Math 4460
4/28/25

HW 5

$\gcd(2,14) = 2 \neq 1$

$$\mathbb{Z}_{14} = \{\cancel{\overline{0}}, \overline{1}, \cancel{\overline{2}}, \overline{3}, \cancel{\overline{4}}, \overline{5}, \cancel{\overline{6}}, \cancel{\overline{7}}, \cancel{\overline{8}}, \overline{9}, \cancel{\overline{10}}, \overline{11}, \cancel{\overline{12}}, \overline{13}\}$$

$\boxed{14 = 2 \cdot 7}$

multiples of 14

14
28
42
56
70
84
98
⋮

$$\mathbb{Z}_{14}^{\times} = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}$$

inverses

$\overline{1}^{-1} = \overline{1}$

$\left.\begin{array}{l}\overline{3}^{-1} = \overline{5} \\ \overline{5}^{-1} = \overline{3}\end{array}\right\}$ $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$

$\left.\begin{array}{l}\overline{9}^{-1} = \overline{11} \\ \overline{11}^{-1} = \overline{9}\end{array}\right\}$ $\overline{9} \cdot \overline{11} = \overline{99} = \overline{1}$

$\overline{13}^{-1} = \overline{13}$ } $\overline{13} \cdot \overline{13} = \overline{(-1)}\,\overline{(-1)} = \overline{1}$

primitive root

$\overline{3}^1 = \overline{3}$

$\overline{3}^2 = \overline{9}$

$\overline{3}^3 = \overline{27} = \overline{13}$

$\overline{3}^4 = \overline{39} = \overline{11}$

$\overline{3}^5 = \overline{33} = \overline{5}$

$\overline{3}^6 = \overline{15} = \overline{1}$

$\overline{3}$ is a primitive root

In $\mathbb{Z}_{14}^{\times}$ calculate $\overline{11}^{1,000}$

Know: since $\overline{11} \in \mathbb{Z}_{14}^{\times}$ $\leftarrow$ $\boxed{\gcd(13,14)=1}$

by Euler we get $\overline{11}^{\varphi(14)} = \overline{1}$

which is $\boxed{\overline{11}^6 = \overline{1}}$ because

$\varphi(14) = |\mathbb{Z}_{14}^{\times}| = |\{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}|$
$= 6.$

Then,

$$\begin{array}{r} 166 \\ 6 \overline{)1000} \end{array}$$

$$\overline{11}^{1000} = \overline{11}^{6(166)+4}$$

$$= \left(\overline{11}^{6}\right)^{166} \cdot \overline{11}^{4}$$

$$= \overline{1}^{166} \cdot \overline{11}^{4}$$

$$= \overline{11}^{4} = \overline{121} \cdot \overline{121}$$

$$= \overline{9} \cdot \overline{9}$$

$$= \overline{81}$$

$$= \overline{11}$$

$$\begin{array}{r} -6 \\ \hline 40 \\ -36 \\ \hline 40 \\ -36 \\ \hline 4 \end{array}$$

$$\begin{array}{r} 8 \\ 14 \overline{)121} \\ -112 \\ \hline 9 \end{array}$$

$$\begin{array}{r} 5 \\ 14 \overline{)81} \\ -70 \\ \hline 11 \end{array}$$

HW 5

(13) Show that $19 \nmid 4n^2+4$ for all $n \in \mathbb{Z}$.

<u>proof:</u> Suppose, by way of contradiction, that $19 \mid 4n^2+4$ for some $n \in \mathbb{Z}$.

Then, $4n^2+4 = 19k$ where $k \in \mathbb{Z}$.

Then, in $\mathbb{Z}_{19}$ we get

$$\overline{4}\,\overline{n}^2 + \overline{4} = \overline{0}$$

in $\mathbb{Z}_{19}$.

There is no such $\overline{n} \in \mathbb{Z}_{19}$ by the following table.

$\overline{n}$	$\overline{4}\,\overline{n}^2+\overline{4}$
$\overline{0}$	$\overline{4}$
$\overline{1}$	$\overline{8}$
$\overline{2}$	$\overline{20}=\overline{1}$
$\overline{3}$	$\overline{40}=\overline{2}$
$\vdots$	$\vdots$
$\overline{18}$	$\overline{1300}=\overline{8}$

never get $\overline{0}$ here

(fill in table)

We thus have a contradiction and $19 \nmid 4n^2+4$ for all n. $\blacksquare$

HW 5

(14) Let $n \in \mathbb{Z}$, $n \geq 2$.
Let $a, b, c \in \mathbb{Z}$.
If $\gcd(a,n) = 1$ and $\bar{a}\bar{b} = \bar{a}\bar{c}$ in $\mathbb{Z}_n$, then $\bar{b} = \bar{c}$ in $\mathbb{Z}_n$.

<u>proof:</u> Since $\gcd(a,n) = 1$ we know that $\bar{a}$ has a multiplicative inverse $\bar{a}^{-1}$ in $\mathbb{Z}_n$.

Then, $\bar{a}\bar{b} = \bar{a}\bar{c}$

gives $\bar{a}^{-1}\bar{a}\bar{b} = \bar{a}^{-1}\bar{a}\bar{c}$

yielding $\bar{1}\,\bar{b} = \bar{1}\,\bar{c}$

producing $\bar{b} = \bar{c}$. $\blacksquare$

Can you think of an example of $\overline{a}\,\overline{b} = \overline{a}\,\overline{c}$ in $\mathbb{Z}_n$ but $\overline{b} \neq \overline{c}$ in $\mathbb{Z}_n$?

$\overline{a} = \overline{6}$, $\overline{b} = \overline{2}$, $\overline{c} = \overline{3}$, $n = \overline{6}$

$$\overbrace{\overline{6} \cdot \overline{2}}^{\overline{0}} = \overbrace{\overline{6} \cdot \overline{3}}^{\overline{0}} \text{ in } \mathbb{Z}_6$$

$$\overline{2} \neq \overline{3}$$

<u>$\mathbb{Z}_4$:</u>

$$\overbrace{\overline{2} \cdot \overline{1}}^{\overline{2}} = \overbrace{\overline{2} \cdot \overline{3}}^{\overline{6} = \overline{2}}$$

$$\overline{1} \neq \overline{3}$$

HW 4

If p is prime and $x^2 \equiv y^2 \pmod{p}$ then $p \mid (x+y)$ or $p \mid (x-y)$.

---

proof:

Suppose p is prime and
$x^2 \equiv y^2 \pmod{p}$.

Then, $p \mid (x^2 - y^2)$.

So, $p \mid (x+y)(x-y)$.

Since p is prime, $p \mid (x+y)$ or $p \mid (x-y)$.

$\blacksquare$

USED:

p prime and $p \mid ab$,
then $p \mid a$ or $p \mid b$

$\boxed{\text{HW 3}}$ $\gcd(a,b)>1$ iff $\exists$ prime p w/ $p|a$ & $p|b$

$\boxed{4(a)}$

($\Rightarrow$) Suppose $\gcd(a,b)>1$.

Let $d=\gcd(a,b)$.

Since $d \geq 2$ by the fundamental theorem, d factors into primes.

Pick a prime p in d's factorization.

Then, $p|d$.

Since $d=\gcd(a,b)$ we know $d|a$ & $d|b$.

Since $p|d$ and $d|a$ we get $p|a$.

Since $p|d$ and $d|b$ we get $p|b$.

So p is a prime with $p|a$ and $p|b$.

($\Leftarrow$) If p is prime and $p \mid a$ and $p \mid b$

then $\gcd(a,b) \geq \underbrace{p \geq 2}_{p \text{ prime}} > 1$

$\boxed{/}$