Lecture 7: Modular Arithmetic 2

Yo Dawg I Heard You Like Modular Arithmetic

A Remainder Problem

I want to buy cookies for lecture.
Box A costs $7, Box B costs $10.

Buy only box A: $4 left over
Buy only box B: use up all my money
How much money did I start with?

Mathematically: find x such that
$x \equiv 4 \pmod{7}$
$x \equiv 0 \pmod{10}$

Remainder Solution

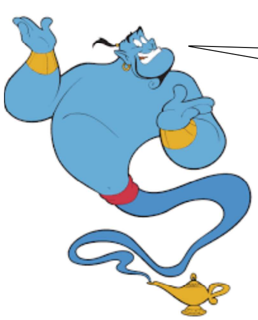
Want x such that $x \equiv 4 \pmod{7}$, $x \equiv 0 \pmod{10}$
Is there a solution? idk...let's try finding one!

List all positive x such that $x \equiv 4 \pmod{7}$:
4, 11, 18, 25, 32, 39, 46, 53, 60, ...
Oh look — $x = 60$ works! So maybe I have $60

But what if I actually have $130? Still works...
Adding multiples of 70 doesn't change equivalences!
Makes sense to consider answer modulo 70.

More Complicated Remainders

$x \equiv 1 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{8}$
Listing method possible, but difficult...



$b_3 = 40$
$b_5 = 96$
$b_8 = 105$

Why did we want these?
$x \equiv 1 \cdot b_3 + 3 \cdot b_5 + 2 \cdot b_8$!

For this problem:

$$x \equiv 40 + 288 + 210$$
$$\equiv 58 \pmod{120}$$

The Quest For b_i

Goal: $b_3 \equiv 1 \pmod{3}, 0 \pmod{5}, 0 \pmod{8}$

Getting last two easy: take $b_3 = 5 \cdot 8 = 40$

Idea: last two still fine for $c \cdot 40$
Choose c st $c \cdot 40 \equiv 1 \pmod{3}$
Means we want $c = 40^{-1} \pmod{3}$!
$40 \equiv 1 \pmod{3}$, so take $c = 1$

For b_5, use $(3 \cdot 8) \cdot (24^{-1} \pmod{5}) = 24 \cdot 4 = 96$

For b_8, use $(3 \cdot 5) \cdot (15^{-1} \pmod{8}) = 15 \cdot 7 = 105$

Exact same values the genie gave us!

Chinese Remainder Theorem

Theorem: Let $n_1, n_2, \ldots, n_k$ be coprime. Then

$$x \equiv a_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

has a solution modulo $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

Proof:

- Suppose have $b_1, b_2, \ldots, b_k$ such that
  - $b_i \equiv 1 \pmod{n_i}$
  - $b_i \equiv 0 \pmod{n_j}$ for $j \neq i$
- Take $x \equiv \prod_{i=1}^{k} a_i b_i \pmod{N}$

Continue CRT

Finish proof: show how to create b_i such that

- $b_i \equiv 1 \pmod{n_i}$
- $b_i \equiv 0 \pmod{n_j}$ for $j \neq i$

Similar to before: $c \cdot \prod_{j \neq i} n_j$ satisfies second point

What should c be?
Want $c \cdot \prod_{j \neq i} n_j \equiv 1 \pmod{n_i}$
So take $c = \left(\prod_{j \neq i} n_j\right)^{-1} \pmod{n_i}$

Note: $\left(\prod_{j \neq i} n_j\right)^{-1} \equiv \left(\prod_{j \neq i} n_j^{-1}\right) \pmod{n_i}$
This is why we need coprimality!

A Small Example

Apply this method to original problem:
$x \equiv 4 \pmod{7}$, $x \equiv 0 \pmod{10}$

$10 \equiv 3 \pmod{7}$, so $b_7 = 10 \cdot (3^{-1} \pmod{7}) = 50$
$b_{10} = 7 \cdot (7^{-1} \pmod{10}) = 21$

Take $x = 4b_7 + 0b_{10} = 200$
Hence $x \equiv 60 \pmod{70}$

Note: didn't actually have to calculate b_{10} here!

A Larger Example

$x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 1 \pmod{5}$,
$x \equiv 3 \pmod{7}$

- $3 \cdot 5 \cdot 7 = 105 \equiv 1 \pmod{2}$
- $a_2 = 105 \cdot (1^{-1} \pmod{2}) = 105$

- $2 \cdot 5 \cdot 7 = 70 \equiv 1 \pmod{3}$
- $a_3 = 70 \cdot (1^{-1} \pmod{3}) = 70$

- $2 \cdot 3 \cdot 7 = 42 \equiv 2 \pmod{5}$
- $a_5 = 42 \cdot (2^{-1} \pmod{5}) = 126$

- $2 \cdot 3 \cdot 5 = 30 \equiv 2 \pmod{7}$
- $a_7 = 30 \cdot (2^{-1} \pmod{7}) = 120$

A Larger Example 2

$x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 1 \pmod{5}$,
$x \equiv 3 \pmod{7}$
Found: $a_2 = 105$, $a_3 = 70$, $a_5 = 126$, $a_7 = 120$

$x = 105 + 2 \cdot 70 + 126 + 3 \cdot 120 = 731$

Hence $x \equiv 101 \pmod{2 \cdot 3 \cdot 5 \cdot 7 = 210}$

Uniqueness

Claim: Solution from CRT is unique $\pmod{N}$.

Proof:

- Suppose have two solutions x and y
- Let $z = x - y$
- For each i, $z \equiv x - y \equiv a_i - a_i \equiv 0 \pmod{n_i}$
- So $n_i | z$ for each i
- n_is coprime, so $N | z$
- Hence, $x - y \equiv z \equiv 0 \pmod{N}$
- Rearrange to $x \equiv y \pmod{N}$

Uniqueness Proof Is Not Unique

Claim: Solution from CRT is unique $\pmod{N}$.

Proof:

- Number of possible a_i values: $\prod_i n_i$
- Number of possible x values: $N = \prod_i n_i$
- Each $x \in \mathbb{Z}_N$ corresponds to 1 set of a_i
- If two x collide, $\exists$ a_is w/o an x
- Contradicts CRT!

Break All The Things

Break time!

Today's Discussion Question:
Should orange juice include pulp?

Bijections

Let f be a function from D to R[1]

f is *one-to-one* (injective) if $f(x) \neq f(x')$ for $x \neq x'$
f is *onto* (surjective) if $(\forall y \in R)(\exists x \in D)(f(x) = y)$
f is *bijective* if is one-to-one *and* onto

Examples:

- $f_1 : \mathbb{N} \to \mathbb{N}$ given by $f_1(x) = 2x$
  - One-to-one, but not onto
- $f_2 : \mathbb{R}^+ \to \mathbb{R}^+$ given by $f_2(x) = x^2$
  - Bijective
- CRT gives bijection: $\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k} \to \mathbb{Z}_N$

[1] This is often denoted $f : D \to R$.

Function Inverses

Alternative definition: f is bijective if has inverse

Theorem: Let $f : D \to R$. f is bijective iff $\exists f^{-1}$ st $f(f^{-1}(y)) = y$ and $f^{-1}(f(x)) = x$.

Proof (if):

- Suppose have f^{-1}
- f onto
  - $\forall y$, $f^{-1}(y) \in D$ st $f(f^{-1}(y)) = y$
- f one-to-one:
  - Suppose $f(x) = f(x')$
  - Then $x = f^{-1}(f(x)) = f^{-1}(f(x')) = x'$

Only If Direction

Theorem: Let $f : D \to R$. f is bijective iff $\exists f^{-1}$ st $f(f^{-1}(y)) = y$ and $f^{-1}(f(x)) = x$.

Proof (only if):

- Suppose f bijective
- Each $y \in R$ has unique $x \in D$ with $f(x) = y$
- Let $f^{-1}(y)$ be this x

Note: f^{-1} is itself a bijection!
Have $(f^{-1})^{-1} = f$

Fermat's Little Theorem

Theorem: Let p be a prime and $a \not\equiv 0 \pmod{p}$.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

- Consider set $S_p = \{1, 2, 3, ..., p-1\}$
- Claim: $f(x) = ax \pmod{p}$ is bijection $S_p \to S_p$
- $\{1, 2, ..., p-1\} = \{a, 2a, ..., (p-1)a\} \pmod{p}$
- Means $\prod_i i \equiv \prod_i ia \equiv a^{p-1} \prod_i i \pmod{p}$
- Multiply by $\prod_i i^{-1}$, get $1 \equiv a^{p-1} \pmod{p}$

Proof Of Claim

To finish FLT proof, need to prove:
Claim: $f(x) = ax \pmod{p}$ is bijection $S_p \to S_p$
Proof:

- Need that for $x \in S_p$, $f(x) \in S_p$
  - If $x \in S_p$, $p \not| x$
  - $p \not| a$ either, so $p \not| ax$
  - Hence $ax \pmod{p} \in S_p$
- Inverse is $f^{-1}(y) = a^{-1}y \pmod{p}$
  - $f^{-1}(f(x)) \equiv a^{-1}ax \equiv x \pmod{p}$
  - $f(f^{-1}(x)) \equiv aa^{-1}x \equiv x \pmod{p}$

Uses For Fermat

Speed up repeated-squaring algorithm

- *Can't* take modulus of exponent
- But if modulus prime, can take modulo $p - 1$

Eg: $3^{661} = (3^6)^{110} \cdot 3 \equiv 3 \pmod 7$

Used critically in RSA cryptosystem!
See more of this next week

Fin

Next time: cryptography!