Mathematical Puzzles, Games and Other Diversions

Day 20

Derrick Chung

April 8, 2021

Still More Modular Arithmetic

JAC Student ID Trick

What makes this trick work is the fact that 7 does not have any non-trivial common factors with the numbers 1 through 6.

Let's start by labeling the cards:
Label the top card as 0, the next one as card 1, and so on with the bottom one being card 6.

- After one turn, card a ends up on top, which you turn face up.
- After one more turn, card $2a \pmod 7$ is on top and also turned face up.
- Once you've gone through the process six times, you've turned over cards $a, 2a, 3a, 4a, 5a, 6a \pmod 7$.

Conclusions

- Card 0 is never turned face up.
- Every other card has been turned over exactly once.

Still More Modular Arithmetic (cont.)

Definition

Two natural numbers are called **relatively prime** if they don't share any non-trivial common factors (i.e. factors other than 1).

Properties

- Suppose p is a prime number. Then a and p are relatively prime if and only if a is NOT divisible by p.
- If a and n are relatively prime, then neither number is divisible by the other.
  This is the same as saying $a \not\equiv 0 \pmod{n}$ and $n \not\equiv 0 \pmod{a}$.
- If a, b are both relatively prime to n, then their product ab is also relatively prime to n.
  That's because if ab shares a factor with n, then it must share a prime factor with n. And that prime factor has to already be either a factor of a or b.

Still More Modular Arithmetic (cont.)

Proof that Card 0 is never turned face up

$1, 2, 3, 4, 5, 6$ and a are relatively prime with 7, which means the same is true for any products of those numbers.

Thus $a, 2a, 3a, 4a, 5a, 6a \not\equiv 0 \pmod 7$.

And since those are the cards that are turned over, card 0 remains face down throughout the entire process.

Proof that every other card is turned over exactly once

If a card has been flipped more than once, that means two of the numbers in $a, 2a, 3a, 4a, 5a, 6a \pmod 7$ must be equal.
We'll show this is impossible using a proof this by contradiction.

Suppose that it is true that two of those numbers are the same.
$k_1 a \equiv k_2 a \pmod 7$, with $1 \leq k_1 < k_2 \leq 6$

Subtracting $k_1 a$ from both sides gives: $0 \equiv k_2 a - k_1 a \pmod 7$

Still More Modular Arithmetic (cont.)

Factoring the right side, we get: $0 \equiv (k_2 - k_1)a \pmod{7}$.

But both a and $(k_2 - k_1)$, which has to be between 1 and 5, are relatively prime to 7.
So their product can't be a multiple of 7. This is a contradiction.
Thus no card can be flipped more than once.
And since the list has 6 items and must be distinct, this means every card other than card 0 must be flipped over exactly once.

Notes

- The arguments hold generally so long as the numbers used to count are relatively prime to the total number of cards.
  11, 17 or 169 cards would work, technically speaking.
- With 8 cards, just restrict the choice to odd numbers.
  Similarly with 9 cards, just avoid multiples of 3.

Still More Modular Arithmetic (cont.)

The Spelling Trick

Given two packets of n cards in reverse order of each other, spelling exactly n cards, as in the trick's procedure, ALWAYS leave the two packets again in reverse order. This is easier to see if you think of the order as a cycle instead of a sequence.

If you play around further, you'll notice that if you start with two n-card packets in reverse order and spell $n-1$ cards, then the top cards will ALWAYS match.

Putting those two observations together, to make the trick work, you just need spell a word with $(n-1)$ or $-1 \pmod{n}$ letters.

The trick as described works because:

DERRICK spells with $7 \equiv -1 \pmod{4}$ letters
CHUNG with $5 \equiv -1 \pmod{3}$ letters, and
SPELL with $5 \equiv -1 \pmod{2}$ letters.

Still More Modular Arithmetic (cont.)

Notes

- You could also accomplish the trick by spelling the same word, ABRACADABRA, every time.
  That's because $11 \equiv -1 \pmod{n}$ when $n = 2, 3$ or 4.
- To make the trick work starting with 5 cards, we just need to find a word that has $5k - 1$ letters.
  For example, anything with $4, 9$ or even 13 letters would work.
- Even with 5 cards, theoretically, we could consistently spell the same word (okay, probably phrase).
  It would however have to be at least 59 letters long.