Thursday, September 19

Homework #1 due Tuesday (before class)

Definition: Let $m \in \mathbb{N}$. Given $a, b \in \mathbb{Z}$, we say a is *congruent to b modulo m*, and write $a \equiv b \pmod{m}$, if $m \mid (b-a)$.

For example, $53 \equiv 7 \pmod{23}$,

$5 \not\equiv 37 \pmod{23}$.

We call m the *modulus* of the congruence.

Usage note: In other fields, "mod" is a function that returns the r from the division algorithm. For us, "congruent (mod m)" is a relation that holds for certain pairs (a,b).

Indeed, it's an "equivalence relation":

- reflexive: $a \equiv a \pmod{m}$
- symmetric: $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$
- transitive: if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

(Proof: Exercise.)

In particular, "congruent (mod m)" partitions $\mathbb{Z}$ into *residue classes* (mod m).

For example, one residue class (mod 23) is

$$\{\ldots, -39, -16, 7, 30, 53, \ldots\}$$

Every residue class (mod m) is of the form $\{a + mk : k \in \mathbb{Z}\}$.

- Note: $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m. (Exercise)

↳ important that $-37 = -8 \cdot 5 + 3$

and not $-37 = -7 \cdot 5 + (-2)$.

Lemma: Let $m \in \mathbb{N}$. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:

Ex (0) If $k \mid m$ then $a \equiv b \pmod{k}$.

(1) $a+c \equiv b+d \pmod{m}$

(2) $ac \equiv bd \pmod{m}$.

Proof of (2): $bd - ac = bd - bc + bc - ac$
$= b(d-c) + c(b-a)$ is a multiple of m. //

Corollary:

- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a-c \equiv b-d \pmod{m}$.
- If $f(X) \in \mathbb{Z}[X]$ is a polynomial with integer coefficients, and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

$\hookrightarrow$ In particular, if $k \in \mathbb{N}$ then
$a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$.

We've seen $\equiv \pmod{m}$ plays nicely with $+, \times, -$. But not division:

$$\begin{cases} 18 \equiv 28 \pmod{10} \\ 2 \equiv 2 \pmod{10} \end{cases} \quad \text{but}$$

$$9 \not\equiv 14 \pmod{10}.$$

The truth is more complicated.

Theorem: $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \left(\bmod \frac{m}{(a,m)}\right)$.

Special cases:

- $ax \equiv ay \pmod{an} \Leftrightarrow x \equiv y \pmod{n}$
- If $(a,m) = 1$, then $ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \pmod{m}$.

Theorem: $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Proof: $\Rightarrow$: Suppose $ax \equiv ay \pmod{m}$ so that $m \mid (ay - ax) = a(y-x)$.

$$\Rightarrow \frac{m}{(a,m)} \,\Big|\, \frac{a}{(a,m)}(y-x).$$

Since $\frac{m}{(a,m)}$ and $\frac{a}{(a,m)}$ are coprime, we deduce that $\frac{m}{(a,m)} \mid (y-x)$.

$$\Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}.$$

$\Leftarrow$: Suppose $x \equiv y \pmod{\frac{m}{(a,m)}}$, so that $\frac{m}{(a,m)} \mid (y-x)$. $\Rightarrow a\frac{m}{(a,m)} \mid a(y-x)$.

Now $m \mid \frac{a}{(a,m)} m \mid \underbrace{a(y-x)}_{ay-ax}$, and thus $ax \equiv ay \pmod{m}$. $\square$

$$12x \equiv 12y \pmod{50}$$

if and only if

$$x \equiv y \pmod{\frac{50}{(12,50)}}$$

$$\Updownarrow$$

$$x \equiv y \pmod{25}.$$

Question: If $a \equiv b \pmod{m}$, is $k^a \equiv k^b \pmod{m}$?

No: $2 \equiv 5 \pmod{3}$ but $(-1)^2 \not\equiv (-1)^5 \pmod{3}$.

Definition: Given $m \in \mathbb{N}$, a *complete residue system* $\pmod{m}$ is a set containing exactly one element from every residue class modulo m.

Examples of complete residue systems modulo $m=5$:

$\{0,1,2,3,4\}$, $\{1,2,3,4,5\}$

$\{-4,-2,0,2,4\}$

$\{537,-532,60,101,9999929\}$

Definition: A reduced residue class $(\mathrm{mod}\ m)$ is a residue class $\{a+mk : k\in\mathbb{Z}\}$ with $(a,m)=1$.

(Note: If $a\equiv b \pmod m$ then $(a,m)=(b,m)$.)

A reduced residue system is a set with exactly one element of each reduced residue class. Example:

$\{1,2,3,4\}$ or $\{-4,-2,2,4\}$

or $\{537,-532,101,9999929\}$.

- A reduced residue system $(\mathrm{mod}\ 12)$ is $\{1,5,7,11\}$.

Definition: Given $m\in\mathbb{N}$, the Euler phi-function $\phi(m)$ is the cardinality of a reduced residue system, that is,

$$\phi(m) = \#\{1\le a\le m : (a,m)=1\}.$$

(sometimes Euler totient function).

Examples: $\phi(5)=4$, $\phi(12)=4$

$\phi(101)=100$ and in fact $\phi(p)=p-1$.

Lemma: Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system $\pmod{m}$, and let a be coprime to m. Then $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ is also a reduced residue system $\pmod{m}$.

Example: $\{1, 5, 7, 11\}$ RRS $\pmod{12}$

$(17, 12) = 1 \Rightarrow \{17, 85, 119, 187\}$ also a RRS $\pmod{12}$.

Proof: Since each r_j is coprime to m, so is each ar_j. If $ar_i \equiv ar_j \pmod{m}$, then $r_i \equiv r_j \pmod{m}$ (since $(a,m)=1$) and hence $i = j$. So the ar_j are in $\phi(a)$ distinct reduced residue classes $\pmod{m}$, and so they represent every reduced residue class. //

Euler's theorem: If $(a,m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Example: $17^4 \equiv 1 \pmod{12}$.

Proof: Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system $\pmod{m}$; then $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ is also a RRS $\pmod{m}$. Then each ar_j is congruent to exactly one $r_i \pmod{m}$, and so the products are congruent $\pmod{m}$:

$$r_1 r_2 \cdots r_{\phi(m)} \equiv (ar_1)(ar_2)\cdots(ar_{\phi(m)})$$
$$= a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Since $(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$, we can cancel to get

$$1 \equiv a^{\phi(m)} \pmod{m}.$$

//

[Algebra aside: the same proof shows that if G is any finite abelian group, then $g^{\#G} = e$ in G.]

<u>Corollary:</u> (Fermat's little theorem)

- If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.
- For all $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

<u>Corollary:</u> Let $(a,m)=1$. If $e,f \in \mathbb{N}$ with $e \equiv f \pmod{\phi(m)}$, then

$$a^e \equiv a^f \pmod{m}.$$

<u>Proof:</u> WLOG suppose $f \geq e$. Write $f-e = \phi(m)k$ where $k \in \mathbb{N}_0$. Then

$$a^f = a^{e+\phi(m)k} = a^e\left(a^{\phi(m)}\right)^k$$
$$\equiv a^e(1)^k = a^e \pmod{m}. \quad //$$