{m+1}}$, and the claim follows. Statement (2) is equivalent to: $|a^s - a^t|_p \leq \frac{1}{p}|s-t|_p$. (3) If $\{x_n\}$ is convergent, then $\{a^{x_n}\}$ is a Cauchy sequence, so a^x is defined. Triangle inequalities yield the inequality in (4) and this helps show that a^x is independent of the choice of $\{x_n\}$. The remaining statements follow similarly. □

A more sophisticated approach to these ideas is to introduce p-adic exponential and logarithm functions and then define $a^x = \exp(x \log a)$. Details appear in Borevich-Shafarevich (1966) pp. 285-288 or Koblitz (1977) pp. 75-82. Since $\log(1+x)$ converges on the open unit ball, $\log(a)$ is defined only if $|a-1|_p < 1$. These two definitions of a^x coincide because they both are continuous extensions of $f(n) = a^n$ on $\mathbf{Z}^+$, which is dense in $\mathbf{Z}_p$.

The lemma implies that if $n \equiv 1 \pmod{p}$ and $f(x) = n^x$ then $f : \mathbf{Z}_p \to \mathbf{Z}_p$ is a contraction mapping: $|f(x) - f(y)|_p < \frac{1}{p}|x-y|_p$. The Banach fixed point theorem states that a contraction mapping f on a complete metric space has a unique fixed point, obtained as $\lim_{n\to\infty} f^n(c)$ for any initial point c. Then in our case, this process reflects ideas developed in earlier sections: the unique $\alpha \in \mathbf{Z}_p$ satisfying $\alpha = n^\alpha$ is obtained from the map $f(x) = n^x$ by choosing any $c \in \mathbf{Z}_p$ and taking the limit of the iterates $f(c) = n \uparrow c$, $ff(c) = n \uparrow n \uparrow c$, $fff(c) = n \uparrow n \uparrow n \uparrow c$, $\ldots$. This $\alpha = \alpha(n)$ is the *unique* solution $x \in \mathbf{Z}_p$ to $x = n^x$, in the case $n \equiv 1 \pmod{p}$.

Before considering cases when $n \not\equiv 1$, we note that another contraction map appears in Lemma 4.3(1). The map $g(x) = x^p$ satisfies: $|g(x) - g(y)|_p \le \frac{1}{p}|x-y|_p$. However, on closer examination we find that this g isn't a contraction on the whole space $\mathbf{Z}_p$, since that inequality fails if $x \not\equiv y \pmod{p}$. We can fix this by separating the metric space $\mathbf{Z}_p$ into p parts,

$$\mathcal{S}_b = \{k \in \mathbf{Z}_p : k \equiv b \pmod{p}\}.$$

Each $\mathcal{S}_b$ is a closed subspace of $\mathbf{Z}_p$, and $g(x) = x^p$ is a contraction sending $\mathcal{S}_b$ to itself. Consequently there is a unique value $\omega(b) \in \mathcal{S}_b$ satisfying $\omega(b)^p = \omega(b)$. The uniqueness implies that this value depends only on the residue $\bar{b} \in \mathbf{Z}/p\mathbf{Z}$. Since $\omega(0) = 0$ we ignore that case and consider ω as a map on the nonzero classes $\omega : (\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{Z}_p$. It's not hard to check that the image of ω is the group of $(p-1)^{\text{st}}$ roots of unity in $\mathbf{Z}_p$. This p-adic integer $\omega(b) = \lim\limits_{m\to\infty} b^{p^m}$ is the "Teichmüller representative" of the residue class $\bar{b}$.

When $n \not\equiv 1 \pmod{p}$ the function $f(k) = n^k$ on $\mathbf{Z}^+$ does not extend continuously to $\mathbf{Z}_p$. Instead there are $p-1$ continuous "branches", or partial extensions. Since $n^{p-1} \equiv 1 \pmod{p}$, the powers $(n^{p-1})^x$ are well defined for $x \in \mathbf{Z}_p$, by (4.3). We would like to take the $(p-1)^{\text{st}}$ root to define n^x, but there are several choices involved.

Following Koblitz (1977) p. 27, if $n \not\equiv 0 \pmod{p}$, define $\langle n \rangle = n/\omega(n) \in \mathbf{Z}_p$. Then $\langle n \rangle \equiv 1 \pmod{p}$ (so that $\langle n \rangle^x$ is well defined) and $\langle n \rangle^{p-1} = n^{p-1}$. We can now find continuous $(p-1)^{\text{st}}$ roots of $(n^{p-1})^x$ by setting $f(x) = \zeta \cdot \langle n \rangle^x$, where $\zeta \in \mathbf{Z}_p$ and $\zeta^{p-1} = 1$. For $k \in \mathbf{Z}^+$, this $f(k)$ equals n^k exactly when $\zeta = \omega(n)^k$. This leads to the definition

$$f_{n,b}(x) = \omega(n)^b \langle n \rangle^x, \quad \text{where } b \in \mathbf{Z}.$$

Then $f_{n,b} : \mathbf{Z}_p \to \mathbf{Z}_p$ is continuous, $f_{n,b}(x)^{p-1} = (n^{p-1})^x$ for all x, and $f_{n,b}(k) = n^k$ for every $k \in \mathcal{S}_b$. This is the unique function with those properties since $\mathcal{S}_b$ is dense in $\mathbf{Z}_p$. The number of different functions here is $o_p(n)$, since $f_{n,b}$ depends on $n^b \pmod{p}$.

Proposition 4.4. Suppose $n \in \mathbf{Z}^+$ and $p \nmid n$. Then $\alpha(n)$ is the unique fixed point of the map $f_{n,b}$ when $b = \alpha_{p-1}(n)$.

Proof. $f_{n,b}$ is a contraction since $|f_{n,b}(x) - f_{n,b}(y)|_p = |\langle n \rangle^x - \langle n \rangle^y|_p \le \frac{1}{p}|x-y|_p$. Therefore there is a unique fixed point in $\mathbf{Z}_p$. For any large t, $n \uparrow\uparrow t \equiv \alpha_{p-1}(n) \equiv b$

(mod $p-1$). Therefore $n\uparrow\uparrow t \in S_b$. Hence $E_{t+1}(n) = n\uparrow(n\uparrow\uparrow t) = f_{n,b}(n\uparrow\uparrow t)$. Now take the limit as $t \to \infty$. □

For every b the function $f_{n,b}$ has a unique fixed point in $\mathbf{Z}_p$. Generally, for $a, c \in \mathbf{Z}_p$ with $c \equiv 1 \pmod p$, the function $f(x) = a{\cdot}c^x$ is a contraction with a fixed point β. Then β/a is the fixed point of $g(y) = c^{ay}$, obtained as the limit $c^a\uparrow c^a\uparrow\cdots$.

As an application of (4.4) we consider the injectivity of α on $\mathbf{Z}^+$.

Proposition 4.5. The map $\alpha = \alpha^{(p)} : \mathbf{Z}^+ \to \mathbf{Z}_p$ sends every multiple of p to 0. On the other positive integers, $\alpha^{(p)}$ is injective.

Proof. If $p\,|\,n$ then $n\uparrow n\uparrow\ldots\uparrow n$ involves high powers of p so the limit is 0 in $\mathbf{Z}_p$. Note that if $c \neq 1$ and $|c-1|_p < 1$ then the map $g(x) = c^x$ is injective. (This follows from the p-adic logarithm, but there is a more elementary proof in the style of (4.3).)

Now suppose $n, m \in \mathbf{Z}^+$, $n, m \not\equiv 0 \pmod p$, and and $x = \alpha(n) = \alpha(m)$ in $\mathbf{Z}_p$. By (4.4), $x = f_{n,b}(x) = f_{m,c}(x)$ for some b, c. Then $x^{p-1} = (n^{p-1})^x = (m^{p-1})^x$ in $\mathbf{Z}_p$ and we find that $((nm^{-1})^{p-1})^x = 1$. With $c = (nm^{-1})^{p-1}$ we have $c \equiv 1$ (mod p) and $c^x = 1$. The injectivity mentioned above implies $c = 1$. But then $n^{p-1} = m^{p-1}$ in $\mathbf{Z}$, so that $n = m$. □

We have been considering towers of powers in $\mathbf{Z}_p$. However it is perhaps more natural to consider those limits without restricting to a single prime p. Whenever $d \mid k$ there is a natural reduction map $\pi_{k,d} : \mathbf{Z}/k\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$, and the projective limit makes sense: $\widehat{\mathbf{Z}} = \varprojlim(\mathbf{Z}/k\mathbf{Z})$. An element $\hat{c} \in \widehat{\mathbf{Z}}$ is defined to be a sequence $\hat{c} = (c_1, c_2, \ldots)$ with $c_k \in \mathbf{Z}/k\mathbf{Z}$ satisfying the "coherence" condition: if $d\,|\,k$ then $\pi_{k,d}(c_k) = c_d$. Unique factorization and the Chinese Remainder Theorem provide a ring isomorphism:

$$\widehat{\mathbf{Z}} \xrightarrow{\cong} \prod_p \mathbf{Z}_p\,,$$

where the direct product is taken over all primes p. Elements of $\widehat{\mathbf{Z}}$ can also be thought of as "profinite integers" as described using factorial representations in Lenstra's paper [17].

If $\{a_n\}$ is a sequence in $\mathbf{Z}^+$, then by (1.11), the numbers $c_n = a_1\uparrow a_2\uparrow\ldots\uparrow a_n$ define an element $\hat{c} = \mathop{\mathrm{E}}\limits_{j=1}^{\infty} a_j \in \widehat{\mathbf{Z}}$. In particular, for $n \in \mathbf{Z}^+$ we have an element $\widehat{\alpha}(n) = \mathop{\mathrm{E}}\limits_{j=1}^{\infty} n = n\uparrow n\uparrow n\uparrow\cdots$ in $\widehat{\mathbf{Z}}$, which induces the element $\alpha^{(p)}(n) \in \mathbf{Z}_p$ for every prime p. The domain of $\widehat{\alpha}$ can be enlarged to include all $\hat{n} \in \widehat{\mathbf{Z}}$ by just taking the limit of the maps $\overline{\alpha}_k : \mathbf{Z}/L(k)\mathbf{Z} \to \mathbf{Z}/k\mathbf{Z}$ defined in §2 to build $\widehat{\alpha} : \widehat{\mathbf{Z}} \to \widehat{\mathbf{Z}}$. That is, if $\hat{c} = (c_1, c_2, \ldots)$, we define $\widehat{\alpha}(\hat{c})$ by setting:

$$\widehat{\alpha}(\hat{c})_k = \overline{\alpha}_k(c_{L(k)}).$$

By (4.5) it follows that the restriction $\widehat{\alpha} : \mathbf{Z}^+ \to \widehat{\mathbf{Z}}$ is injective. However $\widehat{\alpha}$ is not injective on $\widehat{\mathbf{Z}}$. To see this, note that any $\hat{c} \in \widehat{\mathbf{Z}}$ is determined by its list of components $c^{(p)} \in \mathbf{Z}_p$. Define $\hat{c}$ by requiring $c^{(p)} = p$ for every p. Check that $\hat{c} \neq 0$ but $\widehat{\alpha}(\hat{c}) = 0$.

To extend our work with p-adic numbers, we would like to define exponential functions and consider their fixed points. Starting at the finite level, define an exponential map

$$\text{expon}_k : (\mathbf{Z}/k\mathbf{Z}) \times (\mathbf{Z}/\lambda(k)\mathbf{Z}) \to (\mathbf{Z}/k\mathbf{Z}) \quad \text{by:} \qquad \text{expon}_k(\overline{a}, \overline{b}) = \overline{a^b}.$$

This can be a bit confusing since b is a residue class (not an integer) and the value $\overline{a^b}$ corresponds to a term in the "cycle" part of the sequence $1, a, a^2, a^3, \dots$. For instance, when $k = 40$ the powers of 2 are: $1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 24,\ 8,\ 16, \dots$. Since $\lambda(40) = 4$, we find that:

$$\text{expon}_{40}(\overline{2}, \overline{1}) = \overline{2}^{\overline{1}} = \overline{32} \quad \text{in} \quad \mathbf{Z}/40\mathbf{Z},$$

since that's the term in the cycle corresponding to $1 \pmod 4$.

Now take the limit of those maps expon_k as $k \to \infty$, to obtain:

$$\text{expon} : \widehat{\mathbf{Z}} \times \widehat{\mathbf{Z}} \to \widehat{\mathbf{Z}}.$$

We can write $\text{expon}(\hat{a}, \hat{b})$ as $\hat{a}^{\hat{b}}$, but repeat the warning about interpretations. Although $\mathbf{Z}$ embeds as a subring of $\widehat{\mathbf{Z}}$, this exponential map isn't consistent with traditional exponents of integers. For example, 1 and 2 embed as constant sequences $\hat{1}, \hat{2}$ in $\widehat{\mathbf{Z}}$, but $\hat{2}^{\hat{1}}$ does not match 2^1 in $\mathbf{Z}$.

One interesting point is that this exponential map generalizes all the p-adic exponential maps, but without the concerns about convergence. The point is that defining a^x for $a \in \mathbf{Z}/p^m\mathbf{Z}$ requires the exponent x to live in $\mathbf{Z}/p^{m-1}(p-1)\mathbf{Z} \cong \mathbf{Z}/p^{m-1}\mathbf{Z} \times \mathbf{Z}/(p-1)\mathbf{Z}$. Ignoring the $(\mathbf{Z}/(p-1)\mathbf{Z})$-component of x leads to $p-1$ different branches of the exponential function. In $\widehat{\mathbf{Z}}$ those components are not ignored and that difficulty vanishes.

Not surprisingly, the analysis of functions on $\widehat{\mathbf{Z}}$ present various difficulties not arising in $\mathbf{Z}_p$. It should be interesting to investigate whether the exponential maps on $\widehat{\mathbf{Z}}$ are contractions relative to some nice metric, and whether $\widehat{\alpha}(n)$ is the unique fixed point of the function $f(\hat{x}) = n^{\hat{x}}$. We leave further development of this theory to the reader.

5. Some problems.

Here are a few open problems related to topics discussed above.

By (1.11) for given k every sequence $n,\ n^n,\ n^{n^n},\ n\uparrow\uparrow 4, \dots \pmod k$ becomes stable after at most $h(k) + 1$ steps.

Problem 5.1. How fast does the height function $h(k)$ grow?

The corresponding question for the φ-height has been studied. In analogy to Definition 1.10 let the φ-height be $h_\varphi(k) = \min\{s : \varphi^s(k) = 1\}$. In 1943 H. N. Shapiro [23] proved that $h_\varphi(k)$ has multiplicative properties and grows logarithmically.

Does $h(k)$ have the same order of magnitude as $h_\varphi(k)$?

See H. N. Shapiro [24] , Parnami [20] and Erdös and Graham [12] pp. 80-81 for related questions.

Rather than considering all n simultaneously, define a height for each n:

$$\ell_k(n) = \min\{t\ :\ E_t(n) \equiv E_{t+1}(n) \pmod k.$$

For given n, k, note that the sequence $E_t(n) \pmod k$ stabilizes after $\ell_k(n)$ steps:

Lemma 5.2. If $E_{t-1}(n) \equiv E_t(n) \pmod{k}$ then $E_t(n) \equiv E_{t+1}(n) \pmod{k}$.

Proof. To prove that $E_t(n) - E_{t-1}(n)$ divides $E_{t+1}(n) - E_t(n)$ for every n, check that $(n^a - a)\,|\,(n^b - b) \implies (n^{n^a} - n^a)\,|\,(n^{n^b} - n^b)$. □

Consequently, $\ell_k(n) \leq h(k)$. Since $\ell_k(n) = 1 + \ell_{o_k(n)}(n)$ it follows that if s and $L(k)$ are coprime then $\ell_k(n^s) = \ell_k(n)$.

Problem 5.3. Investigate $\ell_k(n)$. As n varies, how do the values $\ell_k(n)$ compare with $h(k)$?

Let $N_t(a \bmod k)$ be the number of solutions to $E_t(x) \equiv a \pmod{k}$, counted in one period. In (3.3) we proved that $N_t(a \bmod k) > 0$ whenever a is a unit. In some cases when $(\mathbf{Z}/k\mathbf{Z})^*$ is cyclic, there is an explicit formula for N_2. For instance, if p is an odd prime and a is coprime to p then:

$$N_2(a \bmod p^m) \;=\; \sum_{d \mid \frac{p-1}{r}} d\,\varphi(\tfrac{p-1}{d})\ ,$$

where $r = o_p(a)$. The proof involves choosing a generator g and counting x values by tabulating s, t such that $x \equiv g^t \pmod{p^m}$ and $x \equiv s \pmod{p^{m-1}(p-1)}$ such that $x^x \equiv g^{st} \equiv a \pmod{p^m}$. Details are omitted.

Problem 5.4. Given k, for which a is there a solution to $x^x \equiv a \pmod{k}$? How about $E_t(x) \equiv a \pmod{k}$? More generally, is there a simple formula for $N_t(a \bmod k)$? For these questions, we consider only those x lying in the cyclic part, $\mathbf{Z}/L_t(k)\mathbf{Z}$.

Most of the information derived so far about the image of E_t in $\mathbf{Z}/k\mathbf{Z}$ is independent of t. In addition to Lemma 5.2, we make another small observation relating these images for different t values:

$$\text{If } E_t(n) \equiv 1 \pmod{k} \quad \text{then} \quad E_{t+1}(n) \equiv 1 \pmod{k}.$$

To see this note that $(E_t(n) - 1) \mid (E_{t+1}(n) - 1)$ since $a\,|\,b \implies (n^a - 1)\,|\,(n^b - 1)$.

Problem 5.5. As t varies, how are the sets $\text{image}(E_t) \subset \mathbf{Z}/k\mathbf{Z}$ related?

Approximations to $\alpha(n) = \alpha^{(p)}(n) \in \mathbf{Z}_p$ can be easily computed, but not much is known about its algebraic properties. We note that $\alpha(n) \notin \mathbf{Q}$:

If $1 < n \in \mathbf{Z}^+$ and $p \nmid n$ then $\alpha(n)$ is irrational.

For if $\alpha(n) = r/s$ in lowest terms, then by (4.4), $(r/s)^{p-1} = (n^{p-1})^{r/s}$ in $\mathbf{Z}_p$. This implies $r^{(p-1)s} = n^{(p-1)r} s^{(p-1)s}$ in $\mathbf{Z}$. But that equation yields $s = 1$ and $r = n^r$, a contradiction.

Problem 5.6. For n as above, is $\alpha^{(p)}(n) \in \mathbf{Z}_p$ transcendental over the field $\mathbf{Q}$ of rational numbers?

For any sequence $\{a_1, a_2, a_3, \dots\}$ in $\mathbf{Z}^+$, the limit $\mathop{\mathrm{E}}\limits_{j=1}^{\infty} a_j \;=\; a_1^{a_2^{\cdot^{\cdot^{\cdot}}}}$ is a well-defined element in $\widehat{\mathbf{Z}}$, the ring of profinite integers. If $\{b_n\}$ is a different sequence in $\mathbf{Z}^+$, it can happen that $\mathop{\mathrm{E}}\limits_{j=1}^{\infty} a_j = \mathop{\mathrm{E}}\limits_{j=1}^{\infty} b_j$ in $\widehat{\mathbf{Z}}$. Examples are easy to produce when some a_i, b_j are allowed to equal 1. For instance:

$$2^{4^5} = 4^{2^{3^2}} \quad \text{and} \quad 9^{2^3} = 3^{2^{2^2}}.$$

Examples of such equalities seem to be harder to find with infinite towers.

Problem 5.7. Suppose $a_1, a_2, a_3, \dots$ and $b_1, b_2, b_3, \dots$ are sequences in $\mathbf{Z}^+$ and every $a_i, b_i \geq 2$. If $\mathop{\mathrm{E}}\limits_{j=1}^{\infty} a_j = \mathop{\mathrm{E}}\limits_{j=1}^{\infty} b_j$ in $\widehat{\mathbf{Z}}$, does it follow that every $a_i = b_i$?

References

[1] Joel Anderson, *Iterated exponentials*, Amer. Math Monthly. **111** (2004) pp. 668-679.

[2] I. N. Baker and P. J. Rippon, *A note on complex iteration*, Amer. Math. Monthly **92** (1985), pp. 501-504.

[3] G. R. Blakley and I. Borosh, *Modular arithmetic of iterated powers*, Comput. Math. Appl. **9** (1983) pp. 567-581.

[4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[5] N. Bromer, *Superexponentiation*, Math. Mag. **60** (1987) pp. 169-174.

[6] R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), pp. 232-238.

[7] R. Crocker, *On a new problem in number theory*, Amer. Math. Monthly **73** (1966) pp. 355-357.

[8] R. Crocker, *On residues of n^n*, Amer. Math. Monthly **76** (1969) pp. 1028-1029.

[9] A. C. Cunningham, *On hyper-even numbers and on Fermat's numbers*, Proc. London Math. Soc. (2) **5** (1907) pp. 237-274.

[10] Robert J. MacG. Dawson, *Towers of powers modulo m*, College. Math. J. **25** (1994) pp. 22-28.

[11] A. Ecker, *Comment on the note: "The congruence $a^{r+s} \equiv a^r$ (mod m)" by A. Livingston and M. L. Livingston*, Amer. Math. Monthly **87** (1980) pp. 811-814.

[12] P. Erdös and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographie no. 28 de L'Enseignement Mathmatique, Geneva, 1980.

[13] R. Hampel, *The length of the shortest period of rests of number n^n*, Ann. Polon. Math. **1** (1955) pp. 360-366.

[14] D. E. Knuth, *Coping with finiteness*, Science **194** (1976), pp. 1235-1242.

[15] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Math. vol. 58, Springer-Verlag, 1977.

[16] N. Koblitz, *p-adic Analysis: a Short Course on Recent Work*, London Math. Soc. Lecture Note Series v. 46, Cambridge Univ. Press, 1980.

[17] H. Lenstra, *Profinite Fibonacci numbers*, Nieuw Arch. Wiskd. (5) **6** (2005) 297-300.

[18] A. E. Livingston and M. L. Livingston, *The congruence $a^{r+s} \equiv a^r$ (mod m)*, Amer. Math. Monthly **85** (1978) pp. 97-100.

[19] H. Maurer, *Über die Funktion $x^{[x^{(x^{(\cdot^{\cdot^{\cdot}})})}]}$ für ganzzahliges Argument (Abundanzen)*, Mittheilungen der Mathematische Gesellschaft in Hamburg **4** (1901), pp. 33-50.

[20] J. C. Parnami, *On iterates of Euler's φ-function*, Amer. Math. Monthly **74** (1967) pp. 967-968.

[21] A. Schinzel and W. Sierpiński, *Sur les congruences $x^x \equiv c$ (mod m) et $a^x \equiv b$ (mod p)*, Collect. Math. 11 (1959) pp. 153-164.

[22] D. B. Shapiro, *Comment on problem 559*, Crux Math. **13** (1987) pp. 291-294.

[23] H. N. Shapiro, *An arithmetic mean arising from the ϕ function*, Amer. Math. Monthly **50** (1943) pp. 18-30.

[24] H. N. Shapiro, *On the iterates of a certain class of arithmetic functions*, Comm. Pure Appl. Math. **3** (1950) pp. 259-272.

[25] H. N. Shapiro, *Introduction to the Theory of Numbers*, John Wiley and Sons, 1983.

[26] W. Sierpiński, *Sur les puissances du nombre 2*, Ann. Soc. Polon. Math. **23** (1950) pp. 246-251.

[27] W. Sierpiński, *Sur la périodicité mod m de certaines suites infinies d'entiers*, Ann. Soc. Polon. Math. **23** (1950) pp. 252-258.

[28] D. Singmaster, *A maximal generalization of Fermat's theorem*, Math. Magazine **39** (1966) pp. 103-107.

[29] I. M. Vinogradov, *Elements of Number Theory*, Dover, 1954.

[30] Problem A - 4 in: *1985 Putnam Competition*, Math. Mag. **59** (1986) pp. 123-126.

[31] Problem 3 in: *Twentieth Annual U.S.A. Mathematical Olympiad*, Math. Mag. **65** (1992) pp. 205 - 206.

Department of Mathematics, Ohio State University, Columbus, OH 43210
E-mail address: shapiro@math.ohio-state.edu

1616 Lexington Ave #D, El Cerrito, CA 94530
E-mail address: gavelmaven@aol.com