# Congruence, part 2

Lecture 4    Jan 31, 2021

# Showing a Diophantine equation has no solution

- **Recall.** $a \equiv b \ \ modulo\, n \iff n \mid (a-b)$ **i.e.** $a-b$ is divisible by $n$
- When working $modulo\ n,$ different integers $a, b$ such that $a-b$ is divisible by $n$ will be the same for us

**Q1***. Show that there are no integers $a, b, c$ such that $a^2 + b^2 - 8c = 6$.

Solution: Work modulo 8.

* Questions taken from https://artofproblemsolving.com/community/c1902h1048955_diophantine_equations_using_congruences

# Showing a Diophantine equation has no solution

- **Q2**. Find integers $x, y$ that solve $x^4 - 6x^2 + 1 = 7 \times 2^y$

- **Solution**: Consider 4 cases $(1) y = 1;\ (2) y = 2;\ (3) y = 3;\ (4)\ y \geq 4$

In case (4), work modulo 16

# A problem with products modulo n

- **An important observation:**

  If $a, b$ are integers and $a \times b = 0$ then one of them MUST be ZERO.

  <u>This is not always true for multiplication $modulo\ n$</u>

  (product of two <u>non-zero</u> numbers <u>modulo n</u> can be <u>zero</u> <u>modulo n</u>)

- Example: Let $n = 6, a = 2,\ b = 3$.
- Then $a, b \not\equiv 0\ modulo\ 6$ , but $a \times b = 2 \times 3 \equiv 0\ modulo\ 6$

# Prime numbers

- **Prime (indecomposable) numbers.**
- **<u>Definition 1</u>:** A positive integer $p > 1$ is called PRIME if $p \mid ab$ implies $p \mid a$ Or $p \mid b$
- ***<u>Definition 2</u>*:** A positive integer $p > 1$ is called PRIME if you can not write it as a product $p = ab$ with $a, b > 1$
- **Prime numbers:** 2, 3, 5, 7, 11, 13, 17, 23, 29, 31, …
- **Historical notes:** Many people have tried to prove formulas that generate prime numbers but … see Here: https://en.wikipedia.org/wiki/Formula_for_primes

# Product modulo prime numbers

- **Lemma**. Suppose $p > 1$ is a PRIME number.

  If $a \times b \equiv 0 \; mod \;\; p$, then either $a \equiv 0 \; mod \;\; p \quad or \quad b \equiv 0 \;\; mod \; p$.

- **Proof**. $ab \equiv 0 \; mod \;\; p$ means $p|\; ab$ . So, by definition of prime, either $p|a \;\; or \;\; p|b$.

That means either $a \equiv 0 \; mod \;\; p \quad or \quad b \equiv 0 \;\; mod \; p$.

We can actually deduce a lot more.

# A Theorem

○ **Theorem**. Suppose $p > 1$ is a PRIME number.

If $a$ is not divisible by $p$ (is not 0 $mod\ p$), then for every $r \in \{1,2, \dots . p-1\}$, there is $x$ such that $ax \equiv r \ \ mod\ p$.

In other words for every $r \in \{1,2, \dots . p-1\}$, there is $x$ such that the remainder of $ax$ divided by $p$ is $r$. $(p|ax - r)$

**Proof.** We use Pigeonhole Principle in the following way. Consider the set

$$\mathrm{S} = \{a, 2a\ , 3a\ , \dots , (p-1)a\}$$

The set S has $p - 1$ elements. By the previous Lemma none of the numbers in S is equal to 0 modulo $p$, so it is congruent to one of $\{1,2, \dots . p-1\}$ (which also has $p - 1$ elements).

○ So there are two possibilities:

1) either for every $r \in \{1,2, \ldots . p-1\}$, there is $x \in \{1, \ldots, p-1\}$

such that $ax \equiv r \ \ mod\ p$

2) Or, by Pigeonhole Principle, there are different $x, y \in \{1, \ldots, p-1\}$

such that $ax \equiv ay \ \ mod\ p$

If (2) happens, then $a(x-y) \equiv 0 \ \ mod\ p$ while none of

$a\ or\ (x-y)$ is divisible by $p$. We know this can not happen for prime numbers.

# Consequences

- Lets discuss this theorem and its consequences in more details
- Lets take $r = 1$. The theorem says:

If $a$ is not divisible by $p$, then there is $x$ such that $ax \equiv 1 \ mod\ p$

- What does this really mean?

It means, in this new system of numbers, there is number whose product with $a$ is equal to 1 ($mod\ p$).

This means $x$ is like $\frac{1}{a}$ ; i.e. $x$ is the multiplicative inverse of $a$.

- For this reason, we usually denote such $x$ by $a^{-1}$

# Examples

- What is a multiplicative inverse of 3 mod 13?

- What is a multiplicative inverse of 10 mod 23?

# Examples

- Find a number $x$ whose product with 4 has remainder 3 modulo 7?

- Find multiplicative inverses of all numbers mod 7 which are not divisible by 7.

# More about inverse

○ **Theorem** (Fermat's Little Theorem) Suppose $p > 1$ is a PRIME number.

For every $a$ we have $a^p \equiv a \ \ mod\ p$.

In particular if $a$ is not $0\ mod\ p$ , for $a^{-1}$ we can take $a^{-1} \equiv a^{p-2}\ mod\ p$

**Example**. $p = 7,\ \ a = 3\ \ \to a^p = 3^7 = 9^3 \times 3 \equiv 2^3 \times 3 \equiv 8 \times 3 \equiv 1 \times 3 \equiv 3\ mod\ 7$

**Proof of Theorem.** Few slides ago we showed

$$\{a, 2a\ , 3a\ , \ldots , (p-1)a\} \equiv \ \{1, 2\ , 3\ , \ldots , (p-1)\}\ \ mod\ p$$

So taking products of the elements in both sets we have

$$a \times 2a \times\ \ \ldots \times (p-1)a \equiv\ 1 \times 2 \times \cdots \times (p-1)\ \ mod\ p$$

i.e. $a^{p-1} \times (p-1)! \equiv\ (p-1)!\ \ mod\ p$. We can now divide by $(p-1)!$ and get the result.

# Chinese Remainder Theorem

- **Theorem** (Chinese Remainder Theorem) Let $n_1, \ldots, n_k$ be integers greater than 1.

If the $n_i$ are pairwise coprime, and if $r_1, \ldots, r_k$ are integers such that $0 \le r_i \le n_i$ for every $i$, then there is a unique integer $x$, such $0 \le x \le N = n_1 \times \cdots \times n_k$ and the remainder of the of $x$ in division by $n_i$ is $r_i$ for every $1 \le i \le k$

- **For Proof** we need to discuss GCD and generalize some of the statements before. We wil come back to this later.