The 4321 5940 Problem Remastered

Evan Kim

January 2020, updated December 2021

0 Introduction

This problem was first introduced on January 29, 2020 in the APCSP classrooms of Tesla STEM High School. The problem asks how one might find an x such that

$$(4321 \cdot x) \,\%\, 5940 = 1.$$

Rather than using %, we introduce the notation $5 \equiv 2 \pmod 3$, which just means that the right and left sides of the triple equal signs are equivalent modulo the number in parentheses.

1 Solution 1

We would like to use the chinese remainder theorem (the name is irrelevant) in reverse, essentially decomposing the problem into smaller ones using the prime factorization of 5940. Specifically, we'll use $5940 = 540 \cdot 11$ and $4321 = 8 \cdot 540 + 1$.

We are given that $4321 \cdot x \equiv 1 \pmod{5940}$. We can write this out as $4321x = 5940k + 1$ where k is some integer. And if two numbers are equal, then if we take mod 540 on both sides[1], they must remain equal,

$$4321x \equiv 5940k + 1 \pmod{540}.$$

Since $4320 = 8 \cdot 540$, we may say $(8 \cdot 540 + 1)x = 8 \cdot 540 + x \equiv x \pmod{540}$. Similarly, $5940k + 1 \equiv 1 \pmod{540}$. Now we can say

$$x \equiv 5940k + 1 \equiv 1 \pmod{540}.$$

We do the same with 11. We know

$$4321x \equiv (392 \cdot 11 + 9)x \equiv 9x \pmod{11}.$$

We also know $5940k + 1 \equiv 1 \pmod{11}$, so $9x \equiv 1 \pmod{11}$. Now we know all numbers are equivalent to 0-10 modulo 11 (those are the only possible remainders!), and by inspection, we can see $x \equiv 5 \pmod{11}$ works, as $45 = 44 + 1$.

Thus, we just have to solve for an x such that

$$\begin{aligned} x &\equiv 5 \pmod{11}, \\ x &\equiv 1 \pmod{540}. \end{aligned}$$

[1] those familiar with number theory may gloss over the next few lines without loss of continuity.

From here, we can brute force it by caseworking with the second equation. We test $x = 1$, that fails, $x = 541$, that fails, $x = 1081$, that fails, $x = 1621$, that fails, and finally $x = 2161 = 106 \cdot 11 + 5$, so that works.

And now we must preserve both the modulo of this mod 11 and mod 540. So the differences to the next solution must be both multiples of 11 and 540, or in other words, multiples of the least common multiple of both, which is 5940, and thus all x of the form $x \equiv 2161 \pmod{5940}$ or $x = 2161 + 5940n$ where n is an integer, work. ■

2 Solution 2

We are guaranteed to find a solution from Bezout's lemma, which tells us that for integers a, b with $\gcd(a, b) = 1$, we can find x and y such that

$$ax + by = 1.$$

Since $\gcd(4321, 5940) = 1$ (this can be checked easily), we know there exist x, y such that

$$4321x + 5940y = 1 \iff 4321x = 1 + (-y) \cdot 5940 \iff 4321x \equiv 1 \pmod{5940}.$$

So we just need to find the right x and y.

To find the right x and y we exploit the Euclidean Algorithm. The idea with the euclidean algorithm is that

$$\gcd(a, b) = \gcd(a - b, b)$$

because if some integer d divides a and b, then it must also divide $a - b$[2]. So we can continue to reduce the gcd problem to smaller and smaller numbers. If we apply the euclidean algorithm for finding the gcd of 4321 and 5940, we get the following (the currrent terms that we're finding the gcd for are bolded):

$$\begin{aligned}
\mathbf{5940} - \mathbf{4321} &= 1619, \quad (5940, 4321)\\
\mathbf{4321} - 2 \cdot \mathbf{1619} &= 1083, \quad (4321, 1619)\\
\mathbf{1619} - \mathbf{1083} &= 536, \quad (1619, 1083)\\
\mathbf{1083} - 2 \cdot \mathbf{536} &= 11, \quad (1083, 536)\\
\mathbf{536} - 48 \cdot \mathbf{11} &= 8, \quad (536, 11)\\
\mathbf{11} - \mathbf{8} &= 3, \quad (11, 8)\\
\mathbf{8} - 2 \cdot \mathbf{3} &= 2, \quad (8, 3)\\
\mathbf{3} - \mathbf{2} &= 1. \quad (3, 2)
\end{aligned}$$

This tells us that $\gcd(4321, 5940) = 1$. There is something more however. That last term right there looks quite similar to the $ax + by = 1$ equation from earlier! This is precisely what we'll be exploiting. Starting with the last equation, we substitute in the previous equation for the boxed term

$$\mathbf{3} - \boxed{\mathbf{2}} = 1.$$

So we put in $\boxed{\mathbf{2}} = \mathbf{8} - 2 \cdot \mathbf{3}$. So

$$\mathbf{3} - (\mathbf{8} - 2 \cdot \mathbf{3}) = 1$$
$$(-1) \cdot \mathbf{8} + 3 \cdot \mathbf{3} = 1.$$

[2] And also $a - nb$ for any integer n, which is why we subtract of multiples in the following section.

You might already be able to see the idea here. First we started with an equation that combined 3 and 2 to get 1, but with the substitution, it has now moved up to the second row, combining 8 and 3 to get 1. So we can continue this process all the way until we get to the top pair! Here's the full process:

$$\begin{aligned}
(-1)\cdot\mathbf{8}+3\cdot(\mathbf{11}-\mathbf{8}) &= 3\cdot\mathbf{11}-4\cdot\mathbf{8}=1,\\
3\cdot\mathbf{11}-4\cdot(\mathbf{536}-48\cdot\mathbf{11}) &= (-4)\cdot\mathbf{536}+195\cdot\mathbf{11}=1,\\
(-4)\cdot\mathbf{536}+195\cdot(\mathbf{1083}-2\cdot\mathbf{536}) &= 195\cdot\mathbf{1083}-394\cdot\mathbf{536}=1,\\
195\cdot\mathbf{1083}-394\cdot(\mathbf{1619}-\mathbf{1083}) &= (-394)\cdot\mathbf{1619}+589\cdot\mathbf{1083}=1,\\
(-394)\cdot\mathbf{1619}+589\cdot(\mathbf{4321}-2\cdot\mathbf{1619}) &= 589\cdot\mathbf{4321}+(-1572)\cdot\mathbf{1619}=1,\\
589\cdot\mathbf{4321}+(-1572)\cdot(\mathbf{5940}-\mathbf{4321}) &= (-1572)\cdot\mathbf{5940}+2161\cdot\mathbf{4321}=1.
\end{aligned}$$

That last one rearranges to $4321\cdot 2161 = 1+1572\cdot 5940$, which is exactly the same result as before! ■

> **Remark:** You may have noticed that this second solution requires quite a bit of number bashing. It is however, much more straightforward and algorithmic. While this might be more boring for humans, this is great for this recent invention called a computer! In fact, this is precisely what computers use in the rsa algorithm to compute the private key! For more details, see appendix A.

A RSA

To be updated...