- Exam on Friday (4/20)
- Assigned seating on TritonED later this week.
- 1 sheet of note (both sides)
  - ↳ do whatever you want.
- Table mod 26 will be provided.

Day 07 – Basic Counting Problems

Merkle-Hellman Knapsack

Alice (Receiver)	Eve	Bob (Sender)
. Super-increasing seq. $a_1, a_2, \ldots, a_n$. . prime $p > \sum a_i$. encryption factor A, A^{-1} exists . compute $(b_1, b_2, \ldots, b_n)$, $b_i = A \cdot a_i \mod p$ →	$(b_1, b_2, \ldots, b_n)$ (does not have to be super-increasing) →	$(b_1, b_2, \ldots, b_n)$
C ←	C ←	plaintext: $x_1, x_2, \ldots, x_n$ (ASCII codes) $C = x_1 b_1 + x_2 b_2 + \ldots + x_n b_n$
$M = A^{-1} \cdot C \mod p$ Solve SSP $x_1 a_1 + x_2 a_2 + \ldots + x_n a_n = M$ for $(x_1, x_2, \ldots, x_n)$		

Example. Alice picks the super increasing sequence

$$(a_1, a_2, \ldots, a_8) = (2,\ 5,\ 9,\ 22,\ 47,\ 99,\ 203,\ 409)$$

the prime $p = 997$ and the encryption factor $A = 60$.

a. Compute the sequence b_i's that Alice will publish

$b_i = A \cdot a_i \mod p$

$60 * 2 \mod p = 120$

$60 * 5 \mod p = 300$

$\vdots$

>> Mod[60*{2, 5, 9, ..., 409}, 997]

b. Suppose Bob wants to send the letter "**b**" (ASCII code: 01100010) to Alice. Find his ciphertext C.

$b_1, b_2, \ldots, b_n$

$C = 0 * b_1 + 1 * b_2 + 1 * b_3 + \ldots + 1 * b_7 + 0 * b_8$

c. Suppose Alice receives $C = 1255$ from Bob. Decrypt this message.

- Alice needs $A^{-1} \mod p$. (Berlekamp's algorithm)

  >> PowerMod[60, -1, 997] = 781

  PowerMod[A, n, p] computes $A^n \mod p$

- Alice computes M by $M = A^{-1} \cdot C \mod p$

  >> Mod[781 * 1255, 997] = 104.

- lastly, solve subset-sum problem. $x_1 a_1 + \ldots + x_8 a_8 = M$

  $x_1(2) + x_2(5) + x_3(9) + \ldots + x_8(409) = 104$

Subtract the biggest a_i possible from RHS

$104 = 99 + 5$

$X = (0, 1, 0, 0, 0, 1, 0, 0)$

Basic Counting Problems and Probability

Example. Suppose the letters A, D, F, G, V, X are written on six cards. In how many ways can a four-letter words be formed (by putting together four different cards)?

A D F G V X

D G A X

_ _ _ _

6 choices for the first card

5 ______ 2nd _

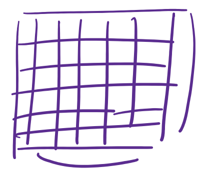
4 ______ 3rd _

3 ______ 4th card

In total : $6 \cdot 5 \cdot 4 \cdot 3 = 360$ 4-letter words

$\frac{6!}{(6-4)!}$

How many keys for ADFGVX?



6

6 = 36 cells

keys = # of way I can pick a value (number or letter) for each cell.

36 choices for 1st cell

35 ______ 2nd _

34 ______ 3rd _

⋮

2 ______ 35th _

1 ______ last _

Total = $1 \cdot 2 \cdot 3 \cdots 36$
$= 36!$

Definition 1 (Permutation). *If an* **ordered list** *or* **permutation** *of k objects is to be formed by selecting from a collection of n objects (where $k \le n$) then there are*

$$n \cdot (n-1) \cdot (n-2) \cdots (n-k+2) \cdot (n-k+1)$$

ways to do form this list. We denote this value by

$$P(n,k) := n \cdot (n-1) \cdot (n-2) \cdots (n-k+2) \cdot (n-k+1) = \frac{n!}{(n-k)!}.$$

$(1,2) \neq (2,1)$

Example. How many different five-card hands are possible from a standard deck of 52 poker cards?

Here, order does not matter $(3\diamondsuit, 5\heartsuit) = (5\heartsuit, 3\diamondsuit)$

$$\begin{pmatrix}\text{\# of ways to pick} \\ \text{and order 5 cards} \\ \text{from 52}\end{pmatrix} = \begin{pmatrix}\text{\# of ways to} \\ \text{pick 5 cards} \\ \text{from 52}\end{pmatrix} \times \begin{pmatrix}\text{\# of ways to} \\ \text{order 5 cards}\end{pmatrix}$$

$$\begin{pmatrix}\text{\# of ways to} \\ \text{pick 5 cards} \\ \text{out of 52}\end{pmatrix} = \frac{(\text{\# of ways to pick \& order 5 card/52})}{(\text{\# of ways to order 5 cards})}$$

$$= \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5!} = \frac{P(52,5)}{5!}$$

$$= \frac{52!/(52-5)!}{5!} = \frac{52!}{5!\,(52-5)!}$$

Definition 2 (Combination)**.** *The number of* ***unordered selections*** *of* ***combinations*** *of n objects selected k at a time is given by*

$$C(n,k) = \frac{P(n,k)}{k!} = \binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

This is called binomial coefficient*, read "n choose k."*

Definition 3 (Probability). *For an experiment where there are n different equally likely possible outcomes, then the* **probability** *of a result that can occur in k possible ways is given by $\frac{k}{n}$.*

(an event)

Example. Find the probability of the following

1. Rolling a 2 with a fair six-sided die $= \frac{1}{6}$

   the outcome of getting 2

   total # of outcomes

2. Rolling an even number with a fair six-sided die

   $= \frac{3}{6}$ → 3 outcomes : 2, 4, or 6

3. A box contains 100 colored balls: 14 reds, 23 blues, 45 greens, and 18 yellows. One ball is picked (blindly) from the box. Find the probability that the ball you pick

   (a) is green $= \frac{45}{100} = 0.45$

   (b) is either yellow **or** red $= \frac{18+14}{100} = \frac{32}{100} = 0.32$

   (c) is **not** blue $= \frac{45+18+14}{100} = \frac{77}{100} = 0.77$ =

   prob. of not getting a blue $= 1 -$ prob. of getting a blue $= 1 - \frac{23}{100}$

In general,

1. If p is the probability of an experimental result then $0 \leq p \leq 1$
2. If p and q are probabilities of **mutually exclusive results** P and Q then the probability of the result "P or Q" is $p + q$
3. If p is the probability of a result P then the probability of the result "not P" is $1 - p$

Example. There are 20 red $\overbrace{\text{balls and 30 blue balls in}}^{\text{total} = 50}$ a box. If we (blindly) pick two balls from the box, what is the probability that

- both chosen balls are red? $= \dfrac{\#\text{ of outcomes that both balls are Red}}{\text{total }\#\text{ of outcomes.}}$

$$= \frac{\binom{20}{2}}{\binom{50}{2}} = \frac{\frac{20!}{2!\ 18!}}{\frac{50!}{2!\ 48!}} = \frac{\frac{19\cdot 20}{2}}{\frac{49\cdot 50}{2}} = \cdots = 0.155$$

- both chosen balls are blue?

$$= \frac{\binom{30}{2}}{\binom{50}{2}} = \cdots = 0.355$$

- the colors are different?

$$P(\text{color are different}) = 1 - P(\text{colors are the same})$$
$$= 1 - \left[P(2R) + P(2B)\right]$$
$$= 1 - \left[0.155 + 0.355\right] = 0.49$$

Example. If there are 50 people in a room, what is the probability that **at least two have the same birthday**? (Ignore leap year)

$$P\left(\begin{array}{c}\text{at least 2 have} \\ \text{same bday}\end{array}\right) = 1 - P\left(\begin{array}{c}\text{everyone has} \\ \text{different bday}\end{array}\right)$$

$$= 1 - \frac{\#\text{ of ways to assign 50 different days to 50 different ppl}}{\text{total }\#\text{ of ways of giving 50 ppl their bday}}$$

$$= 1 - \frac{365 \cdot 364 \cdot 363 \cdot \ldots \cdot (365-50+1)}{365^{50}}$$

$$= 1 - \frac{P(365, 50)}{365^{50}}$$

In general, k ppl: $P\left(\begin{array}{c}\text{at least 2} \\ \text{have same} \\ \text{bday}\end{array}\right) = 1 - \dfrac{P(365, k)}{365^{k}}$

n	1	2	3	10	20	30	40	50
p	0	0.0027	0.0082	0.117	0.411	0.706	0.891	0.97