# Midterm #1

THU, Oct 1

exam: 4:30 - 5:45 PM

upload work by 6:15 PM

PDF

**format**

- check it out ☺ — link in email
- show-your-work problems — ~ 4
- short answer problems — ~ 12

**practice**

- review HW
- practice problems + solutions

**tools**

- calculators allowed — but: show work
- notes allowed — but: watch time

## Questions ?

- Euclidean algorithm, gcd
- prime number theorem
- diophantine equations
- modular inverses
- linear congruences $ax \equiv b \pmod m$ + systems
- Fermat's little theorem $a^{p-1} \equiv 1 \pmod p$
- binary exponentiation $a^2, a^4, a^8, \dots$ (square!)
- numbers in different bases
- Chinese remainder theorem
- quadratic congruences $x^2 \equiv 4 \pmod{55}$ $\Leftrightarrow$ $x \equiv \pm 2 \pmod 5$ and $x \equiv \pm 2 \pmod{11}$ $5 \cdot 11$

**EG**

(A) $3x \equiv 5 \pmod 8$ — 1 solution

(B) $3x \equiv 5 \pmod 9$ — 0 solutions

(C) $3x \equiv 6 \pmod 9$ — 3 solutions

(C') $6x \equiv 3 \pmod 9$ — 3 solutions

(A) $3^{-1}$ exists $\pmod 8$ b/c $\gcd(3,8) = 1$

3

$x \equiv 3^{-1} \cdot 5 \pmod 8$

$\equiv 3 \cdot 5 \equiv -1 \equiv 7$

(B) $3x = 5 + 9y \quad | \div 3$

$x = \frac{5}{3} + 3y$

no integer solutions

$\gcd(3,9) = 3$

[$3^{-1}$ DNE $\pmod 9$]

(C) $3x = 6 + 9y \quad | \div 3$

$x = 2 + 3y$

$\Leftrightarrow x \equiv 2 \pmod 3$

2, 5, 8, 11, ... $\pmod 9$

(C') $6x = 3 + 9y \quad | \div 3$

$2x = 1 + 3y$

$\Leftrightarrow 2x \equiv 1 \pmod 3 \Leftrightarrow x \equiv 2^{-1} \cdot 1 \pmod 3$

$\equiv -1 \equiv 2$

same!