Comp. & Maths. with Appls. Vol. 9, No. 4, pp. 567 581, 1983
Printed in Great Britain.

0097-4943/83 $3.00 + .00
Pergamon Press Ltd.

MODULAR ARITHMETIC OF ITERATED POWERS

G. R. BLAKLEY† and I. BOROSH
Department of Mathematics, Texas A & M University, College Station, TX 77843, U.S.A.

(*Received February* 1982)

Communicated by E. Y. Rodin

Abstract—To give examples of large combinatorial problems D. Knuth modified W. Ackermann's example of a recursive, but not primitive recursive, function to produce a class of nonassociative compositions. These arrow compositions, which we call krata, are defined on the positive integers by setting

$$B\uparrow^1 T = B^T$$
$$B\uparrow^D 1 = B$$
$$B\uparrow^{D+1}(T+1) = B\uparrow^D(B\uparrow^{D+1}T).$$

The function $k(B, D, T) = B\uparrow^D T$, which usually takes on large values, has interesting periodicity properties modulo every positive integer M. For fixed $B, D, T \geq 2$ the sequences $\{B\uparrow^D n\}$, $\{B\uparrow^n T\}$ and $\{B\uparrow^n n\}$ are eventually constant modulo M. Also $\{n\uparrow^D T\}$, $\{n\uparrow^D n\}$, $\{n\uparrow^n T\}$ and $\{n\uparrow^n n\}$ are eventually periodic modulo M. An algorithm for calculating $B\uparrow^D T$ modulo M is given.

1. INTRODUCTION

Knuth's arrow compositions [1–3] are defined recursively on the set P of positive integers as follows:

$$B\uparrow T = B\uparrow^1 T = B^T$$
$$B\uparrow^D 1 = B$$
$$B\uparrow^{D+1}(T+1) = B\uparrow^D(B\uparrow^{D+1}T).$$

In particular

$$B\uparrow B = B\uparrow\uparrow 2 = B\uparrow^2 2 = B^B$$
$$B\uparrow(B\uparrow B) = B\uparrow\uparrow 3 = B\uparrow^2 3 = B^{B^B}$$
$$B\uparrow\uparrow B = B\uparrow\uparrow\uparrow 2 = B\uparrow^3 2$$
$$B\uparrow\uparrow(B\uparrow\uparrow B) = B\uparrow\uparrow\uparrow 3 = B\uparrow^3 3$$

and so on. Although the arrow compositions are not associative it is natural to drop parentheses when the intended association is to the right ([2], p. 111). Thus $8\uparrow\uparrow\uparrow 4 = 8\uparrow\uparrow(8\uparrow\uparrow(8\uparrow\uparrow 8))$ is written, more simply, as

$$8\uparrow\uparrow\uparrow 4 = 8\uparrow\uparrow 8\uparrow\uparrow 8\uparrow\uparrow 8 \neq ((8\uparrow\uparrow 8)\uparrow\uparrow 8)\uparrow\uparrow 8.$$

Bibliographies on iterated powers and allied topics can be found in [4–7]. Papers of related interest are [8–11]. The function $B\uparrow^D T$ is monotone increasing ([2], Theorem 1.1) in each of its arguments. We will use this monotonicity frequently below.

†Author's work supported, in part, by NSF Grant MCS 7908516.

It follows from the binomial theorem that

$$\{1^T, 2^T, 3^T, \ldots\} \qquad (\mathrm{mod}\ m\}$$

is periodic with period m, and from Euler's theorem that

$$\{B^1, B^2, B^3, \ldots\} \qquad (\mathrm{mod}\ m\}$$

is eventually periodic with period $\phi(m)$. Also, it is easy to verify that

$$\{1^1, 2^2, 3^3, \ldots\} \qquad (\mathrm{mod}\ m\}$$

is eventually periodic with period $m\phi(m)$. We will generalize these properties of powers to arrow compositions[3]. In fact let m, B, D and T be fixed integers larger than 1. The sequences

$$\begin{gathered}\{B\uparrow^D 1, B\uparrow^D 2, B\uparrow^D 3, \ldots\}\\ \{B\uparrow^1 T, B\uparrow^2 T, B\uparrow^3 T, \ldots\}\\ \{B\uparrow^1 1, B\uparrow^2 2, B\uparrow^3 3, \ldots\}\end{gathered}$$

will be shown to be eventually constant modulo m, whereas the sequences

$$\begin{gathered}\{1\uparrow^D T, 2\uparrow^D T, 3\uparrow^D T, \ldots\}\\ \{1\uparrow^D 1, 2\uparrow^D 2, 3\uparrow^D 3, \ldots\}\\ \{1\uparrow^1 T, 2\uparrow^2 T, 3\uparrow^3 T, \ldots\}\\ \{1\uparrow^1 1, 2\uparrow^2 2, 3\uparrow^3 3, \ldots\}\end{gathered}$$

will be shown to be eventually periodic modulo m. An algorithm for calculating $B\uparrow^D T$ modulo m will be given.

2. PRELIMINARY RESULTS FROM ELEMENTARY NUMBER THEORY

Euler's theorem

$$a\uparrow\phi(m) \equiv 1 \qquad (\mathrm{mod}\ m),$$

where a is relatively prime to m, simplifies computations with powers modulo m. Primitive roots modulo m, i.e. elements of multiplicative order $\phi(m)$, exist only for m of the form 1, 2, 4, $p\uparrow r$ or $2p\uparrow r$, where p is an odd prime. For all other m the order of every member of the multiplicative group of integers modulo m is a proper divisor of $\phi(m)$. The maximum of these orders for a given m is called ([12], p. 53) the *universal exponent* modulo m, and is written $\lambda(m)$.

It is shown in [12] (pp. 53–54) that $\lambda(m)$ can be evaluated as follows:

$$\begin{aligned}&\lambda(1) = \lambda(2) = 1 = \phi(1) = \phi(2)\\ &\lambda(4) = 2 = \phi(4)\\ &\lambda(2\uparrow x) = 2\uparrow(x-2) = \phi(2\uparrow x)/2\\ &\lambda(p\uparrow r) = \phi(p\uparrow r) = (p-1)p\uparrow(r-1)\\ &\lambda(mt) = \mathrm{lcm}\,\{\lambda(m), \lambda(t)\}\end{aligned}$$

for integer $x \geq 3$, positive integer r, odd prime p, positive integer m relatively prime to positive integer t. It is easy to show that:

(1) $\lambda(m) < m$, if $m \geq 2$;
(2) $\lambda(m)$ is even, if $m \geq 3$;
(3) $\lambda(m) \leq m/2$, if m is even;
(4) $\lambda(m) | \lambda(t)$, if $m | t$.

In dealing with iterated powers it is useful to iterate λ. Thus:
Definition 2.1: Let m, t and k be positive integers. Then let

$$\lambda^{(0)}(m) = m$$
$$\lambda^{(k)}(m) = \lambda(\lambda^{(k-1)}(m))$$
$$h(m) = \min\{y\colon \lambda^{(y)}(m) = 1\}$$
$$L[0, m] = 1$$
$$L[t, m] = \mathrm{lcm}\,\{\lambda^{(h(m))}(m), \lambda^{(h(m)-1)}(m), \ldots \lambda^{(h(m)-t)}(m)\}$$
$$L(m) = L[h(m), m] = \mathrm{lcm}\,\{m, \lambda(m), \lambda^{(2)}(m), \ldots\}$$
$$E(m) = \max\{e(p)\colon p | m\}$$

where $e(p)$ is the exponent of p in the prime power decomposition

$$m = \Pi p \uparrow e(p)$$

of m according to the fundamental theorem of arithmetic.

It is easy to verify that $m!$ is a multiple of $L(m)$. Evidently

$$\lambda^{(h(m)-1)}(m) = 2$$

for every integer $m \geq 2$. We adopt the $\ulcorner\ \urcorner$ notation for *integer ceiling* function. Thus $\ulcorner x \urcorner$ is the smallest integer at least as large as x. For example

$$\ulcorner \pi \urcorner = \ulcorner 4 \urcorner = 4.$$

Lemma 2.1.

$h(m) \leq \log_2(m)$ if m is an even positive integer.

Proof: Evidently $h(2) = 1 = \log_2(2)$. If $m \geq 4$ then $\lambda(m)$ is even and no larger than $m/2$. So, by induction,

$$h(m) = 1 + h(\lambda(m)) \leq 1 + \log_2(\lambda(m)) \leq 1 + \log_2(m/2) = \log_2(m).$$

Corollary 2.1.

$h(m) \leq \ulcorner \log_2(m) \urcorner \leq 1 + \log_2(m)$ if m is a positive integer.

Proof: Evidently $h(1) = 0 = \log_2(1)$. So consider any odd positive integer $m \geq 3$. Evidently $\lambda(m)$ is even, and strictly smaller than m. Therefore, by Lemma 2.1,

$$h(m) = 1 + h(\lambda(m)) \leq 1 + \log_2(\lambda(m)) < 1 + \log_2(m).$$

Since $\log_2(m)$ cannot be an integer it follows that

$$h(m) \leq \ulcorner \log_2(m) \urcorner.$$

Lemma 2.2.

Let $m = \Pi p \uparrow e(p)$ be the factorization of an integer $m \geq 2$ into powers of primes p in accordance with the fundamental theorem of arithmetic. Then

$$h(m) \geq \max\{\lceil (e(2)+1)/2 \rceil,\ \max\{e(p)+1\colon\ p \text{ is an odd prime}\}\}.$$

Proof: Evidently $h(m) \geq 1$. Therefore the inequality is trivial for any prime p, whether even or odd, such that $e(p) = 0$. Also

$$h(m) \geq 1 = \lceil (e(2)+1)/2 \rceil$$

if $e(2) = 1$. If $e(2) = 2$ then $\lambda(m)$ is a multiple of $\lambda(4)$, whence even. Therefore

$$h(m) \geq 2 = \lceil (e(2)+1)/2 \rceil.$$

And if $e(2) \geq 3$ then $2\uparrow(e(2)-2)$ is a factor of $\lambda(m)$. So it is not hard to verify that

$$h(m) \geq \lceil (e(2)+1)/2 \rceil$$

in any case. Finally, let p be an odd prime such that $1 \leq e(p)$. Then $p\uparrow(e(p)-1)$ is a factor of $\lambda(m)$. It is therefore not hard to ascertain that

$$h(m) \geq e(p) + 1.$$

COROLLARY 2.2.

$E(m) \leq 2h(m) - 1$ if m is an integer larger than 1.

Proof: $h(m) \geq \lceil (e(2)+1)/2 \rceil \geq (e(2)+1)/2$. Hence

$$e(2) \leq 2h(m) - 1.$$

For any odd prime p,

$$e(p) \leq h(m) - 1 \leq 2h(m) - 1.$$

Definition 2.2: Let a and m be positive integers. Let

$$m = \Pi p \uparrow e(p)$$

be the prime decomposition of m given by the fundamental theorem of arithmetic. Let

$$V = V(a, m) = \Pi q \uparrow e(q)$$

$$W = W(a, m) = \Pi s \uparrow e(s),$$

where the first product is over all primes q which do not divide a and the second is over all primes s which divide a. The equality

$$m = VW = V(a, m)W(a, m)$$

is called the *orthogonal decomposition* of m with respect to a. We will use V and W rather than $V(a, m)$ and $W(a, m)$ wherever no confusion is likely to result below.

Evidently V is relatively prime to both W and a. In fact V is the maximal factor of m with these two properties.

LEMMA 2.3.

Suppose that $c \geq d \geq E(m)$, and that

$$c \equiv d \qquad (\text{mod } \lambda(m)).$$

Then

$$a\uparrow c \equiv a\uparrow d \qquad (\mathrm{mod}\, m)$$

for every integer a.

Proof: We start with the orthogonal decomposition

$$m = VW = V(a, m)W(a, m)$$

of m with respect to a. Evidently

$$a\uparrow\lambda(V) \equiv 1 \qquad (\mathrm{mod}\ V).$$

Since V is a factor of m it follows that $\lambda(V)$ is a factor of $\lambda(m)$. Hence

$$a\uparrow\lambda(m) \equiv 1 \qquad (\mathrm{mod}\ V).$$

Therefore we know that the congruence

$$a\uparrow c \equiv a\uparrow d$$

holds modulo V. Since W is a factor of m we know that $E(m) \geq E(W)$. It follows from the definition of orthogonal decomposition that every prime factor of W is a factor of a. But by assumption

$$c \geq d \geq E(m) \geq E(W).$$

Therefore

$$a\uparrow c \equiv a\uparrow d \equiv 0 \qquad (\mathrm{mod}\ W).$$

Since the desired congruence holds modulo V and modulo W, it follows from the Chinese Remainder Theorem that it also holds modulo m.

3. EVENTUALLY CONSTANT SEQUENCES OF KRATA

To avoid trivial cases we assume that $A \geq 2$, $m \geq 2$ (whence $h(m) \geq 1$) everywhere below.

Lemma 3.1.

If $K \geq J \geq h(m) + 1$ then

$$A\uparrow\uparrow K \equiv A\uparrow\uparrow J \qquad (\mathrm{mod}\, L(m)).$$

Proof: For brevity let $H = h(m)$. We will start by proving a stronger result by finite induction on t, namely that the congruence

$$(*) \qquad A\uparrow\uparrow(u + t) \equiv A\uparrow\uparrow(y + t) \qquad (\mathrm{mod}\, L[t, m])$$

holds for all positive integers u, y and all nonnegative integers $t \leq H$. It holds trivially for $t = 0$ since $L[0, m] = 1$. So suppose that it holds for some nonnegative integer $t < H$, and for all positive integers u, y. Then the induction hypothesis guarantees that

$$(**) \qquad A\uparrow\uparrow((u + 1) + t) \equiv A\uparrow\uparrow(y + 1) + t) \qquad (\mathrm{mod}\, L[t, m]).$$

But since $\lambda^{(H-t)}(m)$ is a factor of $L[t, m]$ we also have

$$A\uparrow\uparrow(u + t) \equiv A\uparrow\uparrow(v + t) \qquad (\mathrm{mod}\, \lambda^{(H-t)}(m)).$$

However it follows from monotonicity and Corollary 2.2 that

$$A\uparrow\uparrow(u+t) \geq 2\uparrow(t+1) \geq 2(t+1) = 2h(\lambda^{(H-t-1)}(m)) > E(\lambda^{(H-t-1)}(m)).$$

So by Lemma 2.3 we have

$$(***) \qquad A\uparrow\uparrow(u+t+1) = A\uparrow A\uparrow\uparrow(u+t) \equiv A\uparrow A\uparrow\uparrow(y+t) = A\uparrow\uparrow(y+t+1),$$

where the congruence (***) immediately above holds modulo $\lambda^{(H-t-1)}(m)$. Since

$$L[t+1,m] = \operatorname{lcm}\{L[t,m], \lambda^{(H-t-1)}(m)\}$$

we can combine the congruences (**) and (***) to yield

$$A\uparrow\uparrow(u+t+1) \equiv A\uparrow\uparrow(y+t+1) \qquad (\text{mod } L[t+1,m]).$$

The lemma follows from the congruence (*) by letting

$$t = H$$
$$K = u + t = u + H$$
$$J = y + t = y + H.$$

Definition 3.1: Let the sequence

$$N[A,m] = \{N(A,2,m), N(A,3,m), N(A,4,m), \ldots\}$$

be defined recursively by setting

$$N(A,2,m) = h(m) + 1$$

$$N(A,D,m) = \min\{k\colon\ A\uparrow^D(k-1) \geq N(A,D-1,m)\}$$

for every integer $D \geq 3$.

LEMMA 3.2.

$N(A,D,m)$ is a monotone nonincreasing function of D for fixed A and m, and is a monotone nonincreasing function of A for fixed D and m. Moreover

$$A\uparrow^D u \equiv A\uparrow^D y \qquad (\text{mod } L(m))$$

for each integer $D \geq 2$ whenever $u \geq y \geq N(A,D,m)$.

Proof: It follows from monotonicity that

$$A\uparrow^D(N(A,D-1,m)-1) \geq 2\uparrow(N(A,D-1,m)-1) \geq N(A,D-1,m).$$

Consequently

$$N(A,D,m) \leq N(A,D-1,m).$$

To prove the second statement let $A \geq B$. It follows from monotonicity that

$$A\uparrow^D(k-1) \geq B\uparrow^D(k-1)$$

for every positive integer k. Evidently

$$N(A, 2, m) = N(B, 2, m).$$

So assume that

$$N(A, D-1, m) \leq N(B, D-1, m).$$

It then follows that

$$\begin{aligned} N(A, D, m) &= \min\{k\colon A\uparrow^D(k-1) \geq N(A, D-1, m)\} \\ &\leq \min\{k\colon A\uparrow^D(k-1) \geq N(B, D-1, m)\} \\ &\leq \min\{k\colon B\uparrow^D(k-1) \geq N(B, D-1, m)\} \\ &= N(B, D, m). \end{aligned}$$

The congruence will be proved by finite induction on D. The case $D = 2$ follows from Lemma 3.1. So assume that $D \geq 3$ and that

$$A\uparrow^{D-1}u^* \equiv A\uparrow^{D-1}y^* \qquad (\text{mod } L(m))$$

whenever $u^* \geq y^* \geq N(A, D-1, m)$. Choose any u, y such that $u \geq y \geq N(A, D, m)$. We know that

$$A\uparrow^D(N(A, D, m) - 1) \geq N(A, D-1, m).$$

It follows from monotonicity that

$$A\uparrow^D(u-1) \geq A\uparrow^D(y-1) \geq A\uparrow^D(N(A, D, m) - 1) \geq N(A, D-1, m).$$

Therefore

$$A\uparrow^{D-1}A\uparrow^D(u-1) \equiv A\uparrow^{D-1}A\uparrow^D(y-1) \qquad (\text{mod } L(m))$$

by the induction hypothesis. In other words

$$A\uparrow^D u \equiv A\uparrow^D y \qquad (\text{mod } L(m)).$$

The proof of Lemma 3.2 shows that

$$A\uparrow^D u \equiv A\uparrow\uparrow N(A, 2, m) \qquad (\text{mod } L(m))$$

if $u \geq N(A, D, m)$. Hence it is easy to see that

Corollary 3.1.
If $u \geq N(A, C, m)$ and $y \geq N(A, D, m)$ then

$$A\uparrow^C u \equiv A\uparrow^D y \qquad (\text{mod } L(m)).$$

Corollary 3.2.
If $u \geq y \geq \max\{h(m) + 1, 4\}$ then

$$A\uparrow^u T \equiv A\uparrow^y T \qquad (\text{mod } L(m)).$$

Proof: If $T = 1$ or if $A = T = 2$ the congruence is in fact an equality ([2], p. 111). So suppose, first, that $T \geq 3$. Then it follows from ([2], Theorem 4.2) that to each integer $r \geq 3$

there correspond positive integers $G = A\uparrow^r(T-1)$ and F such that

$$A\uparrow^r T = A\uparrow^{r-1}A\uparrow^r(T-1) = A\uparrow^{r-1}G = A\uparrow\uparrow F.$$

Evidently

$$F \geq G = A\uparrow^r(T-1) \geq r+1$$

because of ([2], Theorem 3.5) unless $(A, T) = (2, 3)$ and $r \geq 4$. However, in this subcase, it follows from ([2], pp. 110–111) that

$$2\uparrow^r 3 = 2\uparrow^{r-1}(2\uparrow^r 2) = 2\uparrow^{r-1}4 = 2\uparrow^{r-2}2\uparrow^{r-1}3 = 2\uparrow\uparrow J.$$

for some positive integer J, according to ([2], Theorem 4.2). The assumption $r \geq 4$ governing this subcase means, in view of monotonicity and ([2], Lemma 3.9), that

$$J \geq 2\uparrow^{r-1}3 > r.$$

In summary, then,

$$A\uparrow^r T = A\uparrow\uparrow Q$$

for some $Q \geq r+1$ whenever $T \geq 3$. Hence, if $u \geq y \geq \max\{3, h(m)\}$, it follows from Lemma 3.1 that

$$A\uparrow^u T \equiv A\uparrow^y T \qquad (\text{mod } L(m)).$$

If, finally, $T = 2$ and $A > 2$, then

$$A\uparrow^{r+1}T = A\uparrow^{r+1}2 = A\uparrow^r A$$

and the reasoning of the case $T \geq 3$ (with T now replaced by A) can be invoked.

COROLLARY 3.3.

If $u \geq y \geq \max\{4, 1 + h(m)\}$ then

$$A\uparrow^u u \equiv A\uparrow^y y \qquad (\text{mod } L(m)).$$

Definition 3.2: The *preperiod* of an eventually periodic sequence $\{a(1), a(2), a(3), \ldots\}$ is the smallest integer j such that the subsequence $\{a(j+1), a(j+2), a(j+3), \ldots\}$ is periodic. The term obviously also makes sense for an eventually constant sequence because it is eventually periodic.

From Lemma 3.2, Corollary 3.2 and Corollary 3.3 we have

THEOREM 3.1.

The sequences

$$\{A\uparrow^D 1, A\uparrow^D 2, A\uparrow^D 3, \ldots\}$$
$$\{A\uparrow^1 T, A\uparrow^2 T, A\uparrow^3 T, \ldots\}$$
$$\{A\uparrow^1 1, A\uparrow^2 2, A\uparrow^3 3, \ldots\}$$

are eventually constant modulo $L(m)$, whence modulo m. Considered as sequences of residue classes modulo $L(m)$ the first has preperiod $p \leq N(A, D, m)$, the second has preperiod $p \leq \max\{4, h(m) + 1\}$, and the third has preperiod $p \leq h(m) + 1$.

4. EVENTUALLY PERIODIC SEQUENCES OF KRATA

As in Section 3, assume that $A \geq 2$, $m \geq 2$, whence $h(m) \geq 1$.

LEMMA 4.1.

Suppose that

$$A \equiv B \qquad (\operatorname{mod} L(m))$$

and that $A \geq B \geq E(m)$. Then

$$A \uparrow\uparrow T \equiv B \uparrow\uparrow T \qquad (\operatorname{mod} L(m))$$

for every positive integer T.

Proof: There is nothing to prove if $T = 1$. So we will use finite induction on T. Assume the Tth case. Then

$$A \uparrow\uparrow (T+1) = A \uparrow A \uparrow\uparrow T \equiv A \uparrow B \uparrow\uparrow T \qquad (\operatorname{mod} L(m))$$

by Lemma 2.3, provided that

$$A \uparrow\uparrow T \geq B \uparrow\uparrow T \geq E(m).$$

This is certainly true by monotonicity since

$$A \geq B \geq E(m).$$

From the hypothesis

$$A \equiv B \qquad (\operatorname{mod} L(m))$$

it follows that

$$A \uparrow (B \uparrow\uparrow T) \equiv B \uparrow (B \uparrow\uparrow T) \qquad (\operatorname{mod} L(m))$$

and, consequently, that

$$A \uparrow\uparrow (T+1) \equiv A \uparrow (B \uparrow\uparrow T) \equiv B \uparrow\uparrow (T+1) \qquad (\operatorname{mod} L(m)).$$

COROLLARY 4.1.

Let T be an arbitrary but fixed positive integer. The sequence

$$\{1 \uparrow\uparrow T, 2 \uparrow\uparrow T, 3 \uparrow\uparrow T, \ldots\}$$

is eventually periodic modulo $L(m)$ with period $L(m)$. Moreover its preperiod is less than $E(m)$.

LEMMA 4.2.

Suppose that $D \geq 2$, that $A \geq B \geq \max\{h(m)+1, E(m)\}$, and that

$$A \equiv B \qquad (\operatorname{mod} L(m)).$$

Then

$$A \uparrow^{D} T \equiv B \uparrow^{D} T \qquad (\operatorname{mod} L(m))$$

for every positive integer T.

Proof: We proceed by induction on D. We can assume that $T \geq 2$ since the case $T = 1$ is trivial. Lemma 4.1 provides the case $D = 2$. Fix A and B such that $A \geq B \geq \max\{h(m)+1,\ E(m)\}$. Assuming the truth of the Dth case we find that

$$A\uparrow^{D+1}(T+1) = A\uparrow^{D}A\uparrow^{D+1}T = B\uparrow^{D}A\uparrow^{D+1}T \qquad (\text{mod } L(m))$$

because of the induction hypothesis. However

$$B\uparrow^{D+1}T > B \geq h(m)+1 = N(B,2,m) \geq N(B,D,m).$$

So it follows from Lemma 3.2 that

$$B\uparrow^{D}A\uparrow^{D+1}T \equiv B\uparrow^{D}B\uparrow^{D+1}T = B\uparrow^{D+1}(T+1) \qquad (\text{mod } L(m)).$$

THEOREM 4.1.

The sequences

$$\{1\uparrow^{D}T, 2\uparrow^{D}T, 3\uparrow^{D}T, \ldots\}$$
$$\{1\uparrow^{D}1, 2\uparrow^{D}2, 3\uparrow^{D}3, \ldots\}$$
$$\{1\uparrow^{1}T, 2\uparrow^{2}T, 3\uparrow^{3}T, \ldots\}$$
$$\{1\uparrow^{1}1, 2\uparrow^{2}2, 3\uparrow^{3}3, \ldots\}$$

are eventually periodic modulo $L(m)$, with period $L(m)$. Hence they are eventually periodic modulo m with period $L(m)$ and, as is easily seen, with preperiod at most

$$\max\{4, h(m)+1, E(m)\}.$$

Proof: The first periodicity result follows immediately from Lemma 4.2. Suppose that

$$a \equiv b \qquad (\text{mod } L(m))$$

and that $a \geq b \geq \max\{h(m)+1, E(m)\}$. We prove the second result by noting that Lemma 4.2 and Lemma 3.2 give

$$a\uparrow^{D}a \equiv b\uparrow^{D}a \equiv b\uparrow^{D}b \qquad (\text{mod } L(m)).$$

Henceforth assume also that $a \geq b \geq 4$. We prove the third by appealing to Lemma 4.2 and Corollary 3.2 to get

$$a\uparrow^{a}T \equiv b\uparrow^{a}T \equiv b\uparrow^{b}T \qquad (\text{mod } L(m)).$$

Finally Lemma 4.2, Lemma 3.2 and Corollary 3.2, taken successively, prove that

$$a\uparrow^{a}a \equiv b\uparrow^{a}a \equiv b\uparrow^{a}b \equiv b\uparrow^{b}b \qquad (\text{mod } L(m)).$$

5. AN ALGORITHM FOR COMPUTING $A\uparrow^{D}T$ MODULO m

This section is devoted to describing and justifying procedures for finding the smallest nonnegative integer S such that

$$S \equiv A\uparrow^{D}T \qquad (\text{mod } m).$$

We will assume that $m \geq 3$, $A \geq 2$ since the cases $m = 1$ or 2, and the case $A = 1$, are trivial. The cases $T = 1$ and $D = 1$ raise the question of how hard it is to find the smallest nonnegative integer S such that

$$S \equiv A \uparrow T \qquad (\operatorname{mod} m)$$

or, even more simply, to find the smallest nonnegative integer S such that

$$S \equiv A \qquad (\operatorname{mod} m),$$

where A, T and m are positive integers. We will give only the obvious answer. On the one hand it might take a great deal of computer time to do it if m is very big and A is very much bigger still. On the other hand it is *merely* an application of the division algorithm followed by the operations of forgetting the quotient and remembering the remainder.

Our approach will be simply to take the problem of determining (the smallest nonnegative name of) the residue class modulo m of $A \uparrow T$ for granted. Therefore we also regard the determination of the residue class of $A \uparrow^D T$ modulo m as given if A or D or T is equal to 1. In other words, in the terminology of ([2], p. 113) we will only seek to determine the residue class modulo m of $A \uparrow^D T$ if it is a *nontrivial kratic representation* of a positive integer

$$K = A \uparrow^D T,$$

assuming that the residue classes of

$$A \uparrow 1, A \uparrow 2, A \uparrow 3, A \uparrow 4, \ldots$$

are readily available.

Obviously, the first thing to consider is the size of m, since even writing down numbers S near m can be a daunting task if m is too big. We will confine our attention to positive integers m smaller than $10 \uparrow\uparrow 3$. They will be called *modest numbers* (A positive integer will therefore be a modest number if its decimal representation involves no more than 10,000,000,000 digits).

In addition to assuming that m is a modest number, the algorithm below will presuppose a good bit of knowledge about $L(m)$. In fact it will be based on the supposition that we know

$$m, \lambda(m), \lambda^{(2)}(m), \ldots, \lambda^{(h(m))}(m).$$

This is often the case since, for example, the prime power factorization of $L(m)$ can be found for any modest number

$$m = \Pi p \uparrow e(p)$$

with known factorization into powers of primes $p < 10 \uparrow 50$ in accordance with the fundamental theorem of arithmetic. To see this, merely recall that

$$\lambda(m) = \operatorname{lcm} \{(p-1) p \uparrow (e(p)-1) \colon p \text{ is a prime factor of } m\}.$$

The prime power factorization of $\lambda(m)$ can thus be inferred from the prime power factorization of m with methods available in 1983, since $p - 1 < 10 \uparrow 50$ for every prime divisor p of m. Given this factorization one can now calculate $\lambda(\lambda(m))$. Then one can repeat the argument to show that the prime power factorization of

$$\lambda^{(2)}(m) = \lambda(\lambda(m))$$

can be found, and so on down to

$$\lambda^{(h(m)-1)}(m) = 2, \qquad \lambda^{(h(m))}(m) = 1.$$

Since $L(m)$ is the least common multiple of these numbers, it follows that its prime power factorization is thus known at the end of the process.

Granted these cautions, we now turn our attention to the $D \geq 3$ case of the algorithm for calculating $A\uparrow^D T$ modulo m. From Lemma 3.2 it follows that, if $T \geq N(A, D, m)$, then

$$A\uparrow^D T \equiv A\uparrow\uparrow N(A, 2, m) \qquad (\text{mod } (m))$$

for any $D \geq 2$. If m is a modest number then

$$N(A, 2, m) = 1 + h(m) \leq 2 + \log_2(\text{m}) < 40{,}000{,}000{,}000.$$

It is easy to verify that, for any modest number m,

$$N(2, 3, m) \leq 5, \quad N(2, 4, m) \leq 4, \quad N(2, 5, m) \leq 3 \quad \text{and} \quad N(A, D, m) \leq 3$$

for $A \geq 3$, $D \geq 3$. Thus if $D \geq 3$, m is a modest number, and $T \geq 3$, then

$$A\uparrow^D T \equiv A\uparrow\uparrow N(A, 2, m) \qquad (\text{mod } m)$$

except for

$$2\uparrow\uparrow\uparrow 3 = 65{,}536 \qquad 2\uparrow\uparrow\uparrow\uparrow 3 = 2\uparrow\uparrow\uparrow 4 = 2\uparrow\uparrow 65{,}536.$$

Under any circumstances, then, the problem of calculating $A\uparrow^D T$ modulo m is reduced to the case $D = 2$ when m is a modest number.

So now consider the case $D = 2$. We must find $A\uparrow\uparrow T$ modulo m. This case, in turn, has two subcases, *typical* (i.e. large enough T) and *atypical* (small T). It follows from Lemma 3.1 that

$$A\uparrow\uparrow T \equiv A\uparrow\uparrow(H + 1) \qquad (\text{mod } m)$$

for every integer $T \geq H + 1$. This suggests the *typical subcase* (the large enough T case) of the $\uparrow\uparrow$ algorithm. In this subcase we need merely find the smallest nonnegative integer S such that

$$S \equiv A\uparrow\uparrow(H + 1) \qquad (\text{mod } m).$$

To do this we follow the proof of Lemma 3.1 and define

$$B[1] = 0$$

$$B[2] = \begin{cases} 1 & (\text{if } A \text{ is odd}) \\ 0 & (\text{if } A \text{ is even}). \end{cases}$$

Thus, as we have noted above,

$$B[1] \equiv A\uparrow\uparrow 1 \qquad (\text{mod } \lambda^{(H)}(m)).$$

$$B[2] \equiv A\uparrow\uparrow 2 \qquad (\text{mod } \lambda^{(H-1)}(m)).$$

Proceeding inductively, assume that $t \geq 2$ and suppose we have already found the unique nonnegative integer

$$B[t] < \lambda^{(H+1-t)}(m)$$

which obeys the congruence

$$B[t] \equiv A\uparrow\uparrow t \qquad (\text{mod } \lambda^{(H+1-t)}(m)).$$

Then, as in Section 2, form the orthogonal decomposition

$$VW = V(A, \lambda^{(H-t)}(m))W(A, \lambda^{(H-t)}(m)) = \lambda^{(H-t)}(m)$$

of $\lambda^{(H-t)}(m)$ with respect to A. Thus $(V, W) = (V, A) = 1$, and every prime factor of W is a factor of A. We thus know from the proof of Lemma 3.1 that

$$A\uparrow\uparrow(t+1) \equiv A\uparrow B[t] \qquad \pmod{V}.$$

and

$$A\uparrow\uparrow(t+1) \equiv 0 \qquad \pmod{W}.$$

Applying the Chinese Remainder Theorem we easily find $B[t+1]$, the smallest nonnegative integer such that

$$B[t+1] \equiv A\uparrow\uparrow(t+1) \qquad \pmod{VW}.$$

This completes the $(t+1)$st step in the typical subcase of the $\uparrow\uparrow$ algorithm. Recall that

$$m = \lambda^{(0)}(m) = \lambda^{((H+1)-(H+1))}(m).$$

In this fashion one proceeds until $B[H+1]$ is found. From then on

$$A\uparrow\uparrow T \equiv A\uparrow\uparrow(H+1) \equiv B[H+1] \qquad \pmod{m}$$

for every integer $T \geq H+1$.

Having completed the typical subcase of the $\uparrow\uparrow$ algorithm we turn now to the other subcase, in which $T \leq H$. If $A\uparrow\uparrow(T-1)$ is a modest number, there is nothing to do, in view of our initial assumption that finding the smallest integer congruent modulo modest m to $A\uparrow A\uparrow\uparrow(T-1)$ is possible by means of methods from outside this paper. Otherwise let g be the smallest integer such that $A\uparrow\uparrow g$ is not a modest number. By assumption $\lambda^{(k)}(m)$ is a modest number for every nonnegative integer k. Consequently

$$E(\lambda^{(k)}(m)) < A\uparrow\uparrow g.$$

If $t \geq g$ then

$$A\uparrow\uparrow t \equiv 0 \qquad \pmod{W(A, \lambda^{(k)}(m))}$$

for every nonnegative integer k. Since $A\uparrow\uparrow(g-1)$ is modest we use the Chinese Remainder Theorem to define $B[g]$ to be the smallest nonnegative residue modulo $\lambda^{(T-g)}(m)$ such that

$$B[g] \equiv A\uparrow A\uparrow\uparrow(g-1) \qquad \pmod{V(A, \lambda^{(T-g)}(m))}$$

and

$$B[g] \equiv 0 \qquad \pmod{W(A, \lambda^{(T-g)}(m))}.$$

Thus we have

$$B[g] \equiv A\uparrow\uparrow g \qquad \pmod{\lambda^{(T-g)}(m)}$$

and

$$0 \leq B[g] < \lambda^{(T-g)}(m).$$

From there we proceed inductively. So assume that $B[t]$ is defined for $g \leq t < T$ in such a fashion that

$$B[t] \equiv A\uparrow\uparrow t \qquad (\text{mod } \lambda^{(T-t)}(m))$$

and

$$0 \leq B[t] < \lambda^{(T-t)}(m).$$

Define $B[t+1]$ by setting

$$B[t+1] \equiv \begin{cases} A\uparrow B[t] & \text{mod } V(A, \lambda^{(T-t-1)}(m)) \\ 0 & \text{mod } W(A, \lambda^{(T-t-1)}(m)). \end{cases}$$

Clearly $B[t]$ is the required answer. The algorithm has now been completely specified.

Example 5.1: Computation of the smallest nonnegative integer S such that

$$S \equiv 6\uparrow\uparrow 10 \qquad (\text{mod } 20)$$

according to the first subcase of the $\uparrow\uparrow$ algorithm proceeds as follows.

$$\lambda^{(0)}(20) = 20$$
$$\lambda^{(1)}(20) = \lambda(20) = 1\text{ cm}\,\{\lambda(4), \lambda(5)\} = 1\text{ cm}\,\{2, 4\} = 4$$
$$\lambda^{(2)}(20) = \lambda(\lambda^{(1)}(20)) = \lambda(4) = 2$$
$$\lambda^{(3)}(20) = \lambda(\lambda^{(2)}(20)) = \lambda(2) = 1.$$

Thus

$$H = h(20) = 3$$
$$B[1] = B[2] = 0,$$

whence

$$6\uparrow\uparrow 1 \equiv 0 \qquad (\text{mod } 1)$$
$$6\uparrow\uparrow 2 \equiv 0 \qquad (\text{mod } 2)$$
$$6\uparrow\uparrow 3 = 6\uparrow\uparrow(2+1) \equiv 0 \qquad (\text{mod } 4).$$

Evidently

$$V(6, \lambda^{(3-3)}(20)) = V(6, \lambda^{(0)}(20)) = V(6, 20) = 5$$
$$W(6, \lambda^{(3-3)}(20)) = W(6, 20) = 4.$$

Consequently

$$6\uparrow\uparrow 4 = 6\uparrow\uparrow(3+1) \equiv 6\uparrow B[3] \equiv 6\uparrow 0 \equiv 1 \qquad (\text{mod } 5)$$
$$6\uparrow\uparrow 4 = 6\uparrow\uparrow(3+1) \equiv 0 \qquad (\text{mod } 4).$$

The Chinese Reminder Theorem applied to

$$B[4] \equiv 1 \qquad (\text{mod } 5)$$
$$B[4] \equiv 0 \qquad (\text{mod } 4)$$

produces the solution $B[4] = 16$. Thus

$$6\uparrow\uparrow 4 \equiv 16 \pmod{20}.$$

It follows that

$$6\uparrow\uparrow 10 \equiv 6\uparrow\uparrow 4 \equiv 16 \pmod{20}.$$

REFERENCES

1. D. E. Knuth, Mathematics and computer science: coping with finiteness. *Science* **194**, 1235–1242 (1976).
2. G. R. Blakley and I. Borosh, Knuth's iterated powers. *Advan. Math.* **34**, 109–136 (1979).
3. G. R. Blakley and I. Borosh, Knuth's iterated powers modulo m. Preliminary report, Abstracts of Papers Presented to the American Mathematical Society, Vol. 1, p. 416 (1980).
4. R. B. Burckel, Iterating analytic self-maps of discs. *Am. Math. Monthly* **88**, 396–407 (1981).
5. R. A. Knoebel, Exponentials reiterated. *Am. Math. Monthly* **88**, 235–252 (1981).
6. C. Smorynski, Some rapidly growing functions. *Math. Intell.* **2**, 149–154 (1980).
7. W. J. Thron, Convergence regions for continued fractions and other infinite processes. *Am. Math. Monthly* **68**, 734–750 (1961).
8. P. Erdös and R. Rado, Combinatorial theorems on classifications of subsets of a given set. *Proc. London Math. Soc.* **30**, 417–439 (1951).
9. S. W. Golomb, Iterated binomial coefficients. *Am. Math. Monthly* **87**, 719–727 (1980).
10. J. E. Littlewood, Large numbers, *Math. Gazette* **32**, 163–171 (1948).
11. J. E. Littlewood, *A Mathematician's Miscellany*, pp. 100–116. Methuen, London (1960).
12. W. J. Leveque, *Topics in Number Theory*, Vol. I. Addison-Wesley, Reading, Mass. (1956).
13. G. R. Blanton, Extending Knuth's double arrow to real numbers, Abstracts of Papers Presented to the American Mathematical Society, Vol. 1, p. 71 (1980).
14. J. Spencer (Ed.), Paul Erdös, *The Art of Counting*: *Selected Writings*, pp. 383–405. MIT Press, Cambridge, Mass. (A reprint of [8].)