Maths for Computer Science
Training on divisibility

Denis TRYSTRAM
MoSIG1

november 2023

Divisibility

This exercise was a favorite question asked by the famous mathematician Paul Erdos to his new young students.
He often used it to test their ability in mathematics.

The problem is described as follows:
Let consider the $2n$ first integers.

Question

Take any $n + 1$ integers in this set and prove that there exists a pair (p, q) such that p divides q.

Hint

Write the $2n$ numbers by decomposing the sequence into multiples of powers of 2. When there are multiple ways, we take the one with the largest power of 2 in order to make the decomposition unique.

Hint

Write the $2n$ numbers by decomposing the sequence into multiples of powers of 2. When there are multiple ways, we take the one with the largest power of 2 in order to make the decomposition unique.

Example for $n = 7$:

- 1, 3, 5, 7, 9, 11, 13
- 2, 6, 10, 14
- 4, 12
- 8

Hint

Write the $2n$ numbers by decomposing the sequence into multiples of powers of 2. When there are multiple ways, we take the one with the largest power of 2 in order to make the decomposition unique.

Example for $n = 7$:

- 1, 3, 5, 7, 9, 11, 13
- 2, 6, 10, 14
- 4, 12
- 8

Thus, according to such a decomposition, all the integers of the sequence are written as: $2^k \times m$ where m is odd (and $k \geq 0$). Use the pigeon hole principle to exhibit p and q.

Card tricks

Playing cards with shuffles

Let consider m different cards.
We are interested here in studying the properties of shuffles by means of applying successively the same permutation of $\{1, 2, 3, \cdots, m-1, m\}$.

We focus on two particular popular permutations (called Monge's shuffle and *mélange Faro*)

Monge's shuffle

The rule of shuffling is described below.

- Card 1 is put apart
- Card 2 is placed above card 1 and card 3 is put below it
- Card 4 is placed on the top of all the others
- Card 5 at the bottom
- and so on alternatively until the initial heap becomes empty.

Analysis: Proving some properties

1. Show that for $m = 10$ the card in the fourth position remains fix. Is it still true for odd m?
2. Show that for any m the initial order always appears once again In particular, how many permutation steps are required for $m = 24$?
3. Generalize the previous results: for $m = 6k + 4$ prove that the card in position $2k + 2$ always remains unchanged.
4. For some values of m, show that there exist two cards that are always exchanged.
   Apply this to $m = 22$.

Mélange Faro

Assume m is even, consider for instance a classical deck of 52 cards.

- Split the deck of cards into two equal heaps of 26 cards.
- Put the first card of the second heap apart
- Put the first card of the other heap below it
- Put the second of the second heap below, and so on alternatively until both heaps get empty.

Analysis using the little Fermat theorem

Here, we are interested in the following question: **How many steps are required for obtaining the original order of cards?**

1. what is the position of the card initially in position a after n suffles?
2. As 53 is prime, apply the Fermat Theorem and determine how many steps are required to come back to the original position.
3. Is it possible to do better for some positions a?