Lynchburg Mathathon

Mining Bitcoin - Teacher's Guide

6 - 8th Grade

Discussion

1. What is the maximum value of x_3 that can be found?
2. What if the modulus were much larger than 101, say 10^{600}? Could you find all the solutions in your lifetime?
3. Is it possible to know what value of X_1 will result in an X_3 of 1 without trying every possibility? In other words, is there a method that would find bitcoins more frequently than just guessing at a starting number?
4. Notice that in one direction this problem is easy to solve, but in the other quite hard. Start with $x_1 = 1$ and you can find x_3 without a problem, but start with $x_3 = 1$ and find x_1, that's very different. Can you think of other problems that share this quality?

Below are some notes to help with the discussion section.

1. The solution can't be larger than the dividend minus one. To help think about this, encourage students to simplify the problem, what is the maximum solution to x mod 5? Again, the maximum solution is one less than the dividend of 5. This is why real hashing functions use a very large number for the modulus and it's also the source of the wraparound effect.
2. A typical computer can solve about 10 million (10^6) modulo computations per second. That means 10^7 computations would take 10 times as long or 10 seconds. So 10^{600} computations would only take 10^{594} seconds! Who can figure out how many years this is?
3. Probably not. The source of this difficulty in this particular example is the modulo operator and the fact that once a wraparound happens, information is lost. Even in this simple algorithm that uses small coefficients, there are many numbers that will give the same result when the modulus is applied. Sure you know that for the last iteration $\left(59 \times x_1\right)$ will need to be a multiple of 101 + 1, but which multiple? 102, 203, 304, etc? Imagine yourself finding a path out of the woods and for every iteration of this calculation, you come to an intersection that branches in 10 million different directions. Each of these paths could lead to where you are, but you have to guess which was the one you actually took on the way in, so you pick one, then come to another intersection of a similar size. After a few of these intersections, the odds of finding your way out aren't looking good.
4. It is much harder to solve a Sudoku puzzle than it is to check a solution for correctness.