Lecture 13

HW 2 posted
- due 11/2

Solving linear Congruences $ax \equiv b \bmod n$

1) $ax \equiv b \bmod n$ has an inverse iff $\gcd(a,n)=1$
$ax + ny = \gcd(a,n) = 1$ by Bezout's Identity
$\Rightarrow ax = 1 + n(-y) \Rightarrow ax \equiv 1 \bmod n$
(Recall the modular multiplicative inverse of
$a \in \mathbb{Z}$ is $x \in \mathbb{Z}$ s.t. $ax \equiv 1 \bmod n$)
$\Rightarrow x = a^{-1}$ can be found using Extended Euclidean Algorithm

2) $ax \equiv b \bmod n$ has a solution if $\gcd(a,n) \mid b$

3) if $ax \equiv b \bmod n$ has a solution, i.e. $\gcd(a,n) \mid b$,
then there are $\gcd(a,n)$ solutions separated by $\frac{n}{\gcd(a,n)}$

4) $ca \equiv cb \bmod n \iff a \equiv b \bmod \frac{n}{\gcd(c,n)}$
$\Rightarrow$ We can simplify and cancel a factor of c
but we do not end up in the same modular space.

HM 5 Boston

Ex Modular Inverses

Find $34^{-1} \bmod 143 \iff 34x \equiv 1 \bmod 143$

Apply Bezout's Identity: $34x + 143y = \gcd(34, 143)$

(i) $143 = 4 \times 34 + 7 \Rightarrow 7 = \underline{143} - 4 \times \underline{34}$

(ii) $34 = 4 \times 7 + 6 \Rightarrow 6 = \underline{34} - 4 \times 7$

(iii) $7 = 1 \times 6 + 1 \Rightarrow 1 = 7 - 1 \times 6$

$6 = 6 \times 1 + 0$

$\Rightarrow \gcd(34, 143) = 1 \Rightarrow \exists x$ s.t $ax \equiv 1 \bmod 143$ where $x = a^{-1}$

Substitute to find x, the inverse and the Bezout Coefficient:

$6 = \underline{34} - 4 \times (\underline{143} - 4 \times \underline{34})$

$= 17 \times \underline{34} - 4 \times \underline{143}$

$1 = \underline{143} - 4 \times \underline{34} - 1 \times (17 \times \underline{34} - 4 \times \underline{143})$

$= 5 \times 143 - 21 \times 34 \Rightarrow 34(-21) = 1 - 5(143)$

$\Rightarrow 34^{-1} \equiv -21 \bmod 143$, or $x = -21$

Note: If I do not want to express the inverse as a negative number, I can add a multiple of 143

$\Rightarrow \boxed{34^{-1} \equiv 122 \bmod 143 \text{ or } x = 122}$

Solving Systems of Congruences: Chinese Remainder Theorem

Ex $\left.\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 2 \bmod 4 \\ x &\equiv 1 \bmod 5 \end{aligned}\right\}$ We need $\gcd(3,4)=1$, $\gcd(3,5)=1$, $\gcd(4,5)=1$

Idea: We will work out x in three sections

Mod 3 Mod 4 Mod 5

$x = (\quad) + (\quad) + (\quad)$

To satisfy each of the congruences, I would like to ignore the remaining terms when considering the contribution of each term to x

$\Rightarrow$ One way to do this is to include a multiplicative factor of each modulus to the remaining terms

mod 3 mod 4 Mod 5

$x = (4\times5) + (3\times5) + (3\times4)$

$= 20 + 15 + 12$

Now, $20 \equiv 2 \bmod 3$ ✓ but $12 \not\equiv 1 \bmod 5$

$12\times2 = 24 \not\equiv 1 \bmod 5$, $12\times3 = 36 \equiv 1 \bmod 5$

$\Rightarrow$ We can include a multiplicative factor of 3 to 3rd term

$15 \not\equiv 2 \bmod 4$, $15\times2 \equiv 2 \bmod 4$

$\Rightarrow$ we can include a multiplicative factor of 2 to 2nd term

$= 4\times5 + 3\times5\times2 + 3\times4\times3 = 86 \equiv$ 2 mod 3, 2 mod 4, 1 mod 5 ✓

$\Rightarrow$ Another way to express this is as $26 \bmod 60$ $\Rightarrow$ $\boxed{x = 26 \bmod 60}$

CRT proof

Suppose $n_1, \dots, n_k \in \mathbb{N}$ with $\gcd(n_i, n_j) = 1 \ \forall i \neq j$
and $b_1, \dots, b_k \in \mathbb{Z}$

Then the system of linear congruences

$$x \equiv b_1 \bmod n_1$$
$$\vdots$$
$$x \equiv b_k \bmod n_k$$

has a unique solution modulo $n_1 \times n_2 \times \dots \times n_k = \prod_{i=1}^{k} n_i$

Proof Set $N = n_1 \times n_2 \times \dots \times n_k$, Define $N_i = \frac{N}{n_i}$

Claim $\gcd(N_i, n_i) = 1$

Proof Suppose $d \mid n_i$ and $d \mid N_i$

$\Rightarrow$ Since all of the n_j's relatively prime,
d must divide some $n_j \neq n_i$

$\Rightarrow d \mid n_j$ for $j \neq i$

$\Rightarrow d \mid \gcd(n_j, n_i) \Rightarrow d \mid 1 \Rightarrow d = 1$ □

$\gcd(N_i, n_i) = 1 \Rightarrow N_i$ has an inverse mod n_i

i) $\Rightarrow \exists x_i$ s.t. $N_i x_i \equiv 1 \bmod n_i$ (possible b/c $\gcd(n_i, n_i) = 1$)

ii) $\Rightarrow x_i N_i \equiv 0 \bmod n_j$ for $i \neq j$

because N_i defined as product of little n_i's except for n_i

$\Rightarrow N_i$ a multiple of $n_j \Rightarrow N_i \equiv 0 \bmod n_j$

Consider $x = x_1 N_1 b_1 + x_2 N_2 b_2 + \cdots + x_k N_k b_k$

Modulo n_i every term where subscript not equal to i

will be 0 from (ii) $x_i N_i \equiv 0 \bmod n_j \ (i \neq j)$

and 1 from (i) $x_i N_i \equiv 1 \bmod n_i$

$\Rightarrow$ Ex $x \equiv 0 + \cdots + 0 + x_i N_i b_i + 0 + \cdots \pmod{n_i}$

$x \equiv b_i \pmod{n_i}$ $\quad 1 \leq i \leq k$ from (i)

The $N_i b_i$ are inverse pairs modulo n_i. This proves existence of a solution $\square$

Uniqueness: Sps x, y are sols

$\Rightarrow x \equiv b_i \bmod n_i$

$y \equiv b_i \bmod n_i$

$\Rightarrow \quad x - y \equiv 0 \bmod n_i \quad 1 \leq i \leq k$

$\Rightarrow \quad n_i \mid (x-y) \Rightarrow x - y = c \cdot n_i$

$\Rightarrow n_i$'s are relatively prime,

$N \mid x - y$

$\Rightarrow x \equiv y \bmod N$

(The solutions x, y are equivalent mod N) $\square$

Ex solve $4x \equiv 5 \bmod 9$

$2x \equiv 6 \bmod 20$

Here the setup is slightly different than as stated in CRT

We can manipulate and put in form to apply and solve.

$4x \equiv 5 \bmod 9$

Note $\gcd(4,9) = 1 \Rightarrow$ unique sol obtained by multiplying both sides by multiplicative inverse of 4 mod 9

$4 \times 7 = 28 \equiv 1 \bmod 9 \Rightarrow 7 = 4^{-1}$

$\Rightarrow$ Multiply both sides by 7:

$x \equiv 35 \bmod 9$

or $x \equiv 8 \bmod 9$

Now $2x \equiv 6 \bmod 20$. Note $\gcd(2,20) \neq 1$, but all numbers even, so we can exploit this to write

$2x \equiv 2 \times 3 \bmod 2 \times 10$

$\Rightarrow$ Now we can cancel the common factor from all of these parts

$x \equiv 3 \bmod 10$

Now the system can be reduced

$\Rightarrow$ $x \equiv 8 \bmod 9$, $x \equiv 3 \bmod 10$ $\}$ $N = 90$ $N_1 = 10$ $N_2 = 9$

Solve $N_i x_i \equiv 1 \bmod n_i$

$10 x_1 \equiv 1 \bmod 9 \Rightarrow x_1 \equiv 1 \bmod 9$, $\underline{x_1 = 1}$

$9 x_2 \equiv 1 \bmod 10 \Rightarrow 9 \times 9 = 81 \equiv 1 \bmod 10$

$\underline{x_2 = 9}$

$x = \sum x_i N_i b_i = 1 \cdot 10 \cdot 8 + 9 \cdot 9 \cdot 3$

$x = 80 + 243 = 323$

$\Rightarrow$ should be unique mod 90 $\Rightarrow 53 \bmod 90$

but want to solve mod $n_1 \times n_2 = 180$ (mod N)

$\Rightarrow$ $x \equiv 53 \bmod 180$, $x \equiv 143 \bmod 180$ (adding 90)

Fermat's Little Thm

1.1.13

For $a \in \mathbb{N}$, p prime where $p \nmid a$

$$a^{p-1} \equiv 1 \bmod p$$

Ex: $p=5, a=2$ $(5 \nmid 2)$ $\quad p=3, a=4 \Rightarrow 3 \mid 4^3-1 \Rightarrow 3 \mid 63$ ✓

$$2^{5-1} \equiv 1 \bmod 5 \Rightarrow 2^4 = 16 \equiv 1 \bmod 5$$ ✓

Proof The residues $\{0, 1, \dots, p-1\}$ are all the numbers mod p

Any number must fall in one of these equivalence classes

$\Rightarrow$ any $a \pmod p$ must be one of $0, 1, \dots, p-1$

$\Rightarrow$ Since $p \nmid a$, $a \notin [0]_p$

a cannot be in congruence class of 0

$\Rightarrow$ $a \in \{1, \dots, p-1\}$

Remark Multiplying $1, \dots, p-1$ by any $a \in \mathbb{N}$ preserves the uniqueness of the congruence classes & does not change the residues

Ex $a=8$, $p=5 \Rightarrow (1,2,3,4) \times 8 = 8, 16, 24, 32$

$\bmod 5 \Rightarrow 3, 1, 4, 2 \pmod 5 \equiv 8, 16, 24, 32$

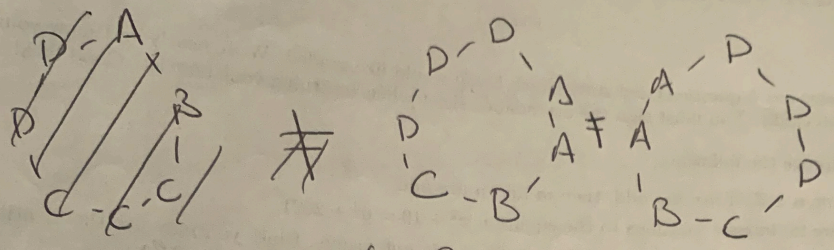
$\Rightarrow a \times (1, 2, \dots, p-1) \equiv 1, 2, 3, \dots, p-1 \bmod p$

$\Rightarrow a, 2a, 3a, \dots, (p-1)a \equiv 1 \times 2 \times 3 \times \dots (p-1) \bmod p$

$\Rightarrow a^{p-1}(p-1)! \equiv (p-1)! \bmod p$

Note $p \nmid (p-1)!$ $\Rightarrow$ We can cancel $\Rightarrow a^{p-1} \equiv 1 \bmod p$

However, two necklaces that are mirror images are different if they cannot be rotated



Here, B should come before C

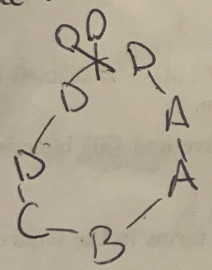
We want to show the total # of necklaces is $\frac{4^7-4}{7}$

$\Rightarrow$ # different necklaces must be an integer

$\Rightarrow$ For this to be the case $7 \mid 4^7-4$ (which is what we want to prove)

Counting Necklaces:

Cut each necklace & straighten it out



$\Rightarrow$ D A A B C D D

Q: There are other ways to cut the necklace producing different strings

$\Rightarrow$ 7 gaps b/t beads so 7 ways of cutting string (7 possible strings)

$\Rightarrow$ 7 different strings of beads:

If we start w/ all possible necklaces & cut in all possible ways, we end up w/ all possible strings

D A A B C D D
A A B C D D D
A B C D D D A
B C D D D A A
C D D D A A B
D D D A A B C
D D A A B C D

But One color necklaces forbidden

How many 1 color necklaces? 4

$\Rightarrow 4^7-4$ strings possible

Every necklace also gives rise to 7 strings

Total # strings: 7 beads, each 4 colors
$= 4^7$ strings

Total # strings:

7 beads, each 4 colors

$4 \times 4 \times 4 \times 4 \times 4 \times 4 \times 4 = 4^7$

But same color necklaces forbidden

$\Rightarrow$ How many one-color necklaces? 4

$\Rightarrow 4^7 - 4$ strings

Also Every necklace under consideration gives rise to 7 different strings

$\Rightarrow$ # different necklaces $= \frac{4^7 - 4}{7}$ □

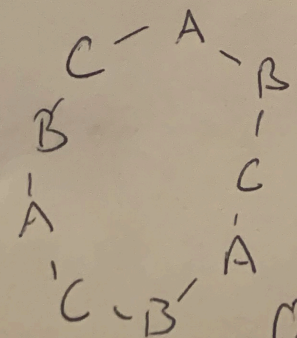
Q: Something weird in this proof.

At no point did we use the fact that 7 prime

$\Rightarrow$ if we replace prime # 7 by composite #, then not all strings that we get by cutting a necklace are necessarily different.

$\Rightarrow$ we needed 7 different strings for each necklace to justify our counting argument.

* Use 9 beads



Things repeat every 3 beads

when we cut necklace in all possible ways, we get 3 different strings, not 9

Q: Can this periodic necklace occur if it has prime # of beads? (and at least 2 colors)