9/30
Monday

HW 3

4460 HW 4

① (b) Is $11 \equiv -5 \pmod{5}$?

$$11-(-5)=16$$

$$5 \nmid 16$$

So, <u>No</u>

$a \equiv b \pmod{n}$
means
$n \mid (a-b)$

Super-duper
equivalence
class thm

In $\mathbb{Z}_n$
$\overline{a}=\overline{b}$ iff
$a \equiv b \pmod{n}$

?

④ (c)

Is $\overline{1} = \overline{13}$ in $\mathbb{Z}_6$?

$1 - 13 = -12$

$-12 = (6)(-2)$

So, $6 \mid (1-13)$.

Thus $1 \equiv -13 \pmod 6$

So, $\overline{1} = \overline{-13}$ in $\mathbb{Z}_6$

⑥ (f) In $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ calculate the following and reduce your answer $\overline{a}$ so that $0 \leq a \leq 6$.

$\overline{5} \cdot \overline{2} + \overline{1} + \overline{2} \cdot \overline{4} \cdot \overline{6}$

$= \overline{10} + \overline{1} + \overline{8} \cdot \overline{6} = \overline{3} + \overline{1} + \overline{1} \cdot \overline{6} = \overline{4} + \overline{6}$

$= \overline{10} = \boxed{\overline{3}}$

$\overline{10} = \overline{3}$

$\overline{8} = \overline{1}$

Number Theory Applications

In number theory, people study integer solutions to Diophantine equations.

Diophantine equations are polynomials in as many variables as you want with integer coefficients.

Ex: Consider

$$x^2 + y^2 = z^2.$$

Q1: Are there solutions where $x, y, z \in \mathbb{Z}$?

Q2: If so, how many solutions are there?

Q3: Is there a formula for all the integer solutions?

Q1. Yes.

$(x,y,z)=(3,4,5)$ since $3^2+4^2=5^2$

$(x,y,z)=(5,12,13)$ since $5^2+12^2=13^2$

Q2: Infinitely many.

For example you can scale any solution.

$(x,y,z)=(3k,4k,5k)$ is a solution for any $k=1,2,3,4,\ldots$

$(3k)^2+(4k)^2=(5k)^2 \Longrightarrow$ More solutions: $\underset{k=2}{(6,8,10)}, \underset{k=3}{(9,12,15)}, \ldots$

Q3: Yes.

$$x=k(m^2-n^2)$$
$$y=k(2mn)$$
$$z=k(m^2+n^2)$$

where k,m,n are positive integers $m>n$, and $\gcd(m,n)=1$, m and n have opposite parity (they can't both be even or both be odd)

Gives all integer solutions to $x^2+y^2=z^2$

MATH 4460

Ex:

$m = 2$
$n = 1$
$k = 1$

$$x = k(m^2 - n^2) = 1 \cdot (2^2 - 1^2) = 3$$
$$y = k(2mn) = 1 \cdot (2 \cdot 2 \cdot 1) = 4$$
$$z = k(m^2 + n^2) = 1 \cdot (2^2 + 1^2) = 5$$

$m = 3$
$n = 2$
$k = 1$

$$x = 1 \cdot (3^2 - 2^2) = 5$$
$$y = 1 \cdot (2 \cdot 3 \cdot 2) = 12$$
$$z = 1 \cdot (3^2 + 2^2) = 13$$

One method to derive the formula:

<u>Idea</u>

$$z^2 = x^2 + y^2 \overset{i^2=-1}{=} (x+iy)(x-iy)$$

Then you use properties of the <u>Gaussian integers</u>

$$\mathbb{Z}[i] = \{x+iy \mid x, y \in \mathbb{Z}\}$$

This set has a unique factorization theorem into primes.

2 is no longer prime in $\mathbb{Z}[i]$

$2 = (1+i)(1-i)$

$5 = (2+i)(2-i)$

$5 = 2^2 + 1^2$

5 is the sum of two squares

p factors iff

$p \equiv 1 \pmod 4$

Ex: (Fermat's Last Theorem)

Fermat claimed to have a proof of:

There are no integer solutions to $x^n + y^n = z^n$ with $n > 2$ except if one of x, y, z are 0.

Andrew Wiles proved this in 1995.

[NOVA documentary "The proof"]

Fermat proved this case

Ex: $x^3 + y^3 = z^3$ has no non-zero integer sols.

($0^3 + 2^3 = 2^3$ is called a trivial sol.)

4460
Hw 4

(14) Prove that there are no integer solutions to

$$x^2 - 5y^2 = 2.$$

You can't just check all x, y

x	y	x^2-5y^2
1	1	-4
2	1	-1
2	2	-16
10	1	95
⋮	⋮	⋮

Idea

If there was an integer solution to $x^2-5y^2=2$ then

$$(x^2-5y^2) \equiv 2 \pmod{n}$$

for any $n \geq 2$.

pf: Suppose there exists $x, y \in \mathbb{Z}$ with $x^2 - 5y^2 = 2$.
We will show that this leads to a contradiction.
Since $x^2 - 5y^2 = 2$ we have that $(x^2 - 5y^2) \equiv 2 \pmod 5$.
Note that $-5 \equiv 0 \pmod 5$.
So we get $x^2 \equiv 2 \pmod 5$.
This is a contradiction by the following table.

x	$x^2 \pmod 5$
0	0
1	1
2	4
3	$9 \equiv 4 \pmod 5$
4	$16 \equiv 1 \pmod 5$

$\Big\}$ The only squares modulo 5 are 0, 1, 4.

So, there is no x with $x^2 \equiv 2 \pmod 5$.
Thus, there are no integers x & y with $x^2 - 5y^2 = 2$. ∎

HW 4 4460

(17) Prove that if $x \in \mathbb{Z}$, $x > 1$, and x ends in a 7 then x is not a square $\left[x \neq a^2 \text{ where } a \in \mathbb{Z} \right]$

Ex: 137 is not a square.

$\boxed{\text{Method 1}}$

$1^2=1$	$7^2=49$
$2^2=4$	$8^2=64$
$3^2=9$	$9^2=81$
$4^2=16$	$10^2=100$
$5^2=25$	$11^2=121$
$6^2=36$	$12^2=144$

$\boxed{\text{Method 2}}$

$$\begin{aligned} 137 &= 130+7 \\ &\equiv 0+7 \pmod{10} \\ &\equiv 7 \pmod{10} \end{aligned}$$

Show 7 is not a square modulo 10.

x	$x^2 \pmod{10}$
0	0
1	1
2	4
3	9
4	$16 \equiv 6 \pmod{10}$
5	$25 \equiv 5 \pmod{10}$
6	$36 \equiv 6 \pmod{10}$
7	$49 \equiv 9 \pmod{10}$
8	$64 \equiv 4 \pmod{10}$
9	$81 \equiv 1 (\mathrm{mod}\ 10$

There are no 7's here.

For a general proof look online at solutions