The Last Digits of Infinity (On Tetrations Under Modular Rings)

William Stowe
Augustana College, Rock Island Illinois

The Last Digits of Infinity (On Tetrations Under Modular Rings)

William Stowe
Augustana College
ISMAA Meeting 2019
30 March 2019

Inspiration

- What are the last two digits of 7^7^...^7 where there are 7 7’s

Inspiration

- What are the last two digits of 7^7^...^7 where there are 7 7’s
- 7^7^7 already has over 600,000 digits

Inspiration

- What are the last two digits of 7^7^...^7 where there are 7 7's
- 7^7^7 already has over 600,000 digits
- Using Wolfram Alpha, we noticed something interesting

Motivation

- $7^7 \equiv 7^{7^7} \equiv 7^{7^{\cdots^7}} \bmod 100$

Motivation

- $7^7 \equiv 7^{7^7} \equiv 7^{7^{\cdots^7}} \mod 100$
- The last 2 digits of every tower of sevens, except the first one, are the same

Motivation

- $7\char`^7 \equiv 7\char`^7\char`^7 \equiv 7\char`^7\char`^...\char`^7 \bmod 100$
- The last 2 digits of every tower of sevens, except the first one, are the same
- When does this convergent behavior occur?

Motivation

- $7\^7 \equiv 7\^7\^7 \equiv 7\^7\^...\^7 \mod 100$
- The last 2 digits of every tower of sevens, except the first one, are the same
- When does this convergent behavior occur?
- Conjecture: For every $a \in Z_n$ there is a tower of a’s that will be congruent to every subsequent tower mod n

Definition of Tetration

- The most known operations for the integers can be defined recursively.

Definition of Tetration

- The most known operations for the integers can be defined recursively.
- (1) Addition $5+3 = 8$

Definition of Tetration

- The most known operations for the integers can be defined recursively.
- (1) Addition 5+3 = 8
- (2) Multiplication 5*3 = 5+5+5 = 15

Definition of Tetration

- The most known operations for the integers can be defined recursively.
- (1) Addition 5+3 = 8
- (2) Multiplication 5*3 = 5+5+5 = 15
- (3) Exponentiation 5^3 = 5*5*5 = 125

Definition of Tetration

- The most known operations for the integers can be defined recursively.
- (1) Addition $5+3 = 8$
- (2) Multiplication $5*3 = 5+5+5 = 15$
- (3) Exponentiation $5^3 = 5*5*5 = 125$
- (4) Tetration $5\uparrow 3 = 5^{5^5} \approx 1.9*10^{2184}$

Modular Exponents

- Given a,b,c $\in$ R, we know
- $a^b = a^c \Leftrightarrow b = c$

Modular Exponents

- Given $a,b,c \in R$, we know:
- $a^b = a^c \Leftrightarrow b = c$
- Using this intuition, we can conjecture:
- $a^b \equiv a^c \bmod n \Leftrightarrow b \equiv c \bmod n$

Modular Exponents

- Given $a,b,c \in R$, we know:
- $a^b = a^c \Leftrightarrow b = c$
- Using this intuition, we can conjecture:
- $a^b \equiv a^c \bmod n \Leftrightarrow b \equiv c \bmod n$
- Consider $2 \in Z_3$ and notice $1 \equiv 4 \bmod 3$

Modular Exponents

- Given $a,b,c \in R$, we know:
- $a^b = a^c \Leftrightarrow b = c$
- Using this intuition, we can conjecture:
- $a^b \equiv a^c \bmod n \Leftrightarrow b \equiv c \bmod n$
- Consider $2 \in Z_3$ and notice $1 \equiv 4 \bmod 3$
- $2^1 \equiv 2^4 \bmod 3$

Modular Exponents

- Given a,b,c $\in$ R, we know:
- a^b = a^c ⇔ b = c
- Using this intuition, we can conjecture:
- a^b ≡ a^c mod n ⇔ b ≡ c mod n
- Consider 2 $\in Z_3$ and notice 1 ≡ 4 mod 3
- 2^1 ≡ 2^4 mod 3
- 2 ≡ 16 mod 3

Modular Exponents: This Time It's Personal

- $a \in Z_n$ a unit
- $\Rightarrow$ a^b ≡ a^c mod n $\Leftrightarrow$ b ≡ c mod |a|

Modular Exponents: This Time It's Personal

- $a \in Z_n$ a unit
- $\Rightarrow a^b \equiv a^c \bmod n \Leftrightarrow b \equiv c \bmod |a|$
- We want to generalize beyond the units, and all we need to do is generalize $|a|$

Cyclic elements

- An element $a \in Z_n$ is *cyclic* means that there is an integer k such that $a^k \equiv a \bmod n$.

Cyclic elements

- An element $a \in Z_n$ is *cyclic* means that there is an integer k such that $a^k \equiv a \bmod n$.
- *a* a unit is sufficient to say *a* cyclic, but it is not necessary.

Cyclic elements

- An element $a \in Z_n$ is *cyclic* means that there is an integer k such that a^$k \equiv a \bmod n$.
- *a* a unit is sufficient to say *a* cyclic, but it is not necessary.
- Consider $2 \in Z_{10}$:

Cyclic elements

- An element $a \in Z_n$ is *cyclic* means that there is an integer k such that $a^k \equiv a \bmod n$.
- a a unit is sufficient to say a cyclic, but it is not necessary.
- Consider $2 \in Z_{10}$:
- $2^5 = 32 \equiv 2 \bmod 10$

Properties of Cyclic Elements

- Form a group under multiplication mod n

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.
- Suppose $a \in Z_n$ cyclic

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.
- Suppose a $\in Z_n$ cyclic
- a^k ≡ a mod n

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.
- Suppose a $\in Z_n$ cyclic
- a^k ≡ a mod n
- a^(k-1)a^j

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.
- Suppose a $\in Z_n$ cyclic
- a^k ≡ a mod n
- a^(k-1)*a^j
- ≡ a^(k-1)*a*a^(j-1)

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.
- Suppose a $\in Z_n$ cyclic
- a^k ≡ a mod n
- a^(k-1)*a^j
- ≡ a^(k)*a^(j-1)

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.
- Suppose $a \in Z_n$ cyclic
- $a^k \equiv a \bmod n$
- $a^{(k-1)} * a^j$
- $\equiv a * a^{(j-1)}$

Properties of Cyclic Elements

- Form a group under multiplication mod n
- Contain an element a^(k-1) that acts as a multiplicative identity.
- Suppose a $\in Z_n$ cyclic
- a^k ≡ a mod n
- a^(k-1)*a^j
- ≡ a^(j)

Non-Cyclic elements

- An element that is not cyclic is said to be non-cyclic

Non-Cyclic elements

- An element that is not cyclic is said to be non-cyclic
- That is to say for $a \in Z_n$ there is no power of a greater than 1 that is congruent to a mod n.

Non-Cyclic elements

- An element that is not cyclic is said to be non-cyclic
- That is to say for $a \in Z_n$ there is no power of a greater than 1 that is congruent to a mod n.
- Consider $2 \in Z_{20}$:

Non-Cyclic elements

- An element that is not cyclic is said to be non-cyclic
- That is to say for $a \in Z_n$ there is no power of a greater than 1 that is congruent to a mod n.
- Consider $2 \in Z_{20}$:
- $2^5 \equiv 12 \bmod 20$

Non-Cyclic elements

- An element that is not cyclic is said to be non-cyclic
- That is to say for $a \in Z_n$ there is no power of a greater than 1 that is congruent to a mod n.
- Consider $2 \in Z_{20}$:
- 2^5 ≡ 12 mod 20
- 2^6 ≡ 4 mod 20

Non-Cyclic elements

- The powers of a non-cyclic element can be divided into 2 disjoint subsets

Non-Cyclic elements

- The powers of a non-cyclic element can be divided into 2 disjoint subsets
- The *head* is the set $\{a^k | \sim \exists\ j > 0: a^k \equiv a^{(k+j)} \bmod n\}$

Non-Cyclic elements

- The powers of a non-cyclic element can be divided into 2 disjoint subsets
- The *head* is the set {a^k|~ ∃ j > 0: a^k ≡ a^(k+j) mod n}
- The *cycle* is the set {a^k | ∃ j > 0: a^k ≡ a^(k+j) mod n}

Properties of Non-Cyclic Elements

- Will always enter into a cycle.

Properties of Non-Cyclic Elements

- Will always enter into a cycle.
- Similar to cyclic elements, the cycle will form a multiplicative group

Properties of Non-Cyclic Elements

- Will always enter into a cycle.
- Similar to cyclic elements, the cycle will form a multiplicative group
- The identity of this group will be a^w, where w is a multiple of the size of the cycle.

Properties of Non-Cyclic Elements

- Will always enter into a cycle.
- Similar to cyclic elements, the cycle will form a multiplicative group
- The identity of this group will be a^w, where w is the size of the cycle.
- Suppose the powers of a have a cycle of size w

Properties of Non-Cyclic Elements

- Will always enter into a cycle.
- Similar to cyclic elements, the cycle will form a multiplicative group
- The identity of this group will be a^w, where w is the size of the cycle.
- Suppose the powers of a have a cycle of size w
- a^w+k ≡ a^k for k greater than the size of the head of a

Properties of Non-Cyclic Elements

- Will always enter into a cycle.
- Similar to cyclic elements, the cycle will form a multiplicative group
- The identity of this group will be a^w, where w is the size of the cycle.
- Suppose the powers of a have a cycle of size w
- a^w+k ≡ a^k for k greater than the size of the head of a
- a^w*a^k ≡ a^k mod n

A Generalized Lemma

- Let |a| be the size of the cycle of a

A Generalized Lemma

- Let |a| be the size of the cycle of a
- b,c greater than the size of the head of a implies, $a^b \equiv a^c \Leftrightarrow b \equiv c \mod |a|$

Proof:

- $a^b \equiv a^c \mod n$.

Proof:

- $a^b \equiv a^c \bmod n$.
- Suppose b,c larger than the head of a. $b = k|a|+j$, $c = m|a|+p$ where $j,p < |a|$

Proof:

- $a^b \equiv a^c \bmod n$.
- Suppose b,c larger than the head of a. $b = k|a|+j$, $c = m|a|+p$ where $j,p < |a|$
- $a^{(k|a|+j)} \equiv a^{(m|a|+p)} \bmod n$

Proof:

- $a^b \equiv a^c \bmod n$.
- Suppose b,c larger than the head of a. $b = k|a|+j$, $c = m|a|+p$ where $j,p < |a|$
- $a^{(k|a|+j)} \equiv a^{(m|a|+p)} \bmod n$
- $a^{k|a|} * a^j \equiv a^{m|a|} * a^p \bmod n$

Proof:

- $a^b \equiv a^c \bmod n$.
- Suppose b,c larger than the head of a. $b = k|a|+j$, $c = m|a|+p$ where $j,p < |a|$
- $a^{(k|a|+j)} \equiv a^{(m|a|+p)} \bmod n$
- $a^{k|a|} * a^j \equiv a^{m|a|} * a^p \bmod n$
- $a^j \equiv a^m \bmod n$

Proof:

- $a^b \equiv a^c \mod n$.
- Suppose b,c larger than the head of a. $b = k|a|+j$, $c = m|a|+p$ where $j,p < |a|$
- $a^{(k|a|+j)} \equiv a^{(m|a|+p)} \mod n$
- $a^{k|a|} * a^j \equiv a^{m|a|} * a^p \mod n$
- $a^j \equiv a^m \mod n$
- Therefore $j \equiv m \mod |a|$. $b \equiv c \mod n$

Proof:

- Suppose b $\equiv$ c mod n, b,c larger than the size of the head of a.

Proof:

- Suppose $b \equiv c \bmod n$. b,c larger than the size of the head of a.
- $b = k|a| + j$, $c = m|a| + j$

Proof:

- Suppose $b \equiv c \bmod n$. b,c larger than the size of the head of a.
- $b = k|a| + j$, $c = m|a| + j$
- $a^b \equiv a^{(k|a|+j)}$

Proof:

- Suppose $b \equiv c \bmod n$. b,c larger than the size of the head of a.
- $b = k|a| + j$, $c = m|a| + j$
- $a^b \equiv a^{(k|a|+j)}$
- $\equiv a^{(k|a|)}a^j$

Proof:

- Suppose b ≡ c mod n. b,c larger than the size of the head of a.
- $b = k|a| + j$, $c = m|a| + j$
- a^b ≡ a^(k|a|+j)
- ≡ a^(k|a|)a^j
- ≡ a^j

Proof:

- Suppose $b \equiv c \bmod n$. b,c larger than the size of the head of a.
- $b = k|a| + j$, $c = m|a| + j$
- $a^b \equiv a^{(k|a|+j)}$
- $\equiv a^{(k|a|)}a^j$
- $\equiv a^j$
- $\equiv a^{(m|a|+j)}$
- $\equiv a^c$

A Smaller Lemma

- Given n>1, for all a $\in Z_n$ $|a| < n$

A Smaller Lemma

- Given $n>1$, for all $a \in Z_n$ $|a| < n$
- $|a| \leq n$

A Smaller Lemma

- Given $n>1$, for all $a \in Z_n$ $|a| < n$
- $|a| \leq n$
- $|a| = n \Rightarrow a$^$k = 0 \Rightarrow |a| = 1$

A Smaller Lemma

- Given $n>1$, for all $a \in Z_n$ $|a| < n$
- $|a| \leq n$
- $|a| = n \Rightarrow a\hat{}k = 0 \Rightarrow |a| = 1$
- So the order of a is a monovariant.

Putting these things together

- Conjecture: For all a $\in Z_n$ there is a tetration of a that is congruent to all subsequent tetrations mod n

Putting these things together

- Conjecture: For all $a \in Z_n$ there is a tetration of a that is congruent to all subsequent tetrations mod n
- We must show there is a finite tower of a’s that will be congruent to every bigger tower of a’s

Putting these things together

- Conjecture: For all a $\in Z_n$ there is a tetration of a that is congruent to all subsequent tetrations mod n
- We must show there is a finite tower of a’s that will be congruent to every bigger tower of a’s
- Start with a guess

Putting these things together

- $a \uparrow k \equiv a \uparrow (k-1) \bmod n$

Putting these things together

- $a \uparrow k \equiv a \uparrow (k-1) \bmod n$
- $\Leftrightarrow a \uparrow (k-1) \equiv a \uparrow (k-2) \bmod |a \in Z_n|$

Putting these things together

- $a \uparrow k \equiv a \uparrow (k-1) \bmod n$
- $\Leftrightarrow a \uparrow (k-1) \equiv a \uparrow (k-2) \bmod |a \in Z_n|$
- $\Leftrightarrow a \uparrow (k-2) \equiv a \uparrow (k-3) \bmod |a \in Z_{|a|}|$

Putting these things together

- $a \uparrow k \equiv a \uparrow (k-1) \bmod n$
- $\Leftrightarrow a \uparrow (k-1) \equiv a \uparrow (k-2) \bmod |a \in Z_n|$
- $\Leftrightarrow a \uparrow (k-2) \equiv a \uparrow (k-3) \bmod |a \in Z_{|a|}|$
- And so on until...

Case 1: Our guess was too small

- The power of a is not big enough to get us into the cycle

Case 1: Our guess was too small

- The power of a is not big enough to get us into the cycle of some modulus.
- We can increment our original guess until it is big enough to enter into the cycle.

Case 2: Our guess was too small

- We’ve gotten to a modulus where our modulo equivalence is not true.

Case 2: Our guess was too small

- We’ve gotten to a modulus where our modulo equivalence is not true.
- We can increment our guess, and try again.

Case 3: End Game

- We have enough numbers in the tower to work our way all the way down into mod 1.

Case 3: End Game

- We have enough numbers in the tower to work our way all the way down into mod 1.
- We will always reach mod 1 with a finite tower, because |a| is a monovariant.

Case 3: End Game

- We have enough numbers in the tower to work our way all the way down into mod 1.
- We will always reach mod 1 with a finite tower, because |a| is a monovariant.
- So we’ve shown that there is a tower that will be congruent to it’s successor.

Finishing up

- Since we have enough in the tower to get down to mod 1, we can equate anything we'd like, including another tower

Finishing up

- Since we have enough in the tower to get down to mod 1, we can equate anything we'd like, including another tower
- Therefore, once we have one tower being congruent to it's successor, every tower after that will be congruent.

Finishing up

- Since we have enough in the tower to get down to mod 1, we can equate anything we'd like, including another tower
- Therefore, once we have one tower being congruent to it's successor, every tower after that will be congruent.
- QED

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- $2^2 \equiv 2 \mod 10$

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- $2^\wedge 2 \equiv 2 \bmod 10$
- Notice $|2 \in Z_{10}| = 4$. $\{2,4,8,6\}$

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- $2^2 \equiv 2 \mod 10$
- $2 \equiv 1 \mod 4$ Case 1.

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- 2^2^2 ≡ 2^2 mod 10

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- 2^2^2 ≡ 2^2 mod 10
- 2^2 ≡ 2 mod 4 Case 2

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- $2^\wedge 2^\wedge 2^\wedge 2 \equiv 2^\wedge 2^\wedge 2 \bmod 10$

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- $2^\wedge 2^\wedge 2^\wedge 2 \equiv 2^\wedge 2^\wedge 2 \bmod 10$
- $2^\wedge 2^\wedge 2 \equiv 2^\wedge 2 \bmod 4$

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- $2^\wedge2^\wedge2^\wedge2 \equiv 2^\wedge2^\wedge2 \bmod 10$
- $2^\wedge2^\wedge2 \equiv 2^\wedge2 \bmod 4$
- $2^\wedge2 \equiv 2 \bmod 1$

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- 2^2^2^2 ≡ 2^2^2 mod 10
- 2^2^2 ≡ 2^2 mod 4
- 2^2 ≡ 2 mod 1
- Winner!

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- 2^2^2 ≡ 6 mod 10

Example

- What tetration of 2 is congruent to all subsequent tetrations of 2 mod 10?
- $2^{\wedge}2^{\wedge}2 \equiv 6 \bmod 10$
- So the tetrations of 2 converge on 6 mod 10

Elements of Z_{10}

- 0 -> 0
- 1 -> 1
- 2 -> 6
- 3 -> 7
- 4 -> 6
- 5 -> 5
- 6 -> 6
- 7 -> 3
- 8 -> 6
- 9 -> 9

Thank you

To the ISMAA,
To Dr. Andrew Sward and Dr. Tom Bengtson,
To Earl H. Beiling,
And to you, for being a lovely audience.