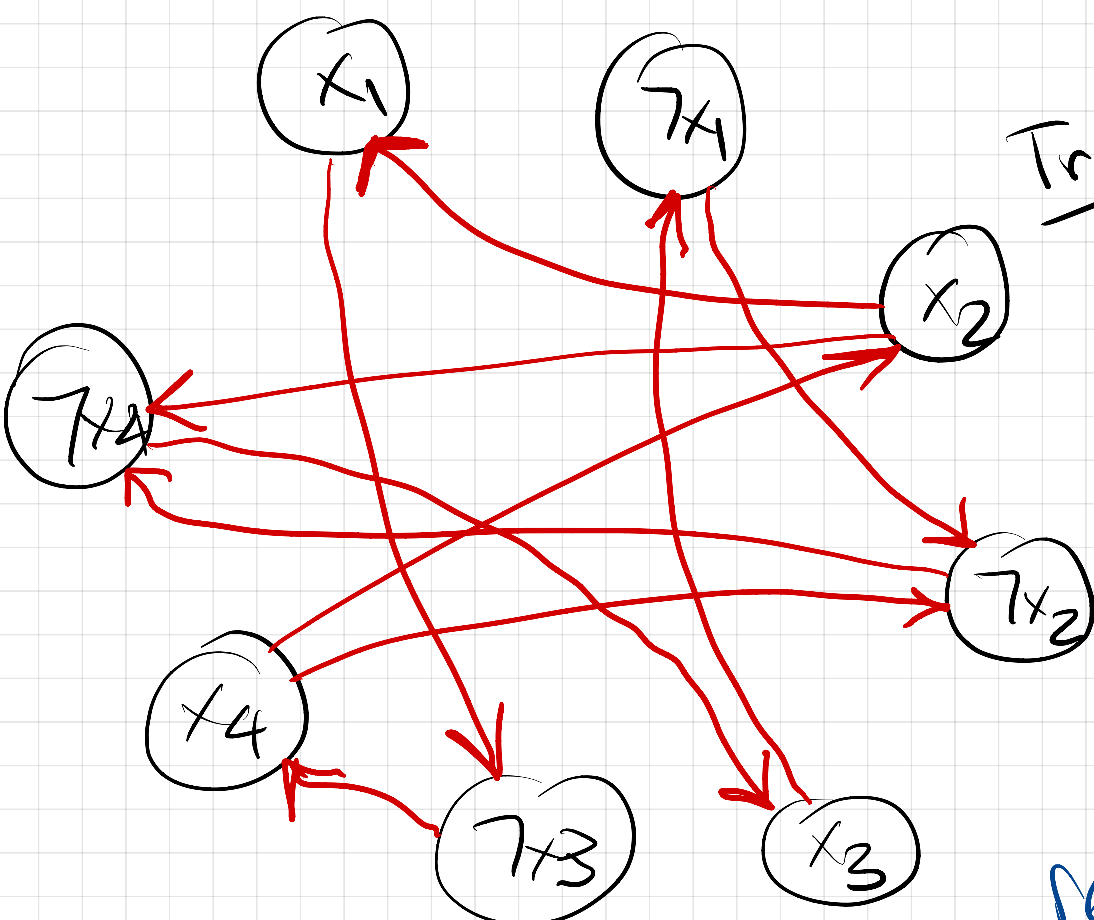
Lecture 11 October 18

- Hom PB 2 due Thursday – 3 more days.
- Number Theory part 2: GCD, Euclid, Multip. Inverse
- Intro to probabilities:
  - probab as counting, spaces, events, outcomes
  - uniform prob distribution
  - non-uniform probabilities
  - random variables

Hom PB2 <u>hint</u>

$$(x_1 \vee \neg x_2) \wedge (\neg x_1 \vee \neg x_3) \wedge (x_3 \vee x_4) \wedge (\neg x_2 \vee \neg x_4) \wedge (x_2 \vee \neg x_4)$$

$\neg x_1 \Rightarrow \neg x_2$	$x_1 \Rightarrow \neg x_3$	$\neg x_3 \Rightarrow x_4$	$x_2 \Rightarrow \neg x_4$	$\neg x_2 \Rightarrow \neg x_4$
$x_2 \Rightarrow x_1$	$x_3 \Rightarrow \neg x_1$	$\neg x_4 \Rightarrow x_3$	$x_4 \Rightarrow \neg x_2$	$x_4 \Rightarrow x_2$



Trial and error (intelligent)

Try $x_1 = T \Rightarrow \neg x_3 = T$ $(x_3 = F)$

$\Rightarrow x_4 = T$ $\Rightarrow x_2 = T$ / $\Rightarrow \neg x_2 = T$ contrad

So $x_1 = F \Rightarrow \neg x_1 = T$

Want RunTime $\leq 2m^2$

really care about

poly-quadratic $3m^4 + 5m^2$ Ok

Modulo arithmetic part 2

primes : 2, 3, 5, 7, 11, 13, 17, 19, 23 . . . divide with $1, -1$, it, -it

$\forall n \in \mathbb{N} \Rightarrow$ unique prime decomposition

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

$b = 15 = 3 \cdot 5$

GCD = take common primes (including repetitions in common)

$GCD(12, 15) = 3$

$a = 110 = 2 \cdot 5 \cdot 11$

$b = 66 = 2 \cdot 3 \cdot 11$

$GCD(110, 66) = 2 \cdot 11 = 22$

$a = 128 = 2^7$

$b = 10931 = ?$ no "2"

$GCD(128, 10931) = 1$

no prime in common

GCD properties (theorems)

1) GCD(a,b) = the biggest value $d \in \mathbb{Z}$ divides both

Proof by contradiction

assume $d = GCD(a,b)$ is NOT the biggest common divisor

$\Rightarrow \exists\, g > d \quad g|a \quad g|b$

$g > d \Rightarrow$ there at least a prime factor p in g more than in d

$\Rightarrow p|g \Rightarrow p|a, p|b \Rightarrow p$ also part of GCD.

$\Rightarrow p$ factor of d

contradiction

2) $n \mid a$; $n \mid b$ $\Big\} \Rightarrow n \mid GCD(a,b)$

n = common divisor

proof exercise (use decompositions into primes for n)

$n = p_1^{d_1} \cdot p_2^{d_2} \cdots p_k^{d_k} \Rightarrow \ldots \rightarrow n \mid d = GCD(a,b)$

Euclid Algorithm / Theorem (assume $a > b$)

- $d = GCD(a,b) \iff d = GCD(\underline{a-b}, b)$

  subtract "one" b

$a = 110 \quad b = 66$

$a - b = 44$

$gcd(110, 66) = gcd\left(\begin{smallmatrix}66\\44\end{smallmatrix}\right)$

- consequence : subtract all "b"s

$a = b \cdot q + r \qquad r \in \{0, \ldots, b-1\}$

$GCD(a,b) = GCD(a - b \cdot q, b)$

$= GCD(r, b)$

$a = 22 \quad b = 6$

one b subtract: $(\overset{16}{22-6}, 6)$, $(\overset{10}{16-6}, 6)$ $(\overset{4}{10-6}, 6)$

$(22,6) = (22 - 3 \cdot 6, 6)$ q r

all of them $22 = 6 \cdot 3 + 4$

Euclid Algorithm

repeat $GCD(a,b) = GCD(b,r)$ $a = bq + r$

untill GCD is found.

a	b	q	r
51	9	5	6
9	6	1	$\boxed{3}$ GCD
6	3	2	0

a	b	q	r
22	6	3	4
6	4	1	$\boxed{2}$ GCD
4	$\boxed{2}$	2	0

$$\left.\begin{array}{l} 51 = 3 \cdot 17 \\ 9 = 3^2 \end{array}\right\} \Rightarrow GCD = 3$$

a	b	q	r
108	60	1	48
60	48	1	$\boxed{12}$ GCD
48	12	4	0

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

$$108 = 2^2 \cdot 3^3$$

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

Modulo-inverse

def inverse of a mod n $= b = a^{-1}$ notation

iff $a \cdot b \equiv 1 \mod n$.

b = inverse of a $\iff$ a = inverse of b — unique

$b = a^{-1} \mod n$ $\qquad$ $a = b^{-1} \mod n$

Inverse doesn't always exists. $\to$ iff $\gcd(a,n)=1$
relative prime

ex: $a=4$ $n=9$ want inverse of 4 mod 9

$= 4^{-1} \mod 9 = b$ s.t. $4 \cdot b \equiv 1 \mod 9$

$b = 7$ $\qquad 4 \cdot 7 = 28 = 1 \mod 9$

$a = 12 \mod 15$ want $12^{-1} \mod 15$ that is b

doesnot exist! $\qquad 12 \cdot b = 1 \mod 15$
$\gcd(12,15) = 3$

Find the inverse using multiplicative group order

req: $\gcd(a, n) = 1$

Look at power(a) group mod n

$a, a^2, a^3, a^4, a^5, \ldots$ mod n until we get 1

$a = 4$ mod $n = 9$

$4, \; 4^2 \bmod 9 = 7, \; 4^3 \bmod 9 = 1$

$4 \cdot 4^2 = 1 \bmod 9$

inverse $4^2 = 7$

$a = 5$ mod 7

$5, \; \underset{\text{mod } 7}{5^2 = 4}, \; 5^3 = 4 \cdot 5 = 6, \; 5^4 = 30 = 2, \; 5^5 = 2 \cdot 5 = 3$

$5^6 = 3 \cdot 5 = 1 \Rightarrow \underset{\text{inverse}}{5^{-1}} = 5^5 = \underset{\text{mod } 7}{3}$

$a=7 \quad n=10$

$7,\ 7^2=49=9=-1,\ 7^3=\cdots,\ 7^4=(7^2)^2=(-1)^2=1$

$7^{-1}_{\text{inverse}}=7^3$

$a^v \equiv 1 \mod n \qquad v=$ multiplicative order of a

$a^{v-1}=$ inverse because

$a\cdot a^{v-1}=a^v\equiv 1 \mod n.$

Th if $GCD(a,n)=1$ relatively prime

$\iff \exists v$ s.t. $a^v\equiv 1 \mod n$.

Probabilities Intro.

requires uniform prob ad space

- spaces, events, uniform prob.

$\Rightarrow$ prob $= \boxed{\dfrac{\text{count numerator}}{\text{count denominator}}} = \dfrac{\text{count favorable}}{\text{count all}}$

(informal)

- random variables, joint, conditional

$\Rightarrow$ not simple counts + fractions

functions (R.V) like expectation, variance, entropy

- $\boxed{\text{non-uniform distributions}}$: prob $\neq \dfrac{\text{numerator}}{\text{denominator}}$

doesn't work

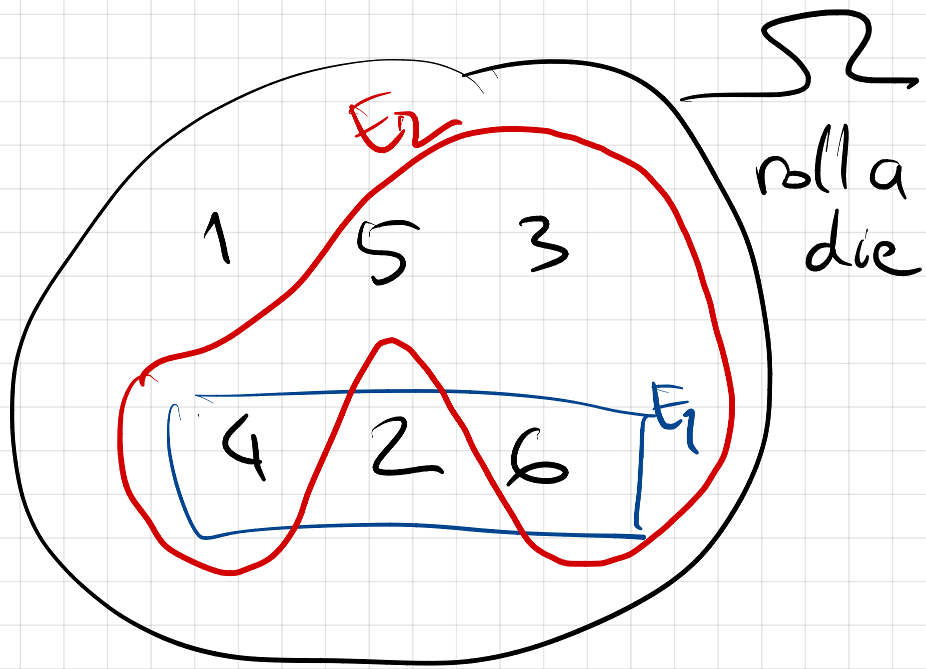
probability • random experiment $\Rightarrow$ outcome

set of outcomes Ω

outcome $w \in \Omega$

Event: subset $E \subset \Omega$

E outcomes "favorable"



probab = measure

$p(\text{outcome}) \in \mathbb{R}^+$

$0 \le p(w) \le 1$

total

$$\sum_{w \in \Omega} p(w) = 1$$

uniform $p(w) = \frac{1}{|\Omega|}$

E_1 = even outcome $= \{2,4,6\}$

$p(E_2) = 4/6 = 2/3$

E_2: outcome $\geq 3 = \{3,4,5,6\}$

$$P(E_1) = \sum_{w \in E_1} p(w)$$

uniform p $\Rightarrow P(E_1) = \frac{3}{6} = \frac{1}{2}$

$\boxed{\text{2 fair die roll}}$

$$\Omega = \{ (1,1), (1,2), \ldots (1,6)$$
$$(2,1)\ (2,2) \ldots (2,6)$$
$$\vdots$$
$$(6,1)\ (6,2) \ldots (6,6) \}$$

$$|\Omega| = 36$$

E = sum of 7

$$= \{ (1,6), (2,5), \ldots (6,1) \} \qquad |E| = 6$$

$$P(E) = 6/36 = 1/6$$

E_2 = sum > 8

= 9 or 10, 11, 12

36 46 56 66
45 55 65
54 64
63

10

$$P(E_2) = \frac{10}{36}$$

$\boxed{\text{deck of cards}}$

4 suits ♠ ♣ ♦ ♥

values $\underbrace{2, 3, 4 \ldots 10}_{\text{vals}}, \underbrace{J, Q, K, A}_{\text{faces}}$

random exp : pick a card

$E_1 =$ "face card" $= \dfrac{16}{52}$

2 suits

$E_2 =$ " value red between " $= \dfrac{\overset{\heartsuit}{9} + \overset{\diamondsuit}{9}}{52}$

2 an 10

15 red balls 10 blue balls in urn.

- draw 1 at random $\quad P(\text{red}) = \dfrac{15}{25}$

- draw 3 at once (without repetition)

$$p(3 \text{ reds}) = \frac{\binom{15}{3} \text{ favorable possib}}{\binom{25}{3} \text{ all possib of 3 out of 25}}$$

- draw 3 with replacement

$$p(3 \text{ reds}) = \frac{15^3 \rightarrow \text{all red possib with rep}}{25^3 \rightarrow \text{all possib w/ repet}}$$