Why Is the 3X + 1 Problem Hard?

Ethan Akin
Mathematics Department
The City College
137 Street and Convent Avenue
New York City, NY 10031

June, 2002

Published in 2004
Chapel Hill Ergodic Theory Workshops
(ed. I. Assani) Contemp Math **356**:1-20.

"It works over the two-adics." - D. Sullivan

Start with an odd natural number x. Multiply by 3 and add 1. From the resulting even number, divide away the highest power of 2 to get a new odd number $T(x)$. If you keep repeating this operation do you eventually hit 1, no matter what odd number you began with?

Simple to state, this problem remains unsolved. The operation T is easy to program on even a hand calculator. The numbers dance about in a tantalizing fashion, at times appearing to take off towards infinity but finally dropping down to 1.

One evening after dinner, Dennis Sullivan and I nibbled on this old chestnut. After the remark quoted above, he added "It illustrates the difficulty of describing particular orbits in an ergodic system." At the time I didn't see what he meant and the conversation meandered off to other subjects.

Over the next two weeks I finally saw the ergodic theory perspective which Dennis had been pointing along. This viewpoint, worked out by him and David Ruelle over lunch one day, does not solve the problem. Instead, it suggests why it is hard to solve.

In what follows I hope I can inspire you to share the delight I found in this peculiar reinterpretation of such an apparently simple system.

1 The Two-adic Integers

Because of the divisions by 2 in the operation it is easiest to deal with the natural numbers by writing them in base 2. So we think of a natural number as a finite sequence $a_0a_1a_2... = a_02^0 + a_12^1 + a_22^2 + ...$ with each $a_i = 0$ or 1. To add:

$$\begin{array}{rl} & a_0a_1a_2... \\ + & \underline{b_0b_1b_2...} \end{array} \tag{1.1}$$

first add $a_0 + b_0$ by $0 + 0 = 0; 0 + 1 = 1 + 0 = 1$; and $1 + 1 = 0$, carry the 1 to the next place. Then add $a_1 + b_1$ and the carry if any. Notice that I am writing the base 2 digits, i.e. the *bits*, in the reverse of the standard order so that you carry to the right.

For multiplication we can use the fact that each b_i is 0 or 1 to write:

$$\begin{array}{rl} & a_0a_1a_2... \\ \times & \underline{b_0b_1b_2...} \\ b_0\cdot & a_0a_1a_2... \\ b_1\cdot & \quad a_0a_1... \\ b_2\cdot & \qquad a_0... \\ \cdot & \qquad\quad \cdot \\ + & \underline{\qquad\quad} \end{array} \tag{1.2}$$

where we just cross out row i if $b_i = 0$ and include it if $b_i = 1$.

Notice now that these operations will work just fine even if the sequences are of infinite length. In multiplication, for example, because the rows are receding to the right, the i^{th} place of the answer will involve adding at most $2i$ 1's ($i+1$ rows and less than i carries). The infinite sequences of 0's and 1's with this notion of $+$ and $\times$ are called *two-adic integers* and the uncountable set of them is denoted $\mathbf{Z}_2$.

Since we generalized from the set of natural numbers, it is perhaps surprising that subtraction is always defined. Subtraction is again by the grade school rule but the trick is that you are allowed to "borrow" 1 from infinity if necessary. Alternatively, notice that

$$\begin{array}{r} 1111.... \\ +\ \underline{1000....} \\ 0000.... \end{array} \tag{1.3}$$

and so $-1 = 1111...$ Now for any sequence $a = a_0a_1a_2...$ define $\bar{a}$ by $\bar{a}_i = 0$ if $a_i = 1$ and vice-versa. Clearly, $a + \bar{a} = 1111... = -1$. So $a + (\bar{a} + 1) = 0$, or

$$-a \quad = \quad \bar{a} \ + \ 1. \tag{1.4}$$

From our original conception it is clear that a natural number, $0, 1, 2, ...$ is a 2-adic integer whose expansion terminates in a string of 0's. From (1) it follows that the negative integers $-1, -2, ...$ can be identified with the 2-adic integers whose expansions terminate in a string of 1's. We will reserve for the word *integer* its usual meaning, i.e. the natural numbers and their negatives, and refer to typical elements of $\mathbf{Z}_2$ as 2*-adics*.

As you might expect from the peculiar folding together of positive and negative integers, the order relation on the integers does not extend to the 2-adics.

The distinction between even and odd does extend. Call a 2-adic a *even* if $a_0 = 0$ and *odd* if $a_0 = 1$. Since multiplication by $2 = 0100...$ introduces a zero at the left end, i.e.

$$2 \ \times \ a_0a_1a_2... \quad = \quad 0a_0a_1... \tag{1.5}$$

it is clear that a number is even iff it is divisible by 2. You cannot divide and odd 2-adic by 2.

However, you can divide by any odd 2-adic:

$$\begin{array}{rl} & b_0 \\ 1a_1a_2... & |\overline{b_0b_1b_2...} \\ - & \underline{b_0c_1c_2...} \\ & \ \ d_1d_2... \end{array} \tag{1.6}$$

where $c_1c_2... = b_0 \times a_1a_2...$ Then continue the usual long division routine. Alternatively, we can construct the reciprocal $1/a$ for a odd by reversing the multiplication algorithm. For example:

$$
\begin{array}{rr}
1 & 1100000... \\
1 & 110000... \\
0 & 00000... \\
1 & 1100... \\
0 & 000... \\
1 & 11... \\
\cdot & \cdot \\
\cdot & + \quad \cdot \\
\hline
 & 1000000...
\end{array}
\tag{1.7}
$$

shows that for $3 = 11000...$, $1/3 = 11010101...$ Also, $3 \times (101010...) = 111...$ so that $-1/3 = 101010...$

We can also build the set of 2-adics by an inverse limit construction using congruence mod 2^k. This bit of abstract algebra provides a useful complement to the previous algorithmic approach.

Recall that two integers are congruence mod 2^k if their difference is divisible by 2^k. Because $+$ and $\times$ preserve congruence, these operations can be defined on the mod 2^k equivalence classes yielding the ring of integers mod 2^k, denoted $\mathbf{Z}/2^k$. Two natural numbers a and b are congruent mod 2^k, written $a \equiv b \bmod 2^k$, precisely when the base 2 expansions of a and b agree in the first k places. The mod 2^k congruence classes can be represented by the 2^k possible initial strings of k 0's and 1's. To add or multiply mod 2^k we just proceed as usual and ignore the results after the k^{th} bit.

Because congruence mod 2^k implies congruence mod 2^{k-1} there is an obvious restriction map $\rho_k : \mathbf{Z}/2^k \to \mathbf{Z}/2^{k-1}$ which forgets the last bit. The map preserves $+$ and $\times$, i.e. it is a ring homomorphism.

This business of ignoring everything after the k^{th} bit works for infinite sequences as well and so defines a map $\mathbf{Z}_2 \to \mathbf{Z}/2^k$ which preserves $+$ and $\times$. For $a \in \mathbf{Z}_2$ we define $[a]_k$ to be the mod 2^k congruence class of a:

$$[a]_k \quad =_{def} \quad \{b \in \mathbf{Z}_2 : b \equiv a \bmod 2^k\}. \tag{1.8}$$

So $[a]_k = [b]_k$ iff $a_i = b_i$ for $i = 0, 1, ..., k-1$. Notice that the restriction map corresponds to set inclusion:

$$\rho_k[a]_k \;=\; [b]_{k-1} \quad\Longleftrightarrow\quad a \equiv b \bmod 2^{k-1} \quad\Longleftrightarrow\quad [a]_k \;\subset\; [b]_{k-1}. \tag{1.9}$$

$\mathbf{Z}_2$ is the inverse limit of the sequence of rings $\mathbf{Z}/2^k$ and the connecting homomorphisms ρ_k. This means, first, that each $a \in \mathbf{Z}_2$ is uniquely described by the coherent sequence of congruence classes $\{[a]_k : k = 1, 2, ...\}$ where a sequence $\{\alpha_k \in \mathbf{Z}/2^k : k = 1, 2, ...\}$ is called *coherent* when $\rho_k\alpha_k = \alpha_{k-1}$. This much is true of the natural numbers as well. But for $\mathbf{Z}_2$ the correspondence to coherent sequences of congruence classes is onto as well as one-to-one. That is, every coherent sequence $\{\alpha_k\}$ determines a 2-adic. As we run along the coherent sequence the new information provided by α_k given α_{k-1} is precisely the k^{th} bit in the expension. It tells us whether a 0 or a 1 goes in the 2^{k-1} place.

This identification between the elements of $\mathbf{Z}_2$ and coherent sequences makes it easy to check what we have so far merely presumed implicitly: the usual arithmetic rules are true for $\mathbf{Z}_2$. The commutative, associative and distributive laws are inherited from the rings $\mathbf{Z}/2^k$.

Finally, we will call a 2-adic x *rational* if it can written $x = a/b$ for some integers a, b with b odd. We conclude this section with a series of exercises which shows that a 2-adic x is rational iff it is *terminally periodic*, that is, there exists a positive integer K such that $x_{i+K} = x_i$ for all sufficiently large i. If K is the smallest such integer then K is called the *period* of x. If $x_{i+K} = x_i$ for all i then x is called *periodic*. We have already seen that the integers are precisely those 2-adics which are terminally periodic of period 1, i.e. which are either eventually 0 or eventually 1. $0 = 000...$ and $-1 = 111...$ are the two 2-adics which are periodic of period 1.

Exercise 1 *(a) If x is periodic of period K then $x = -a/(2^K - 1)$ for some natural number a (Hint: Compute $x - 2^K x$).*

(b) Compute the expansion of $-1/(2^K - 1)$.

(c) Assume that x and y are terminally periodic and that n is an integer. Prove that $x + y$, $-x$ and $n \cdot x$ are terminally periodic.

(d) Prove: If x is terminally periodic then x is rational (Hint: Write $x = n + 2^L y$ with n a nonnegative integer and y periodic).

(e) *If n is an odd integer then n divides $2^K - 1$ for some K (Hint: Use the Euler ϕ function. Let $K = \phi(n)$ and use Fermat's Theorem from elementary number theory.)*

(f) *Prove: If x is rational then x is terminally periodic.*

2 The Two-adic Shift Map

Before wrestling with the operation T itself let us simplify (grossly) by omitting the multiplication by 3. Starting with an odd natural number x, divide away the highest power of 2 in $x+1$ to get the odd number $S(x)$. Clearly, $S(1) = 1$ while $S(x) < x$ if $x > 1$. So the sequence of iterates of S, $\{S^n(x)\}$ decreases monotonically to 1.

Instead of performing all of the divisions by 2 at once we can do them one at a time by defining:

$$s(x) \quad = \quad \begin{cases} x/2 & \text{if } x \text{ is even} \\ (x+1)/2 & \text{if } x \text{ is odd.} \end{cases} \tag{2.1}$$

Suppose we are given a set X and a function $q : X \to X$. We can define a dynamical system on X by iterating q. We imagine that the points of X evolve according to the rule $x_{t+1} = q(x_t)$ so that with each tick of the clock each point moves to its image under the mapping q. For $x \in X$ the *q-orbit* of x is the sequence in X: $\{x, q(x), (q \circ q)(x), ...\} = \{q^n(x) : n = 0, 1, 2, ...\}$.

Starting with an odd natural number x, look at the s-orbit of x. The S-orbit of x is precisely the subsequence of odd numbers in the s-orbit. If $s(x), ..., s^{k-1}(x)$ are all even and $s^k(x)$ is odd then k is called the *first return time* to the set of odds and $S(x) = s^k(x)$.

Because even 2-adics can be uniquely divided by 2 definition (2.1) works for the 2-adics as well, defining a function $s : \mathbf{Z}_2 \to \mathbf{Z}_2$. It will be more convenient to conjugate by -1 and define $\sigma(x) = -s(-x)$. So $\sigma : \mathbf{Z}_2 \to \mathbf{Z}_2$ is defined by:

$$\sigma(x) \quad = \quad \begin{cases} x/2 & \text{if } x \text{ is even} \\ (x-1)/2 & \text{if } x \text{ is odd.} \end{cases} \tag{2.2}$$

σ is called the *shift map* on $\mathbf{Z}_2$ because you get the base 2 expansion of $\sigma(x)$ by deleting x_0 and shifting the remaining bits left one place, i.e.

$$\sigma(x)_i \quad = \quad x_{i+1} \qquad \text{for } i \ = \ 0, 1, ... \tag{2.3}$$

So for the σ-orbit of x: $x = \sigma^0(x), \sigma^1(x), \sigma^2(x), ...$ it is clear that

$$x_i \quad = \quad \sigma^i(x)_0 \qquad \text{for } i \;=\; 0, 1, ... \tag{2.4}$$

which we can restate as:

$$x_i \quad = \quad \begin{cases} 0 & \text{if } \sigma^i(x) \text{ is even} \\ 1 & \text{if } \sigma^i(x) \text{ is odd.} \end{cases} \tag{2.5}$$

Thus, the base 2 expansion of x can be thought of as a coded tape describing the successive parities along the σ-orbit of x.

While the map σ is clearly onto, it is not one-to-one. In fact, for any $y \in \mathbf{Z}_2$ the equation $\sigma(x) = y$ has precisely two solutions correponding to the possible values of the initial digit of x deleted by σ. We can describe these by defining:

$$\tilde{\sigma}_0(y) \quad = \quad 2y \qquad \text{and} \qquad \tilde{\sigma}_1(y) \quad = \quad 2y + 1. \tag{2.6}$$

So we see that $\tilde{\sigma}_\epsilon(y)$ is just y shifted right one place with ϵ inserted in the now vacant 2^0 place. Thus, starting from any point in $\mathbf{Z}_2$ there are two different ways of moving backwards one step: an even way, $\tilde{\sigma}_0$ and an odd way $\tilde{\sigma}_1$.

Let us look at some special σ orbits.

x is a nonnegative integer iff $\sigma^i(x) = 000... = 0$ for i sufficiently large. On the other hand, x is a negative integer iff $\sigma^i(x) = 111... = -1$ for i sufficiently large. 0 and -1 are the only fixed points of σ, the only solutions of $\sigma(x) = x$. The integers are those 2-adics whose orbits eventually arrive at one of the fixed points.

σ has one cycle of period 2. Recall that $-1/3 = 101010...$ and so $-2/3 = 010101...$ Hence, $\sigma(-1/3) = -2/3$ and $\sigma(-2/3) = -1/3$.

In general, x is periodic iff x is a fixed point for some iterate of σ, i.e. $\sigma^K(x) = x$ for some positive integer K. The orbit of x returns to x after K iterates and thereafter repeats the cycle. That is, the base 2 expansion of x is periodic iff the σ-orbit of x is periodic. The results of Exercise 1 say that x is rational iff its σ-orbit eventually reaches such a periodic point and then enters a cycle.

3 The Two-adic 3X + 1 Map

Instead of looking at T directly it will be convenient to introduce the single step map τ which is related to T as s, defined by (2.1), was to S.

$$\tau(x) \quad = \quad \begin{cases} x/2 & \text{if } x \text{ is even} \\ (3x+1)/2 & \text{if } x \text{ is odd.} \end{cases} \tag{3.1}$$

As before, the T-orbit of x is the subsequence of odd numbers in the τ-orbit of x. So the original problem is equivalent to the conjecture that $\tau^i(x) = 1$ for some i whenever x is a positive integer. Notice, though, that 1 is not a fixed point for τ. Instead, $\tau(1) = 2$ and $\tau(2) = 1$. So the τ-orbit of 1 is a cycle of period 2.

Definition (3.1) extends as before to define a map $\tau : \mathbf{Z}_2 \to \mathbf{Z}_2$. Again we look for the sequence encoding the successive parities along the τ-orbit. For the shift map the base 2 expansion of x gave the coding. For τ it is no longer true that the expansion of x bears any simple relation to the coding. Instead we define the function $Q : \mathbf{Z}_2 \to \mathbf{Z}_2$ by:

$$Q(x)_i \quad = \quad \tau^i(x)_0 \qquad \text{for } i \; = \; 0, 1, ... \tag{3.2}$$

or, equivalently:

$$Q(x)_i \quad = \quad \begin{cases} 0 & \text{if } \tau^i(x) \text{ is even} \\ 1 & \text{if } \tau^i(x) \text{ is odd.} \end{cases} \tag{3.3}$$

Again τ maps $\mathbf{Z}_2$ onto itself and the equation $\tau(x) = y$ two solutions described by the two functions:

$$\tilde{\tau}_0(y) \quad = \quad 2y \qquad \text{and} \qquad \tilde{\tau}_1(y) \quad = \quad (2y-1)/3, \tag{3.4}$$

moving backwards along τ-orbits either the even way or the odd way.

Exactly because we have lost the simple relationship between the expansion and the map, it is worthwhile pausing here to see how the $\tilde{\tau}_\epsilon$'s are used.

Inductively, for $a_0 ... a_{k-1}$ a list of 0's and 1's of length k, we define:

$$\tilde{\tau}_{a_0 ... a_{k-1}}(y) \quad =_{def} \quad \tilde{\tau}_{a_0}(\tilde{\tau}_{a_1 ... a_{k-1}}(y)). \tag{3.5}$$

In other words, we start with y and move backwards the a_{k-1} way, then the a_{k-2} way, ... and finally the a_0 way, arriving at $x = \tilde{\tau}_{a_0 ... a_{k-1}}(y)$. Now if we start at x and move forward via τ for k steps we are back at y and along the way the parities are given by $a_0, a_1, ...$ Thus, $\tau^k(x) = y$ and

$$Q(x)_i \quad = \quad a_i \qquad \text{for } i \ = \ 0, 1, ..., k-1. \tag{3.6}$$

We now show that Q defines a *conjugacy* between τ and the shift map σ. This means that Q provides a recoding or change of coordinates on $\mathbf{Z}_2$ and under this change of coordinates τ is transformed into σ.

Theorem 1 *The function Q is a one-to-one map of $\mathbf{Z}_2$ onto itself. It defines a conjugacy between τ and σ. That is, we have following equation of composed maps:*

$$Q \circ \tau \quad = \quad \sigma \circ Q. \tag{3.7}$$

Proof: The conjugacy relation (3.7) is easy because for all x and i

$$Q(\tau(x))_i \ = \ \tau^i(\tau(x))_0 \ = \ \tau^{i+1}(x)_{i+1} \ = \ \sigma(Q(x))_i \tag{3.8}$$

by definitions (2.4) and (3.2).

The hard part is to prove that Q is one-to-one and onto. We use the correspondece between the 2-adics and the coherent sequences of mod 2^k congruence classes. We need a bit of algebraic spadework.

Notice first that for $k \geq 1$:

$$x \equiv x' \bmod 2^k \qquad \Longleftrightarrow \qquad x_0 = x'_0 \quad \text{and} \quad \sigma(x) \equiv \sigma(x') \bmod 2^{k-1}. \tag{3.9}$$

This just says that the first k bits agree iff the initial bits do and then the next $k-1$ bits agree as well.

The analogous result is true for τ as well. That is, for $k \geq 1$:

$$x \equiv x' \bmod 2^k \qquad \Longleftrightarrow \qquad x_0 = x'_0 \quad \text{and} \quad \tau(x) \equiv \tau(x') \bmod 2^{k-1}. \tag{3.10}$$

This time we have to use a bit of algebra. Clearly, $x \equiv x' \bmod 2^k$ implies $x_0 = x'_0$. If this common value is 0 then $\tau(x) = x/2 = \sigma(x)$ and $\tau(x') = x'/2 = \sigma(x')$. So in that case (3.10) follows from (3.9). Now suppose that $x_0 = x'_0 = 1$.If we let $\tau(x) = y$ and $\tau(x') = y'$ then we are going backwards the odd way and so $x = \tilde{\tau}_1(y) = (2y-1)/3$ and $x' = \tilde{\tau}_1(y') = (2y'-1)/3$. Thus, $x - x' = 2(y-y')/3$. Now $y \equiv y' \bmod 2^{k-1}$, i.e. $y - y'$ is divisible by 2^{k-1} iff $2(y-y')$ is divisible by 2^k. Multiplying by $1/3$ we see that this is true iff $2(y-y')/3$ is divisible by 2^k, i.e. iff $x \equiv x' \bmod 2^k$.

From these equivalences we derive:

Proposition 2 *For any $y \in \mathbf{Z}_2$, $Q^{-1}([y]_k) = \{x \in \mathbf{Z}_2 : Q(x) \equiv y \text{ mod } 2^k\}$ is a single mod 2^k congruence class. In particular, for $x, x' \in \mathbf{Z}_2$*

$$x \equiv x' \text{ mod } 2^k \qquad \Longleftrightarrow \qquad Q(x) \equiv Q(x') \text{ mod } 2^k. \tag{3.11}$$

Proof: If $w \in \mathbf{Z}_2$ and $x = \tilde{\tau}_{y_0 \dots y_{k-1}}(w)$ then by (3.6) $Q(x) \equiv y$ mod 2^k. Thus, the set $Q^{-1}([y]_k)$ is nonempty. It suffices to demonstrate (3.11) in order to complete the proof.

We prove (3.11) by induction on k. For the initial step, $k = 0$, observe that $x_0 = Q(x)_0$ and $x'_0 = Q(x')_0$. For the inductive step we use the conjugacy equation (17) which we have already proved.

First assume $x \equiv x'$ mod 2^k. Apply (3.10) to get $x_0 = x'_0$ and $\tau(x) \equiv \tau(x')$ mod 2^{k-1}. By inductive hypothesis, $Q(\tau(x)) \equiv h(\tau(x'))$ mod 2^{k-1}. The conjugacy equation (3.7) allows us to rewrite this as $\sigma(Q(x)) \equiv \sigma(Q(x'))$ mod 2^{k-1}. Meanwhile, $Q(x)_0 = x_0 = x'_0 = Q(x')_0$. So (3.9) implies $Q(x) \equiv Q(x')$ mod 2^k. Furthermore, the reasoning we have just used is completely reversible to prove the implication the other way.

This completes the proof of Proposition 2 and we use it to complete the proof of the theorem by showing that given $y \in \mathbf{Z}_2$ there exists a unique $x \in \mathbf{Z}_2$ such that $Q(x) = y$. Proposition 2 implies that $\{Q^{-1}([y]_k) : k = 0, 1, \dots\}$ is a sequence of mod 2^k congruence classes. Recall from (4) that coherence of the sequence just says that the sequence of sets is monotonically decreasing. Because this is true for the sequence $\{[y]_k\}$ it is clearly true for $\{Q^{-1}([y]_k)\}$. The coherent sequence $\{Q^{-1}([y]_k)\}$ corresponds to the unique $x \in \mathbf{Z}_2$ defined by $\{x\} = \cap_k Q^{-1}([y]_k)$. Because $Q(x) \equiv y$ mod 2^k for all k, $Q(x) = y$.

QED

The conjugacy h transforms τ-orbits to σ-orbits. To see this, do an easy induction on (3.7) to get

$$Q \circ \tau^i \quad = \quad \sigma^i \circ Q \qquad \text{for } i = 0, 1, 2, \dots \tag{3.12}$$

So if we apply Q to the τ-orbit: $x, \tau(x), \tau^2(x), \dots$ we get the σ-orbit of $Q(x)$: $Q(x), \sigma(Q(x)), \sigma^2(Q(x)), \dots$ We use this to see that for any positive integer K, $Q(\tau^K(x))$ is exactly $Q(x)$ truncated by the removal of the initial K bits.

In order to understand how τ behaves on a subset N of $\mathbf{Z}_2$, we need only compute $Q(N)$. In particular, when N is the set of positive integers our problem becomes transformed as follows.

Proposition 3 *If x is a positive integer then $\tau^i(x) = 1$ for some i iff the 2-adic $-3Q(x)$ is a positive integer, in which case, as a positive integer it is relatively prime to 3.*

Proof: For 2 and 1/3 the τ-orbits are, respectively: $2, 1, 2, 1, ...$ and $1/3, 1, 2, 1, ...$ Consequently:

$$\begin{array}{rcccc} Q(1) & = & 101010... & = & -1/3 \\ Q(2) & = & 010101... & = & -2/3 \\ Q(1/3) & = & 110101... & = & 1/3 \end{array} \tag{3.13}$$

Now suppose that x is an integer greater than 2 and $\tau^i(x) = 1$ for some i. Let k be the smallest such i and let $y = Q(x)$. Because $\sigma^k(Q(x)) = Q(\tau^k(x)) = Q(1)$, we have $Q(x) = y_0 y_1 ... y_{k-1} 1010...$ and

$$Q(\tau^{k-1}(x)) \;=\; \sigma^{k-1}(Q(x)) \;=\; y_{k-1}1010... \tag{3.14}$$

Were $y_{k-1} = 1$ this would mean that $Q(\tau^{k-1}(x))$ would be $1/3$ and so $\tau^{k-1}(x) = 1/3$ which is impossible for integral x. Hence, $y_{k-1} = 0$. Similarly, $y_{k-2} = 0$ for if not then $Q(\tau^{k-2}(x)) = 1010... = Q(1)$ and k was defined to be the smallest i such that $\tau^i(x) = 1$.

Thus, if we let n be the nonnegative integer with binary expansion $y_0 y_1 ... y_{k-3} 000...$ then $Q(x) = n + 2^k \cdot (-1/3)$ and so $-3Q(x) = 2^k - 3n$.

If $-3Q(x)$ were divisible by 3 as a whole number then $Q(x)$ would be a negative integer whose expansion terminates in a string of 1's. But -1 is a fixed point for τ and so $Q(-1) = 111... = -1$. As -1 cannot lie on the τ-orbit of a positive integer like x, it follows that $Q(x)$ cannot terminate in a string of 1's.

Finally, it is easy to check that if $Q(x) = -a/3$ with a a positive integer prime to 3 then the expansion of $Q(x)$ terminates in the cycle 1010... Since Q is one-to-one the τ-orbit of x then terminates in the cycle $1, 2, 1, 2, ...$

QED

While suggestive, these results are not as helpful as they might appear to be. Unfortunately, the only way to compute $Q(x)$ is to use the definition (3.3) which requires knowledge of the entire τ-orbit of x.

One idea is to compute $Q(x) \bmod 2^k$. By (3.11) we can define the bijection $[Q]_k : \mathbf{Z}/2^k \to \mathbf{Z}/2^k$ by $[Q]_k([x]_k) = [Q(x)]_k$. Perhaps we can discern a pattern from these finite approximations.

But probably not. It is time to raise the difficulty which underlies this whole approach to the original problem. The method is too general. It will work just as well if instead of using τ we define, for a any odd 2-adic, the map $\tau_a : \mathbf{Z}_2 \to \mathbf{Z}_2$ by

$$\tau_a(x) \quad = \quad \begin{cases} x/2 & \text{if } x \text{ is even} \\ (ax+1)/2 & \text{if } x \text{ is odd.} \end{cases} \tag{3.15}$$

We can then define $Q_a : \mathbf{Z}_2 \to \mathbf{Z}_2$ by replacing τ by τ_a in (3.2) and (3.3), i.e.

$$Q_a(x)_i \quad = \quad \tau_a^i(x)_0 \qquad \text{for } i \ = \ 0, 1, ... \tag{3.16}$$

The analogue of Proposition 2 with Q repaced by Q_a is still true with the same proof (replace multiplication by $1/3$ with multiplication by $1/a$). Just as before Q_a is a one-to-one onto map with

$$Q_a \circ \tau_a \quad = \quad \sigma \circ Q_a. \tag{3.17}$$

With $a = 5$, for example, $13, 33, 83, 208, 104, 52, 26, 13$ and $1, 3, 8, 4, 2, 1$ are disjoint cycles. The original problem appears to depend delicately upon the choice of $a = 3$. However, this approach might be useful for a portion of the problem.

Proposition 4 *Let a be an odd 2-adic. For $x \in \mathbf{Z}_2$ the τ_a-orbit eventually enters a cycle iff $Q_a(x)$ is a rational 2-adic.*

Proof: If K, L are positive integers and $\tau_a^{i+K}(x) = \tau_a^i(x)$ for all $i \geq L$ then by (3.16), $Q_a(x)_{i+K} = Q_a(x)_i$ for all $i \geq L$. Thus, $Q_a(x)$ is terminally periodic and so is rational by Exercise 1.

Conversely, suppose that $Q_a(x)$ is terminally periodic so for some K, L, $Q_a(x)_{i+K} = Q_a(x)_i$ for all $i \geq L$. Conjugacy with the shift map implies that $Q_a(\tau_a^{i+K}(x)) = Q_a(\tau_a^i(x))$ for all $i \geq L$. Since Q_a is one-to-one, it follows that $\tau_a^{i+K}(x) = \tau_a^i(x)$ for all $i \geq L$. Thus, the τ_a-orbit of x is eventually cyclic.

QED

Theorem 5 *Let a be an odd, rational 2-adic. If for $x \in \mathbf{Z}_2$, $Q_a(x)$ is rational then x is rational.*

Proof: By Proposition 4, the τ_a-orbit of x is eventually periodic. That is, there exist positive integers K, L such that $\tau_a^{i+K}(x) = \tau_a^i(x)$ for all $i \geq L$. Let $y = \tau_a^L(x) = \tau_a^{L+K}(x)$ so that $\tau_a^{i+K}(y) = \tau_a^i(y)$ for all nonnegative integers i.

Following (3.4) define

$$\tilde{\tau}_{a0}(y) \quad = \quad 2y \qquad \text{and} \qquad \tilde{\tau}_{a1}(y) \quad = \quad (2y-1)/a. \tag{3.18}$$

Notice that the coefficients are rational because a is rational.

Let $h_0 ... h_{K-1}$ be the first K bits of $Q_a(y)$. The periodicity of τ_a-orbit of y implies that

$$y \quad = \quad \tilde{\tau}_{ah_0}(\tilde{\tau}_{ah_1}(...\tilde{\tau}_{ah_{K-1}}(y))...)). \tag{3.19}$$

This in turn says that y is the solution of an equation:

$$y \quad = \quad 2^K c_1 y \; + \; c_2 \tag{3.20}$$

with c_1 and c_2 rational. Hence, $y = -c_2/(2^K c_1 - 1)$ is rational.

Finally, let $k_0 ... k_{L-1}$ be the first L bits of $Q_a(x)$. Just as before we have

$$x \quad = \quad \tilde{\tau}_{ak_0}(\tilde{\tau}_{ak_1}(...\tilde{\tau}_{ak_{L-1}}(y))...)). \tag{3.21}$$

Hence,

$$x \quad = \quad 2^K d_1 y \; + \; d_2 \tag{3.22}$$

with d_1 and d_2 rational. Thus, x is rational as well.

QED

We label the -definitely unproved- converse:

Rationality Conjecture 6 *Let a be an odd, rational 2-adic. If for $x \in \mathbf{Z}_2$, x is rational then $Q_a(x)$ is rational. That is, the map $Q_a : \mathbf{Z}_2 \to \mathbf{Z}_2$ preserves rationality.*

If x is a positive, odd integer then there are a priori two ways by which the τ-orbit of x might avoid 1. It may remain bounded and so enter a cycle, but some as yet undiscovered cycle disjoint from the cycle of period 2 which contains 1. Alternatively, the orbit might tend to infinity in which case we call it a *divergent orbit*. The Rationality Conjecture rules out such divergent orbits. Furthermore, if true, the conjecture rules out divergent orbits for τ_a with a any positive, odd integer.

Exercise 2 *For any positive integer k, compute the smallest positive number x such that the τ-orbit of x begins with k odd numbers. That is, compute the unique $x < 2^k$ such that $Q(x) \equiv -1 \text{ mod } 2^k$.*

Exercise 3 *For all $x \in \mathbf{Z}_2$ prove $Q(2x) = 2Q(x)$.*

Exercise 4 *For a, b odd 2-adics define the functions $\mu_b, \tau_{a,b} : \mathbf{Z}_2 \to \mathbf{Z}_2$ by $\mu_b(x) = b \cdot x$ and*

$$\tau_{a,b}(x) \quad = \quad \begin{cases} x/2 & \text{if } x \text{ is even} \\ (ax+b)/2 & \text{if } x \text{ is odd.} \end{cases} \tag{3.23}$$

Prove that μ_b is one-to-one and onto and prove the conjugacy

$$\mu_b \circ \tau_a \quad = \quad \tau_{a,b} \circ \mu_b. \tag{3.24}$$

Exercise 5 *Define the real-valued function v on $\mathbf{Z}_2$ by $v(0) = 0$ and for $x \neq 0$, $v(x) = 2^{-k}$ where 2^k is the highest power of 2 dividing x, i.e. k is the number of 0's which precede the first 1 in the expansion of x. (v is called the* 2-adic valuation function.*) Let $d(x, x') =_{def} v(x - x')$. Prove that $d : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{R}$ satisfies the conditions (for all $x, x', x" \in \mathbf{Z}_2$):*

1. $d(x, x') = 0$ *iff* $x = x'$.

2. $d(x, x') = d(x', x)$.

3. $d(x, x') \leq max(d(x, x"), d(x", x'))$.

Show that condition 3 (called the ultrametric inequality*) implies the* triangle inequality $d(x, x') \leq d(x, x") + d(x", x')$*. Consequently, we can define distance on* $\mathbf{Z}_2$ *by using the metric* d*. Show that if* r *is a real number between* 2^{-k} *and* 2^{-k+1} *then for* $y \in \mathbf{Z}_2$

$$\{x : d(y, x) < r\} \quad = \quad \{x : d(y, x) \leq r\} \quad = \quad [y]_k. \tag{3.25}$$

(The resulting topology is the same as the product topology obtained by regarding $\mathbf{Z}_2$ *as the countable product of copies of* $\{0, 1\}$*. Thus, the set of* 2*-adics has the structure of a compact topological ring.)*

Exercise 6 *Using the metric* d *defined in the previous exercise, prove that* $\tau_{a,b}$ *defined in Exercise 4 satisfies*

$$d(\tau_{a,b}(x), \tau_{a,b}(x')) \quad \leq \quad 2d(x, x'). \tag{3.26}$$

Conclude that σ *(*$a = 1$ *and* $b = -1$*) and* τ *(*$a = 3$ *and* $b = 1$*) are continuous. Prove that* Q *and* μ_b *are isometries, e.g.* $d(Q(x), Q(x')) = d(x, x')$ *(Use (3.11)).*

4 Ergodic Theory Viewpoint

Think of $y = y_0 y_1 y_2 ...$ in $\mathbf{Z}_2$ as the typical outcome of an infinite sequence of independent flips of a so-called "fair coin", labeled 0 on one side and 1 on the other. This tactic introduces probability theory into our study of the 2-adics. We assume that the two outcomes of each flip are equally likely and that the outcomes of the separate flips are independent of one another. The probability of a 0 or a 1 on each flip is thus $\frac{1}{2}$. From the independence assumption all 2^k possible outcomes $y_0 y_1 ... y_{k-1}$ are equally likely. For any subset $A \subset \mathbf{Z}_2$ we will write $PR(A)$ for the probability that y lies in A.

Technically, this is defined only for certain *measurable subsets* but these will include all that we will consider. So for $y \in \mathbf{Z}_2$

$$\text{Probability that } \; x \equiv y \bmod 2^k \quad = \quad PR([y]_k) \quad = \quad 2^{-k}. \tag{4.1}$$

A map $H : \mathbf{Z}_2 \to \mathbf{Z}_2$ is said to *preserve probability* if for any measurable subset A of $\mathbf{Z}_2$

$$\text{Probability that } \; H(x) \in A \quad = \quad PR(H^{-1}(A)) \quad = \quad PR(A). \tag{4.2}$$

In order to check that (4.2) holds, it in fact suffices to check the equation for sets A of the form $[y]_k$.

For example, the shift map σ preserves probability since $\sigma(x) \in [y]_k$ says that the bits $x_1 ... x_k$ are specified by the list $y_0 ... y_{k-1}$ and this event has probability 2^{-k}.

The study of such probability preserving mappings is the domain of ergodic theory. For a nice introduction see Billingsley (1965).

In addition to being probability preserving, σ is *mixing*. This property says that information about the initial state x is gradually lost as we move along the σ-orbit of x. For example, if we know that $x \in [y]_k$ then the first k bits of x are specified by y, but we know nothing about $\sigma^k(x)$. The initial data puts no constraint whatever on $\sigma^i(x)$ for $i \geq k$. In fact, for $i \geq k$ the events $x \in [y]_k$ and $\sigma^i(x) \in [y']_{k'}$ are independent in the same sense that two different flips of the coin are independent.

Contrast this with the translation map $\alpha : \mathbf{Z}_2 \to \mathbf{Z}_2$ given by $\alpha(x) =_{def} x + 1$. α preserves probability because

$$\alpha^{-1}([y]_k) \quad = \quad [y-1]_k, \tag{4.3}$$

which has probability 2^{-k}. On the other hand, $\alpha^i(x) \equiv x \bmod 2^k$ whenever 2^k divides i. So the condition $x \in [y]_k$ implies $\alpha^i(x) \in [y]_k$ whenever 2^k divides i and so for infinitely many i. Thus, α is not mixing.

Like σ the map τ preserves probability and is mixing. This in turn follows from the fact that the conjugacy map Q preserves measure. To prove the Q result notice that Proposition 2 says that $Q^{-1}([y]_k)$ is a mod 2^k congruence class and so has probability 2^{-k}.

As described in Billingsley (1965) an important consequence of the mixing property is *ergodicity*.

Suppose that $f : \mathbf{Z}_2 \to \mathbf{R}$ is a real-valued (and measurable) function. For simplicity we will suppose that f takes on only finitely many values:

$f_1, ..., f_n$. Define p_i to be the probability that $f(x) = f_i$ for $i = 1, ..., n$. The *space average* or *mean* or *expected value* of f on $\mathbf{Z}_2$ is given by

$$E(f) \quad =_{def} \quad \sum_{i=1}^{n} f_i p_i. \tag{4.4}$$

The name comes from imagining that we compute the average value of f by choosing randomly a large number of points in $\mathbf{Z}_2$: $x^1, ..., x^N$. For approximately Np_i of these points it will be true that $f(x) = f_i$. So the statistical average will satisfy

$$\frac{1}{N}\sum_{j=1}^{N} f(x^j) \quad \sim \quad \frac{1}{N}\sum_{i=1}^{n} f_i N p_i \quad = \quad E(f). \tag{4.5}$$

On the other hand, suppose that $H : \mathbf{Z}_2 \to \mathbf{Z}_2$ is a probability preserving mapping. Starting from an initial point $x \in \mathbf{Z}_2$ the associated *time average* $\hat{f}(x)$ is obtained by averaging the values along the H-orbit of x.

$$\hat{f}(x) \quad =_{def} \quad Lim_{N \to \infty} \frac{1}{N}\sum_{i=0}^{N-1} f(H^i(x)) \tag{4.6}$$

provided that the limit exists.

If H preserves probability and is mixing then the Birkhoff Ergodic Theorem says that for almost every initial state x the time average $\hat{f}(x)$ exists and equals the space average $E(f)$. The remaining points, those at which the limit of (4.6) either fails to exist or exists and is unequal to $E(f)$, together form a set of measure zero. $\{x : \hat{f}(x) = E(f)\}$ might not be the whole space $\mathbf{Z}_2$ but it does have probability 1.

Let us apply this to the *characteristic function* of the congruence class $[y]_k$ which is given by

$$1_{[y]_k}(x) \quad =_{def} \quad \begin{cases} 1 & \text{if } x \equiv y \bmod 2^k \\ 0 & \text{otherwise.} \end{cases} \tag{4.7}$$

Clearly, the space average of $1_{[y]_k}$ is the probability of $[y]_k$ which is 2^{-k}.

On the other hand, the sum

$$\sum_{i=0}^{N-1} 1_{[y]_k}(H^i(x)) \tag{4.8}$$

is just the number of occurrences of $[y]_k$ among the first N elements of the H-orbit of x. The Ergodic Theorem says that for a typical element x the congruence $H^i(x) \equiv y \bmod 2^k$ occurs approximately once in every run of 2^k elements along the orbit.

We will call a point H *generic* if this typical behavior occurs for every congruence class. That is, x is generic if for every congruence class $[y]_k$

$$Lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N-1} 1_{[y]_k}(H^i(x)) \quad = \quad 2^{-k}. \tag{4.9}$$

We call a point *exceptional for* H if it is not H generic.

While $\mathbf{Z}_2$ is uncountable, there are only countably many congruence classes and so (4.6) imposes only countably many conditions. It follows that the set of exceptional points has measure zero. It is important to notice that any countable set has measure zero and so the exceptional set can be infinite.

Now apply this with $H = \tau$. If x is a τ generic point in $\mathbf{Z}_2$ then for every pair of positive integers y and k, $\tau^i(x) \equiv y \bmod 2^k$ infinitely often. On the other hand, the original conjecture says that for any positive integer x eventually $\tau^i(x)$ is either 1 or 2. Such a point could not be τ generic. In fact, the τ-orbit of a τ generic point cannot enter any cycle. Thus, the Rationality Conjecture would say that every rational x is exceptional.

This at last answers the question of our title. The problem is hard because we are looking at a particular countable subset of the uncountable set $\mathbf{Z}_2$ and on it we are trying to demonstrate that a kind of behavior occurs which we know to be completely atypical. This is what Sullivan meant by his comment quoted in the introduction.

5 Concluding Remarks

We mentioned earlier that a proof of the conjecture will have to provide an explanation of the essential role of the number 3 (as opposed to 5 say) in the definition of τ. From probability theory we can derive a heuristic expanation - possibly misleading - of why 3 is special.

Recall that our original operation $T(x)$ is the first return of the τ-orbit of an odd number x to the set of odds. We let $\nu(x)$ be the first return time to the set of odds:

$$\nu(x) \quad =_{def} \quad \min \, \{i \geq 1 : \tau^i(x)_0 \; = \; 1\}. \tag{5.1}$$

If $x = 0$ or $-1/3$ then $\tau(x) = 0$ and $\nu(x) = \infty$. Otherwise, $\tau(x)$ is nonzero and $\nu(x)$ is one more than the number of initial 0's in the expansion of $\tau(x)$. Recall that when y is even, $\tau(y) = \sigma(y)$. Alternatively, recall that $Q(x)$ is sequence of parities along the τ-orbit of x. Thus, the successive return times are the number of iterations between successive 1's. So if x is an odd number then

$$\nu(x) > k \quad \Longleftrightarrow \quad \tau(x) \equiv 0 \bmod 2^k \quad \Longleftrightarrow \quad Q(x) \equiv 1 \bmod 2^{k+1}. \tag{5.2}$$

Now if x is an odd number then we define the *multiplier* $M(x) =_{def} 3 \cdot 2^{-\nu(x)}$. For an odd integer x, the multiplier $M(x)$ is approximately the ratio $T(x)/x$. The initial odd step multiplies by approximately $3/2$ and each successive even step multiplies by $1/2$. In particular, the multiplier is less than 1 and $T(x) < x$ unless $\nu(x) = 1$, i.e. $\tau(x)$ is odd.

Proposition 7 *Regarding M as a real-valued function on the odd 2-adics, its mean or expected value $E(M)$ is 1.*

Proof: When we restrict to the subset of odd numbers we are considering the conditional probability of an event assuming oddness. If A is a subset of the odd numbers then this conditional probability, $PR_o(A)$, is exactly $2 \cdot PR(A)$ since the probability of the set of odds is $\frac{1}{2}$. From (5.2) we have

$$\begin{aligned} PR_o(\{x : x_0 = 1 \text{ and } \nu(x) > k\}) &= \\ 2 \cdot PR(\{x : Q(x) \equiv 1 \bmod 2^{k+1}\}) &= 2^{-k} \end{aligned} \tag{5.3}$$

and so

$$\begin{aligned} PR_o(\{x : \nu(x) = k\}) &= \\ PR_o(\{x : \nu(x) > k-1\}) - PR_o(\{x : \nu(x) > k\}) &= 2^{-k}. \end{aligned} \tag{5.4}$$

Hence, $PR_o(\{x : M(x) = 3 \cdot 2^{-k}\}) = 2^{-k}$ and so

$$E(M) \quad = \quad \sum_{k=1}^{\infty} 3 \cdot 2^{-k} \cdot 2^{-k} \quad = \quad 1. \tag{5.5}$$

QED

On the other hand, suppose we proceed analogously for τ_a with a an odd integer larger than 3. Define $\nu_a(x)$ as the first return time to the odds for the τ_a-orbit of x and define for odd x the multiplier $M_a(x) = a \cdot 2^{\nu_a(x)}$. The computation in Proposition 7 then yields $E(M_a) = a/3 > 1$.

Thus, 3 is special in that, on average, $T(x)$ is roughtly the same size as x. However, when we replace 3 by the odd integer a the size of the odd numbers along the τ_a-orbit appear to be increasing geometrically with ratio $a/3$. This suggests that for such a most orbits should be divergent.

Wait a minute here! The computations of $E(M_a)$ are fine but the ratio interpretations we have given them may be just elaborate flim-flam. The heuristics only apply to integer values of x. As we have seen, not only are the integers of measure zero but they are probably completely atypical points for the systems we are examining.

As we seem to be in danger of wandering into nonsense perhaps we should stop here and return the problem to the imagination of the reader who may wish to consult some of the works listed below. The surveys Lagarias (1985), Müller (1991) and Wirsching (1998) are good places to start.

At this point I would like to acknowledge the help of the referee whose intimate knowledge of the subject greatly exceeds my passing acquaintance. In addition to supplementing my bibliography below, he provided some remarks which I would like to pass along to the reader.

First, the 2-adic, ergodic theory approach to the $3X + 1$ problem has a continuing history which began before the lunchtime discussion between Sullivan and Ruelle. This viewpoint was taken in Mathews and Watts (1984, 1985) and recent work extending it appears in Venturini (1992), Bernstein (1994), Bernstein and Lagarias (1996), Wirsching (1998) and in Monks and Yazinski (2002).

Second, the peculiar expected value computations given above support the idea that divergent trajectories exist for the $aX + 1$ map on the integers when a is an odd integer greater than 3. This would mean that the Rationality Conjecture is false for τ_a with $a \geq 5$. In fact, various authors have conjectured that such divergent trajectories may in fact be generic points for τ_a. For $a = 3$ divergent trajectories may or may not exist, this is exactly the open $3X + 1$ problem, but it is an implicit consequence of some recent work of Monks and Yazinski (2002) that rational points are at least not generic points for τ.

Theorem 8 *Every rational point of* $\mathbf{Z}_2$ *is an exceptional point for the map*

τ associated with $a = 3$.

Proof If $x = \frac{p}{q}$ with q odd then the τ-iterates of x all lie in $\frac{1}{q}\mathbf{Z}$ and so either enter a periodic orbit or diverge. If the periodic orbit has period d then the iterates cannot be equidistributed mod 2^{d+1} since some residue classes are omitted. In the divergent case, Monks and Yazinski (2002) have shown (their Theorem 2.7b) that

$$lim\ inf_{k\to\infty}\frac{1}{k}(Q(x)_0+...+Q(x)_{k-1}) \quad \geq \quad (log2)/(log3) \quad > \quad 0.63. \tag{5.6}$$

For a generic point x this limit would exist and equal .5. QED

Bibliography

D.J. Bernstein (1994) *A non-iterative 2-adic statement of the $3x+1$ conjecture* Proc. Amer. Math. Soc. **121**: 405-408.

D.J. Bernstein and J.C. Lagarias (1996) *The $3x+1$ conjugacy map* Canad. J. Math. **48**: 1154-1169.

P. Billingsley (1965) **Ergodic theory and information** John Wiley and Sons, New York.

F.P. Gouvêa (1993) **p-adic numbers** Springer-Verlag, Berlin.

J.C. Lagarias (1985) *The $3x+1$ problem and its generalizations* Amer. Math. Monthly **92**:3-21.

J.C. Lagarias (1990) *The set of rational cycles for the $3x+1$ problem* Acta Arith. **56**:33-53.

G.T. Leavens and M. Vermeulen (1992) *$3x+1$ search programs* Computers and Mathematics with Applications **24**: 79-99.

K.R. Matthews and A.M. Watts (1984) *A generalization of Hasse's generalization of the Syracuse algorithm* Acta Arithmetica **43**: 167-175.

K.R. Matthews and A.M. Watts (1985) *A Markov approach to the generalized Syracuse algorithm* Acta Arithmetica **45**: 29-42.

K. Monks and J. Yazinki (2002) *The autoconjugacy of the* $3x + 1$ *function*, to appear.

H. Müller (1991) *Das* $3n + 1$ *problem* Mitteilungen der Math. Ges. Hamburg **12**:231-251.

G. Venturini (1992) *Iterates of number theoretic functions with periodic rational coefficients (generalization of the* $3x + 1$ *problem)* Studies in Applied Math. **86**: 185-218.

S. Wagon (1985) *The Collatz problem* Math. Intelligencer **7**:72-76.

G.J. Wirsching (1998) **The dynamical system generated by the 3n+1 function** Lect. Notes in Math. No. 1681, Springer-Verlag, Berlin.