Collatz Generalization and the 0-cycle problem

Jasper Dekoninck

9/9/20

Summary
In this paper, I use a possible generalization of the Collatz Conjecture as a motivation to study the "0-cycles-problem". The "0-cycles-problem" is solved, but the existence of easier solutions cannot be excluded. These reformulations are left as future research.

1 Introduction

1.1 The Collatz Conjecture

The Collatz Conjecture is probably one of the most well known and easy to understand unproved conjectures so far. The conjecture considers a certain function on a number n. This function $f^1 : \mathbb{N}_0 \to \mathbb{N}_0$ can be defined as follows:

$$f^1(n) = \begin{cases} \frac{n}{2} & n \equiv 0 \pmod 2 \\ 3n+1 & n \not\equiv 0 \pmod 2 \end{cases} \tag{1}$$

For $k \in \mathbb{N} \setminus \{0,1\}$, $f^k : \mathbb{N}_0 \to \mathbb{N}_0$ can be defined recursively as $f^k(n) = f(f^{k-1}(n))$.

The Collatz conjecture can now be stated as:

Conjecture 1. *Given any $n \in \mathbb{N}$. Then there exists a $k \in \mathbb{N}_0$ such that $f^k(n) = 1$.*

The conjecture has been checked for enormous numbers, though nobody succeeded so far in proving it.

1.2 The Collatz generalization

In order to generalize the conjecture, we first of all need to define a generalization of the Collatz-function (1). Let $a, b, c \in \mathbb{N}_0$ and $a > 1$. Then $f^1_{a,b,c} : \mathbb{N}_0 \to \mathbb{N}_0$ is defined as:

$$f^1_{a,b,c}(n) = \begin{cases} \frac{n}{a} & n \equiv 0 \pmod a \\ bn+c & n \not\equiv 0 \pmod a \end{cases} \tag{2}$$

Then we can define $f^k_{a,b,c} : \mathbb{N}_0 \to \mathbb{N}_0$ for $k \in \mathbb{N} \setminus \{0,1\}$ recursively as $f^k(n) = f(f^{k-1}(n))$.

Now we can ask ourselves for which triplet of numbers (a,b,c) $f^k_{a,b,c}(n)$ stays finite for every n. This is to say that for every $n \in \mathbb{N}$ there exists a number $M \in \mathbb{N}$ such that $f^k_{a,b,c}(n) < M$ for every k. You may note that this statement is a less strong statement as the one considered in Conjecture 1, as it now only needs to stay finite, it doesn't need to hit 1. However, the statement has quite a lot in common with the original conjecture. The reason numbers go to 1 in Conjecture 1, is because there is a loop going from 1 to 2 to 4 back to 1. Using the pigeon hole principle, it is very easy to see that in order to stay finite, a number needs to get stuck in such a loop.

Instead of trying to prove for which triplets the given statement is correct (which is a problem far too difficult for this author), the next pages are dedicated to a proof for which numbers the statement is definitely incorrect. Given a triplet (a,b,c), if there exists a number n such that $f^k_{a,b,c}(n)$ is never divisible by a, then the given statement is incorrect for this triplet. So we're going to investigate for which numbers this is the case.

2 0-cycle problem

2.1 Defining the problem

Because we're only interested in the value of $f^k(n) \pmod a$, we can restrict ourselves to finding so called cycles starting at $n < a$. More specifically, we can restate our problem as:

Definition 1. *Let $a, b, c \in \mathbb{N}$, $a > 1$ and $n_0 \in \{0, 1, 2, ..., a-1\}$. Let $n_k = ((bn_{k-1} + c) \pmod a)$ for all $k \in \mathbb{N}_0$. The 0-cycle problem asks for what triplets (a,b,c) the following statement is true:*

$$\forall n_0 \in \{0, 1, 2, ..., a-1\}, \exists k \in \mathbb{N}_0 : n_k = 0$$

You may note that this problem is the exact opposite of how we originally stated it.

2.2 Definitions

Before we can go on to explore the problem, we first need a few definitions.

Definition 2. *The cycle of* (a, b, c, n_0) *is only defined if there exists a* $k > 0$ *such that* $f^k_{a,b,c}(n_0) \pmod a = n_0$. *Otherwise, it is equal to* $u \in \mathbb{N}^m$ *defined as:*

1. $u_0 = n_0$
2. m *is the number of unique elements in the set* $\{f^k(n) \pmod a\}$.
3. $\forall k \in \{1, ..., m-1\} : u_k = f^k_{a,b,c}(n_0) \pmod a$

For example, the cycle of $(7, 3, 1, 1)$ is equal to $(1, 4, 6, 5, 2, 0)$ because:

$$\begin{aligned}
(3 \cdot 1 + 1) &\pmod 7 = 4 \\
(3 \cdot 4 + 1) &\pmod 7 = 6 \\
(3 \cdot 6 + 1) &\pmod 7 = 5 \\
(3 \cdot 5 + 1) &\pmod 7 = 2 \\
(3 \cdot 2 + 1) &\pmod 7 = 0 \\
(3 \cdot 0 + 1) &\pmod 7 = 1 = n_0
\end{aligned}$$

At first sight you might doubt that $f^m_{a,b,c}(n_0) = n_0$ if m is defined like this. First of all, let's note that there can be no i with $0 < i < m$ such that $f^i_{a,b,c}(n_0) = n_0$. If this was the case, then the unique elements that get infinitely repeated are $(n_0, ..., f^{i-1}_{a,b,c}(n_0))$ which can be at most i different numbers. Now let's say that $f^m_{a,b,c}(n_0) \neq n_0$. Because of the pigeon hole principle, there would exist two indices $0 < i < j \leqslant m$ such that $f^i_{a,b,c}(n_0) = f^j_{a,b,c}(n_0)$, but then again the numbers between i and j get infinitely repeated. This ensures that there is actually no cycle of (a, b, c, n_0).

There are two types of cycles:

Definition 3. *A 0-cycle of* (a, b, c) *is a cycle* u *of* (a, b, c, n_0) *for a* $n_0 \in \{0, 1, ..., a-1\}$ *that contains the number* 0.

Definition 4. *A non-0-cycle of* (a, b, c) *is a cycle* u *of* (a, b, c, n_0) *for a* $n_0 \in \{0, 1, ..., a-1\}$ *that doesn't contain the number* 0.

3 Solution 0-cycle problem

3.1 Easy cases

A first exploration of the problem, leads to some basic lemma's. The following lemma is trivial, but is mentioned nonetheless for completeness.

Lemma 1. *For given values of* (a, b, c, n_0) *there is at most one cycle of* (a, b, c, n_0).

Proof. This lemma follows trivially from the definition. As soon as the first value of the cycle is given, the next values are deterministic. □

The next theorem solves the question for the easy or trivial cases $c \equiv 0 \pmod a$.

Theorem 1. *Let* $a, b, c \in \mathbb{N}$ *and* $c \equiv 0 \pmod a$. *There exist no non-0-cycles of* (a, b, c) *if and only if for each prime number* p *that divides* a *it applies that it also divides* b.

Proof. Assume there is a prime number p such that $p \mid a$ and $p \nmid b$. We prove there is a non-0-cycle. Let v be a sequence, $v_0 = 1$ and $v_k = f^k_{a,b,c}(1)$. Thus $v_k = (b^k \pmod a)$. If $b^k \pmod a = 0$, then $p \mid a \mid b^k$ which is impossible. Hence $v_k \neq 0$. Because $b^k \pmod a$ can only take finitely many values, there must be a non-0-cycle hiding within v.

Assume that for each prime number p that divides a it applies that it also divides b. It follows that there is a number k such that $a \mid b^k$. We prove there can be no non-0-cycle. Assume there is one called u. Then $u_k = (u_0 b^k \pmod a) = 0$ which is impossible for a non-0-cycle. □

As an example, take $a = 3$, $b = 2$ and $c = 3$. There are two cycle in this example: (0) and $(1, 2)$. Thus the theorem here is indeed correct. As another example, take $a = 3$, $b = 9$ and $c = 0$. There is only one cycle in this example, namely (0). All other numbers eventually become 0 and get stuck in this 0-cycle.

3.2 Solution for prime numbers

Unfortunately, before getting any further, we first need to prove a lot of lemma's. The first of them is only necessary to prove another one that we're going to encounter later on.

Lemma 2. *If a 0-cycle of (a, b, c) exists that starts with n_0, then this cycle is equal to (0) if and only if $c \equiv 0 \pmod a$.*

Proof. Assume that the cycle is equal to $(0) = u$. Thus we know that $b \cdot 0 + c \equiv 0 \pmod a$.

Assume $c \equiv 0 \pmod a$. Let $u \in \mathbb{N}^k$ be the 0-cycle of (a, b, c) that starts with n_0. If $n_0 = 0$, than the statement follows trivially because $b \cdot 0 + c \equiv 0 \pmod a$ and the cycle ends. Assume now that $n_0 \neq 0$. Because u is a 0-cycle, there exists an index m such that $u_m = 0$. If $m \neq k - 1$, then $u_{m+1} = 0$. However, this means that the cycle can't be a cycle as $u_{m+j} = 0$ for any $j \geqslant 0$. Hence $m = k - 1$. But then again, $n_0 = (bu_m + c) \pmod a = 0$ which is something we dismissed. □

The next lemma is the first lemma that contains an actual interesting result, a first hint to the nice patterns found in the problem.

Lemma 3. *Let $u \in \mathbb{N}^{k_1}$ and $v \in \mathbb{N}^{k_2}$ be two 0-cycles of (a, b, c). Then $k_1 = k_2$.*

Proof. To prove this, we consider the 0-cycle $w \in \mathbb{N}^{k_3}$ of (a, b, c) starting with 0. We prove that there exists an m_1 such that $u_0 = w_{m_1}$. If $u_0 = 0$ this is trivially true. Say $u_0 \neq 0$. We know that there exists an index $l > 0$ such that $u_l = 0$. We now know that $w_0 = u_l$ and because of this by applying the generalized Collatz function $(k_1 - l)$ times, $w_{k_1 - l} = u_{k_1} = u_0$. Completely analogous, we can prove that there exists an index m_2 such that $v_0 = w_{m_2}$. Now define $x = (w_0, w_1, w_2, ..., w_{k_3 - 1}, w_0, w_1, w_2, ..., w_{k_3 - 1})$. Because of the remark at the definition of a cycle, we know that $w_0, w_1, w_2, ..., w_{k_3 - 1}$ are all different. Thus if there were two indices $i < j$ such that $x_i = x_j$ then $j - i = k_3$. Because of lemma 1, $u_0 = 0$ implies $k_1 = k_3$. If $u_0 = w_{m_1} = x_{m_1} = x_j$ for an index j then, because of our previous remark, $j - m_1 = k_3$. Again by applying lemma 1 and starting at index m_1 for x, we can infer that $k_3 = k_1$. Completely analogous we can prove the same for v. □

The following formula is never going to be used in this paper, but because it is slightly easier than the next one and the proofs are quite similar, I mention them both.

Formula 1. *Let u be a non-0-cycle of (a, b, c, n_0) of length k and let $b \neq 1$. Then,*

$$u_0(1 - b^k) \equiv c\frac{1 - b^k}{1 - b} \pmod a$$

Proof. We know that:

$$\begin{aligned}
&b \cdot u_0 + c \equiv u_1 \\
&b \cdot u_1 + c \equiv u_2 \\
&b \cdot u_2 + c \equiv u_3 \\
&... \\
&b \cdot u_{k-1} + c \equiv u_0
\end{aligned}$$

Recursively going backwards through these equations gives:

$$u_0 \equiv b^k \cdot u_0 + b^{k-1} \cdot c + b^{k-2} \cdot c + ... + b \cdot c + c$$

Giving us the required formula after rewriting it a bit.

$$\begin{aligned}
u_0 - b^k \cdot u_0 &\equiv c(1 + b + b^2 + ... + b^{k-1}) \\
u_0(1 - b^k) &\equiv c\frac{1 - b^k}{1 - b}
\end{aligned}$$

□

An important formula that is going to be used in different proofs, concerns the formula for 0-cycles. For conciseness, the formula is mentioned in a format that is not direclty applicable for $b = 1$, however, by using limits it is perfectly admissable for $b = 1$.

Formula 2. *Let u be a 0-cycle of (a, b, c, n_0) of length k. Let s be the index of the occurring 0 in the cycle. Then,*

$$u_0 \equiv c\frac{1 - b^{k-s}}{1 - b} \pmod{a}$$

Proof. Once again we know that

$$\begin{aligned}
&b \cdot u_0 + c \equiv u_1 \\
&b \cdot u_1 + c \equiv u_2 \\
&b \cdot u_2 + c \equiv u_3 \\
&... \\
&b \cdot u_{s-1} + c \equiv u_s \equiv 0 \\
&b \cdot u_s + c \equiv u_{s+1} \equiv c \\
&b \cdot u_{s+1} + c \equiv u_{s+2} \equiv bc + c \\
&... \\
&b \cdot u_{k-1} + c \equiv u_0
\end{aligned}$$

Let $g = k - s$. By going recursively backwards through these equations up until u_s, we get:

$$u_0 \equiv b^{g-1} \cdot (b \cdot u_s + c) + b^{g-2} \cdot c + ... + b \cdot c + c$$

Giving us the required formula after rewriting it a bit.

$$\begin{aligned}
u_0 &\equiv c(1 + b + b^2 + ... + b^{g-1}) \\
u_0 &\equiv c\frac{1 - b^g}{1 - b}
\end{aligned}$$

□

Before continuing, we are in need of a more general lemma that doesn't directly have anything to do with 0-cycles.

Lemma 4. *Let $d, e \in \mathbb{Z}_0$ and $\gcd(d, e) = 1$. Then for all $k \in \{0, 1, ..., d-1\}$ there exist a number $n \in \{0, 1, ..., d-1\}$ such that $e \cdot n \equiv k \pmod{d}$.*

Proof. We prove that there can be no two natural numbers n_1 and n_2 smaller than d such that $e \cdot n_1 \equiv e \cdot n_2 \pmod{d}$. The lemma is then a result of the pigeon hole principle. Assume $e \cdot n_1 \equiv e \cdot n_2 \pmod{d}$, then $d \mid e(n_1 - n_2)$. This is impossible because $\gcd(d, e) = 1$ and $|n_1 - n_2| < d$ and $n_1 - n_2 \neq 0$. □

We only need one last lemma before we can proceed with some more theorems for the solution of our problem.

Lemma 5. *If there is no non-0-cycle of (a, b, c) and $c \not\equiv 0 \pmod{a}$, then the greatest common divisor of a and $b - 1$ doesn't equal 1.*

Proof. Assume $\gcd(a, b-1) = 1$. We prove that there is a natural number n such that $n \equiv bn + c \pmod{a}$. Because $c \not\equiv 0 \pmod{a}$ and because there exists no non-0-cycle, this results in a contradiction.

Because of lemma 4, we know there exists a number n such that $n(1 - b) \equiv c \pmod{a}$. Thus $n \equiv bn + c \pmod{a}$. □

Finally, we're prepared enough to prove the next theorem concerning the solution for our problem if a is prime.

Theorem 2. *Let a be a prime number and $c \not\equiv 0 \pmod{a}$. Then there is no non-0-cycle if and only if $b \equiv 1 \pmod{a}$.*

Proof. Assume there is no non-0-cycle. We use lemma 5. The greatest common divisor of a and $b - 1$ cannot be 1. Because a is prime, it follows immediately that $b - 1 \equiv 0 \pmod{a}$.

Assume $b \equiv 1 \pmod{a}$ and assume that there is a non-0-cycle $u \in \mathbb{N}^k$. We know that $u_s \equiv u_0 + sc \pmod{a}$. Thus $u_0 \equiv u_0 + kc \pmod{a}$. Hence $kc \equiv 0 \pmod{a}$. We know that $0 < k < a$. The facts that a is prime and $c \not\equiv 0 \pmod{a}$ imply $\gcd(a, c) = 1$. But then it is never possible that $kc \equiv 0 \pmod{a}$. □

As an example, let's check the statement for $a = 5$, $b = 2$ and $c = 1$. The cycles here are $(0, 1, 3, 2)$, (4). As expected, there is a non-0-cycle. Now let's set $b = 6$. There is only one cycle here, namely $(0, 1, 2, 3, 4)$. As expected, there are no non-0-cycles.

3.3 Powers of primes

We can immediately proceed with powers of primes. The first theorem is for all prime powers for primes bigger than 2, the second one is for the special case of 2.

Theorem 3. *Let a be a prime number bigger than 2, $c \not\equiv 0 \pmod{a}$ and $t \in \mathbb{N} \setminus \{0, 1\}$. There exists no non-0-cycle of (a^t, b, c) if and only if $b \equiv 1 \pmod{a}$.*

Proof. Assume there is no non-0-cycle of (a^t, b, c). Then we know there is also no non-0-cycle of (a, b, c). Suppose that such a cycle did exist, call it u. We know that u_k cannot be 0 modulo a and thus it can also not be 0 modulo a^t. Hence a repeating cycle starting at u_0 can never hit 0 and must consequently contain a non-0-cycle. The statement now follows because of theorem 2.

Assume now that $b \equiv 1 \pmod{a}$. Say $b = a \cdot s + 1$. We calculate the length of a 0-cycle of (a^t, b, c) called $u \in \mathbb{N}^k$ with $u_0 = 0$. We use formula 2:

$$c \cdot \frac{1 - (as + 1)^k}{1 - (as + 1)} \equiv 0 \pmod{a^t}$$

Using the Binomium of Newton:

$$c \cdot \frac{1 - \sum_{n=0}^{k} \binom{k}{n} (as)^n}{-as} \equiv 0 \pmod{a^t}$$

Let $m \in \mathbb{Z}$ and rewrite:

$$c \cdot \sum_{n=0}^{k-1} \binom{k}{n+1} (as)^n = a^t \cdot m$$

Because the greatest common divisor of a and c is equal to 1, we know that c divides m. Then we divide the above equation by c:

$$\sum_{n=0}^{k-1} \binom{k}{n+1} (as)^n = a^t \cdot \frac{m}{c} \tag{3}$$

We can take a look at (3) modulo a:

$$\sum_{n=0}^{k-1} \binom{k}{n+1} (as)^n \equiv 0 \pmod{a}$$

We can remove the sum, because for $n > 0$, the term is a multiple of a:

$$0 \equiv k \pmod{a}$$

Thus k is a multiple of a, or $k = ak_1$.

We now proof that if $k = a^x k_x$ ($x \in \{1, ..., t-1\}$), that k is also divisible by a^{x+1}. If this is the case, we have proved that the 0-cycle starting at 0 contains all elements from 0 up to and including $a - 1$ and hence no non-0-cycle can exist.

We take a look at (3) modulo a^{x+1}.

$$\sum_{n=0}^{a^x \cdot k_x - 1} \binom{a^x \cdot k_x}{n+1} (a \cdot s)^n \equiv 0 \pmod{a^{x+1}}$$

Because $a^x k_x$ is bigger than $x + 1$ ($a > 2$), we can once again remove the sum:

$$a^x k_x \equiv 0 \pmod{a^{x+1}}$$

This ensures that $a \mid k_x$ and thus $a^{x+1} \mid k$. This proves our theorem. □

Theorem 4. *Let $a = 2$, $c \not\equiv 0 \pmod 2$ and $t \in \mathbb{N} \setminus \{0, 1\}$. There exists no non-0-cycle of (a^t, b, c) if and only if $b \equiv 1 \pmod 4$.*

Proof. First of all we note that there exists no non-0-cycle of $(4, b, c)$ with $c \not\equiv 0 \pmod 2$ if and only if $b \equiv 1 \pmod 4$. This can be proven by going over all cases.

Now assume there doesn't exist a non-0-cycle of $(2^t, b, c)$. Then we know there also doesn't exist a non-0-cycle of $(4, b, c)$. Suppose that such a cycle did exist, call it u. We know that u_k cannot be 0 modulo a and thus it can also not be 0 modulo 2^t. Hence a repeating cycle starting at u_0 with the triplet (a^t, b, c) can never hit 0 and so must contain a non-0-cycle. The statement now follows from the paragraph above.

The proof in the opposite way is entirely analogous to the proof of theorem 3. The only difference is that you need to say that $b = 4s + 1$ instead of $as + 1$. □

Another example is at its place here. Let's take a look at $a = 9$, $b = 4$ and $c = 2$. There is one cycle here, namely $(0, 2, 1, 6, 7, 3, 5, 4)$. As expexted, no non-0-cycle. If $b = 2$, then there is a non-0-cycle, namely $(1, 4)$.

3.4 General case

At last, we can get ready to solve the general case and see the most beautiful patterns in the problem. Before continuing, we first need to introduce the concept of repeating cycles.

Definition 5. *A repeating cycle of* (a, b, c, n_0) *is defined as the sequence* u *with* $u_0 = n_0$ *and* $u_k = f^k_{a,b,c}(n_0) \pmod a$ *for* $k > 0$.

Definition 6. *A repeating 0-cycle of* (a, b, c) *is a repeating cycle* u *of* (a, b, c, n_0) *for a* $n_0 \in \{0, 1, ..., a-1\}$ *such that there is an* $m > 0$ *with* $u_m = 0$.

Definition 7. *A repeating non-0-cycle of* (a, b, c) *is a cycle* u *of* (a, b, c, n_0) *for a* $n_0 \in \{0, 1, ..., a-1\}$ *such that there is no* $m > 0$ *with* $u_m = 0$.

You can see that these concepts are not really new as every repeating 0-cycle contains a 0-cycle and every repeating non-0-cycle contains a non-0-cycle. The repeating cycles make the prove of the last theorem a bit easier. However before continuing to the general case, we first need two more lemma's.

Lemma 6. *If* $c \neq 0 \pmod a$*, then there can only exist a 0-cycle of* (a, b, c) *if* $\gcd(a, bc)$ *is equal to* $\gcd(a, c)$.

Proof. If $b = 1$, the theorem is trivial. Assume $\gcd(a, bc) \neq \gcd(a, c)$ (implying $\gcd(a, bc) > \gcd(a, c)$) and assume a 0-cycle u of length k exists. Let v be the 0-cycle starting with 0 (also of length k because of lemma 3) . According to lemma 2, there must be at least one number $n \in \{1, ..., a-1\}$ such that there is an index i with $u_i = n$. We can assume $i = 0$ by moving the entire cycle i indices. Using theorem 2 we know that (omitting $\pmod a$ for brevity):

$$n \equiv c\frac{1 - b^g}{1 - b} \tag{4}$$

$$0 \equiv c\frac{1 - b^k}{1 - b} \tag{5}$$

Note that $g < k$. Taking the difference between the first and the second equation:

$$n \equiv c\frac{1 - b^g - 1 + b^k}{1 - b}$$

or:

$$n \equiv cb^g\frac{b^{k-g} - 1}{1 - b}$$

Because $g > 0$, this means that $\gcd(a, bc) \mid n$ and thus there exists a natural number l such that $n = l \cdot \gcd(a, bc)$. Using this result in (4), we get for a natural number x:

$$l \cdot \gcd(a, bc) + a \cdot x = c\frac{1 - b^g}{1 - b}$$

$\gcd(a, bc)$ divides the left-hand side. However, it doesn't divide the right hand side as $\frac{1-b^g}{1-b} \equiv 1 \pmod b$ and because $\gcd(a, bc) \nmid c$ because of our assumption that $\gcd(a, bc) > \gcd(a, c)$. This results in a contradiction.

□

Because of its simplicity, the lemma provides a first quick check for the existence of non-0-cycles. However, it is also a lemma that is heavily used in upcoming proofs in order to get to a general solution. The last lemma we prove, concerns the length of 0-cycles.

Lemma 7. *Let* $c \not\equiv 0 \pmod a$*. If there exists no non-0-cycle of* (a, b, c)*, then there exists a 0-cycle of* (a, b, c) $u \in \mathbb{N}^k$ *where* $k = \frac{a}{\gcd(a,bc)}$.

Proof. That u exists, is easy. Just consider the cycle starting at 0 (because there are no non-0-cycles, this must be a cycle). Note we showed in the proof of lemma 6 that any number n of the 0-cycle is divisible by $\gcd(a, bc)$. Say there exists natural numbers smaller than a, divisible by $\gcd(a, bc)$, but no element of u. We prove that for at least one of those numbers n_1, the following statement is true: $bn_1 + c \equiv 0 \pmod{a}$.

We first of all prove that if n is divisible by $\gcd(a, bc)$, then $bn + c$ is also divisible by $\gcd(a, bc)$:

$$bn + c = bl_1 \gcd(a, bc) + c = bl_1 \gcd(a, c) + c = l_2 \gcd(a, c) = l_2 \gcd(a, bc)$$

Note that we made use of lemma 6. Assume that there exists no number n_1 as mentioned above. Because of the above this means that there exists a non-0-cycle (consisting of at least some of the numbers divisible by $\gcd(a, bc)$). This is a contradiction. Thus n_1 exists. We know that there also exists an n_2, an element of u, for which $bn_2 + c \equiv 0 \pmod{a}$. So $b(n_1 - n_2) = 0 \pmod{a}$. Because both n_1 and n_2 are multiples of $\gcd(a, bc)$ and because both are smaller than a, there exists a natural number $m < \frac{a}{\gcd(a,bc)}$ that is bigger than 0 such that $b \cdot m \cdot \gcd(a, bc) = 0 \pmod{a}$. This however is impossible, because $m \cdot \gcd(a, bc) < a$ and b has no common divisors with a that are not already contained in $\gcd(a, bc)$. This is a contradiction.

We can conclude that a number $n < a$ is an element of u if and only if it is a multiple of $\gcd(a, bc)$. Because of this, u has exactly $\frac{a}{\gcd(a,bc)}$ elements. □

And here it is, the final proof.

Theorem 5. *Let a be a number with at least 2 different prime divisors and let $c \not\equiv 0 \pmod{a}$. Let e and f be two natural numbers such that $a = ef$ and $\gcd(e, f) = 1$. Then there is no non-0-cycle of (a, b, c) if and only if there is no non-0-cycle of (e, b, c) and if there is no non-0-cycle of (f, b, c).*

Proof. First of all, we know that:

$$n \equiv 0 \pmod{a} \Leftrightarrow n \equiv 0 \pmod{e} \wedge n \equiv 0 \pmod{f} \tag{6}$$

Let u be a repetitive cycle of (a, b, c). Let v be a repetitive cycle of (e, b, c) with $u_0 \pmod{e} = v_0$ and let w be a repetitive cycle of (f, b, c) with $u_0 \pmod{f} = w_0$. We may note that $u_k \equiv v_k \pmod{e}$ and $u_k \equiv w_k \pmod{f}$. This can easily be shown using induction.

We now prove that u is a repetitive non-0-cycle if v is a repetitive non-0-cycle or if w is a repetitive non-0-cycle. This proves the theorem from left to right (via contraposition). Suppose v is a repetitive non-0-cycle. Then there exists no number k such that $v_k = 0$. Because $u_k \equiv v_k \pmod{e}$, there exists no number k such that $u_k \equiv 0 \pmod{a}$. Thus u is a repetitive non-0-cycle. The proof is analogous if w is a repetitive non-0-cycle.

We now prove that if v and w are repetitive 0-cycles, u is also a repetitive 0-cycle. Note that this proves the theorem from right to left. Indeed, u is a random repetitive cycle and we can always construct two repetitive cycles v and w as stated. Because v and w cannot be repetitive non-0-cycles, they must be repetitive 0-cycles. This means that u must be a repetitive 0-cycle and so can't a repetitive non-0-cycle.

Making use of lemma 7, we can see that for a given $k, n \in \mathbb{N}$, $v_n = v_k$ if and only if there exists an $m_1 \in \mathbb{N}$ such that $k - n = m_1 \cdot \frac{e}{\gcd(e,bc)}$ and that $w_n = w_k$ if and only if there exists an $m_2 \in \mathbb{N}$ such that $k - n = m_2 \cdot \frac{f}{\gcd(f,bc)}$. Let i_e be the smallest index such that $v_{i_e} = 0$ and define i_f analogously for w. Hence we know:

$$v_k = 0 \Leftrightarrow k = i_e + m_1 \cdot \frac{e}{\gcd(e, bc)} \tag{7}$$

$$w_k = 0 \Leftrightarrow k = i_f + m_2 \cdot \frac{f}{\gcd(f, bc)} \tag{8}$$

We prove there exists a number k such that v_k and w_k are both 0. If this is the case, u_k is also 0 because of (6).

If i_e and i_f are equal, the existence of such k is trivial. We now suppose $i_e > i_f$. The proof is completely analogous for $i_f > i_e$. Using (7), we can say that $v_k = w_k = 0$ if:

$$i_e + m_1 \cdot \frac{e}{\gcd(e, bc)} = i_f + m_2 \cdot \frac{f}{\gcd(f, bc)}$$

Or:

$$i_e - i_f = -m_1 \cdot \frac{e}{\gcd(e, bc)} + m_2 \cdot \frac{f}{\gcd(f, bc)} \tag{9}$$

We now prove there exists a solution for the equation above. Because $\gcd(e, f) = 1$ and because $\frac{e}{\gcd(e,bc)}$ divides e and $\frac{f}{\gcd(f,bc)}$ divides f, we know that:

$$\gcd(\frac{e}{\gcd(e, bc)}, \frac{f}{\gcd(f, bc)}) = 1$$

Applying Bachet-Bézout:

$$\exists g_1, g_2 \in \mathbb{Z} : g_1 \cdot \frac{e}{\gcd(e, bc)} + g_2 \cdot \frac{f}{\gcd(f, bc)} = 1$$

The equation above also applies for the following values:

$$g_1 - h \cdot \frac{f}{\gcd(f, bc)}$$
$$g_2 + h \cdot \frac{e}{\gcd(e, bc)}$$

for an $h \in \mathbb{N}$. We make h big enough such that $g_1 - h \cdot \frac{f}{\gcd(f,bc)} < 0$ and $g_2 + h \cdot \frac{e}{\gcd(e,bc)} > 0$. Using $g_1 - h \cdot \frac{f}{\gcd(f,bc)}$ as $-\frac{m_1}{(i_e - i_f)}$ and $g_2 + h \cdot \frac{e}{\gcd(e,bc)(i_e - i_f)}$ as $\frac{m_2}{(i_e - i_f)}$, we can see that:

$$-\frac{m_1}{(i_e - i_f)} \cdot \frac{e}{\gcd(e, bc)} + \frac{m_2}{(i_e - i_f)} \cdot \frac{f}{\gcd(f, bc)} = 1$$

and thus that the m_1 and m_2 chosen are a solution for (9).

□

We may note a peculiarity about the theorem. It is independent of your choice of e and f. The only requirement is that they are relatively prime.

However, the theorem also has it's downsides. It requires us to factor a given number, a non-trivial task that reduces the effectiveness of the theorems. Fortunately the factorization only needs to be done once per value of a, ensuring that you can check multiple values of b and c without much more computations, something a brute-force approach is not able to do. It would have been easier if the final theorem would say something along the line of lemma 6. Such a reformulation has not been found and is left as future research.

4 Example

Before going to an example, let's make an overview of the steps to take if you want to solve the question for given values of a, b and c:

1. If $c \equiv 0 \pmod{a}$, use theorem 1.
2. If a is prime, use theorem 2.
3. If a is a power of a prime bigger than 2, use theorem 3. You need to use lemma 6 to exclude $c \equiv 0 \pmod{p}$.
4. If a is a power of 2, use theorem 4. You need to use lemma 6 to exclude $c \equiv 0 \pmod{2}$.

5. If none of the above apply, factor a in two relatively prime numbers e and f, restart this schedule from step 1 for both e and f and combine the results according to theorem 5.

Let's apply the schedule, but not for particular values of b and c, but just for a particular value of a and taking a look at all values of b and c smaller than a. Let $a = 12$.

If $c = 0$, we use theorem 1 to find that only $b = 0$ and $b = 6$ result in triplets that don't have any non-0-cycles.

If $c \neq 0$, we split 12 in 3 and 4.

For 3, we find that the following combinations of b and c (only mentioning them modulo 3) are allowed:
$b = 0, c = 0$ (theorem 1)
$b = 1, c = 1$ (theorem 2)
$b = 1, c = 2$ (theorem 2)

For 4, we find the following combinations:
$b = 0, c = 0$ (theorem 1)
$b = 2, c = 0$ (theorem 1)
$b = 1, c = 1$ (theorem 4)
$b = 1, c = 3$ (theorem 4)

Combining the result using theorem 5, we get:
$b = 1, c = 1$
$b = 1, c = 5$
$b = 1, c = 7$
$b = 1, c = 11$
$b = 4, c = 4$
$b = 4, c = 8$
$b = 9, c = 3$
$b = 9, c = 9$
$b = 10, c = 4$
$b = 10, c = 8$

5 Conclusion

Starting out with a possible generalization of the Collatz Conjecture, we studied and solved a problem that was called the "0-cycles-problem". The resulting theorems give an indication of nice structures hidden within the problem. Using these theorems, one can use some simple steps to compute whether or not given triplets (a, b, c) suffice the "0-cycles-problem" or not. However, because one of the steps requires us to factor a number, the resulting computational gain compared to a brute-force approach, is not miraculous. There could be reformulations of the given theorems to more computationally attractive theorems that might uncover even more of the underlying structure, but this is left as future research.

References

[1] Collatz Conjecture. (2019, November 13). In *Wikipedia*. Accessed at 8 september 2020 on `https://en.wikipedia.org/wiki/Collatz_conjecture`