Boise Math Teachers' Circle: Division with Remainders

Zach Teitler

BOISE STATE UNIVERSITY

March 3, 2018

Zoe's three children love cookies, but they have to have the same number of cookies, or else there'll be trouble! Unfortunately there were two cookies left over.

Thinking quickly, Zoe said she wanted some cookies too. Then Zoe and her three kids were able to divide up the cookies so everyone got the same number. Trouble avoided!

Zoe's three children love cookies, but they have to have the same number of cookies, or else there'll be trouble! Unfortunately there were two cookies left over.

Thinking quickly, Zoe said she wanted some cookies too. Then Zoe and her three kids were able to divide up the cookies so everyone got the same number. Trouble avoided!

1. Let's write x for the number of cookies.

Zoe's three children love cookies, but they have to have the same number of cookies, or else there'll be trouble! Unfortunately there were two cookies left over.

Thinking quickly, Zoe said she wanted some cookies too. Then Zoe and her three kids were able to divide up the cookies so everyone got the same number. Trouble avoided!

1. Let's write x for the number of cookies.
2. Can you figure out what x was?

Zoe's three children love cookies, but they have to have the same number of cookies, or else there'll be trouble! Unfortunately there were two cookies left over.

Thinking quickly, Zoe said she wanted some cookies too. Then Zoe and her three kids were able to divide up the cookies so everyone got the same number. Trouble avoided!

1. Let's write x for the number of cookies.
2. Can you figure out what x was?
3. Were there other possible values of x?

A group of 11 wicked pirates tried to evenly divide a chest of gold coins, but there was 1 coin left over. The pirates mutinied, marooning their captain on a desert island with the one extra coin.

The remaining 10 pirates tried again to divide the coins, but this time there were 2 coins left over. So they marooned the first mate with 1 coin (to be fair!) and sailed off.

Once again the 9 pirates tried to divide the coins, but now there were 4 coins left over.

Clearly the treasure was cursed; they threw it overboard and renounced their pirating ways.

A group of 11 wicked pirates tried to evenly divide a chest of gold coins, but there was 1 coin left over. The pirates mutinied, marooning their captain on a desert island with the one extra coin.

The remaining 10 pirates tried again to divide the coins, but this time there were 2 coins left over. So they marooned the first mate with 1 coin (to be fair!) and sailed off.

Once again the 9 pirates tried to divide the coins, but now there were 4 coins left over.

Clearly the treasure was cursed; they threw it overboard and renounced their pirating ways.

1. How many coins did those silly pirates start with?

A group of 11 wicked pirates tried to evenly divide a chest of gold coins, but there was 1 coin left over. The pirates mutinied, marooning their captain on a desert island with the one extra coin.

The remaining 10 pirates tried again to divide the coins, but this time there were 2 coins left over. So they marooned the first mate with 1 coin (to be fair!) and sailed off.

Once again the 9 pirates tried to divide the coins, but now there were 4 coins left over.

Clearly the treasure was cursed; they threw it overboard and renounced their pirating ways.

1. How many coins did those silly pirates start with?
2. Were there other possible numbers of coins?

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.
- When three kids have two cookies left over, it means $x = 3a + 2$ for some integer a.

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.
- When three kids have two cookies left over, it means $x = 3a + 2$ for some integer a.
- When the four of them can split the cookies evenly, it means $x = 4b$ for some integer b.

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.
- When three kids have two cookies left over, it means $x = 3a + 2$ for some integer a.
- When the four of them can split the cookies evenly, it means $x = 4b$ for some integer b.
- So $3a + 2 = 4b$, or, $4b - 3a = 2$.

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.
- When three kids have two cookies left over, it means $x = 3a + 2$ for some integer a.
- When the four of them can split the cookies evenly, it means $x = 4b$ for some integer b.
- So $3a + 2 = 4b$, or, $4b - 3a = 2$.
- Clever idea: Let's try to solve $4b_1 - 3a_1 = 1$, then multiply everything by 2 to find a and b.

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.
- When three kids have two cookies left over, it means $x = 3a + 2$ for some integer a.
- When the four of them can split the cookies evenly, it means $x = 4b$ for some integer b.
- So $3a + 2 = 4b$, or, $4b - 3a = 2$.
- Clever idea: Let's try to solve $4b_1 - 3a_1 = 1$, then multiply everything by 2 to find a and b.
- For example, $a_1 = 1$, $b_1 = 1$ works. Then $a = 2$, $b = 2$.

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.
- When three kids have two cookies left over, it means $x = 3a + 2$ for some integer a.
- When the four of them can split the cookies evenly, it means $x = 4b$ for some integer b.
- So $3a + 2 = 4b$, or, $4b - 3a = 2$.
- Clever idea: Let's try to solve $4b_1 - 3a_1 = 1$, then multiply everything by 2 to find a and b.
- For example, $a_1 = 1$, $b_1 = 1$ works. Then $a = 2$, $b = 2$.
- So $x = 3a + 2 = 8$ (or, $x = 4b = 8$).

The pirate problem will be easier to solve if we can find a systematic approach. Let's go back to the cookies.

- Say Zoe and her kids had x cookies.
- When three kids have two cookies left over, it means $x = 3a + 2$ for some integer a.
- When the four of them can split the cookies evenly, it means $x = 4b$ for some integer b.
- So $3a + 2 = 4b$, or, $4b - 3a = 2$.
- Clever idea: Let's try to solve $4b_1 - 3a_1 = 1$, then multiply everything by 2 to find a and b.
- For example, $a_1 = 1$, $b_1 = 1$ works. Then $a = 2$, $b = 2$.
- So $x = 3a + 2 = 8$ (or, $x = 4b = 8$).
- Were there other possible numbers for x?

Let's try the pirate problem. Say x is the number of coins.

- When 11 pirates have 1 coin left over, that means $x = 11a + 1$ for some integer a.

Let's try the pirate problem. Say x is the number of coins.

- When 11 pirates have 1 coin left over, that means $x = 11a + 1$ for some integer a.
- When 10 pirates have 2 coins left over, after leaving 1 coin with the captain, that means $x - 1 = 10b + 2$ for some integer b.

Let's try the pirate problem. Say x is the number of coins.

- When 11 pirates have 1 coin left over, that means $x = 11a + 1$ for some integer a.
- When 10 pirates have 2 coins left over, after leaving 1 coin with the captain, that means $x - 1 = 10b + 2$ for some integer b.
- Finally $x - 2 = 9c + 4$ for some integer c.

Let's try the pirate problem. Say x is the number of coins.

- When 11 pirates have 1 coin left over, that means $x = 11a + 1$ for some integer a.
- When 10 pirates have 2 coins left over, after leaving 1 coin with the captain, that means $x - 1 = 10b + 2$ for some integer b.
- Finally $x - 2 = 9c + 4$ for some integer c.
- Start with $11a + 1 = 10b + 3$, or $11a - 10b = 2$. Then $a = b = 2$ works, so $x = 23$ is a solution for the first equation.

Let's try the pirate problem. Say x is the number of coins.

- When 11 pirates have 1 coin left over, that means $x = 11a + 1$ for some integer a.
- When 10 pirates have 2 coins left over, after leaving 1 coin with the captain, that means $x - 1 = 10b + 2$ for some integer b.
- Finally $x - 2 = 9c + 4$ for some integer c.
- Start with $11a + 1 = 10b + 3$, or $11a - 10b = 2$. Then $a = b = 2$ works, so $x = 23$ is a solution for the first equation.
- But $x = 23$ doesn't work for the third equation.

We can't avoid it. We have to know more solutions of the first two equations, to see which ones will work for the third equation.

We can't avoid it. We have to know more solutions of the first two equations, to see which ones will work for the third equation.

- What are all the solutions to $11a - 10b = 2$?

The solutions are $a = 2 + 10k$, $b = 2 + 11k$, for any integer k.

The solutions are $a = 2 + 10k$, $b = 2 + 11k$, for any integer k.

So $x = 11a + 1 = 23 + 110k$ (or, $x = 10b + 3 = 23 + 110k$).

Now we need to solve $23 + 110k = 9c + 6$, or $9c - 110k = 17$.

The solutions are $a = 2 + 10k$, $b = 2 + 11k$, for any integer k.

So $x = 11a + 1 = 23 + 110k$ (or, $x = 10b + 3 = 23 + 110k$).

Now we need to solve $23 + 110k = 9c + 6$, or $9c - 110k = 17$.

Can you guess the solution?

The solutions are $a = 2 + 10k$, $b = 2 + 11k$, for any integer k.

So $x = 11a + 1 = 23 + 110k$ (or, $x = 10b + 3 = 23 + 110k$).

Now we need to solve $23 + 110k = 9c + 6$, or $9c - 110k = 17$.

Can you guess the solution?

If not, try the **Extended Euclidean Algorithm**.

Secret Sharing

Cookies are kept in a highly secure and undisclosed location.

- Zoe's three children are the only ones with access.
- Access requires at least two children to cooperate, to prevent any rogue cookie snacking.
- However, in case of cookie emergency in which one child is cookie-incapacitated, the other two need to be able to enter the jar.
- Is there a way to "share" a secret so that any two of the three can figure it out, but one alone can't?

(The undisclosed location may or may not be a jar; this can be neither confirmed nor denied.)

Using remainders for secret sharing

- The code to enter the jar is a three-digit number, x.
- Alice knows that when x is divided by 37, the remainder is 18.
- Bob knows that when x is divided by 41, the remainder is 27.
- Charlotte knows that when x is divided by 35, the remainder is 34.

Would that work? What do you think?

Using remainders for secret sharing

- The code to enter the jar is a three-digit number, x.
- Alice knows that when x is divided by 37, the remainder is 18.
- Bob knows that when x is divided by 41, the remainder is 27.
- Charlotte knows that when x is divided by 35, the remainder is 34.

Would that work? What do you think?

Would any two of them be able to solve for x? Would they get the same value of x?

Chinese Remainder Theorem

Suppose m and n are relatively prime ($\gcd(m,n) = 1$) positive integers and a, b are any numbers, where $0 \leq a < m$ and $0 \leq b < n$. We consider the problem: Find an integer x such that when x is divided by m, the remainder is a, and when x is divided by n, the remainder is b.

1. There exists a solution x_1 to this problem.
2. The solution is not unique. If y is any solution to the problem, then so is $y + mn$, or for that matter $y + mnk$ for any integer k. In particular, $x_1 + mnk$ gives an infinite list of solutions.
3. Those are all the solutions: if y is any solution to the problem, then $y = x_1 + mnk$ for some k. In particular, there is one and only one solution between 0 and mn.
4. Also there exists a method to find the solutions.

The Chinese mathematician Sunzi refered to these ideas in the 3rd century AD, posing the puzzle:

"There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?"
(according to Wikipedia).

(Other sources online quote elaborate stories. In one version, a nobleman's horse steps on an old woman's basket at the market, and breaks all the eggs in the basket. He offers to pay for them, but the woman doesn't know how many eggs there were. She just knows that when she lined them up in three rows, there were two left over, etc.)

(With deep apologies to J.R.R. Tolkien.) The army of goblins moved into the valley, filling it with the clinking of armor, the glimmer of mail and steel, the rippling of banners. From the noise and smells, one wondered if every one of the fifty-thousand goblins in Middle Earth had gone to war!

That night the men and hobbits met and planned the next day's battle. One of the men stood up. "I slipped into their camp yesterday and observed them as they passed out their rations. They eat nothing but biscuits. The cook makes enough each day for each goblin to have twelve. He cooks them in batches of 100, but makes 4 extra in the last batch."

An elf rose after him, and in the smoky room he described his discovery. At the beginning of the week they give each goblin seven flasks, a flask of wine for each day of the week. These are brought over the mountains horseback from the wineries of Gogoroth, a gross at a time. There are always five extra flasks, which the lead goblin drinks that first night.

Slowly Gandalf stood. "We know the lead goblin and that he has divided the remainder of the army into thirteen equal regiments."

"So we know the number of goblins in the valley," said Elrond.

Everyone turned to stare at him.

How many goblins are there?[1]

[1] Taken from http://www.shsu.edu/kws006/Professional/Concepts_files/ChineseRemainderTheorem.pdf by Ken W. Smith, SHSU.

The pirates screamed and shouted as they dragged the large chest of gold aboard the ship. In minutes they had forced it open and gold coins poured onto the deck. The captain waved them back from the pile of gold and slowly began dividing the coins into equal piles, one for each of the 17 pirates. At the end of this division, there was one lone coin. One pirate reached for it and just as he got it into his fist, the ruffian next to him killed him with his dagger.

The captain sighed, dropped the extra coin in the dead man's pile and began to divide these coins among the remaining 16 crew members. Soon there were 16 equal piles of gold on the deck and 15 coins remaining. Who would not get a coin?

The pirates glanced at each other and suddenly one struck down his neighbor. Again they divided the coins; this time they had one too many; again, in the scramble for that coin, a man was killed.

Once more they divided coins (and the captain began to wonder how he would command an undermanned ship!)

Again, there was an extra coin; quickly the captain grabbed the coin and hurled it into the sea.

How many coins were in the chest?[2]

[2] Taken from http://www.shsu.edu/kws006/Professional/Concepts_files/ChineseRemainderTheorem.pdf by Ken W. Smith, SHSU.

Replacing one complicated calculation with multiple simpler remainders

If you have a complicated formula for N, you can try computing N's remainder for several small numbers, then reassemble N from the various remainders.

This can sometimes help because if all you care about is the remainder when you divide by 25 (say) then you can "cast out 25s."

Some examples:[3]

- What are the last two digits of 49^{19}?
- What is the remainder when $12^{34^{56^{78}}}$ is divided by 90?

[3] From Brilliant.org, `https://brilliant.org/wiki/chinese-remainder-theorem/?subtopic=modular-arithmetic&chapter=basic-applications`

One time the Chinese Remainder Theorem was used for math research was to compute the Kazhdan-Lusztig-Vogan polynomials for E_8:

https://www.aimath.org/E8/

This was in the news in 2007 as "An Answer the Size of Manhattan."

(The part where Chinese Remainder Theorem is mentioned is here: http://www.liegroups.org/kle8.html).

A few more questions taken from Brilliant.org.[4]

1. The comets 2P/Encke, 4P/Faye, and 8P/Tuttle have orbital periods of 3 years, 8 years, and 13 years, respectively. The last perihelions of each of these comets were in 2017, 2014, and 2008, respectively. What is the next year in which all three of these comets will achieve perihelion in the same year?
   For this problem, assume that time is measured in whole numbers of years and that each orbital period is constant.
2. Show that there exist 99 consecutive integers $a_1, a_2, \ldots, a_{99}$ such that each a_i is divisible by the cube of some integer greater than 1.
3. What are the last two non-zero digits in 2018! ?

[4] https://brilliant.org/wiki/chinese-remainder-theorem/?subtopic=modular-arithmetic&chapter=basic-applications