Math 312, lecture 7, 24/5/2018

Last time: Congruence: $4+5\equiv 0\ (9)$
+ arithmetic $\quad 5+7\equiv 2\ (10)$
$5+7\equiv 3\ (9)$

Application: $10\equiv 1\ (9)$
$\Downarrow$
$10\cdot 10\equiv 1\cdot 1\equiv 1\ (9)$

Ex: By induction on k, $10^k\equiv 1\ (9)$ for all $k\in\mathbb{Z}_{\geq 0}$.

$\Rightarrow$ If we write $n\in\mathbb{Z}_{\geq 1}$ in decimal notation:

$$n=\sum_{k=0}^{d} a_k\cdot 10^k$$

Then $\quad n\equiv \sum_{k=0}^{d} a_k\cdot 1 = \sum_{k=0}^{d} a_k \leftarrow$ write $S(n)$ for this
call it "digit sum" of n.

~~Lemma~~ Conclusion: $n\equiv S(n)\quad (9)$

(also this means $n\equiv S(S(n))$, $n\equiv S(S(S(n)))\ldots$)

Use 1: To compute the class of n mod 9, repeatedly replace n with $S(n)$ until the number is between 1 and 9.
~~Eg.~~ (final result is the "digit root")

Eg can tell if $9|n$. $\quad$ ($9|n$ iff $n\equiv 0\equiv 9\ (9)$)

Use 2: Clock arithmetic!

Note that if $a \equiv a' (9)$ and $b \equiv b'$ (9) then

$$\begin{aligned} ab &\equiv a'b' \\ a \pm b &\equiv a' \pm b' \end{aligned} \quad (9)$$

Whatever the answer to $786 \cdot 1{,}534$ is, its class mod 9 is:

$s(786) = 7+8+6 = 21$, so $s(s(786)) = 2+1 = 3$

i.e. $786 \equiv 3$ (9)

$s(1{,}534) = 13$, $s(s(1534)) = 4$

so $786 \cdot 1{,}534 \equiv 3 \cdot 4 \equiv 12 \equiv 3$ (9)

HW: Develop test for divisibility by 11.

Observe: $3|9$ so if $a \equiv b$ (9) $3|9|a-b$ so $a \equiv b$ (3)

eg. $15 \equiv 6$ (9) so $15 \equiv 6$ (3)

but $3 \equiv 6$ (3) but $3 \not\equiv 6$ (9)

The class of a mod 9 determines its class mod 3:

classes mod 9: 0, 1, 2, 3, 4, 5, 6, 7, 8

classes mod 3: 0, 1, 2, 0, 1, 2, 0, 1, 2

(can just reduce each $0 \le r < 9$ mod 3)

POV 1: Finding class mod 9 helps test divisibility by 3

POV 2: Each class mod 3 splits up as 3 classes mod 9:

$$a \equiv 1 \ (3) \iff a \equiv 1 \text{ or } 4 \text{ or } 7 \pmod 9$$

both sides represt set $\{1, 4, 7, 10, 13, \ldots$
$-2, -5, -8, \ldots\}$

Equations: negatives and inverses

Paradigm: To solve $ax + b = c$ need to subtract b, divide by a

Now what about $ax + b \equiv c \ (m)$?

Eg. ~~10x~~ $x + 5 \equiv 2 \ (7)$

$10x \equiv 33 \ (7)$

(1) Subtraction

Instead of "subtract b" think of "add $-b$".

$-b$ is the number s.t. $b + (-b) = 0$

Always, if $b \in \mathbb{Z}$, $b + (-b) \equiv 0 \ (m)$

~~But~~ What about reduced residues? if $0 \le b < m$ then $-b$ may not be in $[0, m-1]$, but if $b \ge 1$ then $m - b$ is. Eg.: $5 + 4 \equiv 0 \ (9)$

Lemma: Given b, there is a unique residue class c

st $b + c \equiv 0 \ (m)$

Pf: Suppose also $b + c' \equiv 0 \ (m)$

Add c to both sides:

$$c + (b + c') \equiv c + 0 \equiv c \ (m)$$
$$|||$$
$$(c + b) + c' \equiv 0 + c' \equiv c' \ (m)$$

so $c \equiv c' \ (m)$

Aside: really "better" to view modular arithmetic as a number system with m numbers (residue classes)

(e) Division:

Def: Call b a "modular inverse" to a $\overset{\text{mod } m}{}$ if $ab \equiv 1 \ (m)$

Say b is invertible if it has an inverse

Ex: $2 \cdot 3 \equiv 1 \ (5)$ so 2,3 are invertible mod 5.

but $2 \cdot 3 \equiv 0 \ (6)$ so 2,3 can't be invertible mod 6

indeed, if $\bar{2}$ mod 6 had $2 \cdot \bar{2} \equiv 1 \ (6)$ then:

$$0 \equiv \bar{2} \cdot 0 \equiv \bar{2} \cdot (2 \cdot 3) \equiv (\bar{2} \cdot 2) \cdot 3 \equiv 1 \cdot 3 \equiv 3 \ (6)$$

but $0 \not\equiv 3 \ (6)$

Lemma: The inverse is unique, if it exists.

Pf: say $b \cdot c \equiv b \cdot c' \equiv 1 \ (m)$

so $c \cdot (b \cdot c') \equiv c \cdot 1 \equiv c \ (m)$

but $c(b \cdot c') \equiv (c \cdot b) \cdot c' \equiv 1 \cdot c' \equiv c' \ (m)$.

Finding inverses

Example: find inverse of $\cancel{8}\ 5$ mod 73.

Means solving $5x \equiv 1 \ (73)$

with implicit variable, need to solve $5x + 73y = 1$

$\Rightarrow$ need $\gcd(5,73)=1$ for this to work

$\Rightarrow$ if $\gcd(5,73)$ can find x using Euclid's algorithm:

$3 = 73 - 70 = 73 - 14 \cdot 5$

$1 = 6 - 5 = 2 \cdot 3 - 5 = 2 \cdot 73 - 29 \cdot 5$

so $5 \cdot (-29) \equiv 1 \ (73)$ or $5 \cdot 44 \equiv 1 \ (73)$

Prop: If $(a,m)=1$ then a is invertible.

Pf: By Bezout's thm there are $x, y \in \mathbb{Z}$ s.t. $ax + my = 1$

then $ax \equiv 1 \ (m)$.

Prop: If $d=\gcd(a,m)>1$ then a is a zero-divisor (hence not invertible).

Pf: $d\cdot\frac{m}{d}=m\equiv 0\ (m)$

$\frac{m}{d}\in\mathbb{Z}$, and $1\le\frac{m}{d}<m$ since $d>1$.

mult by $\frac{a}{d}\in\mathbb{Z}$ get:

$$a\cdot\frac{m}{d}=\frac{a}{d}\cdot d\cdot\frac{m}{d}\equiv\frac{a}{d}\cdot 0\equiv 0\ (m)$$

so $a\cdot\frac{m}{d}\equiv 0\ (m)$ but $\frac{m}{d}\not\equiv 0\ (m)$

If there was $\bar{a}$ s.t. $\bar{a}\cdot a\equiv 1\ (m)$ we'd also have

$$0\equiv\bar{a}\cdot\left(a\cdot\frac{m}{d}\right)\equiv(\bar{a}\cdot a)\cdot\frac{m}{d}\equiv\frac{m}{d}$$ contradiction.

Bottom line: a is invertible mod m iff $(a,m)=1$

("invertible" and "prime to m" are equivalent)

Cute example:

$-1 \bmod 641.$

$5 \cdot 128 = 10 \cdot 64 = 640$ i.e. $2^7 \cdot (-5) \equiv 1 \ (641)$

Also $641 = 625 + 16$ i.e. $2^4 \equiv -5^4 \pmod{641}$

So $2^{32} = 2^{28+4} = (2^7)^4 \cdot 2^4 \equiv (2^7)^4 \cdot (-5^4)$

2^{2^5}

$\equiv -(2^7 \cdot 5)^4 \equiv -(-1)^4 \equiv -1 \ (641)$

So $2^{2^5} + 1 \equiv 0 \ (641)$, i.e. $641 \mid 2^{2^5} + 1$.

not prime!

Solving Equations

Eg: $x + 5 \equiv 2 \ (7)$ add 2 to both sides gets:

$\Downarrow$

$x \equiv 2 + 2 \equiv 4 \ (7)$ $(5 + 2 \equiv 0 \ (7))$

Conversely, $4 + 5 = 9 \equiv 2 \ (7)$

(or: $x + 5 \equiv 2 \ (7) \iff x + 5 + 2 \equiv 2 + 2 \ (7)$
$\iff x \equiv 4 \ (7)$)

Eg: $10x \equiv 33 \ (7)$

reduce coeff mod 7 $\Updownarrow$

$3x \equiv 5 \ (7)$

notice $2 \cdot 3 = 6 \equiv -1 \ (7)$

so $(-2) \cdot 3 \equiv 1 \ (7)$ ← side calc: find inverse of 3 mod 7

or $5 \cdot 3 \equiv 1 \ (7)$

mult by -2:

$\iff -2 \cdot 3 \cdot x \equiv -10 \ (7)$ i.e. $x \equiv 4 \ (7)$

or

$3x \equiv 5 \ (7) \iff 5 \cdot 3x \equiv 5 \cdot 5 \ (7)$

i.e. $x \equiv 4 \ (7)$ $\quad 25 = 4 + 21$

This really is an equivalence since 5 is invertible (mod 7)

Aside: Back to $10x + 7y = 33$

writing this as $10x \equiv 33 \ (4)$ we found $x \equiv 4 \ (7)$

i.e. $x = 4 + 7k$

solve for y: $10(4 + 7k) + 7y = 33$

$$\Updownarrow$$

$$40 + 70k + 7y = 33$$

$$\Updownarrow$$

$$7y = -7 - 70k$$

$$\Updownarrow$$

$$y = -1 - 10k$$

General solution: $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 \\ -1 \end{pmatrix} + \begin{pmatrix} 7 \\ -10 \end{pmatrix} k, \ k \in \mathbb{Z}$

Bottom line: Equation $ax + b \equiv c \ (m)$ has the unique solution $x \equiv \bar{a}(c - b) \ (m)$ <u>if</u> a is invertible

What if $(a,m) > 1$?

E.g. $20x \equiv 66 \ (14) \iff 6x \equiv 10 \ (14)$

This says $14 \mid 6x-10$ i.e. $2\cdot 7 \mid 2\cdot(3x-5)$

note $\frac{6x-10}{14} = \frac{3x-5}{7}$, i.e. $6x \equiv 10 \ (14)$

$$\Updownarrow$$

$$3x \equiv 5 \ (7)$$

If we want to divide by a non-invertible number, this number must <u>divide the modulus</u> and we divide the modulus too:

$$a \equiv b \ (m) \iff ad \equiv bd \ (md)$$

Conclusion: The solution to $20x \equiv 66 \ (14)$ seems to be

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

But class $x \equiv 4 \ (7)$ splits as: $x \equiv 4$ or $\underset{\substack{\uparrow \\ 4+7}}{11}$ mod 14

In general, $x \equiv a \ (m)$ ~~then~~ same as

$$x \equiv a \text{ or } a+m \text{ or } a+2m \text{ or } \dots \ a+(d-1)m \quad (\text{mod } m\cdot d)$$

$\boxed{\text{* multiple solutions mod 14!}}$

What about $10x \equiv 65 \ (14)$

want to divide by $10 = 2 \cdot 5$ 5 is not a problem,

but $2 = \gcd(10, 14)$ is: not invertible

If $d = \gcd(a, m)$ does not divide b,

no solutions at all to $ax \equiv b \ (m)$

To solve $ax \equiv b \ (m)$, let $d = \gcd(a, m)$.

If $d \nmid b$, no solutions

If $d \mid b$, solve $\frac{a}{d} \cdot x \equiv \frac{b}{d} \ \left(\frac{m}{d}\right)$,

return to classes mod m.

(c.f. sol'n to $ax + my = b$)