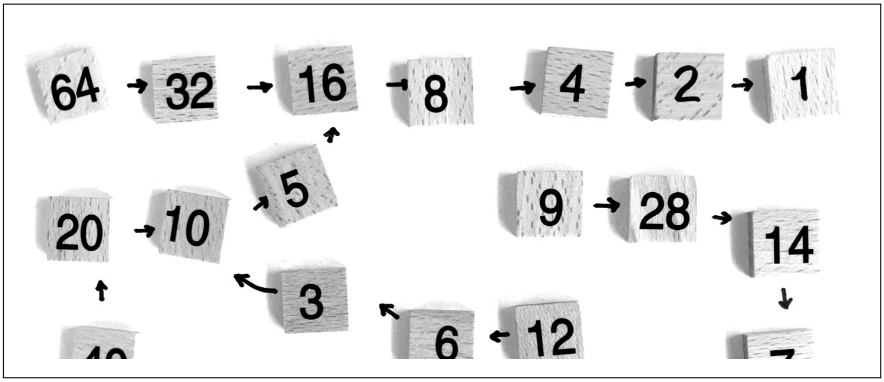


Chapter 1

What's the problem?

I'll pick a number between one and two,
And I'll ask myself, "What would Julius Caesar do?"
Bob Dylan

Math kook

I once read a book about a regular person, by which I mean they didn't own a surfboard or know how to surf. Yet they gave themselves a goal: within one year, they would get *barreled*. That's when a giant wave breaks above your head, and you shoot gracefully through a rolling tube of water. Also known as getting pitted, slotted, tubed, or kegged.

This regular person was what surfers call a **kook**, a novice, and … kooks don't get barreled. They get slammed and concussed, and they are constantly in the way, but they don't get barreled. So, I really respected that author for setting such an awesome goal. I can't remember how the book ends. Maybe they did it! At least they got a deep understanding of the power and chaos of the ocean, and finally, they were no longer a kook.

This is not a book about surfing. It's about math. Two years ago, I was a math kook. I took high-school math, but I never took calculus or number theory in college. I liked computers, so I went on to study computer science, but math was always a weak spot for me.

So, being a kook, I naturally decided to tackle one of the most notorious unsolved problems in mathematics, one that has confounded the world's best mathematicians for decades.

The 3n+1 problem

Here's the problem:

> Take any number.
> If it's odd, multiply it by 3 and add 1.
> If it's even, divide it by 2.
> Then repeat.

For example, let's start with 7. It's odd, so the next number is 22, which is even, and so on:

> 7 - 22 - 11 - 34 - 17 - 52 - 26 - 13 - 40 - 20 - 10 - 5 - 16 - 8 - 4 - 2 - 1

The numbers kind of bounce up and down. Or start with 84:

> 84 - 42 - 21 - 64 - 32 - 16 - 8 - 4 - 2 - 1

How can this be one of the most notorious unsolved problems in mathematics? Despite a great deal of effort, the world's mathematicians have been unable to resolve the **3n+1 conjecture**:

> The 3n+1 Conjecture. All numbers eventually reach 1.

Every number that's ever been tried ends up at 1. Like this one:

> 1438 - 719 - 2158 - 1079 - 3238 - 1619 - 4858 - 2429 - 7288 - 3644 - 1822 - 911 - 2734 - 1367 - 4102 - 2051 - 6154 - 3077 - 9232 - 4616 - 2308 - 1154 - 577 - 1732 - 866 - 433 - 1300 - 650 - 325 - 976 - 488 - 244 - 122 - 61 - 184 - 92 - 46 - 23 - 70 - 35 - 106 - 53 - 160 - 80 - 40 - 20 - 10 - 5 - 16 - 8 - 4 - 2 - 1

Each number takes its own winding, random-looking path. When I say the numbers kind of bounce up and down, that's an understatement. How they bounce around is, as Winston Churchill once described Russia, a riddle wrapped in a mystery inside an enigma.

Speaking of Russia

At the height of the Cold War, Soviet government scientists devised the 3n+1 conjecture as a fiendishly difficult mathematical puzzle. Using a coded one-time pad, they sent the conjecture to Franz-Josef Vogler, an assistant professor in Yale University's math department, and a KGB plant. Professor Vogler casually described the problem to his colleagues in the faculty lounge, and they were instantly entranced.

Working feverishly throughout the day, the professors filled up several blackboards. They forgot to eat their packed lunches. Fresh coffee was brought in. It went on like this for weeks. During that time, renowned Stanford topologist Evin Wilson was invited to present his research in Yale's Distinguished Lecture series. A few days later, Wilson carried the 3n+1 puzzle back to the West Coast, where UCLA professor Miles Kovic heard about it. Kovic added it to his plenary talk at the Annual Symposium on Number Theory in Madrid, Spain. Within a few months, Western mathematical research had ground to a halt. No one worked on anything except the intractable 3n+1 problem.

Actual history of the 3n+1 problem

It's an apocryphal story! But based on actual jokes made by frustrated Yale faculty.

The real origin of the 3n+1 problem is less clear. Mathematicians discussed problems like 3n+1 at meetings from the 1930s to the 1960s, but since these problems proved difficult to solve, no one published anything. Credit for the 3n+1 conjecture is usually given to German mathematician Lothar Collatz (1910-1990), who wrote in his notebook on July 1, 1932:

$$g(n) = \begin{cases} 2n / 3 & \text{if } n \equiv 0 \pmod 3 \\ (4n - 1) / 3 & \text{if } n \equiv 1 \pmod 3 \\ (4n + 1) / 3 & \text{if } n \equiv 2 \pmod 3 \end{cases}$$

This is the **original Collatz problem**, and it's a variation of the 3n+1 problem with three conditions instead of two. We'll come back to it in Chapter 13. Collatz played with such problems and circulated them at math conferences. Because of his work, the 3n+1 problem is usually referred to as the **Collatz conjecture**. It's also known as the "Ulam conjecture," "Kakutani's problem," the "Syracuse problem," and the "3x+1 problem."

What would a solution look like?

The 3n+1 conjecture posits that all numbers eventually reach 1. There are three ways you could resolve the conjecture.

First, you could find a concrete **counter-example** that proves the conjecture false. For example, you could discover a number that **cycles** back on itself, looping forever, never reaching 1. If you found such a number, you could publish your results as one of the shortest papers in mathematical history:

> The 3n+1 problem has a cycle
> by You
>
> The number
> 23,948,732,663,490,720,393,736,942,873,965,298,579,834,019
> loops back on itself after 19,439,298,097 steps
> of the 3n+1 procedure.

Or, you could find a number that **diverges** to infinity, always reaching greater and greater heights. Now, this would be harder for us to confirm. How would we know it doesn't eventually come down? You'd need to provide an airtight argument. (Chapter 4 gives an example of such an argument.)

Finally, you could prove that the 3n+1 conjecture is true. You'd need an airtight argument here, too. It's not enough to say, "I tried a few thousand numbers, and they all reached 1, so… yeah."

What does an airtight argument look like, generally speaking?

Let's start with a simpler conjecture:

> Every even number can be written as the sum of two odd numbers.

It's easy to generate examples like $18 = 11 + 7$ or $32 = 29 + 3$, but that doesn't prove the conjecture holds for *every* even number. An airtight proof might go like this: "Take any even number n. Clearly, $n = (n-1) + 1$. Since $n-1$ is adjacent to an even number, it's odd. So is 1. So, we've written any even number n as the sum of two odd numbers: $(n-1)$ and 1."

> *Editor*: Can you please remove the formula? Each formula in a popular-science book reduces sales by half.
> *Author*: What? It's just plus, minus, and equals!
> *Editor*: Kevin, this is an ironclad principle of publishing. You might as well be lighting hundred-dollar bills on fire.
> *Author*: Wait, we're making *hundreds of dollars*?!

Of course, this proof is only airtight if we all agree that odd numbers are adjacent to even numbers. And we also have to agree on what an odd number *is*, in the first place. A more formal proof would look like this:

1. A number n is even if $n = 2m$ for some whole number m.

2. A number n is odd if $n = 2m - 1$ for some positive whole number m.
3. Take any even number $n = 2m$.
4. Then, $n = 2m - 1 + 1 = (2m - 1) + (2 - 1) = (2m - 1) + (2 \cdot 1 - 1)$.
5. So, n is the sum of two numbers, each of the form $2m - 1$ … that is, two odd numbers.

That seems detailed enough. But, how do we even know that it's okay to replace 2 with $(2 \cdot 1)$ in step 4? Well, in the early 20th century, English mathematicians Bertrand Russell and Alfred North Whitehead tried to clear everything up once and for all. They wrote a foundational three-volume series called *Principia Mathematica*. After carefully defining addition, multiplication, the number zero, and many other things, they managed to prove that $1 + 1 = 2$, on page 86 … of the second volume!

Bertrand Russell was a philosopher who wrote extensively on logic, mathematics, war, politics, and free thought. While imprisoned for pacifist speeches, he wrote a book called *Introduction to Mathematical Philosophy*. My father had yet another Bertrand Russell book on his bookshelf when I was growing up, called *Why I am Not a Christian*. I didn't read that book, but I remember staring at the spine for a long time in amazement, and I particularly remember that the word "Not" was printed in a different color from the other words. Russell didn't get the Nobel Prize in mathematics—there's no such thing—but he got the Nobel Prize for Literature in 1950. "I wish I could switch places with Bertrand Russell for a day," my college roommate used to say. "Even though he's dead."

Counter-examples

Finding a counter-example to the 3n+1 conjecture sounds easier than devising an airtight proof. In searching for counter-examples, computer programmers have already checked the first billion-billion numbers, and every one of them eventually reaches 1. Here's a start number I picked randomly just now:

28,828,795,202,195,990,691 - 86,486,385,606,587,972,074 - 43,243,192,803,293,986,037 - 129,729,578,409,881,958,112 - 64,864,789,204,940,979,056 - 32,432,394,602,470,489,528 - 16,216,197,301,235,244,764 - 8,108,098,650,617,622,382 -
…
- 638 - 319 - 958 - 479 - 1438 - 719 - 2158 - 1079 - 3238 - 1619 - 4858 - 2429 - 7288 - 3644 - 1822 - 911 - 2734 - 1367 - 4102 - 2051 - 6154 - 3077 - 9232 - 4616 - 2308 - 1154 - 577 - 1732 - 866 - 433 - 1300 - 650 - 325 - 976 - 488 - 244 - 122 - 61 - 184 - 92 - 46 - 23 - 70 - 35 - 106 - 53 - 160 - 80 - 40 - 20 - 10 - 5 - 16 - 8 - 4 - 2 - 1

Sure enough, after 494 steps, it also reaches 1. But in the cosmic scheme of things, 28,828,795,202,195,990,691 is still a tiny number. Mind-blowing fact:

> Almost all positive whole numbers are bigger than 28,828,795,202,195,990,691.

So, is there any hope of finding a 3n+1 counter-example?

An inspiring precedent

In 1951, British mathematician Louis Mordell considered this equation:

$$x^3 + y^3 + z^3 = 3$$

If you get the feeling something weird might be lurking behind this innocent equation, then congratulations, you're already edging out of math-kook territory. (By the way, x^3 means $x \cdot x \cdot x$. The dot means multiplication. Normally, I'd write multiplication with an x, as in 2 x 2 = 4, but then we'd have too many x's in a row.)

Louis Mordell knew of two solutions:

$$1^3 + 1^3 + 1^3 = 3$$
$$4^3 + 4^3 + (-5)^3 = 3$$

We can verify the second solution like this:

$$(4 \cdot 4 \cdot 4) + (4 \cdot 4 \cdot 4) + (-5 \cdot -5 \cdot -5) = 64 + 64 - 125 = 3$$

Mordell searched for other solutions, but he couldn't find any. He therefore had a natural conjecture on his hands:

> Mordell's conjecture:
> The equation $x^3 + y^3 + z^3 = 3$ only has two integer solutions.

Mathematicians and computer scientists tried millions of values for x, y, and z and came up with nothing. So that was that … until 2019, when Andrew Booker and Andrew Sutherland found another solution:

$$569,936,821,221,962,380,720^3 +$$
$$(-569,936,821,113,563,493,509)^3 +$$
$$(-472,715,493,453,327,032)^3 = 3$$

Whoa! The moral of this story? A huge counter-example to the 3n+1 conjecture might exist. But to find it, we need to know where to look.

Math for this book

The 3n+1 problem has been called "the simplest math problem that no one can solve." To understand it, you only need to know how to add, multiply, and divide whole numbers. Ideally, a proof of the 3n+1 conjecture would stick to these basic operations. But it's sometimes useful to invoke fractions or even logarithms when we analyze the 3n+1 problem. In this book, I'll assume some 10th-grade math, but no calculus.

Why do people care?

Why do people care about the 3n+1 conjecture? Surfers claim there's cosmic significance to slotting into a rolling tube of water while standing on a slab of polyurethane. Some say the 3n+1 problem is of similar deep consequence.

There's also the prize money. In 1970, Canadian academic Harold Scott MacDonald Coxeter offered $50 to whoever could solve the 3n+1 problem. That may not excite you. But in 2021, Bakuage Co., Ltd., of Tokyo, significantly upped the ante to 120 million Japanese yen (about $1,000,000) for "whoever has elucidated the truth of the Collatz conjecture." That's a lot of cash, and now it's easier to explain to my brother-in-law what the heck I'm doing.

Bakuage Co., Ltd. has posted detailed rules on its website. If you read them carefully, you can learn some interesting things. For example, the company reserves the right to withhold the prize money from any "member of an organized crime group," or "a person for whom five (5) years have not yet passed since leaving an organized crime group." World-class gangster mathematicians? There's a movie plot in there.

Best be quick, though. When German doctor Paul Wolfskehl died in 1906, he left behind 100,000 marks to the first person to solve the famous **Fermat's Last Theorem**. It was a huge prize, more than 100 times the average annual wage. But after the German hyperinflation of the 1920s, 100,000 marks couldn't buy a loaf of bread.

What are the implications?

The stock market often resembles 3n+1 sequences. While writing this book, I held a real-life stock that opened at $14 a share, landed on 16, then promptly went to 8, 4, 2, and 1. I doubt solving the 3n+1 conjecture will help anyone predict stock prices, but who knows? Some of the richest people in the world are mathematicians and physicists who apply math to finance.

Does the 3n+1 have military implications? Probably not. In 1940, English mathematician G. H. Hardy bragged, "No one has yet discovered any warlike purpose to be served by the theory of numbers… and it seems unlikely that anyone will do so for many years." However, soon afterwards, mathematicians *did* develop secure military cryptography around the *discrete log* problem, which we'll look at in Chapter 6.

What other applications does number theory have? I recently attended a mathematics conference, where each speaker presented their work to an auditorium of professional colleagues. I couldn't understand any of it. After a while, I realized that nobody else in the audience did either. Each talk was so esoteric that only a couple of audience members, steeped in the relevant sub-field, could understand it.

The real reason for the academic conference was the coffee breaks. "Oh," Professor Erickson might say to Professor Rodriguez, "Yamazaki has a theorem that might be what you need." Rodriguez would then hunt down Yamazaki at the snack table.

During one talk, the speaker announced, "Now, I will describe some applications of my main theorem." I sat upright. Finally! The speaker then described how her theorem made it *easy to prove other theorems* … which she illustrated with several examples. At that moment, I was disappointed, yet illuminated. If a mathematician says there are a lot of **applications** for their work, this is probably what they mean.

> Old math joke:
>
> What do you call a person who reads a journal article on Tarskian geometry? A co-author.

So, what's the point?

When mathematicians look at a famous classic theorem or a surprising new result, they don't use words like "proficient" or "applicable." Instead, they say "stunning" or "beautiful" or "elegant," the same words we use to describe paintings and novels. These things have their practical uses, of course, and it's a mystery, if anything, why basic mathematical results have such diverse applications. But the main point is the artistry. As Hardy put it:

> "Real mathematics must be justified as art if it can be justified at all."
>
> \- G. H. Hardy

Notes and references

Jefferey C. Lagarias provides invaluable material on the 3n+1 problem in his edited volume *The Ultimate Challenge: The 3x+1 Problem* (2010). This book contains technical surveys, important early papers, and historical notes.

Lagarias references a private discussion (circa 1981) between himself and mathematician Shizuo Kakutani on various obsessions with the 3n+1 problem at Yale University and the University of Chicago around 1960, and the Russian conspiracy jokes that followed. The book also includes Lothar Collatz's paper "On the Motivation and Origin of the (3n+1)-Problem," in which Collatz reminisces about his discovery. (Curiously, this paper was originally published in Chinese!)

To see how computers are used to check 3n+1 start numbers, see Tomás Oliveira e Silva's 2010 paper, "Empirical verification of the 3n+1 and related conjectures," in Lagarias' edited volume.

Andrew Booker and Andrew Sutherland describe solving $x^3 + y^3 + z^3 = 3$ in their paper "On a Question of Mordell" (https://arxiv.org/abs/2007.01209). Their work used the *Charity Engine*, a global network of 500,000 volunteered personal computers.

The site https://mathprize.net hosts the rules for the million-dollar 3n+1 prize offered by Bakuage Co., Ltd. of Tokyo, Japan.

The quotations from G. H. Hardy are taken from the book *A Mathematician's Apology*, where Hardy passionately defends the value of theoretical mathematics and a career immersed in it.

Winston Churchill's description of Russia, re-purposed here, is from a 1939 BBC Radio Broadcast.

Hundreds of pages into *Principia Mathematica* (1912), authors Bertrand Russell and Alfred North Whitehead are finally[1] able to prove $1 + 1 = 2$, and they cannot resist adding a wry comment:

$$*110 \cdot 643. \vdash . 1 +_c 1 = 2$$

Dem.

$$\vdash . * 110 \cdot 632 . * 101 \cdot 21 \cdot 28 . \supset$$
$$\vdash .1 +_c 1 = \hat{\xi}\{(\exists y).y \in \xi . \xi - \iota‘y \in 1\}$$
$$[*54 \cdot 3] = 2 . \supset \vdash . \text{Prop}$$

The above proposition is occasionally useful.

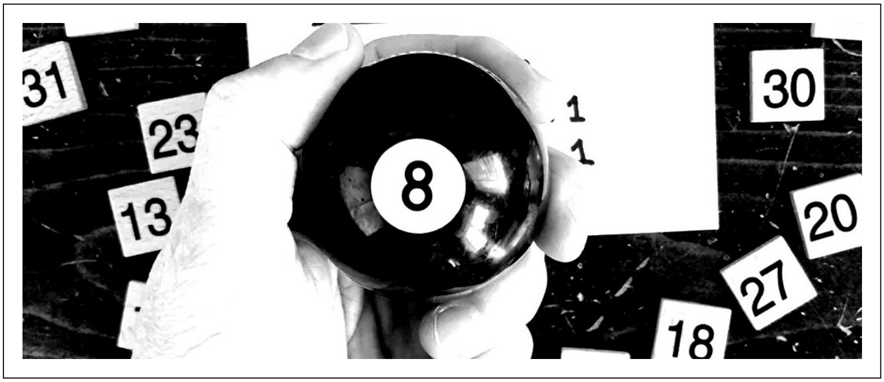
For the full story behind *Principia Mathematica* in graphic-novel form, see *Logicomix*, by Apostolos Doxiadis and Christos Papadimitriou (2009).

The chapter's opening quote is from Bob Dylan's song "My Own Version of You" (2020). In his 2004 autobiography, Dylan writes cryptically about a mathematical system for music that he discovered, which "works in a cyclical way. Because you're thinking in odd numbers instead of even numbers, you're playing with a different value system." Let's put that in our pocket for future use. Dylan was always interested in math. In the program notes for his *Never-Ending Tour* (as reported by NME.com), he said, "I wouldn't even think about playing music if I was

[1] https://quod.lib.umich.edu/u/umhistmath/AAT3201.0002.001/126?rgn=full+text;view=pdf; ↩ q1=principia+mathematica

born in these times... I'd probably turn to something like mathematics. That would interest me. Architecture would interest me. Something like that."

So impactful were the writings of Bertrand Russell, Winston Churchill, and Bob Dylan that all three received the Nobel Prize in Literature without writing a single noted work of literary fiction.



Chapter 13

What can compute 3n+1?

"Young man, in mathematics you don't understand things.
You just get used to them."
John von Neumann

Reducing one problem to another

What else can we do when faced with a hard problem? Mathematicians often try to reduce their problem into some other problem that people already know how to solve:

My problem → [Reduction] → Known easy problem

For example, if I want to find the shortest route from A to B on a map, I can convert the map into a flat list of road segments:

Road(p_1, p_2, 120)   (a 120-meter road connects places p_1 and p_2)
Road(p_2, p_3, 51)
Road(p_2, p_4, 204)
...

You might think this isn't too helpful. But in 1959, Dutch computer scientist Edsger Dijkstra figured out how to take any list like this and find the guaranteed shortest path between any two places. Even better, his method works very fast. So, we saved ourselves a lot of problem-solving by reducing our problem to his, then using his efficient solution.

We already did a bit of reduction in our 3n+1 no-circuit proof. We converted the problem of finding 3n+1 circuits to a problem of equation solving—namely, does $3^x - 2^x = m(2^{k-x} - 1)$ have a solution in whole numbers? If someone has tools to solve a Diophantine equation like this, then we can use their tools.

3n+1 problem → [Reduction] → Diophantine equation solving

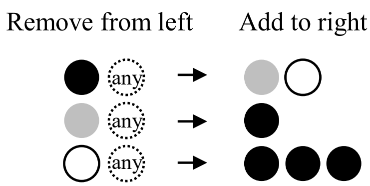
Mathematicians sometimes do reductions in the opposite direction:

Known hard problem → [Reduction] → My problem

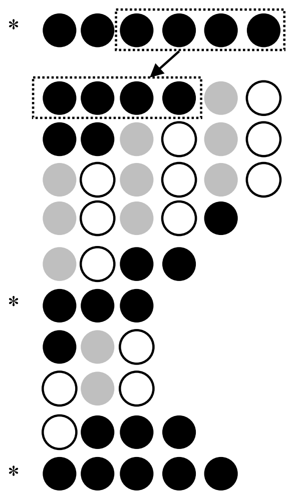
The idea is to find out how hard your problem is. You might not have a solution to your problem (yet), but maybe you could show that a solution would suddenly enable the solution to another problem, one that hundreds of determined, smart people have previously failed to solve. That would be great, of course, but meanwhile you've learned a sobering fact: your problem is objectively hard. You might even learn that your problem is unsolvable. For example, any solution to your problem might, as a necessary side effect, produce two whole numbers p and q such that $p/q = \pi$. Since we know no such fraction exists, we can conclude that your problem has no solution.

De Mol's tag system

Let's reduce the 3n+1 problem to a marble game. We start with some sequence of
2 marbles and repeatedly apply these three rules:



For example, if we start with 6 black marbles, we remove 2 marbles from the left (black and black), and add 2 marbles to the right (gray and white). Any collection of such rules is called a **tag system**. Here's what happens if we keep using these three rules:



I've put a star (*) next to each line that contains only black marbles. If we start with 6 black marbles, we eventually get 3 black marbles, and later 5 black marbles. If we keep going, we get 6 - 3 - 5 - 8 - 4 - 2 - 1. That's a 3n+1 trajectory! Amazingly, this tag system computes 3n+1, but without any explicit arithmetic.

Notice that the reduction involves a slowdown. In simulating 3n+1, the tag system introduces some intermediate steps.

> *Question 29:* How many steps does it take to get from 10 black marbles to 5 black marbles?

3n+1 problem → Reduction → Tag system

Liesbeth de Mol discovered this tag system as part of her Ph.D. in philosophy at the University of Ghent in Belgium. She subsequently moved to the University of Lille, and much of her later work focuses on the history and philosophy of computing.

Why reduce the 3n+1 problem to a tag system? Because tag systems have been extensively studied ever since their invention in 1922 by Emil Post. A central question in the theory of tag systems is:

Given m rules, each of which replaces n marbles on the left, will the system terminate on all input sequences?

A tag system terminates when it reaches a sequence with fewer than n marbles. De Mol's system terminates when there is one black marble left. So, the question of whether de Mol's tag system always terminates is the same as the 3n+1 conjecture.

Emil Post developed a method for answering the termination problem for tag systems. Given any set of rules, it will automatically tell you whether all input sequences terminate. Great! What happens when we ask the method about de Mol's tag system? Unfortunately, Post's method only works for the case $m = 2$, while de Mol uses 3 colors of marbles. (Post actually never published his 2-color method, but de Mol worked it out in her dissertation.)

Post tried to create methods for checking the termination of tag systems with larger values of m, but he failed. And for a good reason: a sufficiently-large tag system $(m = 288)$ can simulate a general-purpose computer, as first shown by Marvin Minsky in the 1960s.

General-purpose computer $\rightarrow$ [Reduction] $\rightarrow$ Tag system $(m = 288)$

This means you can take any Python or C++ program, plus any input to that program, and convert them into a marble sequence for a specific tag system. The subsequent evolving marble sequences mimic the evolving internal state of a computer, including the program, input, and any scratch-pad computations. The tag system terminates if (and only if) the computer program stops.

Here's the kicker. It's impossible to tell whether a computer program is going to stop. This was first shown by Alan Turing in the 1930s. He called it the **halting problem**. Consider three sample programs:

(a) for i = 1 to 10, print i; halt.
(b) x = 0; repeat until x is odd: x = x + 2.
(c) x = 3512; repeat until x is a Wieferich prime: x = x + 1.

Clearly, program (a) terminates, and clearly, program (b) will run forever. But how about program (c)? Nobody knows whether there are any Wieferich primes greater than 3511, but there might be. Even after running program (c) for 100 years, we wouldn't be able to conclude anything. At any given moment, it might be about to discover a new Wieferich prime.

That means there's no method that tells whether any tag system (with $m \geq 288$) terminates, because if there were, we could use the method to solve an unsolvable problem. I feel bad for Emil Post. Working in the pre-Gödel, pre-Turing 1920s, he didn't even know there were unsolvable problems, much less that he was working on one. Even today, my father insists that any problem is solvable.

Summarizing the situation:

> For tag systems with m ≤ 2, there's a method to check whether it terminates on all inputs.

> For tag systems with m ≥ 288, there can be no method.

For a tag system with $m = 3$ (like de Mol's), neither fact applies. Ultimately, our knowledge about tag systems doesn't help us solve the 3n+1 problem. Perhaps it will work out in the reverse way: solving the 3n+1 problem may tell us something about tag systems one day.

An amazing computer assault on the 3n+1 problem

In 2021, three researchers reported an amazing assault on the 3n+1 problem, quite
32 different from anything tried before. Emre Yolcu, Scott Aaronson, and Marijn J. H. Heule (I'll call them YAH) reduced the 3n+1 problem to a **rewrite system** and used computer power to check for termination.

3n+1 problem → [Reduction] → Rewrite system

YAH's key idea was a *mirror world*. We know that normal 3n+1 trajectories jump up and down: 6 - 3 - 5 - 8 - 4 - 2 - 1. If they *only* went down, then they'd be guaranteed to reach 1. Maybe there's a mirror world whose parallel trajectories always go down.

Imagine every number had a twin in the mirror world, such as:

Twin(1) = 5	Twin(2) = 9	Twin(3) = 20	Twin(4) = 12
Twin(5) = 18	Twin(6) = 23	Twin(7) = 26	Twin(8) = 14

Then every 3n+1 trajectory would have a corresponding mirror-world trajectory. For example,

Real world trajectory:	6	-	3	-	5	-	8	-	4	-	2	-	1
Mirror world trajectory:	23	-	20	-	18	-	14	-	12	-	9	-	5

Now imagine every time we take a step in the real world, by applying either $\frac{3n+1}{2}$ or $\frac{n}{2}$, the corresponding mirror-world sequence decreases, like in the example above. Then every mirror-world trajectory would eventually have to stop, and therefore, so would its corresponding real-world trajectory, which would confirm the 3n+1 conjecture.

Like de Mol, YAH work with marble sequences instead of numbers. Instead of just three kinds of marbles (black, gray, and white), YAH use seven kinds:

f, t, o, 1, 2, <, >

Here's a typical trajectory:

YAH:	<t>	<2>	<ft>	<f2>	…
Real-world interpretation:	3	5	5	8	…
Mirror-world interpretation:	[84 0]	[78 0]	[69 0]	[62 0]	…

YAH sequences are more compact than de Mol's. For example, 8 is just <f2>, and 2187 is <ooooooo>. In the latter case, De Mol would need 2187 (black) marbles, but YAH only need 9.

To enable trajectories, YAH use eleven rules:

Rule #1:	t> → 2>	Rule #5:	<1 → <ff	Rule #9:	t1 → 2f
Rule #2:	<2 → <ft	Rule #6:	fo → of	Rule #10:	t2 → 2t
Rule #3:	f> → >	Rule #7:	f2 → 1f	Rule #11:	f1 → ot
Rule #4:	<o → <t	Rule #8:	to → 1t		

Rule #1 means, anywhere you see t>, you can replace it with 2>. In a rewrite system, replacements are allowed anywhere in a marble sequence, not only on the left or right edge. Rewrite systems aren't deterministic like tag systems or the 3n+1 rule. That's okay. YAH just need to show that no matter what rules we apply, the mirror-world interpretation consistently decreases.

How do we know <t> means 3 in the real-world interpretation? Each type of marble is associated with a function:

f: $2n$	o: $3n$	<: 1
t: $2n+1$	1: $3n+1$	>: n
	2: $3n+2$	

We apply those functions left-to-right. Here are some examples:

`<t>` $^{<}\boxed{1} \to 1 \to {}^{t}\boxed{2n+1} \to 3 \to {}^{>}\boxed{n} \to 3$

`<f2>` $^{<}\boxed{1} \to 1 \to {}^{f}\boxed{2n} \to 2 \to {}^{2}\boxed{3n+2} \to 8 \to {}^{>}\boxed{n} \to 8$

`<2>` $^{<}\boxed{1} \to 1 \to {}^{2}\boxed{3n+2} \to 5 \to {}^{>}\boxed{n} \to 5$

Each of YAH's rules properly reflect the 3n+1 rule. For example, when Rule #1 replaces t> (2n+1) with 2> (3n+2), it's essentially applying $\frac{3n+1}{2}$ to an odd number 2m+1, because $3(2m+1)+1)/2 = (6m+4)/2 = 3m+2$.

Question 30: What's the interpretation of `<f>`?

Lastly, we need a way to do a mirror-world interpretation. See how the mirror-world numbers go steadily down in this example?

YAH:	<t>	<2>	<ft>	<f2>	<1f>	<1>	<ff>	<f>	<>
Real world:	3	5	5	8	8	4	2	2	1
Mirror world:	[84 0]	[78 0]	[69 0]	[62 0]	[41 0]	[27 0]	[26 0]	[14 0]	[12 0]

You've probably noticed that YAH's mirror world consists of *pairs* of numbers (vectors) instead of single numbers. How do we interpret `<t>` as [84 0]? This time, we proceed through `<t>` right-to-left, instead of left-to-right, as befits a mirror world. A good way to convert one vector into another is with matrix multiplication and addition, so YAH associate with each marble-type an **affine function**:

f: $\begin{bmatrix}1&1\\1&0\end{bmatrix}x$ o: $\begin{bmatrix}7&2\\2&5\end{bmatrix}x+\begin{bmatrix}1\\0\end{bmatrix}$ <: $\begin{bmatrix}1&5\\0&0\end{bmatrix}x$

t: $\begin{bmatrix}1&3\\3&4\end{bmatrix}x+\begin{bmatrix}1\\1\end{bmatrix}$ 1: $\begin{bmatrix}2&1\\1&1\end{bmatrix}x+\begin{bmatrix}1\\0\end{bmatrix}$ >: $\begin{bmatrix}2\\2\end{bmatrix}$

2: $\begin{bmatrix}2&2\\2&4\end{bmatrix}x+\begin{bmatrix}0\\2\end{bmatrix}$

To compute the mirror-world interpretation of `<t>`, we apply these functions right-to-left:

$$^{>}\boxed{\begin{bmatrix}2\\2\end{bmatrix}} \to \begin{bmatrix}2\\2\end{bmatrix} \to {}^{t}\boxed{\begin{bmatrix}1&3\\3&4\end{bmatrix}x+\begin{bmatrix}1\\1\end{bmatrix}} \to \begin{bmatrix}9\\15\end{bmatrix} \to {}^{<}\boxed{\begin{bmatrix}1&5\\0&0\end{bmatrix}x} \to \begin{bmatrix}84\\0\end{bmatrix}$$

Question 31: What's the mirror-world interpretation of `<f>`? If it helps: $\begin{bmatrix}a&b\\c&d\end{bmatrix}\begin{bmatrix}e\\f\end{bmatrix} = \begin{bmatrix}ae+bf\\ce+df\end{bmatrix}$ and $\begin{bmatrix}a\\b\end{bmatrix}+\begin{bmatrix}c\\d\end{bmatrix} = \begin{bmatrix}a+c\\b+d\end{bmatrix}$.

Now, YAH didn't come up with these seven affine functions by hand. Instead, they asked a computer to sift through zillions of combinations of matrices. One computer run yielded the matrices above.

So, did YAH win the million-dollar prize for solving the 3n+1 conjecture? Almost. It turns out these matrices work nicely for the trajectory in our example, but only because it doesn't use Rule #11. With Rules #1-10, the matrices guarantee the mirror-world interpretations will decrease. But if we apply Rule #11, the mirror-world interpretation might go up. Since some start numbers need Rule #11, we can't guarantee the rewrite system will terminate.

There's nothing especially tricky about Rule #11—the computer can also find matrices that work for all 10 rules except Rule #3. But it isn't able to find matrices for all 11 rules together. YAH had success with problems similar to 3n+1, and there are many more things to try along these lines. Bringing brute-force computer power into the picture could change the game, as it did for the Four Color Theorem.

A cellular automaton

33 In 1992, Slovak mathematician Ivan Korec reduced the 3n+1 problem to a **cellular automaton**, situating it inside another highly-studied field.

3n+1 problem → [Reduction] → Cellular automaton

In a one-dimensional cellular automaton, an initial marble sequence is put into an infinite row of cells. Korec used 7 types of marbles (–, 0, 1, 2, 3, 4, 5, and 6). The trajectory proceeds row by row, as shown on the left below.

Sample trajectory

–	1	1	–	–	–	–
–	–	3	4	–	–	–
–	–	1	5	–	–	–
–	–	–	5	4	–	–
–	–	–	2	5	–	–
			...			
–	–	–	–	–	–	1

Rule matrix

	–	0	1	2	3	4	5
–	–	–	–	1	1	2	2
0	–	0	0	1	1	2	2
1	4	3	3	4	4	5	5
2	–	0	0	1	1	2	2
3	4	3	3	4	4	5	5
4	–	0	0	1	1	2	2
5	4	3	3	4	4	5	5

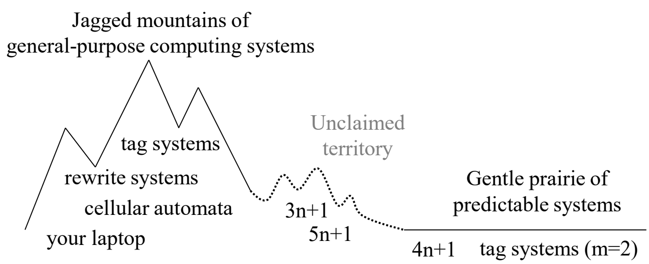
The pattern 11 evolves into 34 (shifted over one position), then 15, and so on: 11 - 34 - 15 - 54 - 25- ... - 1. This doesn't look like a 3n+1 trajectory. But if we convert these numbers from base-6 to base-10, we get an accurate 3n+1 trajectory: 7 - 22 - 11 - 34 - 17 - ... - 1.

The automaton's rules for constructing each subsequent row are shown on the right. Each cell takes a value that depends only on the cell above it (across the top of the rule matrix), and the cell to the left of that (down the left of the rule matrix).

Korec's automaton faithfully simulates the 3n+1 rule. Notice there's no slow-down, which means Korec's automaton can provide a fast, practical way to compute 3n+1 trajectories without arithmetic.

Is there a general method for telling whether some cellular automaton reaches some target pattern (like 1) from all starting inputs? I'm sorry to say, no. The reasons are similar to before. Since some cellular automata can implement a general-purpose computer, there's no general method for predicting what an arbitrarily-given cellular automaton will do.

Of course, many individual cellular automata *are* predictable. For example, if we replace every entry in Korec's rule table with a dash (–), we can certainly predict what happens to every start pattern. Korec's 3n+1 automaton itself might be likewise predictable one day, or it might turn out to have general-purpose computing ability. Or maybe something in between, unable to run arbitrary programs, but unpredictable nonetheless. Currently, 3n+1 lies in unclaimed territory:



The Farkas rule

When you're faced with a hard problem, one strategy is to simplify it. Unfortunately, 3n+1 is already very simple! Another strategy is to generalize it.

For example, if I want to get from Los Angeles to Honolulu by car, I might keep planning different routes. Hmm, maybe if I go through the Aleutian Islands in Alaska? Then down to Vietnam? Hmm. If I'm a mathematician, I will step back at some point and ask, "Wait, how can I plan a route from *anywhere to anywhere*?"

It seems like I made my problem harder. But there's actually a straightforward method that solves the anywhere-to-anywhere problem, which we saw earlier, from Edsger Dijkstra. Armed with that, I can return to view my LA-to-Honolulu difficulties in a new light. Ah, we *can't* get from LA to Honolulu by car. We can get from LA to Pensacola Beach, Florida, though. Maybe we'll go there instead.

In fact, we've already generalized the 3n+1 problem to the qn+1 problem, which was pretty helpful. The 3n+1 problem doesn't have non-trivial circuits, while the 5n+1 problem does. The 181n+1 has a cycle of length 15, and the 1093n+1 problem has numbers that provably diverge to infinity. We may find these facts useful when we're trying to resolve the 3n+1 conjecture.

Another way to generalize 3n+1 is to increase the number of if-then conditions in the rule. Here's our familiar two-way rule:

If n is even, replace it with $n/2$.
If n is odd, replace it with $(3n + 1)/2$.

Or stated another way:

If $n \equiv 0$ (mod 2), replace it with $n/2$.
If $n \equiv 1$ (mod 2), replace it with $(3n + 1)/2$.

And here's a new **multi-way rule**:

If $n \equiv 0$ (mod 6), replace it with $n/2$.
If $n \equiv 1$ (mod 6), replace it with $(n - 1)/3$.
If $n \equiv 2$ (mod 6), replace it with $n/2$.
If $n \equiv 3$ (mod 6), replace it with $(3n + 1)/2$.
If $n \equiv 4$ (mod 6), replace it with $(n - 1)/3$.
If $n \equiv 5$ (mod 6), replace it with $(3n + 1)/2$.

We divide n by 6, and if there's no remainder, we take the first branch. If there's a remainder of 1, we take the second branch, and so forth. The particular rule above is called the **Farkas rule**, after Israeli-American mathematician Hershal Farkas. Its trajectories are often shorter than 3n+1 trajectories:

Farkas rule	3n+1 rule
3 - 5 - 8 - 4 - 2 - 1	3 - 5 - 8 - 4 - 2 - 1
7 - 2 - 1	7 - 11 - 17 - 26 - 13 - 20 - 10 - 5 - 8 - 4 - 2 - 1

Farkas proved that all start numbers *do* go to 1 under this rule, and YAH automatically obtained a mirror-world proof. So, the Farkas rule provides a 3n+1-type problem that's amenable to the attacks we've been looking at.

Question 32: What makes the Farkas-rule trajectory for 7 so short? What's the main difference between 3n+1 and the Farkas rule?

The original Collatz rule

Back in Chapter 1, we mentioned that Lothar Collatz wrote another multi-way rule
38 in his notebook on July 1, 1932:

If $n \equiv 0$ (mod 3), replace it with $2n/3$.
If $n \equiv 1$ (mod 3), replace it with $(4n - 1)/3$.
If $n \equiv 2$ (mod 3), replace it with $(4n + 1)/3$.

This is called the **original Collatz rule**. Because John Conway popularized it, it's sometimes called the **Conway map**. Here are some cycles induced by the rule:

1 - 1
2 - 3 - 2
4 - 5 - 7 - 9 - 6 - 4
44 - 59 - 79 - 105 - 70 - 93 - 62 - 83 - 111 - 74 - 99 - 66 - 44

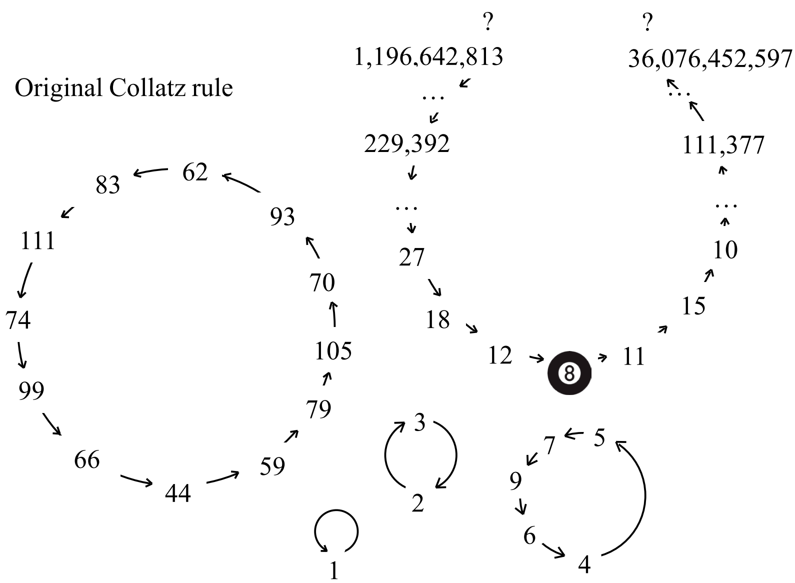
The rest of the numbers seem to run off to infinity. I like to imagine Lothar Collatz on the train with his notebook, mumbling to himself, “What the heck?”

There’s one big difference between the original Collatz rule and the 3n+1 rule. In the 3n+1 rule, numbers often have two predecessors. For example, you can get to 8 from either 5 or 16. Not so with the original Collatz rule, where every number has a unique predecessor. It’s easier to see this if we rewrite the rule like this:

3n goes to 2n
3n + 1 goes to 4n + 1
3n + 2 goes to 4n + 3

Every number matches exactly one of 3n, 3n + 1, or 3n + 2, so it has a unique successor. But every number *also* matches exactly one of 2n, 4n + 1, or 4n + 3, giving it a unique predecessor. Instead of the Collatz tree, we get something quite different-looking:

Original Collatz rule



Here, the cycles are nicely self-contained. Unlike qn+1 cycles, they don’t suck in other numbers. 1, 2, 3, 4, 5, 6, and 7 participate in known cycles. But 8 is a mystery. If we start at 8 and keep going, will we ever get back to 8? Nobody knows. The magic 8-ball says: “Ask again later!”

> *Question 33:* Does this make you think about fate, determinism, and free will? If 8 were alive, what would you tell it?

A consistent rule format

Now let’s put every rule into a common format:

3n+1:	$(1n+0)/2$	when $n \equiv 0 \pmod 2$
	$(3n+1)/2$	when $n \equiv 1 \pmod 2$
5n+1:	$(1n+0)/2$	when $n \equiv 0 \pmod 2$
	$(5n+1)/2$	when $n \equiv 1 \pmod 2$
Original Collatz:	$(2n+0)/3$	when $n \equiv 0 \pmod 3$
	$(4n-1)/3$	when $n \equiv 1 \pmod 3$
	$(4n+1)/3$	when $n \equiv 2 \pmod 3$

In this format, every rule has d conditions, with values of a_i, b_i, and d unique to that rule:

$$
\begin{array}{ll}
(a_0 n + b_0)/d & \text{when } n \equiv 0 \pmod d \\
(a_1 n + b_1)/d & \text{when } n \equiv 1 \pmod d \\
\quad\ldots & \\
(a_{d-1} n + b_{d-1})/d & \text{when } n \equiv d-1 \pmod d
\end{array}
$$

The Matthews-Watts conjecture

The 3n+1 conjecture says that all numbers reach a cycle, namely the trivial 1-2-1
43 loop. Part of its plausibility is this: if we take two steps, one even and one odd, then we’ll end up replacing n with approximately $n\frac{1}{2}\frac{3}{2} = \frac{3}{4}n$. So, trajectories trend downwards. The opposite happens in the 5n+1 problem, where n typically gets replaced by $\frac{5}{4}n$ after two steps, so we expect almost all numbers to diverge to infinity.

How about the original Collatz rule? If its three branches are taken equally often, then we might expect n to be replaced by $\frac{2}{3}\frac{4}{3}\frac{4}{3}n = \frac{32}{27}n$. Since $\frac{32}{27} > 1$, we again expect almost all numbers to diverge, which is consistent with our observations.

Notice that $\frac{2}{3}\frac{4}{3}\frac{4}{3} = \frac{2\cdot4\cdot4}{3^3}$. Let’s call $\frac{a_0\,a_1 \ldots a_{d-1}}{d^d}$ the **critical density** of a 3n+1-type rule. The **Matthews-Watts conjecture** says:

Matthews-Watts conjecture:

1) If the critical density $\frac{a_0\ a_1 \ldots a_{d-1}}{d^d} < 1$ (**contracting rule**), then every start number reaches a cycle.

2) If the critical density $\frac{a_0\ a_1 \ldots a_{d-1}}{d^d} > 1$ (**expanding rule**), then almost all start numbers diverge to infinity.

3) In either case, the number of distinct cycles is finite.

Note! Only applies to rules where $a_0\ a_1 \ldots a_{d-1}$ and d are co-prime.

K. R. Matthews is an Australian mathematician. I like to imagine that his co-author A. Watts is the Zen philosopher Alan Watts, who once said: "If a flower had a God, it would not be a transcendental flower, but a field," which sounds like a pretty deep mathematical observation. If K. R. Matthews happens to read this, he can tell me about the real A. Watts.

The Matthews-Watts conjecture includes the 3n+1 conjecture as a special case, since the 3n+1 rule is contracting. But Matthews-Watts is more general. The more you fool around with multi-way systems, the more you believe in it. A stunning feature of the Matthews-Watts conjecture is that the little +1s and -2s (the b_i values) aren't mentioned! The conjecture says they're irrelevant to the overall behavior of the system.

A barely expanding system

It should be fun to torture the Matthews-Watts conjecture by designing a rule where the critical density is *very close to 1*. Here's such a rule. I can't decide whether to call it the "near-flat universe rule" or the "Eurozone economy" rule:

$(1n + 0)/5$	when $n \equiv 0$ (mod 5)
$(2n + 3)/5$	when $n \equiv 1$ (mod 5)
$(3n + 4)/5$	when $n \equiv 2$ (mod 5)
$(521n + 2)/5$	when $n \equiv 3$ (mod 5)
$(1n + 1)/5$	when $n \equiv 4$ (mod 5)

The critical density is $(1 \cdot 2 \cdot 3 \cdot 521 \cdot 1)/5^5 = 3126/3125 \approx 1.0003$. What happens with a barely-expanding rule like this? Let's try the start number 3:

3 - 313 - 32,615 - 6523 - 679,697 - 407,819 - 81,564 - 16,313 - 1,699,815 - 339,963 - 35,424,145 - 7,084,829 - 1,416,966 - 566,787 - 340,073 - 35,435,607 - 21,261,365 - 4,252,273 - 443,086,847 - 265,852,109 - 53,170,422 - 31,902,254 - 6,380,451 - 2,552,181 - 1,020,873 - 106,374,967 - 63,824,981 - 25,529,993 - 2,660,225,271 - 1,064,090,109 - 212,818,022 - 127,690,814 - 25,538,163 - 2,661,076,585 - 532,215,317 - 319,329,191 - 127,731,677 - 76,639,007 - 45,983,405 - 9,196,681 - 3,678,673 - 383,317,727 - 229,990,637 - 137,994,383 - 14,379,014,709 - …

As expected, 3 seems to be rocketing to infinity. But, let's go a little further:

… - 2,875,802,942 - 1,725,481,766 - 690,192,707 - 414,115,625 - 82,823,125 - 16,564,625 - 3,312,925 - 662,585 - 132,517 - 79,511 - 31,805 - 6361 - 2545 - 509 - 102 - 62 - 38 - 3960 - 792 - 476 - 191 - 77 - 47 - 29 - 6 - 3

Whoa, back to 3! This is the craziest cycle yet. Next time some trajectory passes the two-billion mark, I won't give up on it. Here are more trajectories that lead to cycles under this rule:

4 - 1 - … - 1
5 - 1 - … - 1
7 - 5 - 1 - … - 1
8 - 834 - 167 - 101 - 41 - 17 - 11 - 5 - 1 - … - 1
9 - 2 - … - 2
13 - 1355 - 271 - 109 - 22 - 14 - 3 - … - 3

Of the start numbers from 1 to 100, all but nine are quickly dragooned into cycles. Has the Matthews-Watts conjecture failed us? Remember, it predicts that even with a barely-expanding rule, almost all numbers should diverge to infinity. Let's measure the percentage of numbers that get quickly caught in a cycle:

Range of start numbers	1-100	1-1000	1-100,000	…
5n+1 rule	40%	17%	3%	…
Near-flat universe rule	91%	86%	83%	…

Ah … presumably, these percentages will get closer and closer to zero, as the range increases. Puny, human-sized start numbers may fall into cycles, but ultimately, they're just a bunch of rare exceptions, and everything else diverges to infinity. Or so says the Matthews-Watts conjecture!

3n+1 without the +1

The Matthews-Watts conjecture makes no reference to the additive b's, like the "+1"
52 in the 3n+1 rule. Do we even need the "+1"? If there were a 3n+1 rule without any +1's, it might be easier to analyze. Such a rule would simply look like this:

Replace n by $a_0 n$	when $n \equiv 0 \pmod{d}$
Replace n by $a_1 n$	when $n \equiv 1 \pmod{d}$
$\dots$	
Replace n by $a_{d-1} n$	when $n \equiv d-1 \pmod{d}$

Here, we allow a_i to be any fraction.

We can easily implement operations like $\frac{1}{2}n$ or 3n with such a rule, but how to implement 3n+1? We need two tricks. One is to use scratch space. Like in de Mol's tag system, we need not implement 3n+1 in a *single* step of our new rule. The other is to encode trajectory numbers inside exponents. If we want to start with 6, we use start number 2^6 instead. For example:

Old style:	3	-	10	-	5	-	16	-	8	-	4	-	2	-	1
New style:	2^3	- … -	2^{10}	- … -	2^5	- … -	2^{16}	- … -	2^8	- … -	2^4	- … -	2^2	- … -	2^1
	8	- … -	1024	- … -	32	- … -	65,536	- … -	256	- … -	16	- … -	4	- … -	2

What kind of rule can implement this new-style trajectory? First, let's make a rule that turns 2^x into 2^{3x+1}, for any odd x. Here's a sample trajectory:

$$2^3 - 2^2 3^1 5^3 - 2^1 3^1 5^6 - 3^1 5^9 - 5^{10} - 2^1 5^9 - 2^2 5^8 - 2^3 5^7 - 2^4 5^6 - 2^5 5^5 - \dots - 2^9 5^1 - 2^{10}$$

You can see the strategy. We decrement the exponent of 2 from 2^3 to 2^2 to 2^1 to 2^0, while simultaneously incrementing the exponent of 5 from 5^0 to 5^3 to 5^6 to 5^9, giving us 9, which is almost what we want. We change 9 to 10 and drop the 3^1, giving us 5^{10}. Finally, we turn 5^{10} into 2^{10}.

The trick is to replace the "plus one" with "times five," so that each step of the trajectory involves a simple multiplication. For example, to get from $3^1 5^9$ to 5^{10}, we multiply by $\frac{5}{3}$, and to get from $2^9 5^1$ to 2^{10}, we multiply by $\frac{2}{5}$.

> *Question 34:* Can you annotate the trajectory above ($2^3 - \dots - 2^{10}$) with a multiplier fraction between each pair of terms?

How do we know whether to apply $\frac{5}{3}$ or $\frac{2}{5}$? Just like the regular 3n+1 rule branches on odds and evens, here we branch on remainders modulo 30:

Replace n by $\frac{375}{2}$n when n $\equiv$ 2 or 8 (mod 30) 2^{odd}

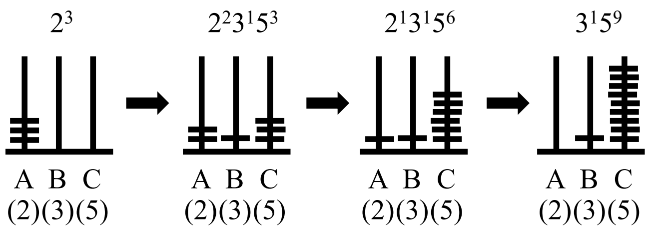
Replace n by $\frac{125}{2}$n when n $\equiv$ 0 (mod 30) $2^x3^y5^z$

Replace n by $\frac{5}{3}$n when n $\equiv$ 15 (mod 30) 3^x5^y

Replace n by $\frac{2}{5}$n when n $\equiv$ 5, 10, 20, or 25 (mod 30) 5^x or 2^x5^y

Notice that the second condition (n $\equiv$ 0 mod 30), is only invoked on numbers of the form $2^x3^y5^z$ $(x, y, z > 1)$, because you're only divisible by 30 if you're divisible by 2, 3, and 5. The same principle is used to identify numbers of the form 2^x5^y, 3^x5^y, and the like.

The trajectory itself is like some crazy version of the **Tower of Hanoi puzzle** where poles A, B, and C correspond to 2, 3, and 5. At each step, we add or remove discs from each pole.



For example, if all the discs start on pole A, then we move one of them to pole B, and add three new discs to pole C. Likewise, if we see all three poles occupied, we remove a disc from A and add three discs to C.

The previous rule only works for odd x. For *even* x, let's build another rule to map 2^x into $2^{x/2}$:

2^{10} - 2^83^1 - 2^63^2 - 2^43^3 - 2^23^4 - 3^5 - 3^45^1 - 3^35^2 - 3^25^3 - 3^15^4 - 5^5 - 2^15^4 - …- 2^5

Now we decrement the exponent of our start number from 2^{10} to 2^8 to … 2^0, while simultaneously incrementing the exponent of 3 from 3^0 to 3^1 to … 3^5. At this point, the exponent of 3 holds our answer: we've cut our 10 in half. Next, we execute similar operations to turn 3^5 into 5^5, and then 5^5 into our final 2^5.

Replace n by $\frac{3}{4}$n	when $n \equiv 4, 6, 12, 16, 18$, or 24 (mod 30)	2^{even}, 2^x3^y
Replace n by $\frac{5}{3}$n	when $n \equiv 3, 9, 15, 21$, or 27 (mod 30)	3^x or 3^x5^y
Replace n by $\frac{2}{5}$n	when $n \equiv 5, 10, 20$, or 25 (mod 30)	5^x or 2^x5^y

Why not go directly from 3^3 to 2^3, skipping the 5^x business? That would regrettably introduce numbers of the form 2^x3^y, which already trigger the $\frac{3}{4}$n branch of our rule. A number like 2^23^4 can't trigger $\frac{3}{4}$ sometimes and $\frac{2}{5}$ other times. Each number on the scratch pad has to pack all the needed information into its exponents, because the next step depends on it exclusively.

Finally, let's combine the two rules (even and odd) together, to obtain a single 30-way rule that fully implements 3n+1 without any +1s:

New 3n+1 rule:

Replace n by $\frac{375}{2}$n	when $n \equiv 2$ or 8 (mod 30)	2^{odd}
Replace n by $\frac{125}{2}$n	when $n \equiv 0$ (mod 30)	$2^x3^y5^z$
Replace n by $\frac{5}{3}$n	when $n \equiv 3, 9, 15, 21$, or 27 (mod 30)	3^x or 3^x5^y
Replace n by $\frac{2}{5}$n	when $n \equiv 5$, 10, 20, or 25 (mod 30)	5^x or 2^x5^y
Replace n by $\frac{3}{4}$n	when $n \equiv 4, 6, 12, 16, 18$, or 24 (mod 30)	2^{even} or 2^x3^y

In the end, it's a pretty simple rule! Here's a complete trajectory for $2^3 = 8$, written this time without prime factorizations:

8 (• • •) - 1500 - 93,750 - 5,859,375 - 9,765,625 - 3,906,250 - 1,562,500 - 625,000 - 250,000 - 100,000 - 40,000 - 16,000 - 6400 - 2560 - 1024 (• • • • • • • • • ••) - 768 - 576 - 432 - 324 - 243 - 405 - 675 - 1125 - 1875 - 3125 - 1250 - 500 - 200 - 80 - 32 (• • • • •) - 6000 - 375,000 - 23,437,500 - 1,464,843,750 - 91,552,734,375 - 152,587,890,625 - 61,035,156,250 - 24,414,062,500 - 9,765,625,000 - 3,906,250,000 - 1,562,500,000 - 625,000,000 - 250,000,000 - 100,000,000 - 40,000,000 - 16,000,000 - 6,400,000 - 2,560,000 - 1,024,000 - 409,600 - 163,840 - 65,536 (• • • • • • • ••) - 49,152 - 36,864 - 27,648 - 20,736 - 15,552 - 11,664 - 8748 - 6561 - 10,935 - 18,225 - 30,375 - 50,625 - 84,375 - 140,625 - 234,375 - 390,625 - 156,250 - 62,500 - 25,000 - 10,000 - 4000 - 1600 - 640 - 256 - 192 - 144 - 108 - 81 - 135 - 225 - 375 - 625 - 250 - 100 - 40 - 16 (• • ••) - 12 - 9 - 15 - 25 - 10 - 4 (••) - 3 - 5 - 2 (•)

Similarly, the start number 2^{31} takes 202,215 steps to reach 2^1.

> *Question 35:* Why does the trajectory above contain the nice, round number 100,000,000?

Properties of the 30-way rule

Does every start number 2^x wind up at 2^1? That's the same question as the 3n+1 conjecture. If we feel the pesky +1 complicates our 3n+1 analyses, we can decide to work with this 30-way rule instead.

Is this rule expanding or contracting, according to Matthews-Watts? The density factor is $(\frac{375}{2})^2(\frac{125}{2})(\frac{5}{3})^5(\frac{2}{5})^4(\frac{3}{4})^6 = 128,750 \gg 1$, making this a heavily-expanding rule. So, the Matthews-Watts conjecture should predict that almost all numbers will diverge to infinity. Has the conjecture failed?

Intuitively, the conjecture shouldn't apply at all here. Unlike the 3n+1 problem, the conditions of our 30-way rule are invoked with very different frequencies. In fact, they're engineered that way. Furthermore, the Matthews-Watts disclaimer says the conjecture only applies to rules with coefficients $(a_0, a_1, \ldots, a_i, d)$ where all the a_i are co-prime with d, which is not the case here. Our modulus 30 is engineered to be highly composite $(30 = 2 \cdot 3 \cdot 5)$.

This table shows how some of types of numbers behave mod 30:

x	1	2	3	4	5	6	7	8	9	10
2^x mod 30	2	4	8	16	2	4	8	16	2	4
3^x mod 30	3	9	27	21	3	9	27	21	3	9
5^x mod 30	5	25	5	25	5	25	5	25	5	25

We see the old familiar cycle patterns, although this time, there's no "1" at the end of each cycle, because Fermat's Little Theorem only applies to (a^x mod p) when a and p are co-prime.

Cycles revisited

The trivial 3n+1 cycle 1-2-4-1 has a trajectory of length 15 under the 30-way rule. It's a cycle because 2^1 multiplied by these 15 fractions is again 2^1:

$$2^1 \cdot \frac{375}{2} \cdot \frac{5}{3} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{3}{4} \cdot \frac{3}{4} \cdot \frac{5}{3} \cdot \frac{5}{3} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{3}{4} \cdot \frac{5}{3} \cdot \frac{2}{5} = 2^1$$

Generally speaking, if there's a 3n+1 cycle starting at n, then $2^n = 2^n \cdot p$, where p=1 is a product of fractions drawn (with repeats) from the set $\{\frac{375}{2}, \frac{125}{2}, \frac{5}{3}, \frac{2}{5}, \frac{3}{4}\}$. Besides the list of 15 fractions above, what other lists of fractions have a product $p = 1$? The shortest such list is:

$$\frac{125}{2} \cdot \frac{5}{3} \cdot \frac{5}{3} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{3}{4} \cdot \frac{3}{4} = 1$$

However, no trajectory uses those particular fractions, in any order. For example, the $\frac{125}{2}$ fraction is only employed directly after a $\frac{375}{2}$ fraction when $n > 1$. So, $p = 1$ is a necessary condition for a 3n+1 cycle, but not a sufficient one.

Other fraction lists with p = 1 have lengths 20, 25, 30, 35, and so on. If we hit a list whose members can be re-arranged to form a legal trajectory, then we'll have found a 3n+1 cycle. Of course, that list must contain tens of millions of members—even more, considering the slowdown!

Monks' simulator

The idea of "3n+1 minus the +" appeared in Ken Monks' similarly-named 2002 paper. Monks essentially gave a 1,021,020-way rule to simulate 3n+1:

$$
\begin{array}{lll}
\text{Replace n with } \frac{1}{11}\text{n} & \text{when n} \equiv 0 & \text{(mod 1,021,020)} \\
\text{Replace n with 7n} & \text{when n} \equiv 1 & \text{(mod 1,021,020)} \\
\text{Replace n with } \frac{5}{2}\text{n} & \text{when n} \equiv 2 & \text{(mod 1,021,020)} \\
 & \cdots & \\
\text{Replace n with } \frac{33}{4}\text{n} & \text{when n} \equiv 128 & \text{(mod 1,021,020)} \\
 & \cdots & \\
\text{Replace n with 7n} & \text{when n} \equiv 1,021,019 & \text{(mod 1,021,020)}
\end{array}
$$

Here is Monks' rule in action, starting with 2^7:

$\boxed{2^7}$ - $2^5 3^1 11^1$ - $2^5 3^1$ - $2^3 3^2 11^1$ - $2^3 3^2$ - $2^1 3^3 11^1$ - $2^1 3^3$ - $3^3 5^1$ - $2^3 3^2 17^1$ - $2^3 3^2 5^1$ - $2^6 3^1 17^1$ - $2^6 3^1 5^1$ - $2^9 17^1$ - $2^9 5^1$ - $\boxed{2^{11}}$ - $2^9 3^1 11^1$ - $2^9 3^1$ - … - $\boxed{2^{17}}$ - … - $\boxed{2^{26}}$ - …

2^7 (128) matches the 129th condition of Monks' rule, which says to replace n with $(33/4)$n. This gives $128 \cdot (33/4) = 1056 = 2^5 \cdot 3^1 \cdot 11^1$, the next number in the trajectory. 2^7 eventually gives way to 2^{11}, followed later by 2^{17}, then 2^{26}, and so on. This is how Monks' rule simulates the 3n+1 trajectory 7 - 11 - 17 - 26 - 13 - 20 - 10 - 5 - 8 - 4 - 2 - 1.

I say that Monks "essentially" gave a 1,021,020-way rule. If we wrote the whole rule, we'd see it contains only 10 distinct multipliers:

$$(\frac{1}{11}, \frac{136}{15}, \frac{5}{17}, \frac{4}{5}, \frac{26}{21}, \frac{7}{13}, \frac{1}{7}, \frac{33}{4}, \frac{5}{2}, \frac{7}{1})$$

These are the multipliers that Monks gave, in that order. You're supposed to interpret the multipliers like this:

If n is divisible by 11, replace it by $(1/11)$n.
Otherwise if n is divisible by 15, replace it by $(136/15)$n.
Otherwise if n is divisible by 17, replace it by $(5/17)$n.
…
Otherwise, replace it by 7n.

The 1,021,020-way rule is just an expansion of this simple rule. This new rule format is just an ordered list of fractions whose use is governed by implicit *ifs* and *otherwises*.

Question 36: Can you expand the *if-then* list $(\frac{1}{3}, \frac{4}{5}, \frac{5}{1})$ into a 3n+1-like 15-way rule?

Fractran

John Conway invented this *if-then-otherwise* rule format, named it **Fractran**, and proved something mind-blowing:

> No matter what computation you want to do,
> there's a Fractran rule that can do it.

Certainly, a Fractran rule can loop around and apply if-statements, but Conway's claim seems extraordinary. Want to compute a number's 3n+1 trajectory? There's a Fractran rule for that. Want to test if a number is prime? There's a Fractran rule for that. Want to sort a list of numbers, increase the contrast on a JPEG image, or translate a Russian sentence into French? There are Fractran rules for that. That means Fractran joins a club, together with tag systems, rewrite systems, and cellular automata, called **universal computers**.

When we say "Fractran is a universal computer," what do we mean?

Suppose I want to sort any list of numbers. I could wire up some specialized circuitry for that. You'd supply the numbers as electrical voltages on the left side of the wired-up circuit, and sorted numbers would appear in LEDs on the right side of the circuit. It would be a sorting machine. If I wanted to test numbers for primality, then I could wire up a different circuit. Maybe this circuit would have special memory transistors, allowing it to cycle through possible divisors. This would be a primality-testing machine.

However, a much better idea is to build just one machine: a laptop computer. Instead of handing it some numerical input, you also hand it a program-number plus an input-number. Then the laptop runs the program on the input and reports its results. In this way, the laptop can simulate the sorting machine or the primality-testing machine, but using fixed circuitry.

When we say "Fractran is a universal computer," we don't only mean what we said before:

> No matter what computation you want to do,
> there's a Fractran rule that can do it.

We also mean:

There's a *single* Fractran rule that accepts any program as its start number, and simulates that program.

A universal Fractran rule

Your laptop is a pretty complicated piece of circuitry, so you might imagine a universal Fractran rule to be equally complicated. Not so. John Conway proved the existence of such a rule in 1972, and he provided a concrete universal rule in his very funny 1987 paper ("FRACTRAN: A Simple Universal Programming Language"). Here's the rule:

$$(\frac{583}{559}, \frac{629}{551}, \frac{437}{527}, \frac{82}{517}, \frac{615}{329}, \frac{371}{129}, \frac{1}{115}, \frac{53}{86}, \frac{43}{53}, \frac{23}{47}, \frac{341}{46},$$
$$\frac{41}{43}, \frac{47}{41}, \frac{29}{37}, \frac{37}{31}, \frac{299}{29}, \frac{47}{23}, \frac{161}{15}, \frac{527}{19}, \frac{159}{7}, \frac{1}{17}, \frac{1}{13}, \frac{1}{3})$$

Just like your laptop comes with a programming manual, Conway provided a programming manual (of sorts) for his universal Fractran rule. It starts like this:

With start number $c \cdot 2^{(2^n)}$,
the universal Fractran rule will run program c on input n.
If its trajectory reaches a number of the form $2^{(2^m)}$, it outputs m.

Conway guarantees that no matter what program you want to run, there's a number c for it. He helpfully supplies a table of sample programs and their c values:

Program number	Program description
c = 847	Ignores its input n and always outputs 1
c = 37,485	Subtracts one from its input ($n = n - 1$)
c = 2,268,945	Adds one to its input ($n = n + 1$)

And so on. According to Conway's claim, somewhere down the list, there should be a program described as "If n is even, n = n/2; otherwise, n = (3n+1)/2" and another one described as "Translate a French sentence into English."

It's sometimes hard to tell if Conway is joking. Let's test out his Fractran rule by asking it to perform the subtraction "3 minus 1" using his program number $c = 37,485$. Our start number becomes $37,485 \cdot 2^{(2^3)} = 9,596,160$, and here's the 187-step trajectory:

9,596,160 - 102,998,784 - 763,534,464 - 633,139,584 - 4,693,491,264 - 5,601,908,928 - 4,390,685,376 - 5,012,234,304 - 3,928,507,968 - 40,504,271,808 - 300,259,927,968 - 248,982,141,408 - 1,845,715,439,568 - 2,202,950,685,936 - 1,726,637,024,112 - 1,971,061,140,048 - 1,544,885,758,416 - ... - 63,147,001,528,611 - 10,015,578,579,006 - 11,481,273,005,202 - 1,821,014,287,092 - 2,087,504,182,764 - 331,093,506,744 - 379,546,215,048 - 60,198,819,408 - 69,008,402,736 - 128,997,470,160 - 147,875,148,720 - 72,364,434,480 - 629,255,952 - 37,015,056 - 2,847,312 - 219,024 - 16,848 - 1296 - 432 - 144 - 48 - 16

We go until we hit a number of the form $2^{(2^m)}$. Here, $16 = 2^{(2^2)}$, so our answer is $m = 2$. In other words, $3 - 1 = 2$, which is correct!

How does Conway do this? If I didn't know what was going on, I'd assume this trajectory was like any other random-looking 3n+1 trajectory we've seen so far in this book. It starts around ten million, wiggles its way up to just short of two trillion, then descends to sixteen. But Conway's programming manual explains. Here's the same trajectory with prime factors exposed:

9,596,160	=	2^8	3^2	5^1	7^2		17^1			
102,998,784	=	2^8	3^1		7^3		17^1		23^1	
763,534,464	=	2^7	3^1		7^3	11^1	17^1			31^1
633,139,584	=	2^7	3^1		7^3	11^1		19^1	23^1	
...										
16	=	2^4								

What Conway is doing is storing the state of a universal computer in the exponents of the prime factors. We can think of each prime factor as a separate memory register, a piece of computer memory. The initial state $2^8 3^2 5^1 7^2 17^1$ is a combination of the program number $c = 37,485 = 3^2 5^1 7^2 17^1$ and the input $n = 3$, stored as $2^{(2^3)} = 2^8$.

When the rule turns $2^8 3^2 5^1 7^2 17^1$ into $2^8 3^1 7^3 17^1 23^1$, it's actually decrementing registers 3 and 5, while incrementing registers 7 and 23. The next step decrements register 2, among other things. Register 2 is very important; it's where the final answer appears, once the other registers are zeroed out.

When Conway selected the fractions of the universal Fractran rule, he was actually looking at another universal computer (a "Minsky machine"), and setting up the fractions specifically to simulate that other computer. If a program loops forever on a Minsky machine, it will also loop forever under the universal Fractran rule, meaning no number of the form $2^{(2^m)}$ will ever appear in its trajectory.

Question 37: Can you use the universal Fractran rule to compute $1+1$?

The importance of Fractran

If you're like me, you're probably asking, what's all this Fractran stuff got to do with the 3n+1 problem? Let me try to explain. The universal Fractran rule is just a compact way of writing a rule in our familiar format:

$$\begin{array}{ll}
(a_0 n + b_0)/d & \text{when } n \equiv 0 \text{ (mod d)} \\
(a_1 n + b_1)/d & \text{when } n \equiv 1 \text{ (mod d)} \\
\quad \ldots & \\
(a_{d-1} n + b_{d-1})/d & \text{when } n \equiv d-1 \text{ (mod d)}
\end{array}$$

In that way, it's similar to the 3n+1 rule:

$$\begin{array}{ll}
(1n + 0)/2 & \text{when } n \equiv 0 \text{ (mod 2)} \\
(3n + 1)/2 & \text{when } n \equiv 1 \text{ (mod 2)}
\end{array}$$

Conway's universal rule isn't *the* 3n+1 rule, but it's *a* 3n+1 rule, or at least a 3n+1-*type* rule. Conway is saying that some 3n+1-type rules are full-blown computers, and it's useless to try to predict their behavior.

That's how Conway's mind works. He looks at the 3n+1 rule and thinks, "3n+1 is a kind of bird. It has two legs. A bird is a kind of vertebrate. Some vertebrates go surfing and eat burritos. There are other kinds of birds, such as penguins. Penguins don't fly. So, not all birds fly."

Is 3n+1 is a flightless bird? Does it eat burritos? I don't know. It might.

Notes and references

Liesbeth de Mol describes a tag system that simulates 3n+1 in "Tag Systems and Collatz-like Functions" (*Theoretical Computer Science*, vol. 390, no. 1, 2008). She provides more historical background on simple computing devices in her dissertation, "Tracing Unsolvability. A Historical, Philosophical and Mathematical Analysis with a special focus on Tag Systems" (Department of Philosophy, Ghent University, 2007).

Emre Yolcu, Scott Aaronson, and Marijn J. H. Heule describe their rewrite system and computer-based attack on the 3n+1 problem in "An Automated Approach to the Collatz Conjecture" (*Proceedings of the International Conference on Automated Deduction*, 2021).

The first cellular automaton for 3n+1 appeared in Ivan Korec's paper, "The 3x+1 Problem, Generalized Pascal Triangles, and Cellular Automata" (*Math. Slovaca*, 42, 1992).

The Farkas variant of the 3n+1 rule was introduced by Hershel Farkas in "Variants of the 3N+1 conjecture and multiplicative semigroups" (*Geometry, Spectral Theory, Groups, and Dynamics*, 2005).

John Conway popularized the original Collatz rule in an accessible article, "On Unsettleable Arithmetical Problems" (*American Mathematical Monthly*, March, 2013), based on work he reported in "Unpredictable Iterations" (*Proceedings of the Number Theory Conference*, Boulder, 1972).

The Matthews-Watts conjecture appears in K. R. Matthews' paper "Generalized 3x+1 Mappings: Markov Chains and Ergodic Theory," in the collection *The 3x+1 Problem: The Ultimate Challenge*, edited by Jeffrey Lagarias. Edward G. Belaga and Maurice Mignotte write extensively on the conjecture in "Walking Cautiously into the Collatz Wilderness: Algorithmically, Number Theoretically, Randomly" (*Fourth Colloquium on Mathematics and Computer Science, Discrete Mathematics and Theoretical Computer Science*, 2006).

Conway describes Fractran in "FRACTRAN: A Simple Universal Programming Language for Arithmetic" (*Open Problems in Communication and Computation*, 1987, and in Lagarias' edited volume.) You may also be interested in Lagarias' tribute "Conway's Work on Iteration: In memory of John Horton Conway (1937–2020)" (*The Mathematical Intelligencer* 43, 2021).

Ken Monks' paper is "3x+1 Minus the +," *Discret. Math. Theor. Comput. Sci.* 5, 2002.

Many other papers expand on the computational power of simple, 3n+1-like rules. For example:

- Stuart A. Kurtz and Janos Simon, "The Undecidability of the Generalized Collatz Problem," *Theory and Applications of Models of Computation*, 2007.
- Frantisek Kascak, "Small Universal One-State Linear Operator Algorithms," *Proc. MFCS*, 1992.
- Pascal Michel, "Busy Beaver Competition and Collatz-like Problems," *Arch. Math. Logic*, 32, 1993.
- Turlough Neary and Damien Woods, "Tag Systems and the Complexity of Simple Programs," *Workshop on Cellular Automata and Discrete Complex Systems*, 2015.

The chapter's opening quote[1] ("Young man, in mathematics you…") is from Hungarian-born mathematician John von Neumann, inventor of game theory and standard computer architecture, among many other things. I love it when famous scientists joke around.

[1] John von Neumann responding to physicist Felix Smith's doubts, according to Gary Zukav's *The Dancing Wu Li Masters*, 1979.

Glossary

3n+1. Start with any positive whole number n. If n is odd, multiply it by 3 and add 1. If n is even, divide it by 2. Then repeat this procedure. For example: 5-16-8-4-2-1. For most of this book, we use the equivalent *revised* 3n+1 rule, where "If n is odd, multiply it by 3 and add 1, then immediately divide by 2." For example: 5-8-4-2-1.

3n+1 conjecture. The hypothesis that all start numbers eventually reach 1 under the 3n+1 rule. The conjecture has been verified for all start numbers up to 10^{20}, but there is no proof for all numbers. A counter-example would be a number that fails to reach 1 by cycling or diverging to infinity.

3n+1 tree. An infinite tree in which each number points to its successor according to the 3n+1 rule. Every number has one successor and one or two predecessors.

3n-1 problem. A variation of the 3n+1 problem with "-1" instead of "+1". Some non-trivial cycles for the 3n-1 problem are known: one starts with 5, and the other starts with 17.

5n+1 problem. A variation of the 3n+1 problem in which odd numbers are multiplied by 5 instead of 3. Unlike the 3n+1 problem, 5n+1 trajectories trend upwards, and it is conjectured that almost all numbers diverge to infinity.

abc-conjecture. If a, b, and c are co-prime, and $a + b = c$, then c is greater than the product of the unique prime factors of a·b·c, raised to any power greater than 1, with only finitely many exceptions.

Affine transformation. A function that transforms vectors into vectors while adhering to certain restrictions. A sample affine transformation is $y = Ax + B$, where A is a matrix and B is a constant vector.

Almost all. When mathematicians say "almost all" integers are composite, they don't mean 90% or 99% of them, as in colloquial English. They mean: "the percentage of numbers between 1 and x that are composite gets closer and closer to 100%, as x gets bigger and bigger."

Almost no. The flip-side of almost all. "Almost no numbers are prime" means the percentage of numbers between 1 and x that are prime gets closer and closer to 0%, as x increases.

Aperiodic. A sequence (or necklace) is aperiodic if it can't be chopped into identical pieces. The sequence 010001 is aperiodic, but 001001 is not, because it can be chopped into 001 and 001.

Application. In math-speak, a mathematical result has applications if it enables (or eases) the creation of other mathematical results.

Bakuage prize. A prize worth 120 million Japanese yen, established by Bakuage Co., Ltd., of Tokyo, Japan, for a successful resolution of the 3n+1 conjecture.

Basel problem. Posed by Pietro Mingoli and solved by Leonhard Euler, the Basel problem asks for a closed-form expression for $1/1^2 + 1/2^2 + 1/3^2 + 1/4^2 + \ldots$

Beta. In this book, a member of a 3n+1 cycle takes the form beta/$(2^k - 3^x)$.

Catalan's conjecture. A conjecture made in 1844, and proven in 2002, which states that $x^a - y^b = 1$ has only one whole-numbered solution (when $a > 1$ and $b > 1$), namely $3^2 - 2^3 = 1$.

Ceiling. The first whole number greater than or equal to a given real number. For example, ceiling$(2.5) = \lceil 2.5 \rceil = 3$. It is always true that $\lceil x \rceil \geq x$.

Cellular automaton. A rule for transforming one sequence into another. The automaton replaces each item of the current sequence with a new item, where the new item depends only on the old item and its neighbors, as specified by the rule. 3n+1 trajectories can be mimicked by a simple one-dimensional cellular automaton. The most famous two-dimensional automaton is Conway's Game of Life.

Chaos. A word used in exasperation or amazement to describe how simple mathematical definitions (such as for prime numbers) lead to apparently pattern-less, unpredictable behaviors.

Chinese remainder theorem. If $n \equiv a_i \pmod{m_i}$, for $i = 1$ to k, there is a whole-numbered solution n if $m_1, m_2, \ldots, m_k$ are pairwise co-prime. Also, for any solution n, there is another solution $n + m_1 m_2 \ldots m_k$. The theorem is used to solve linear Diophantine equations.

Church-Turing thesis. The proposal that any computable function can be implemented by some Turing machine or equivalently powerful device.

Circuit. A type of cycle in which all odd terms precede all even terms. For the 5n+1 problem, the cycle 13-33-83-208-104-52-26-13 is a circuit.

Clock math. *See* Modular arithmetic.

Collatz conjecture. See 3n+1 conjecture.

Composite. An integer that is not prime. *See* Prime.

Composition. A single function that replaces a pipeline of two functions. For example, if $f(x) = x+1$ and $g(x) = x^2$, we can rewrite $g(f(x))$ as a single function $x^2 + 2x + 1$.

Congruent. Two whole numbers x and y are congruent ($x \equiv y$) mod p if they have the same remainder when divided by p.

Conway map. *See* Original Collatz rule.

Co-prime. Two integers are co-prime if they share no common factor other than 1. For example, 9 and 35 are co-prime, but 12 and 15 are not (both have 3 as a factor). About 61% of (n, m) pairs are co-prime.

Contracting system. A 3n+1-type rule whose coefficients suggest that trajectories will trend downwards. *See also:* Critical density, Matthews-Watts conjecture.

Counter-example. An example that demonstrates the falsity of a conjecture. For example, we might conjecture that $n^2 - n + 41$ is always prime, because we observe values like 41 ($n = 1$), 43 ($n = 2$), 47 ($n = 3$), ... 1447 ($n = 38$), and so on. But $n = 41$ is a counter-example, since $41^2 - 41 + 41 = 41^2$, which is not prime.

Critical density. A 3n+1-type system with conditions of the form "$(a_i n + b_i)/d$, when $n \equiv i$ (mod d)," for $0 \le i \le d - 1$, has critical density $(a_0 a_1 \ldots a_{d-1})/d^d$. If the critical density is 1.2, then a start number n might be expected to reach about 1.2n after d "average" steps. If the critical density is smaller than one, it's conjectured that every start number reaches a cycle.

Cycle. A sequence of numbers that loops back on itself. There is only one known 3n+1 cycle among positive whole numbers, the trivial one: 1-2-1.

Diffie-Hellman key exchange. A cryptographic protocol that allows two participants to develop a shared secret key. They develop their shared secret by exchanging messages encrypted with private keys using fast modular exponentiation. An eavesdropper can only discover the shared secret by solving a discrete log problem for which there is no known practical method.

Diophantine equation. An equation whose variables take on integer values. For example, $2x + 5y = 100$ has many solutions, including $x = 25$, $y = 10$. But $2x = 7$ has no solutions.

Discrete log. The discrete log of x, using base b and modulus p, is the exponent y such that $b^y \equiv x$ (mod p). Unlike the popular real-valued logarithm, the variables x, b, p, and y are all integers. The discrete log is very difficult to calculate for large integers. Its apparent difficulty is the basis of many encryption algorithms.

Divergent number. In the context of the 3n+1 problem, a number that never enters a cycle, but whose trajectory reaches ever-increasing heights, heading toward infinity. No divergent numbers are known, and there is no proof of their existence or non-existence.

Elementary proof. A proof about some property of integers that employs addition and multiplication, avoiding mathematical techniques such as real analysis, complex or transcendental numbers, trigonometry, and so on.

Expanding system. A 3n+1-type rule whose coefficients suggest that trajectories will trend upwards. *See also:* Critical density, Matthews-Watts conjecture.

Expected value. The predicted value of a variable, given different probabilities for different values. For example, the expected value of a die roll is $1/6 \cdot 1 + 1/6 \cdot 2 + \ldots + 1/6 \cdot 6 = 3.5$. If you keep rolling, your rolls will average out to around 3.5.

Euclid sequence. Given an initial list of primes $p_1, p_2, p_3, \ldots p_m$, we compute $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m + 1$. If n is prime, we add it to the end of the list. If n is composite, we add its *smallest* prime factor to the end of the list. If we start with $p_1 = 2$ and continually repeat this procedure, we get the Euclid sequence: 2, 3, 7, 43, 13, 53…

Euclidean algorithm. An efficient way to identify the greatest common divisor (gcd) of two numbers. If the gcd equals 1, then the two numbers are co-prime.

Euler product. A rewrite of a sum over all whole numbers into a product over all prime numbers. For example, $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots = \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{7}{6} \cdot \ldots$ Both sides of this equation diverge to infinity.

Farkas rule. Start with any number n. Let k be the remainder of n when divided by 6. If k is 0 or 2, replace n with n/2; if k is 3 or 5, replace n with (3n+1)/2; otherwise, replace n with (n-1)/3. Repeat this procedure. It's known that with the Farkas rule, all numbers eventually reach 1.

Fermat's Last Theorem. The equation $x^n + y^n = z^n$ has no integer solutions when $n > 2$. This conjecture was unresolved for over 350 years before being proved true by Andrew Wiles in 1995.

Fermat's Little Theorem. For any prime p, and b indivisible by p, $b^{p-1} \equiv 1$ (mod p). For example, $2^4 = 16 \equiv 1$ (mod 5).

Floor. The first whole number less than or equal to a given real number. For example, floor(2.5) $= \lfloor 2.5 \rfloor = 2$. It's always true that $\lfloor x \rfloor \leq x$.

Fractran. A programming language devised by John Conway. In Fractran, a program is simply a list of fractions. The program takes an input number and iteratively transforms it, creating a computational trajectory that is similar to a 3n+1 trajectory.

Fundamental theorem of arithmetic. Every whole number greater than 1 has a unique prime factorization.

Game of Life. A two-dimensional cellular automaton invented by John Conway. The automaton controls the evolution of a grid of black and white squares. The evolution follows a simple rule, but the results are intricate and complex.

Greatest common divisor. The greatest common divisor, gcd(x, y), is the largest number that divides both x and y. For example, $\gcd(12, 15) = 3$. In the case where $\gcd(x, y) = 1$, x and y are co-prime. Also called *greatest common factor* or *greatest common denominator*.

Germain prime. A prime p such that $2p + 1$ is also prime.

Glider. An oscillating pattern in the Game of Life that moves across the grid.

Glider gun. A Life object that emits gliders, usually at some regular frequency.

Halting problem. The problem of determining whether an arbitrarily-given program will terminate or loop forever. Alan Turing showed that there is no algorithm to solve the halting problem.

Harmonic numbers. A number with no prime factors except 2 and 3. Examples include 6 ($2^1 \cdot 3^1$), 16 (2^4), and 144 ($2^4 \cdot 3^2$).

Harmonic series. The infinite list of fractions $(1/1), (1/2), (1/3), (1/4)$, and so on. Their sum diverges to infinity as the list grows.

Height. The height of n is the number of steps it takes n to reach 1, not counting even numbers. For example, 13 has a height of 2, because the trajectory 13-20-10-5-8-4-2-1 passes through odd terms 5 and 1.

Heuristic argument. Informal evidence for (or against) a mathematical conjecture. For example, if all 3n+1 trajectories were to encounter even and odd terms with equal frequency, then they would all eventually reach 1. As heuristic arguments rest on unproven assumptions, they do not count as proofs.

High cycle. Considering all cycles of a certain length, the high cycle is the one whose bottom member is greatest.

Infinite sum. The result of adding up an infinitely-long list of numbers. Even though the list is infinite, the sum may be finite. For example, $1/2 + 1/4 + 1/8 + 1/16 + \ldots$ gets closer and closer to 1, but never exceeds it. So, the sum converges to 1. Other infinite sums diverge. For example, $1 + 1 + 1 + \ldots$ diverges to infinity, as does $1/2 + 1/3 + 1/4 + 1/5 + \ldots$

Intel Pentium-chip bug. A hardware bug that caused a particular computer chip to make occasional arithmetic errors. The bug was discovered by a mathematician doing calculations with prime numbers.

Irrational number. A number that cannot be written as the ratio of two integers. For example, there are no integers p and q such that $\sqrt{2} = p/q$, even though a ratio like 3363/2378 comes close.

k. In this book, the length of a 3n+1 cycle.

Kook. In surfing lingo, a novice surfer.

Lattice points. Points on graph paper where lines intersect. Lattice points have integer coordinates, such as (3, 4).

Life. *See* Game of Life.

Linear function.. A function that can be expressed in the form $y = mx + b$.

Linear Diophantine equation. An equation such as $5b-2c = 14$, where a solution consists of whole-numbered values for b and c.

Linear Diophantine inequality. An inequality such as $5b + 2c \leq 14$, where a solution consists of whole-numbered values for b and c.

Log. *See* Logarithm.

Logarithm. The logarithm of x, using base b, is denoted $y = \log_b(x)$. It is the y such that $b^y = x$.

Log base 2. $\log_2(x)$ is the y such that $2^y = x$. As an example, $\log_2(32) = 5$.

Log base 10. $\log_{10}(x)$ is the y such that $10^y = x$. As an example, $\log_{10}(1000) = 3$.

Lower bound. A function whose values always stay below those of another function. For example, $x - 3$ is a lower bound for x^2.

Lyndon word. An aperiodic necklace.

Mathematical induction. A technique for proving that some property holds for every member of an infinite set. The base step handles the first member of the set, while the inductive step shows that if the property holds for the ith element of the set, then it also holds for the (i+1)-st element of the set.

Matthews-Watts conjecture. A more-general variation of the 3n+1 conjecture. Matthews and Watts classify multi-way rules as "expanding" or "contracting," depending on their coefficients. It predicts that for contracting rules (including 3n+1), all numbers eventually reach a cycle, while for expanding rules (including 5n+1), almost all numbers diverge to infinity. *See also:* Multi-way rule.

Modular arithmetic. Arithmetic over a finite subset of whole numbers, sometimes called "clock math." In the clock analogy, 8 hours past 6 o'clock is not $8 + 6 = 14$ o'clock, but rather 2 o'clock, because $8 + 6 \equiv 2 \pmod{12}$. In general, $x \equiv y \pmod{p}$ means that x and y have the same remainder when divided by p. Possible remainders run from 0 to $p - 1$, and p is called the modulus.

Modular exponentiation. The process of calculating $b^a \bmod p$, that is, the remainder of b^a when divided by p.

Modulus. *See* Modular arithmetic.

Multiplicative order. The multiplicative order of x modulo p is the smallest whole number b such that $x^b \equiv 1 \pmod{p}$.

Multi-way rule. The 3n+1 rule has two branches, one for odd n, and one for even n. A multi-way rule has three or more branches. For example, it may branch on whether the remainder of n divided by 3 is 0, 1 or 2.

Natural log. $\ln(x) = \log_e(x) =$ the y such that $e^y = x$, where e is a transcendental number with value 2.718… For large x, $\log_e(x)$ is roughly 2.3 times the number of decimal digits of x.

Necklace. A sequence that is considered unchanged by rotation. For example, a necklace consisting of three contiguous 1s and two contiguous 0s can be written (equivalently) as 11100, 11001, 10011, 00111, or 01110.

Non-trivial cycle. Any cycle not containing the terms 0 or 1.

Normal number. A number in which all subsequences of any length n occur with equal frequency. Numbers like π are believed to be normal, though this has not been proven.

Number. An object whose definition is beyond the scope of this book.

Odd Goldbach conjecture. The conjecture that every odd number greater than 5 is the sum of three primes.

Operation sequence. A linear arrangement of the operations $\frac{3n+1}{2}$ and $\frac{n}{2}$. For example: $\frac{3n+1}{2}$, $\frac{3n+1}{2}$, $\frac{n}{2}$, $\frac{n}{2}$, $\frac{n}{2}$. For any operation sequence, there is a unique rational number that loops back on itself.

On-Line Encyclopedia of Integer Sequences. A vast, crowd-sourced, curated collection of integer sequences available for browsing and search at *oeis.org*.

Order. *See* Multiplicative order.

Original Collatz rule. Start with any number n. Divide it by 3. If there is no remainder, replace n with 2n/3. If the remainder is 1, replace n with (4n-1)/3. If the remainder is 2, replace n with (4n+1)/3. Each number n has a unique successor and a unique predecessor.

Prime. A positive integer that is only divisible by 1 and itself. For example, 23 is prime.

Prime factors. The prime factors of n are those primes whose product is n. For example, $63 = 3 \cdot 3 \cdot 7$. Every number has a unique prime factorization.

Prime number theorem. As x tends to infinity, the number of primes less than x gets closer and closer to $x/\log_e x$, where $\log_e x$ is the natural log of x.

Primorial. The nth primorial is the product of the first n primes. The first few primorials are 2, 6, 30, 210, 2310, 30030, …

Proof by cases. A proof technique that breaks a complex problem down into an exhaustive set of cases, then handles those cases one by one. To prove a fact about all whole numbers, we might first prove it for all odd numbers (using one method), then prove it for all even numbers (using another method).

Provable. *See* Unprovable.

qn+1 problem. Start with any whole number n. If n is even, replace it by n/2. If n is odd, replace it by (qn+1)/2. Then repeat.

Rational number. A number that can be written as the ratio of two integers, for example, 3.8 = 19/5.

Real number. Very roughly speaking, some specific distance down the number line, such as 7, or 19/5, or π, or 3.333…

Reduced fraction. A fraction whose numerator and denominator cannot be reduced to smaller values, because they are co-prime. For example, 42/20 is not a reduced fraction, but 21/10 is.

Reductio ad absurdum. A technique for proving a proposition by first assuming its opposite. If this leads us to a contradiction or absurd conclusion, then we know the proposition's opposite is false, so the proposition itself must be true.

Relatively prime. *See* Co-prime.

Repeated squaring. A fast method for modular exponentiation. When computing something like 2^b (mod p), for very large b, repeated squaring avoids having to expand 2^b.

Rewrite system. A set of rules for transforming one sequence into another. The system selects a rule that matches some portion of the current sequence and replaces the matched portion with new items. It then repeats this procedure on the resulting sequence. If no rules match, the system stops.

Riemann Hypothesis. An unproven conjecture about the values of the Riemann zeta function, with many potential applications in number theory.

Riemann zeta function. The zeta function applied to complex numbers.

Rule 110. A simple cellular automaton discovered by Stephen Wolfram, proved by Matthew Cook to be a universal computer.

Squarefree. A number is squarefree if it doesn't have any repeated prime factors.

Spoiler factor. In this book, a factor of q, not shared by p, that proves p/q is not a whole number.

State. A snapshot of a computation that contains all of the information required for the computation to continue.

Stirling's approximation. A useful approximation to the factorial function, $n! = 1 \cdot 2 \cdot \ldots \cdot n \approx (n/e)^n\sqrt{2\pi n}$, where e is the base of the natural logarithm.

Structure. A pattern or regularity in how numbers behave.

Tag system. A set of rules for transforming one sequence into another. A tag system removes items from the left of the sequence, and adds new items to the right. It then repeats this procedure on the resulting sequence. If the sequence becomes short enough, the system stops. Lisbeth de Mol discovered a tag system that computes 3n+1 trajectories.

Term. A member of a 3n+1 trajectory.

Threeven. Divisible by 3. Come on, English, you can do it!

Total stopping time. The total stopping time of n is the number of 3n+1 steps it takes for n to reach 1. If n never reaches 1, its total stopping time is infinite. For example, the trajectory of 5 is 5-8-4-2-1, so 5 has a stopping time of 4.

Tower of Hanoi puzzle. A puzzle involving disks of various sizes that slot onto three poles. The goal is to move a pyramid of disks from one pole to another, without ever placing a larger disk on top of a smaller one.

Trajectory. A sequence of numbers that follows the 3n+1 rule. For example, 40-20-10-5-8-4-2-1.

Transcendental number. A number that is not the solution to any algebraic equation. $\sqrt{2}$ is not transcendental, because it is a solution to $x^2 = 1$. Transcendental numbers include π, e, and $\log_2(3)$.

Trivial cycle. In the 3n+1 problem, the trivial cycle is 1-2-1-2-1 ...

Twin primes. A pair of prime numbers separated by a distance of two, such as 17 and 19.

Twin prime conjecture. The hypothesis that there are an infinite number of twin primes, an unsolved question in number theory.

Turing machine. A mathematical model of a simple computer that reads and writes symbols on an infinite strip of paper. Anything your laptop can compute, a Turing machine can also compute, albeit more slowly.

Universal computer. A system with problem-solving ability equal to any other computer. The system may not be as fast, but it will convert the same inputs into the same outputs.

Unprovable. Some mathematical assertions are true but unprovable, a counter-intuitive fact first discovered by Kurt Gödel in 1931. Therefore, even if the 3n+1 conjecture is true, there be no way to prove it.

Upper bound. A function whose values always exceed those of another function. For example, x^2 is an upper bound for $x - 3$.

Whole number. A whole number is one of these: 0, 1, 2, 3, 4, ... Expanding this list to include negatives, we get the integers.

Wieferich prime. A prime number p whose square p^2 divides $2^{p-1} - 1$. Or, equivalently, a prime p with $\mathrm{ord}_2(p) \equiv \mathrm{ord}_2(p^2)$. There are only two known Wieferich primes.

Wondrous number. In Douglas Hofstadter's book *Gödel, Escher, Bach: An Eternal Golden Braid*, a wondrous number is any number that eventually reaches 1 via the 3n+1 rule. The 3n+1 conjecture posits that all positive whole numbers are wondrous.

x. In this book, the number of odd terms (or up-moves) in a 3n+1 cycle.

Zeta function. Introduced by Euler, the function $\zeta(s) = (1/1^s)+(1/2^s)+(1/3^s)+(1/4^s) + \ldots$ is useful for counting prime numbers and estimating the chance that two numbers are co-prime, among other applications.