MATH 3360 Lecture 2/14

Benjamin Thompson

Spring 2023, Cornell

Congurences

... are a fundamental concept in modern mathematics.

... can be used to solve some equations over rational numbers.

Eg. Does $x^2+y^2=k$ have a solution where x & y are non-zero rational numbers, for $k=1,2,3$?

Partial Sol

The $k=2$ case is easy!

The $k=1$ case is harder, but still simple:

Note: $a^2+b^2=c^2 \Rightarrow \frac{a^2}{c^2}+\frac{b^2}{c^2}=1$

$$\Leftrightarrow \left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1.$$

Since $3^2+4^2=5^2$,

$x=3/5$ $y=4/5$ solves $x^2+y^2=1$.

What about the $k=3$ case?

... much harder!

We'll prove on Thu it has no solutions using congruences.

Bonus Let $a,b,c \in \mathbb{Z}$ satisfying $a^2+b^2=c^2$. Does $60 \mid abc$?

Def Let n be a positive integer. two integers are congruent mod n if they have the same remainder when divided by n.

We denote congruence using the symbol $\equiv$.

"a and b are congruent mod n"

$$\Longleftrightarrow$$

$$a \equiv b \pmod{n}.$$

Exercise: Are the following true?

$19 \equiv 7 \pmod{3}$

$2023 \equiv 2^{77} \pmod{10}$

$7^{201} \equiv 10^{102} \pmod{7}$

$39^{103} \equiv 39^{101} \pmod{19}$

$4^{99} \equiv 499 \pmod{5}.$

Prop 1 Let $a, b, n \in \mathbb{Z}$, $n > 0$. Then $a \equiv b \pmod{n}$ if and only if $n \mid a - b$.

Pf: ($\Rightarrow$) Assume $a \equiv b \pmod{n}$. Apply the division algorithm to a and b:

$$a = xn + r_a$$

$$b = yn + r_b$$

By definition of $\equiv$, $r_a = r_b$.

So $a - b = (xn + r_a) - (yn + r_b)$

$$= n(x-y) + r_a - r_b$$

$$= n(x-y).$$ Therefore $n \mid a-b$.

($\Leftarrow$): Assume $n \mid a - b$.

Then $a - b = nk$ for some $k \in \mathbb{Z}$, so $a = b + nk$.

Apply the division algorithm to b:

$$b = zn + r \qquad (0 \le r < n).$$

Then

$$a = b + nk$$

$$= zn + r + nk$$

$$= (z+k)n + r.$$

It follows that both b and a have the same remainder r after division by n. Therefore $a \equiv b \bmod n$. $\blacksquare$

Congruence mod n is an equivalence relation:

$a \equiv a \pmod{n}$ (reflexive)

$a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ (symmetry)

$a \equiv b \pmod{n}$ & $b \equiv c \pmod{n}$

$\Rightarrow a \equiv c \pmod{n}$ (transitive)

Prop 2 If $a \equiv c \pmod{n}$ & $b \equiv d \pmod{n}$:

1) $a \pm b \equiv c \pm d \pmod{n}$

2) $ac \equiv bd \pmod{n}$.

Pf: 1) Applying the previous proposition to the assumptions, $n \mid a-c$ and $n \mid b-d$.

Recall Q3 HW1:

If $x \mid y$, $x \mid z$, then $x \mid ky + lz$.

Hence $n \mid (a-c) \pm (b-d)$,

$\Leftrightarrow n \mid (a \pm b) - (c \pm d)$

$\overset{\text{Prop 1.}}{\Longleftrightarrow}$ $a \pm b \equiv c \pm d \pmod{n}$.

2) $n \mid a-c \implies n \mid b(a-c)$

$\iff n \mid ab - bc$

$\underset{\text{Prop. 1.}}{\iff} ab \equiv bc \pmod{n}$.

$n \mid b-d \implies n \mid c(b-d)$

$\iff n \mid bc - cd$

$\underset{\text{Prop 1.}}{\iff} bc \equiv cd \pmod{n}$.

Hence $ab \equiv bc \equiv cd \pmod{n}$. ∎

<u>Exercise:</u> Do the following have solutions (where $x \in \mathbb{Z}$, $x > 0$)?

$3x \equiv 1 \pmod{4}$

$9x \equiv 1 \pmod{5}$

$6x \equiv 1 \pmod{3}$

$7^x \equiv 1 \pmod{11}$.

<u>Prop:</u> Let $a, n \in \mathbb{Z}$, $n > 1$.

Then there is some b such that

$ab \equiv 1 \pmod{n}$ $\boxed{\text{iff}}$ $\gcd(a,n) = 1$.

a common abbreviation of "if and only if"

Pf: ($\Rightarrow$) Assume $ab \equiv 1 \pmod{n}$.

So $n \mid ab-1 \Leftrightarrow ab-1 = nk$

$\Leftrightarrow ab - nk = 1$

Now $\gcd(a,n) \mid ab$

$\gcd(a,n) \mid nk$

$\Rightarrow \gcd(a,n) \mid ab - nk = 1.$

$\therefore \gcd(a,n) = 1.$

($\Leftarrow$): Assume $\gcd(a,n)=1$.

Then $ax + ny = 1$ for some $x, y \in \mathbb{Z}$.

(By the reverse Euclidean algorithm.)

Hence $ax + ny \equiv 1 \pmod{n}$.

Since $ny \equiv 0 \pmod{n}$,

from proposition 2,

$ax + ny - ny \equiv 1 - 0 \pmod{n}$.

$\Leftrightarrow ax \equiv 1 \pmod{n}$. Choose $b = x$. $\blacksquare$

Next time:

- general congruence eqns.
- more congruence properties
- a proof that $x^2 + y^2 = 3$ has no rational solutions.