Number theory

Notation 1 $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

$a \in \mathbb{Z} \iff a$ is an integer

Definition 2: We say that b divides a for $a, b \in \mathbb{Z}$ if there is an integer k such that $b \cdot k = a$

We write $b \mid a$

Examples:
- $3 \mid 12$ because $3 \cdot 4 = 12$
- $-5 \mid 20$ because $(-5) \cdot (-4) = 20$

Definition 3: $p \in \mathbb{Z}$ and $p \geq 2$ is called prime number if there is no $2 \leq x \leq p-1$ with $x \mid p$.

Example: prime numbers: 2, 3, 5, 7, 11, 13, 17, 19
- 20 is not a prime number because $4 \mid 20$

Lemma 4: If $p \mid xy$, then $p \mid x$ or $p \mid y$ (for $p, x, y \in \mathbb{Z}$, p prime)

Example: $8 \cdot 9 = 72$

We know $3 \mid 72$

$\Rightarrow 3 \mid 8$ or $3 \mid 9$

Definition 5 For $a, b, n \in \mathbb{Z}$ and $n \geq 1$ we say $a \equiv b \mod n$ if $n \mid a - b$.

Example
- $13 \equiv 3 \mod 5$
- $12 \equiv -2 \mod 7$

Lemma 6 If $a \equiv b \mod n$, then $b \equiv a \mod n$

Example

$25 \equiv -3 \mod 7$

$17 \equiv 10 \mod 7$

$42 \equiv 7 \mod 7$

$10 \equiv 17 \mod 7$

Lemma 8 For any $a \in \mathbb{Z}$, there is an unique $r \in \mathbb{Z}$ with $0 \leq r \leq n-1$ such that $a \equiv r \mod n$

Problem Show that $n^2 - 2$ is not divisible by 5 for all $n \in \mathbb{Z}$

There is $r \in \mathbb{Z}$ such that $n \equiv r \mod 5$ and $0 \leq r \leq 4$

We either have
- $n \equiv 0 \mod 5$: $n^2 - 2 \equiv 0^2 - 2 = -2 \equiv 3 \mod 5$ $\Rightarrow 5 \nmid n^2 - 2$
- $n \equiv 1 \mod 5$: $n^2 - 2 \equiv 1^2 - 2 = -1 \equiv 4 \mod 5$ $\Rightarrow 5 \nmid n^2 - 2$

- We want to find the remainder of 23 modulo 5
- $23 : 5 =$
- $23 = 4 \cdot 5 + 3$

Theorem 1 (Fermat's Little Theorem) If $a \in \mathbb{Z}$ and p is a prime number, then

$$a^p \equiv a \mod p$$

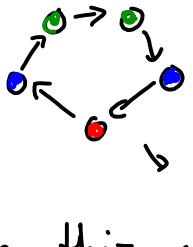
which means $p \mid a^p - a$

Proof: What does a^p mean?
- number of possibilities for choosing 1 of a items for p times

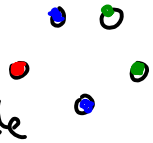
Example: $a = 2$, $p = 3$

$a^p - a$: number of possibilities for choosing 1 of a items for p times without repeating the same item all the time

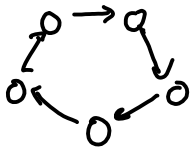
Idea: points on a circle
$a=3,\ p=5$



$a^p - a$ circles



rotate this circle
0 times, 1 time, ..., $p-1$ time
$\rightarrow$ p circles are a family
$a^p - a$ circles
Families of size p
We want to show: the circles in a family are different from each other.



We have a circle and after k rotations, $1 \le k \le p-1$ there is the same circle. Take the smallest k.
- $k \neq 1$
- $k \geq 2$

Consider $p, p+1, \dots, p+k-1$
one of them is divisible by k
There is $l \cdot k$ such that
$p+1 \le l \cdot k \le p+k-1$

After lk rotations still the same circle.
After $lk-p$ rotations still the same circle.
But: $1 \le lk-p \le k-1$

$\hookrightarrow p \mid a^p - a$