Lecture 10

- Exam 1 Recap Problems Thu 10/14 6–9 pm Exam 1
- HW PB 2
- Number Theory Intro + HW PB 3
  (modulo arithmetic)

$\boxed{\text{Intro to modulo arithmetic}}$

$a, b, n, q, r \in \mathbb{Z}$

$n > 1$

$$\boxed{a = nq + r}$$

integer division

$r \in \{0, 1, 2, \ldots n-1\} = \mathbb{Z}_n$

r = remainders at n

q = quotient (sometimes q not specified)

$a \equiv r \mod n$ — a has remainder r at div. with n.

$a - r = nq$ = multiple of n — $n \mid (a-r)$

n divides $(a-r)$

<u>Examples</u>

- $21 \mod 5 = 1$ — $21 = 5 \cdot q + 1$ — $21 \equiv 1 \mod 5$

  $5 \mid (21-1)$ — 5 divides $21 - 1$

- $24 \equiv 10 \equiv 3 \equiv -39 \mod 7$ — $r \in \mathbb{Z}_7 = \{0 : 6\}$

  $24 = 7 \cdot 3 + 3$

  $3 = 7 \cdot 0 + 3$

  $10 = 7 \cdot 1 + 3$

  $-39 = 7 \cdot (-6) + 3$

Th $a \equiv b \mod n \iff n \mid (a-b)$

iff

proof $a = nq_1 + r_1$
$b = nq_2 + r_2$

$a-b = nq_1 + r_1 - nq_2 - r_2 =$
$= n(q_1 - q_2) + r_1 - r_2$

$a \equiv b \mod n \iff r_1 = r_2 \iff a-b = n \cdot \underbrace{\text{something}}_{(q_1-q_2)}$

$\iff n \mid (a-b)$

Example $\underbrace{21 \equiv 11 \mod 5}_{\text{true}} \iff \underbrace{5 \mid (21-11)}_{\text{true } 10 = 5 \cdot 2}$

mod operations.

- $(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

$$(17+4) \bmod 3 = (17 \bmod 3 + 4 \bmod 3) \bmod 3$$
$$0 \qquad\qquad 2 + \underline{1}$$

$$(19+12) \bmod 5 = (19 \bmod 5 + 12 \bmod 5) \bmod 5$$
$$31 \bmod 5 \qquad\qquad 4 + 2$$
$$1$$

- $\underbrace{a}_{=nq_1+r_1} * \underbrace{b}_{=nq_2+r_2} \bmod n = (\overset{r_1}{a \bmod n} \overset{*}{*} \overset{r_2}{b \bmod n}) \bmod n$

$nq_1r_2 + nq_2r_1 + n^2q_1q_2 + r_1r_2$

$ab \bmod n$

$$17 \cdot 4 \bmod 3 = (17 \bmod 3 * 4 \bmod 3) \bmod 3$$
$$2 \qquad\qquad 2 \qquad 1$$

$$19 \cdot 12 \bmod 5 = (19 \bmod 5 * 12 \bmod 5) \bmod 5$$
$$3 \qquad\qquad 4 * 2$$

- power

$$a^k \bmod n = (a \bmod n * a \bmod n \ldots * a \bmod n) \bmod n$$

example $13^{100} \bmod 11 = ?$

$$13^{100} \bmod 11 = 13^{64+32+4} \bmod 11 = \left(\underset{5}{\left(13^{64} \bmod 11\right)} \cdot \underset{4}{\left(13^{32} \bmod 11\right)} \cdot \underset{5}{\left(13^{4} \bmod 11\right)} \right) \bmod 11$$

$$= (5 \cdot 4) \bmod 11 \cdot 5 \bmod 11 = 9 \cdot 5 \bmod 11 = 1$$

Repeated Squaring $a^{2^k} = ?$

$$13 \bmod 11 = 2$$

$$13^2 \bmod 11 = (13 \bmod 11)(13 \bmod 11) = 2 \cdot 2 \bmod 11 = 4$$

$$13^4 \bmod 11 = (13^2 \bmod 11)(13^2 \bmod 11) = 4 \cdot 4 \bmod 11 = 5$$

$$13^8 \bmod 11 = (13^4 \bmod 11)(13^4 \bmod 11) = 5 \cdot 5 \bmod 11 = 3$$

$$13^{16} = \ldots = 3 \cdot 3 \bmod 11 = 9$$

$$13^{32} = \ldots \; 9 \cdot 9 \bmod 11 = (77+4) \bmod 11 = 4$$

$$13^{64} = \ldots \; 4 \cdot 4 \bmod 11 = 5$$

Negatives:

$$5 \cdot 2 \cdot 4 \mod 11 = \underbrace{(5 \cdot 2)}_{-1} \mod 11 \cdot 4 \mod 11$$

$\boxed{10 \equiv -1 \mod 11}$ $\Longleftrightarrow$ $11 \mid (10 - (-1))$

$$(-1 \cdot 4) = -4 \mod 11 = 7$$

Factorization into primes

p = prime $\in \mathbb{Z}$ divides only with $1, -1$, $p, -p$

$2, 3, 5, 7, 11, 13, 17, 19 \ldots$

<u>Granted</u>: any $n \in \mathbb{Z}^+$ has unique decomposition into primes

<u>ex</u>

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$$

$$75 = 5 \cdot 5 \cdot 3 = 5^2 \cdot 3$$

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$$

GCD = greatest common divisor (a,b)

(a,b)

def: take all common primes (with min counts) product of

ex $48 = 2^4 \cdot 3$

$36 = 2^2 \cdot 3^2$

$GCD = 2^2 \cdot 3^1 = 12$

$175 = 5^2 \cdot 7$

$98 = 7^2 \cdot 2$

$GCD = 7^1$

$60 = 2^2 \cdot 3 \cdot 5$

$50 = 5^2 \cdot 2$

$GCD = 2^1 \cdot 5^1 = 10$

$$GCD\left(\underset{(6)}{\frac{60}{10}}, \underset{(5)}{\frac{50}{10}}\right) = 1$$

Property $d = GCD(a,b)$

$$GCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

"coprimes" = no common factors.

Exam 1 – Thu 10/14 6-9pm Take Home

– Same content + rules as regular section

– Submit on Gradescope

Few Recap Problems.

PB1 Two's complement / operations. Convert

A 17 and 13 to twos complement $\boxed{6 \text{ bits}}$ and $\boxed{\text{subtract}}$ 13 from 17 in binary.

unsigned $[0 : 63]$ $2^6 - 1$

$[-32 : 31]$

$$17 = 2^4 + 2^0 = 010001$$

$$13 = 2^3 + 2^2 + 2^0 = 001101$$

$$17 - 13 = 17 + (-13)$$

$$-13 = 110011$$

-2^5 16 2 1

$$-32 + 19$$

$$
\begin{array}{rl}
17 = & 010001 \\
-13 = & 110011 \\
\hline
4 = & 000100
\end{array}
$$

? ✓

Ⓑ convert $428_{(10)}$ in base 5

5^2) 5^3

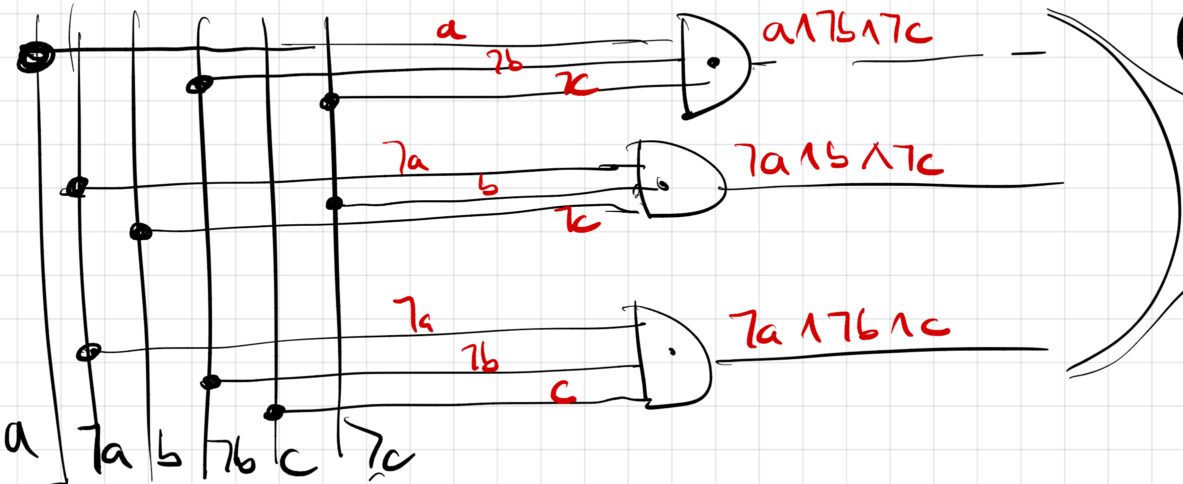
25) 125

$$428 = \underbrace{\boxed{3}\,125}_{375} + \underbrace{\boxed{2}\,25}_{50} + \underbrace{\boxed{3}\,5^0}_{3} = 3203$$

$5^3 = 125$ $\quad 5^2 \quad 5^1 \quad 5^0$

---

	q	r
$428 \div 5 =$	85	3
$85 \div 5 =$	17	0
$17 \div 5 =$	3	2
$3 \div 5 =$	0	3



Formula

PB2

$(a \wedge \neg b \wedge \neg c) \vee (\neg a \wedge b \wedge \neg c)$
$\vee (\neg a \wedge \neg b \wedge c)$

"exactly one must be T"

second formula	a	b	c	$a \wedge \neg b \wedge \neg c$	$\neg a \wedge b \wedge \neg c$	$\neg a \wedge \neg b \wedge c$	formula
0	0	0	0				
	0	0	1			$\boxed{1}$	1
	0	1	0		$\boxed{1}$		1
0	0	1	1				
	1	0	0	$\boxed{1}$			1
0	1	0	1				
0	1	1	0				
0	1	1	1				

Second Formula $(a \vee b \vee c) \wedge \neg(a \wedge b) \wedge \neg(a \wedge c) \wedge \neg(b \wedge c)$

same?

"one true" $\wedge$ "not two of them true"

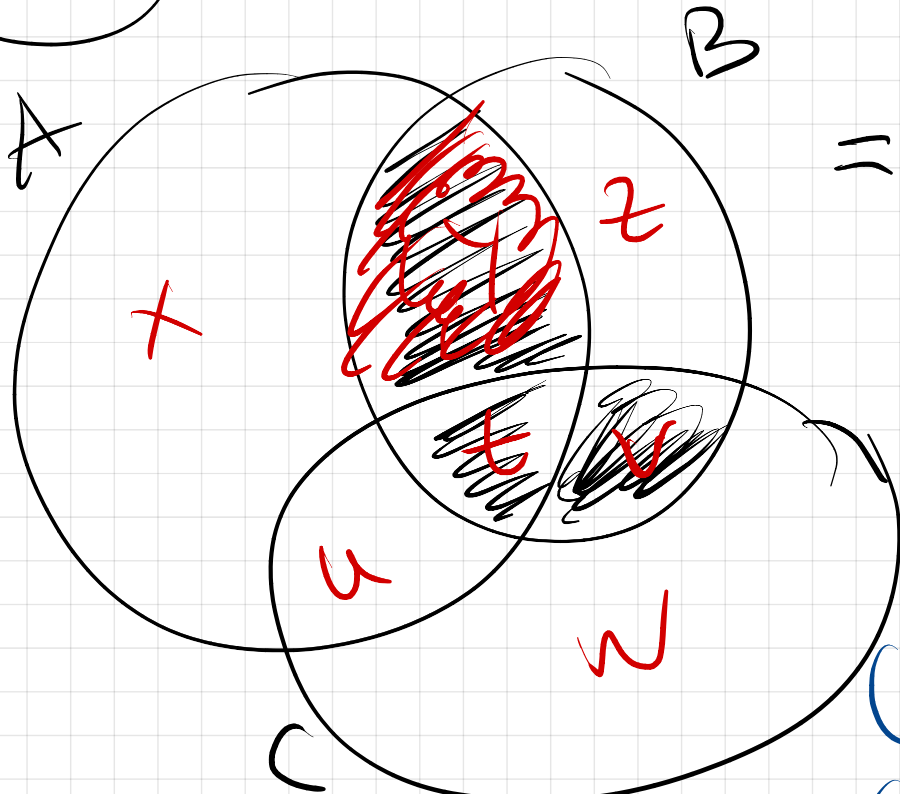
$\equiv$ "exactly one T"

$\neg(\neg a \wedge \neg b \wedge \neg c) \wedge \neg(a \wedge b) \wedge \neg(a \wedge c) \wedge \neg(b \wedge c)$

- each one of these clauses corresponds to a 0 in the table

$\underset{0}{\neg}(\underbrace{\_ \wedge \_ \wedge \_}_{\text{case}})$

PB3 Sets Rule Algebra



$y \cup t \cup v$

$$\boxed{(A \cup C) \cap B} =$$

$$= (A \cap B \setminus C) \cup (A \cap B \cap C) \cup (B \cap C \setminus A)$$

y $\quad$ t $\quad$ $t \cup v \setminus A$

$$(A \cap B \cap \bar{C}) \cup (A \cap B \cap C) \cup (B \cap C \cap \bar{A})$$

$$(A \cap B \cap \bar{C}) \cup \left((B \cap C) \cap (\underbrace{A \cup \bar{A}}_{all})\right)$$

$$(A \cap B \cap \bar{C}) \cup (B \cap C)$$

$$B \cap \left((A \cap \bar{C}) \cup C\right)$$

$$B \cap \left((A \cup C) \cap (\underbrace{C \cup \bar{C}}_{all})\right)$$

$$B \cap (A \cup C) = (A \cup C) \cap B$$

PB 4 Counting with cases (Sum Rule disjoint OR PIE not disjoint)

preferable

$36 = 13$ witches (T) $+ 4$ warlocks (W) $+ 12$ vampires (V) $+ 7$ goblins (G)

distinguishable

3 discussion sessions A, B, C $\Rightarrow$ partition of all, $\boxed{12 \text{ each}}$

(A) How many ways to make sessions?

$$\binom{36}{12}\binom{24}{12}\binom{12}{12}$$

choose session A, choose session B, session C

(B) Sessions with restriction: all warlocks same session.

$$\binom{32}{8}\binom{24}{12}\binom{12}{12} + \binom{32}{12}\binom{20}{8}\binom{12}{12} + \text{warlocks in "C"}$$

nonW

A session W

warlocks in B

(c) session $\quad$ (c) $= 2G + 2V + 4T + 4W$

want (c) to break into 2 groups ("red" "blue") of size 4 each

Constraints:

goblins $\notin$ Blue ; vampires $\notin$ Red.

3 cases: #G in Red group:
- 0
- 1
- 2

red 0G: $\binom{8^{\text{nonGV}}}{4}_{\text{red}} \times \binom{4^{\text{nonGV}} + 2^{V}}{4}_{\text{blue}}$

red 1G: $\binom{2}{1}_{\text{goblin}} \times \binom{8^{\text{nonGV}}}{3}_{\text{red}} \times \binom{5^{\text{nonGV}} + 2V}{4}_{\text{blue}}$

2G: $\binom{2}{2} \times \binom{8\,\text{nonGV}}{2} \times \binom{6\,\text{nonGV} + 2V}{4}_{\text{blue}}$

PB5 triangle(x)   red(x) = x is red
rectangle(x)   blue(x) = x is blue
above(x,y) = x above y $x=y$ equal and $x \neq y$ different

(A) Any red triangle is above any rectangle

$\forall x,y \ red(x) \wedge triangle(x) \wedge rectangle(y) \Rightarrow above(x,y)$

negation: there is a red triangle not above a rectangle

$\exists x,y \ red(x) \wedge triangle(y) \wedge rectangle(y) \wedge \neg above(x,y)$

(B) For any 2 triangles of different colors, there is a blue rectangle in between (above one, below the other)

$\forall x,y \ triangle(x) \wedge triangle(y) \wedge \neg(blue(x) \wedge blue(y)) \wedge$
$\wedge \neg(red(x) \wedge red(y)) \Rightarrow \exists z \ blue(z) \wedge rectangle(z) \wedge$
$(above(x,z) \wedge above(z,y)) \vee (above(y,z) \wedge above(z,x))$

negation: There are 2 triangles of different colors and there is no rectangle in between them.

$$\exists x, y \; triangle(x) \wedge triangle(y) \wedge \neg(blue(x) \wedge blue(y)) \wedge$$
$$\wedge \neg(red(x) \wedge red(y)) \wedge$$
$$\left[\forall z . \; blue(z) \wedge rectangle(z) \Rightarrow \begin{pmatrix} above(z, x) \\ \wedge \\ above(z, y) \end{pmatrix} \vee \begin{pmatrix} above(x, z) \\ \wedge \\ above(y, z) \end{pmatrix}\right]$$

PB6 50 cats + 50 dogs in 9 rooms. What is min

A guaranteed to be in a room?

$$\left\lceil \frac{100}{9} \right\rceil = 12$$

B per room: no more than 6 cats; at least 2 dogs

what is the maximum # animals in a room

R = room with max animals = 6 cats + max dogs

$\Rightarrow$ all other 8 rooms (except R) minimize # dogs

$8 \times 2 = 16$ dogs $\Longrightarrow$ R has $50 - 16 = 34$ dogs

$+ 6$ cats

40.