Lynchburg Mathathon

VECTOR SPACE

Mining Bitcoin

6 - 8th Grade

If you want to mine bitcoin, all you have to do is provide a number that transforms into 1 when you insert your number into a specific equation. But before we can try, we need to understand the modulo operator.

The modulus is the remainder after the division of two numbers.

8 mod 5 = 3, because 8 divided by 5 is 1 with a remainder of 3
10 mod 5 = 0, because 10 divided by 5 is exactly 2 without a remainder
15 mod 7 = 1
17 mod 3 = ?

Now that we understand modulo, let's try to mine a bitcoin. Feel free to use a calculator (Online modulus calculator available here: https://www.calculators.org/math/modulo.php)

1. Choose a number from 1 to 100, $x_1 =$
2. Now solve for x_2, $x_2 = (59 \times x_1) mod\ 101$
   $x_2 =$
3. And x_3, $x_3 = (59 \times x_2) mod\ 101$
   $x_3 =$
4. Does your x_3 equal 1? If so, your teacher owes you a bitcoin! If not, pick a new value for x_1 and try again!

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?

Note that the actual method and equations used in mining bitcoin is quite a bit more complex than this exercise. We have greatly simplified the process in order to work with pencil and paper, while preserving similar principles to the process of bitcoin mining.