Math 312, lecture 5, 22/5/2018

Last time: examples

Today (1) linear equations & Euclid's algorithm
(2) Congruence

~~Recall~~, Def: A Diophantine equation is one where the unknowns are integers

Examples $x^2+y^2=z^2$ $\quad$ $6x+7y=15$
$x^3+y^3=z^3$ $\quad$ $2x=7$
$x^4+y^4=z^4$

Results: - $2 \nmid 7 \iff 2x=7$ has no solutions

- $6x+7y=15$ has solutions since $(6,7)=1$

- $x^2+y^2=z^2$ has many solutions (e.g. $3^2+4^2=5^2$)

- $x^4+y^4=z^4$ has no solutions beyond $xyz=0$ (Fermat)

- $x^3+y^3=z^3$ has no non-trivial solutions (Euler)

Example: $x^2+y^2=z^2$

Step (1): Common factors

Say prime p divided ~~both~~ two of x,y,z.

Then p divides the square of the third

So p divides the third (if $p|a\cdot a$ then $p|a$ or $p|a$)

Then $p^2|x^2$, $p^2|y^2$, $p^2|z^2$ so can divide x,y,z by p.

Still have $\left(\frac{x}{p}\right)^2+\left(\frac{y}{p}\right)^2=\left(\frac{z}{p}\right)^2$

Keep doing this until no common factors

$\Rightarrow$ Can write sol'n as $x=d\cdot x'$, $y=d\cdot y'$, $z=d\cdot z'$

where $d\in\mathbb{Z}$, x',y',z' pairwise relatively prime

$\Rightarrow$ Assume from now on this holds

Step (2): Constraints from congruence

~~x,y can't both be even~~

Now if x,y,z pairwise prime, x,y can't both be even

HW: If x is even, x^2 is divisible by 4

If x is odd, x^2 has remainder 1 when divided by 4

If x,y were both odd, x^2,y^2 would each have form $4q+1$

So $z^2=x^2+y^2$ would have form $4q+2$ impossible

So can't have both even or both odd. Wlog x is odd, y is even. So x^2+y^2 is odd, so z is odd

Step (3): Unique factorization

We have $x^2+y^2=z^2 \Leftrightarrow y^2 = z^2-x^2 = (z-x)(z+x)$

Both x,z odd, y even so also have

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right)$$

Can a prime p divide both $\frac{z-x}{2}$, $\frac{z+x}{2}$?

No: if $p \mid \frac{z+x}{2}$, and $p \mid \frac{z-x}{2}$ then $p \mid z = \frac{z+x}{2} + \frac{z-x}{2}$

and $p \mid x = \frac{z+x}{2} - \frac{z-x}{2}$.

if p divides a,b it divides $a \pm b$

So if we write $\frac{z+x}{2} = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$

$\frac{z-x}{2} = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}$

in the factorization $\left(\frac{y}{2}\right)^2 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \cdot q_1^{f_1} \cdots q_s^{f_s}$

all p_i, q_j distinct. But in $\frac{y}{2}$ every prime occurs an <u>even</u> number of times, so e_i, f_j are even

$36 = 2^2 \cdot 3^2$, $900 = 2^2 \cdot 3^2 \cdot 5^2 = (2^* \cdot 3^*)(5^*)$

$= (2^2 \cdot 3^2) \cdot (5^2)$

So $\frac{z+x}{2}$, $\frac{z-x}{2}$ are squares.

Say $\frac{z+x}{2} = n^2$, $\frac{z-x}{2} = m^2$.

Then m, n have no common factors (any common factors would divide x and z)

Bottom line: If $\frac{z+x}{2} = n^2$, $\frac{z-x}{2} = m^2$ then

$$z = n^2 + m^2, \quad x = n^2 - m^2, \quad y = 2mn$$

$$\left(\frac{y}{2}\right)^2 = m^2 n^2$$

revert assumption of primality

i.e.: If $x^2 + y^2 = z^2$ then have d, m, n with $(m,n) = 1$, $n > m$, one of m, n even

s.t.

$$x = d \cdot (n^2 - m^2)$$
$$y = d \cdot 2mn$$
$$z = d \cdot (m^2 + m^2)$$

e.g. $3 = 2^2 - 1^2$
$4 = 2 \cdot 2 \cdot 1$
$5 = 2^2 + 1^2$

Step 4: Check:

$$(d(n^2-m^2))^2 + (d \cdot 2mn)^2 = d^2(n^4 - 2m^2n^2 + m^4) + d^2(4m^2n^2)$$

$$= d^2(n^4 + 2m^2n^2 + m^4) = d^2(n^2+m^2)^2$$

$$= (d \cdot (n^2+m^2))^2 \quad \checkmark$$

Simpler version

consider $x^2 = 2y^2$

has sol'n $0^2 = 2\cdot 0^2$. Suppose $x, y \neq 0$

Let p be an odd prime st $p | x$ then $p | x^2$ so $p | 2y^2$

so $p | 2$ or $p | y$ or $p | y$ so $p | y$

then $p^2 | x^2$, $p^2 | y^2$ and $\left(\frac{x}{p}\right)^2 = 2\left(\frac{y}{p}\right)^2$

Repeatedly doing this, eventually no odd prime divides x or y.

So x is power of 2: $x = 2^k$ so $x^2 = 2^{2k}$

and y is a power of 2: $y^2 = 2^\ell$ $2y^2 = 2^{2\ell+1}$

So can't have $x^2 = 2y^2$.

$\Leftrightarrow \left(\frac{x}{y}\right)^2 = 2$ has no integral solutions! ("$\sqrt{2}$ is irrational")

Lemma: If $x = \prod_p p^{e_p}$ then $x^2 = \prod_p p^{2e_p}$ ← every exponent is even

Pf: $\left(\prod_p p^{e_p}\right)\cdot\left(\prod_p p^{e_p}\right) = \prod_p p^{e_p+e_p} = \prod_p p^{2e_p}$.

Congruence

Go back to $10x + 7y = 33$

Solved by: (1) using Bezout to find particular sol'n:

$(10, 7) = 1 = 3\cdot 7 - 2\cdot 10. \Rightarrow 33 = -66\cdot 10 + 99\cdot 7$

(2) Finding the general sol'n to homogeneous eqn

$$10x + 7y = 0$$

$7 \mid 7y$ so $7 \mid 10x$ so $7 \mid x$ $((7, 10) = 1)$ so $x = 7k$

so $y = -10k$.

Put together:

$$\begin{cases} x = -66 + 7k \\ y = 99 - 10k \end{cases}$$

(consecutive integer pts on line differ by $\pm\begin{pmatrix} 7 \\ -10 \end{pmatrix}$)

New interpretation: $10x + \begin{pmatrix}\text{multiple} \\ \text{of } 7\end{pmatrix} = 33$

implicit unknown: 7y

Solution was: $x = -66 + \begin{pmatrix}\text{multiple} \\ \text{of } 7\end{pmatrix}$

Also $x = 4 + \begin{pmatrix}\text{multiple} \\ \text{of } 7\end{pmatrix}$

<u>New notation:</u> Instead of $10x + \begin{pmatrix}\text{mult}\\ \text{of } 7\end{pmatrix} = 33$

or $10x = 33 + \begin{pmatrix}\text{mult of}\\ 7\end{pmatrix}$

write (Gauss)

$$10x \equiv 33 \quad (7)$$

or $10x \equiv 33 \quad (\text{mod } 7)$

or $10x \equiv 33 \quad \text{mod } 7$

<u>Say</u> "10x is <u>congruent</u> to 33 <u>modulo</u> 7".

Instead of $x = -66 + \begin{pmatrix}\text{mult of}\\ 7\end{pmatrix}$

or $x = -4 + \begin{pmatrix}\text{mult}\\ \text{of } 7\end{pmatrix}$

write $x \equiv 4 \quad (7)$

$x \equiv 4 \quad (\text{mod } 7)$

$x \equiv 4 \quad \text{mod } 7.$

<u>Examples</u> $365 = 1 + \underbrace{7 \cdot 52}$ ← mult of 7

$\Rightarrow 365 \equiv 1 \quad (7)$

Bottom line: Equation $10x+7y=33$ has ∞'ly many solutions: $\left\{\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-66\\99\end{pmatrix}+\begin{pmatrix}7\\-10\end{pmatrix}k\right\}$

Congruence $10x\equiv 33\ (7)$ has the "unique" solution $x\equiv 4\ (7)$

Aside: One way to solve congruence $10x\equiv 33\ (7)$ is to put back the implicit variable, convert to equation $10x+7y=33$

Def: Let $a, b, m \in \mathbb{Z}$, with $m\geq 1$. Say a is congruent to b modulo m if $a-b$ is divisible by m
($\Leftrightarrow$ $a-b=m\cdot k$ for some k, or $a=b+mk$ for some k)
write $a\equiv b\ (m)$
If $a-b$ not divisible by m, say a is not congruent to b mod m, write $a\not\equiv b\ (m)$

Eg: $4\equiv 11\equiv 18\equiv -66\ (\text{mod } 7)$
but $4\not\equiv 11\ (6)$

Earlier today (HW): If $x \equiv 1 \ (2)$ then $x^2 \equiv 1 \ (4)$

Prop: (1) $\cdot \equiv \cdot \ (m)$ is an equivalence relation:

(a) $x \equiv x \ (m)$ for all x

(b) if $x \equiv y \ (m)$ then $y \equiv x \ (m)$

(c) if $x \equiv y \ (m)$ and $y \equiv z \ (m)$ then $x \equiv z \ (m)$

(2) If $x \equiv x' \ (m)$, $y \equiv y' \ (m)$

"Calculus of residues" $\rightarrow$ then $x + y \equiv x' + y' \ (m)$

$x \cdot y \equiv x' \cdot y' \ (m)$