Probability and Random Processes
ECS 315

Asst. Prof. Dr. Prapun Suksompong

prapun@siit.tu.ac.th

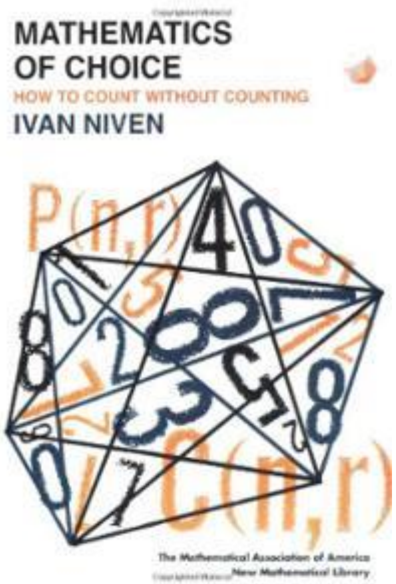
4 Combinatorics

Office Hours:
BKD 3601-7

Monday	**14:00-16:00**
Wednesday	**14:40-16:00**

Reference

- Mathematics of Choice
  How to count without counting
- By Ivan Niven
- permutations, combinations, binomial coefficients, the inclusion-exclusion principle, combinatorial probability, partitions of numbers, generating polynomials, the pigeonhole principle, and much more.



Heads, Bodies and Legs flip-book

Heads, Bodies and Legs flip-book (2)

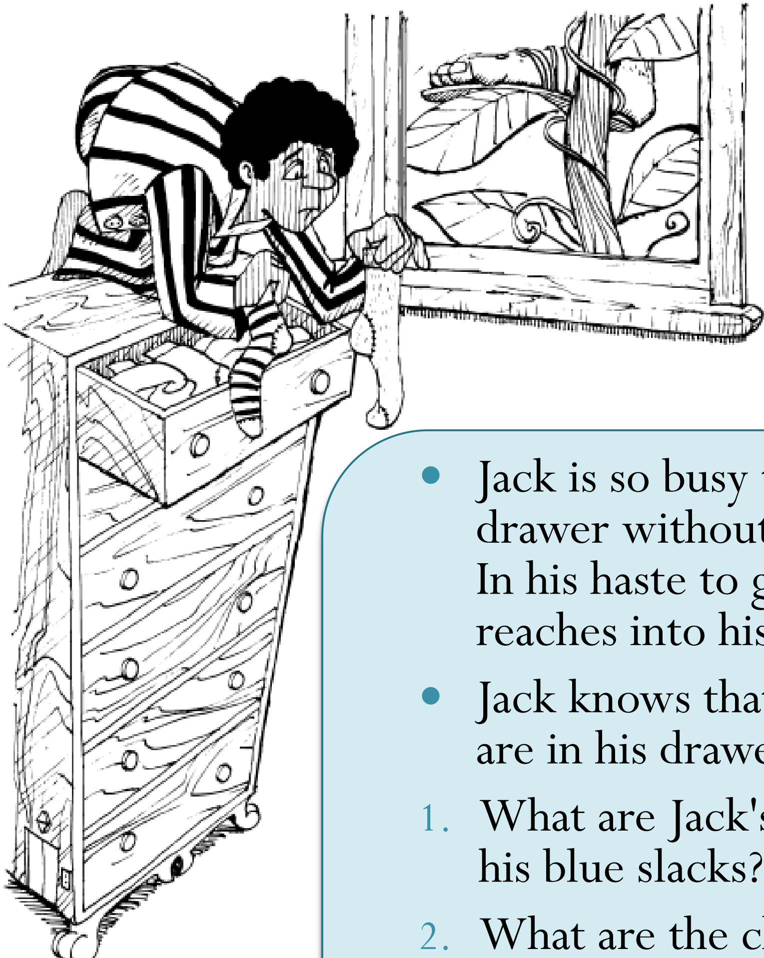
One Hundred Thousand Billion Poems

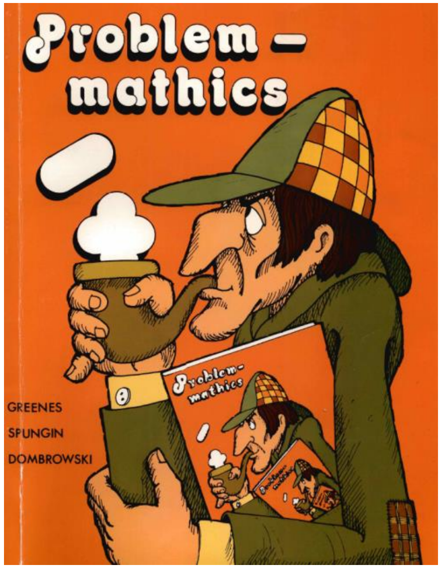
- Cent mille milliards de poèmes

One Hundred Thousand Billion Poems (2)

[Greenes, 1977]

Example: Sock It Two Me





- Jack is so busy that he's always throwing his socks into his top drawer without pairing them. One morning Jack oversleeps. In his haste to get ready for school, (and still a bit sleepy), he reaches into his drawer and pulls out 2 socks.
- Jack knows that 4 blue socks, 3 green socks, and 2 tan socks are in his drawer.

1. What are Jack's chances that he pulls out 2 blue socks to match his blue slacks?
2. What are the chances that he pulls out a pair of matching socks?

3^4*5^2*11^7*13^8

Examples Random

Input:

$3^4 \times 5^2 \times 11^7 \times 13^8$

Result:

32 189 975 201 412 589 275

Scientific notation:

$3.2189975201412589275 \times 10^{19}$

Number names:

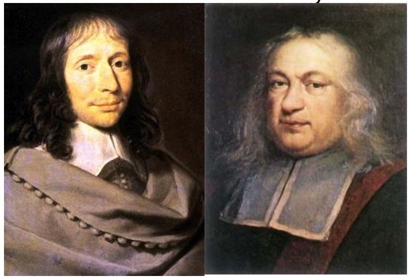
Truncated name

32 quintillion 189 quadrillion 975 trillion 201 billion 412 million 589 thousand 275

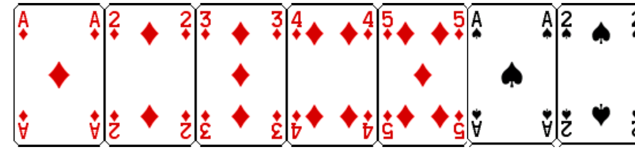
32 billion billion ...

“Origin” of Probability Theory

- Probability theory was originally inspired by **gambling** problems.
  [http://www.youtube.com/watch?v=MrVD4q1m1Vo]
- In 1654, Chevalier de Mere invented a gambling system which bet even money on case B.
- When he began losing money, he asked his mathematician friend Blaise **Pascal** to analyze his gambling system.
- Pascal discovered that the Chevalier's system would lose about 51 percent of the time.
- Pascal became so interested in probability and together with another famous mathematician, Pierre de **Fermat**, they laid the foundation of probability theory.



best known for Fermat's Last Theorem



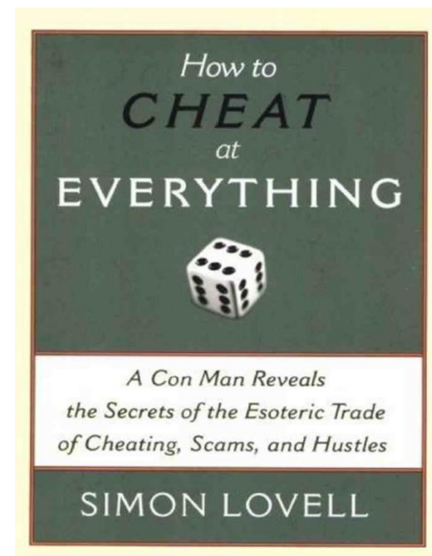
Example: The Seven Card Hustle

- Take five red cards and two black cards from a pack.
- Ask your friend to shuffle them and then, without looking at the faces, lay them out in a row.

- Bet that them can't turn over three red cards.
- The probability that they CAN do it is

$$\frac{(5)_3}{(7)_3} = \frac{\cancel{5}\times 4\times 3}{7\times 6\times \cancel{5}} = \frac{2}{7}$$

$$\frac{\binom{5}{3}}{\binom{7}{3}} = \frac{5!}{\cancel{3!}\,2!}\times\frac{\cancel{3!}\,4!}{7!} = 5\times 4\times 3\times\frac{1}{7\times 6\times 5} = \frac{2}{7}$$



[Lovell, 2006]

Finger-Smudge on Touch-Screen Devices

FRUIT NINJA

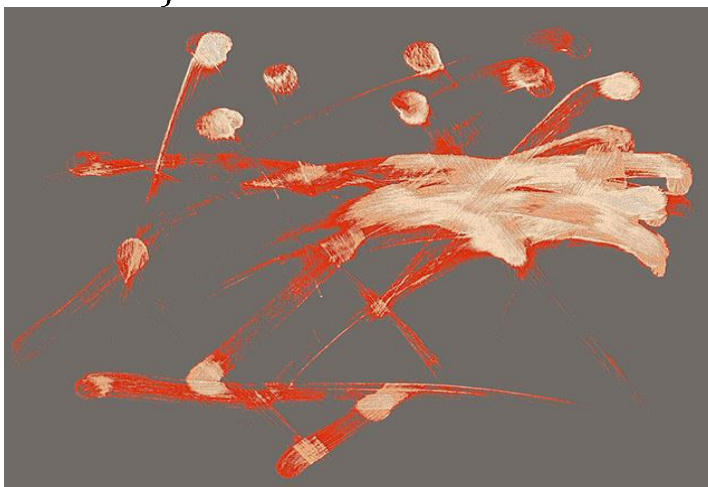
ANGRY BIRDS

- Fingers' oily smear on the screen
- Different apps gives different finger-smudges.
- Latent smudges may be usable to infer recently and frequently touched areas of the screen--a form of **information leakage**.

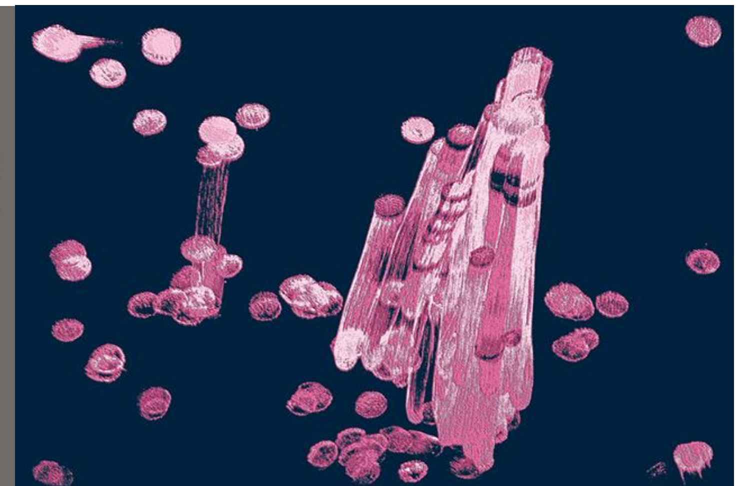
[http://www.ijsmblog.com/2011/02/ipad-finger-smudge-art.html]

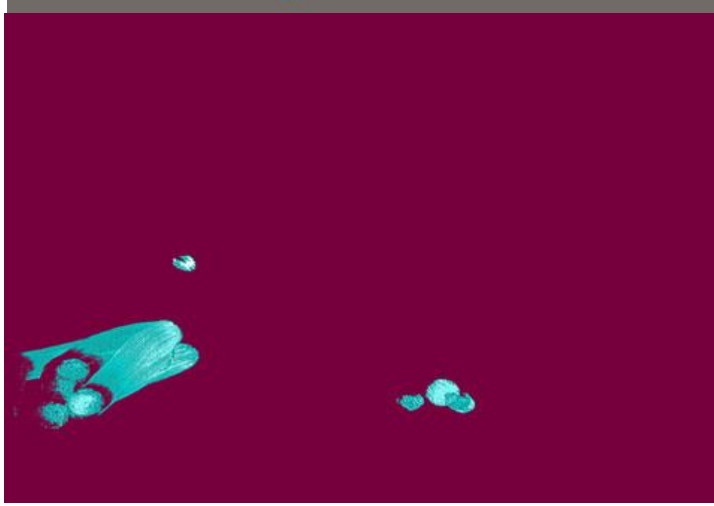
Andre Woolery Art

Fruit Ninja



Facebook





Angry Bird

Mail

For sale… Andre Woolery Art

"Untitled" Mail App Art - Polychrome

$ 34.99

TITLE Acrylic Print 30"x 40" - $ 399.99

ADD TO CART

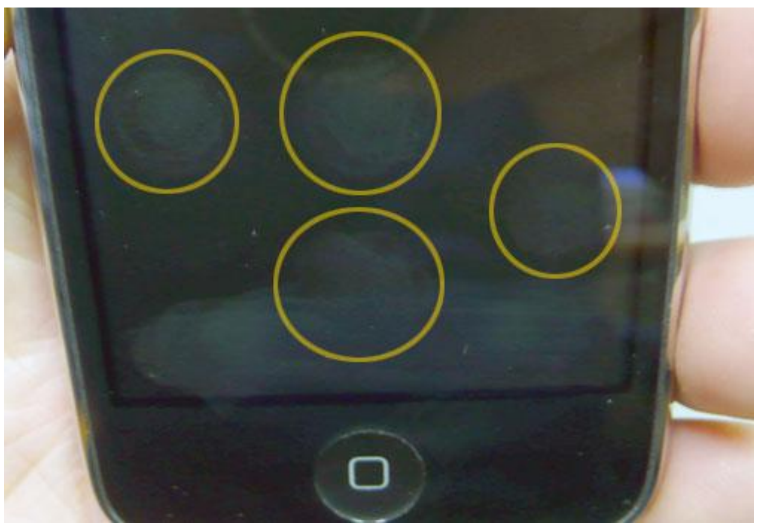
[http://www.andrewooleryart.com/collections/ipad-abstract-art/products/mail-abstract-art-polychrome]

Lockscreen PIN / Passcode

[http://lifehacker.com/5813533/why-you-should-repeat-one-digit-in-your-phones-4+digit-lockscreen-pin]

Smudge Attack

- Touchscreen smudge may give away your password/passcode
- Four distinct fingerprints reveals the four numbers used for passcode lock.



[http://www.engadget.com/2010/08/16/shocker-touchscreen-smudge-may-give-away-your-android-password/2]

Suggestion: Repeat One Digit

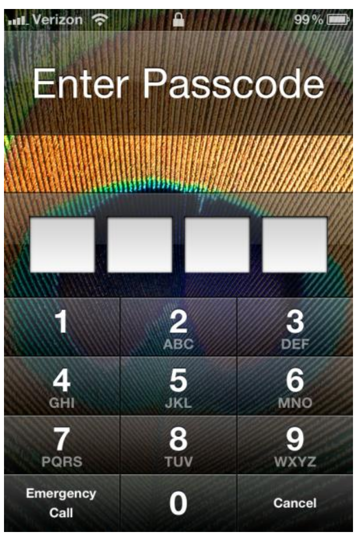
- Unknown numbers:
  - The number of 4-digit different passcodes $= 10^4$
- Exactly four different numbers:
  - The number of 4-digit different passcodes $= 4! = 24$
- Exactly three different numbers:
  - The number of 4-digit different passcodes $= 3 \times (4)_2 = 36$

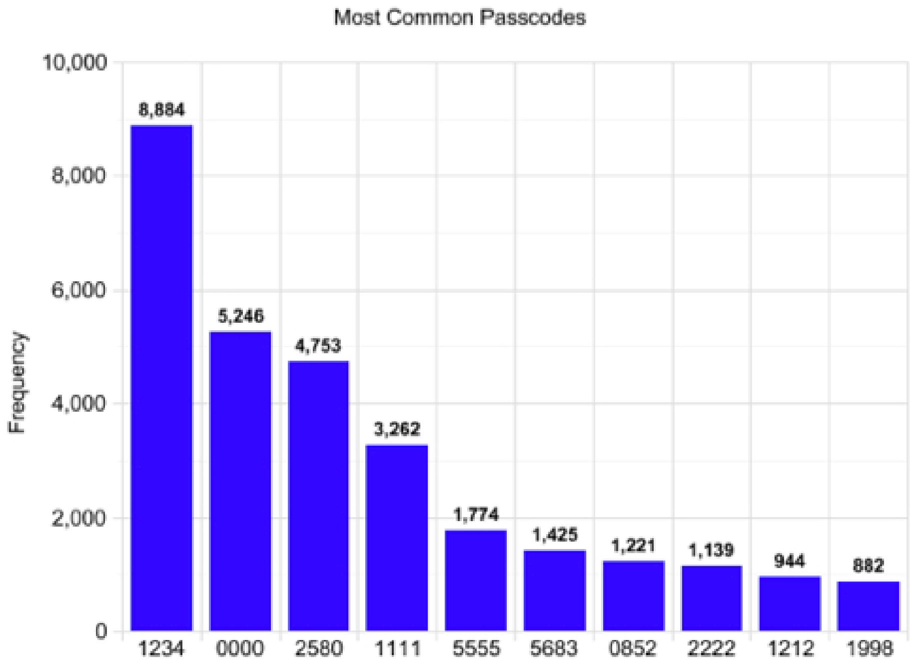
Choose the number that will be repeated

Choose the locations of the two non-repeated numbers.

News: Most Common Lockscreen PINs

- Passcodes of users of Big Brother Camera Security iPhone app
- 15% of all passcode sets were represented by only 10 different passcodes



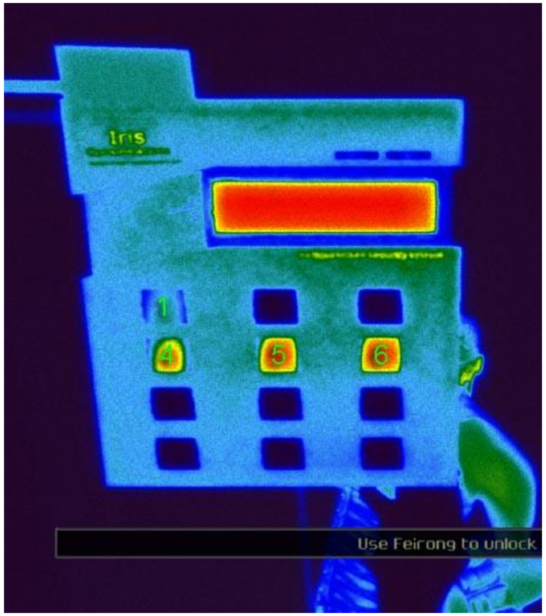


out of 204,508 recorded passcodes

[http://amitay.us/blog/files/most_common_iphone_passcodes.php (2011)]

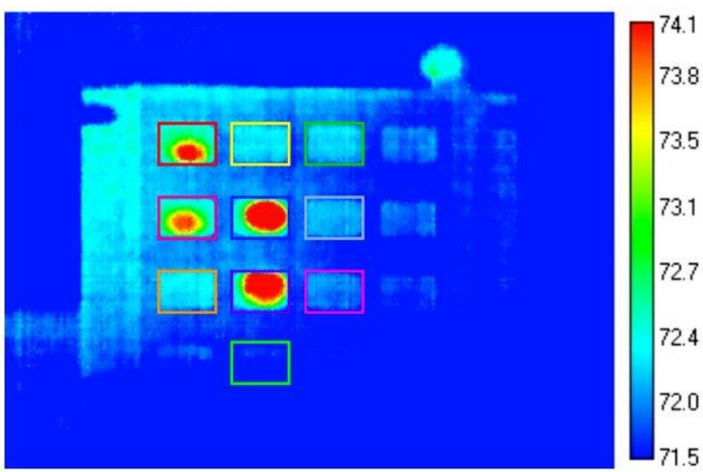
Even easier in Splinter Cell

- Decipher the keypad's code by the heat left on the buttons.
- Here's the keypad viewed with your **thermal goggles**. (Numbers added for emphasis.) Again, the stronger the signature, the more recent the keypress.
- The code is 1456.



Actual Research

- University of California San Diego
- The researchers have shown that codes can be easily discerned from quite a distance (at least seven metres away) and image-analysis software can automatically find the correct code in more than half of cases even one minute after the code has been entered.
- This figure rose to more than eighty percent if the thermal camera was used immediately after the code was entered.



K. Mowery, S. Meiklejohn, and S. Savage. 2011. "Heat of the Moment: Characterizing the Efficacy of Thermal-Camera Based Attacks". Proceedings of WOOT 2011.
http://cseweb.ucsd.edu/~kmowery/papers/thermal.pdf
http://wordpress.mrreid.org/2011/08/27/hacking-pin-pads-using-thermal-vision/

The Birthday Problem (Paradox)

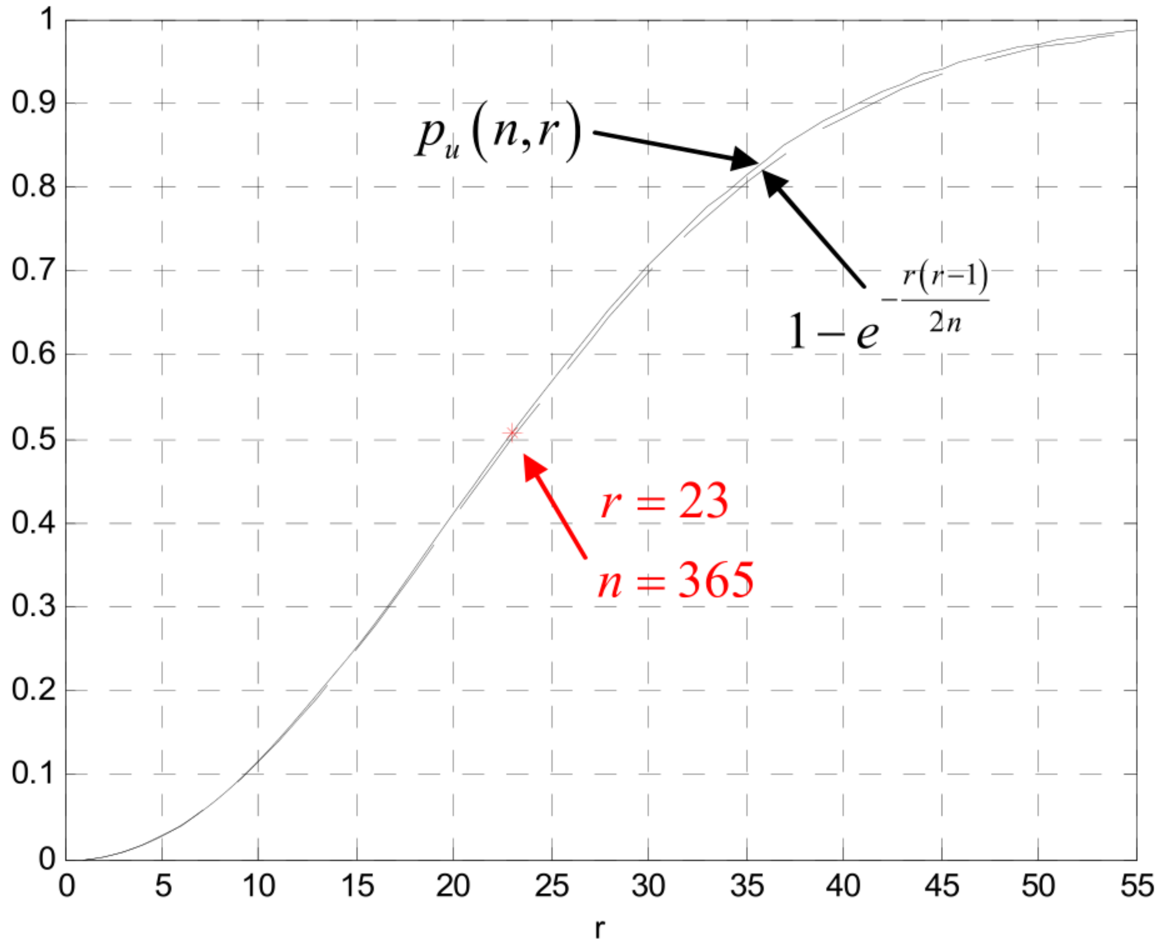
- How many people do you need to assemble before the probability is greater than 1/2 that some two of them have the same birthday (month and day)?
  - Birthdays consist of a month and a day with no year attached.
  - Ignore February 29 which only comes in leap years
  - Assume that every day is as likely as any other to be someone's birthday
- In a group of r people, what is the probability that two or more people have the same birthday?

Probability of birthday coincidence

- Probability that there is at least two people who have the same birthday in a group of *r* persons

$$= \begin{cases} 1, & \text{if } r \geq 365 \\ 1 - \left(\underbrace{\frac{365}{365} \cdot \frac{364}{365} \cdot \ldots \cdot \frac{365-(r-1)}{365}}_{r \text{ terms}} \right), & \text{if } 0 \leq r \leq 365 \end{cases}$$

Probability of birthday coincidence



The Birthday Problem (con't)

- With 88 people, the probability is greater than 1/2 of having three people with the same birthday.
- 187 people gives a probability greater than1/2 of four people having the same birthday

[Rosenhouse, 2009, p 7]

[E. H. McKinney, "Generalized Birthday Problem": *American Mathematical Monthly*, Vol. 73, No.4, 1966, pp. 385-87.]

Birthday Coincidence: 2^{nd} Version

- How many people do you need to assemble before the probability is greater than 1/2 that at least one of them have the same birthday (month and day) as you?

- In a group of *r* people, what is the probability that at least one of them have the same birthday (month and day) as you?

Distinct Passcodes (revisit)

- Unknown numbers:
  - The number of 4-digit different passcodes $= 10^4$
- Exactly four different numbers:
  - The number of 4-digit different passcodes $= 4! = 24$
- Exactly three different numbers:
  - The number of 4-digit different passcodes $= 3\times(4)_2 = 36$
- Exactly two different numbers:
  - The number of 4-digit different passcodes $= \binom{4}{3} + \binom{4}{2} + \binom{4}{1} = 14$
- Exactly one number:
  - The number of 4-digit different passcodes $= 1$
- Check:

$$\binom{10}{4} \cdot 24 + \binom{10}{3} \cdot 36 + \binom{10}{2} \cdot 14 + \binom{10}{1} \cdot 1 = 10{,}000$$

Need more practice? [http://en.wikipedia.org/wiki/Poker_probability]

Ex: Poker Probability

Hand	Frequency	Approx. Probability	Approx. Cumulative	Approx. Odds	Mathematical expression of absolute frequency
Royal flush 	4	0.000154%	0.000154%	649,739 : 1	$\binom{4}{1}$
Straight flush (excluding royal flush) 	36	0.00139%	0.00154%	72,192.33 : 1	$\binom{10}{1}\binom{4}{1} - \binom{4}{1}$
Four of a kind 	624	0.0240%	0.0256%	4,164 : 1	$\binom{13}{1}\binom{12}{1}\binom{4}{1}$
Full house 	3,744	0.144%	0.170%	693.2 : 1	$\binom{13}{1}\binom{4}{3}\binom{12}{1}\binom{4}{2}$
Flush (excluding royal flush and straight flush) 	5,108	0.197%	0.367%	507.8 : 1	$\binom{13}{5}\binom{4}{1} - \binom{10}{1}\binom{4}{1}$
Straight (excluding royal flush and straight flush) 	10,200	0.392%	0.76%	253.8 : 1	$\binom{10}{1}\binom{4}{1}^5 - \binom{10}{1}\binom{4}{1}$
Three of a kind 	54,912	2.11%	2.87%	46.3 : 1	$\binom{13}{1}\binom{4}{3}\binom{12}{2}\binom{4}{1}^2$
Two pair 	123,552	4.75%	7.62%	20.03 : 1	$\binom{13}{2}\binom{4}{2}^2\binom{11}{1}\binom{4}{1}$
One pair 	1,098,240	42.3%	49.9%	1.36 : 1	$\binom{13}{1}\binom{4}{2}\binom{12}{3}\binom{4}{1}^3$
No pair / High card 	1,302,540	50.1%	100%	.995 : 1	$\left[\binom{13}{5} - 10\right]\left[\binom{4}{1}^5 - 4\right]$
Total	**2,598,960**	**100%**	**100%**	**1 : 1**	$\binom{52}{5}$

[http://www.wolframalpha.com/input/?i=probability+of+royal+flush]

Ex: Poker Probability

WolframAlpha computational... knowledge engine

probability of royal flush

Examples Random

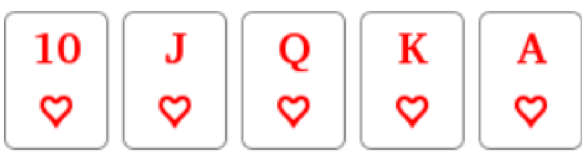
Input interpretation:

poker hand	type	royal flush

Description:

an ace-high straight flush (the 10, jack, queen, king, and ace all of the same suit)

Example of a 5-card royal flush:



Properties:

Show derivations

	number of possible hands	approximate probability	approximate chance
5-card hand	4	1.539×10^{-6}	≈ 1 in 649 740

[http://www.wolframalpha.com/input/?i=probability+of+full+house]

Ex: Poker Probability

WolframAlpha computational knowledge engine

probability of full house

Examples Random

Input interpretation:

poker hand	type	full house

Description:

three matching cards of one rank and two matching cards of another rank

Example of a 5-card full house:

3♣ 3♥ 3♦ 6♠ 6♦

Properties:

Hide derivations

	number of possible hands	approximate probability	approximate chance
5-card hand	3744	0.001441	≈ 1 in 694

[http://www.wolframalpha.com/input/?i=probability+3+queens+2+jacks&lk=3]

Ex: Poker Probability

WolframAlpha computational knowledge engine

Enter what you want to calculate or know about:

probability 3 queens 2 jacks

Examples Random

Input interpretation:

hand of cards	exactly 3 queens
	exactly 2 jacks

Distribution of hands of this type:

Show larger hands

number of cards in hand	number of hands this type	approximate probability	approximate chance
5	24	9.234×10^{-6}	≈ 1 in 108 290

Binomial Theorem

$$(x_1 + y_1)\times(x_2 + y_2)$$

$$= x_1x_2 + x_1y_2 + y_1x_2 + y_1y_2$$

$$(x_1 + y_1)\times(x_2 + y_2)\times(x_3 + y_3)$$

$$= x_1x_2x_3 + x_1x_2y_3 + x_1y_2x_3 + x_1y_2y_3 + y_1x_2x_3 + y_1x_2y_3 + y_1y_2x_3 + y_1y_2y_3$$

$$x_1 = x_2 = x_3 = x$$

$$y_1 = y_2 = y_3 = y$$

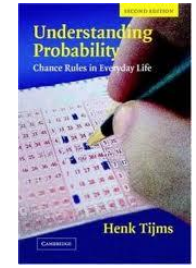
$$(x + y)\times(x + y)$$

$$= xx + xy + yx + yy = x^2 + 2xy + y^2$$

$$(x + y)\times(x + y)\times(x + y)$$

$$= xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$$

$$= x^3 + 3x^2y + 3xy^2 + y^3$$



Success Runs (1/4)

- Suppose that two people are separately asked to toss a fair coin 120 times and take note of the results. Heads is noted as a “one” and tails as a “zero”.
- Results: Two lists of compiled zeros and ones:

1 1 0 0 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 0 1 0 1 0 0 1 1 0 1 0
0 1 0 1 0 1 1 0 1 1 0 0 1 1 0 1 1 1 0 1 0 0 1 0 0 1 1 0 1 0
0 1 1 0 1 0 0 1 1 0 1 0 1 1 0 0 1 1 1 0 0 1 0 1 0 1 0 0 0 1
0 1 0 1 0 1 0 1 0 1 1 0 0 1 0 0 1 0 1 1 0 0 1 0 0 1 1 0 1 1

1 1 1 0 0 0 1 1 1 0 1 0 1 1 1 1 1 1 0 1 0 0 0 1 1 0 0 1 1 0
1 0 1 0 0 0 1 1 0 1 0 0 1 1 1 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0
0 1 1 1 0 1 1 0 0 1 1 1 1 1 1 0 1 1 0 1 0 1 1 1 0 0 0 0 0 0
0 0 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 0 1 1 0 1 1 0 1 0 1

[Tijms, 2007, p 192]

Success Runs (2/4)

- Which list is more likely?

1 1 0 0 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 0 1 0 1 0 0 1 1 0 1 0
0 1 0 1 0 1 1 0 1 1 0 0 1 1 0 1 1 1 0 1 0 0 1 0 0 1 1 0 1 0
0 1 1 0 1 0 0 1 1 0 1 0 1 1 0 0 1 1 1 0 0 1 0 1 0 1 0 0 0 1
0 1 0 1 0 1 0 1 0 1 1 0 0 1 0 0 1 0 1 1 0 0 1 0 0 1 1 0 1 1

1 1 1 0 0 0 1 1 1 0 1 0 1 1 1 1 1 1 0 1 0 0 0 1 1 0 0 1 1 0
1 0 1 0 0 0 1 1 0 1 0 0 1 1 1 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0
0 1 1 1 0 1 1 0 0 1 1 1 1 1 1 0 1 1 0 1 0 1 1 1 0 0 0 0 0 0
0 0 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 0 1 1 0 1 1 0 1 0 1

[Tijms, 2007, p 192]

Success Runs (3/4)

- Fact: One of the two individuals has cheated and has fabricated a list of numbers without having tossed the coin.
- Which list is more likely be the fabricated list?

```
1 1 0 0 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 0 1 0 1 0 0 1 1 0 1 0
0 1 0 1 0 1 1 0 1 1 0 0 1 1 0 1 1 1 0 1 0 0 1 0 0 1 1 0 1 0
0 1 1 0 1 0 0 1 1 0 1 0 1 1 0 0 1 1 1 0 0 1 0 1 0 1 0 0 0 1
0 1 0 1 0 1 0 1 0 1 1 0 0 1 0 0 1 0 1 1 0 0 1 0 0 1 1 0 1 1
```

```
1 1 1 0 0 0 1 1 1 0 1 0 1 1 1 1 1 1 0 1 0 0 0 1 1 0 0 1 1 0
1 0 1 0 0 0 1 1 0 1 0 0 1 1 1 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0
0 1 1 1 0 1 1 0 0 1 1 1 1 1 1 0 1 1 0 1 0 1 1 1 0 0 0 0 0 0
0 0 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 0 1 1 0 1 1 0 1 0 1
```

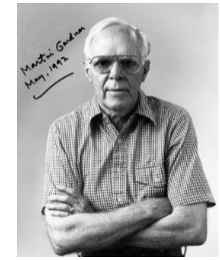

[Tijms, 2007, p 192]

Success Runs (4/4)

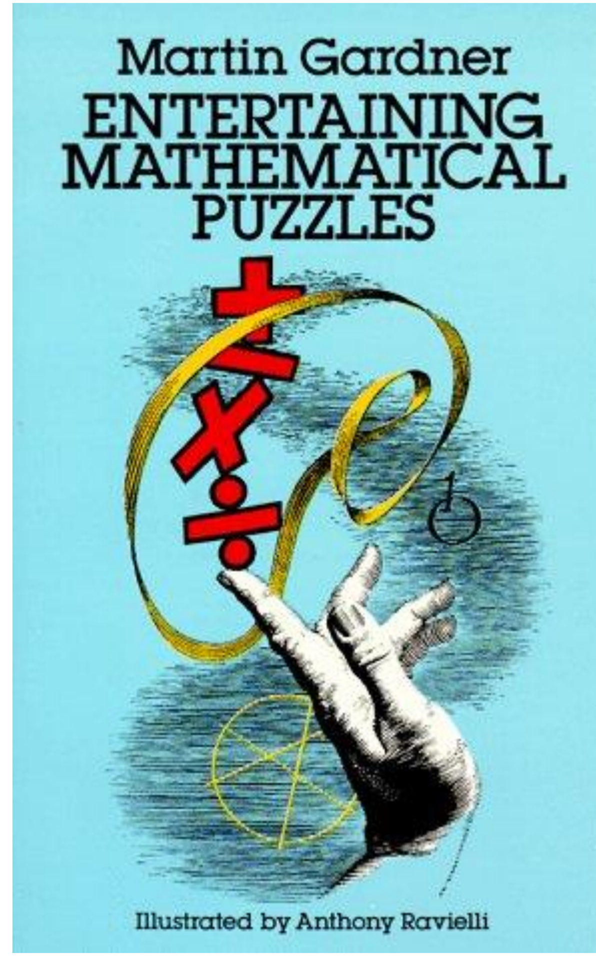
- Fact: In 120 tosses of a fair coin, there is a very large probability that at some point during the tossing process, a **sequence of five or more heads or five or more tails will naturally occur**.
    - The probability of this is approximately 0.9865.
- In contrast to the second list, the first list shows no such sequence of five heads in a row or five tails in a row. In the first list, the longest sequence of either heads or tails consists of three in a row.
- In 120 tosses of a fair coin, the probability of **the longest sequence consisting of three or less in a row** is equal to 0.000053 which is extremely small .
- Thus, the first list is almost certainly a fake.
- Most people tend to avoid noting long sequences of consecutive heads or tails. Truly random sequences do not share this human tendency!

[Tijms, 2007, p 192]

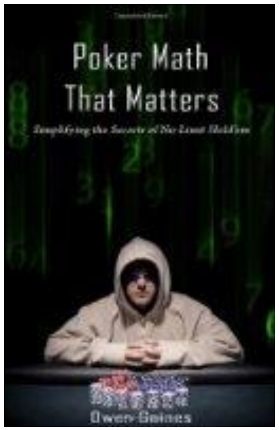
Fun Reading …

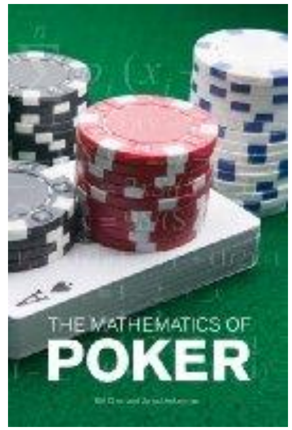


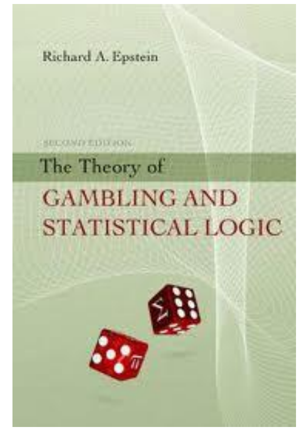
- Entertaining Mathematical Puzzles (1986)
- By Martin Gardner (1914-2010)
- It includes a mixture of old and new riddles covering a variety of mathematical topics: money, speed, plane and solid geometry, **probability (Part VII)**, topology, tricky puzzles and more.
- Carefully explained solutions follow each problem.

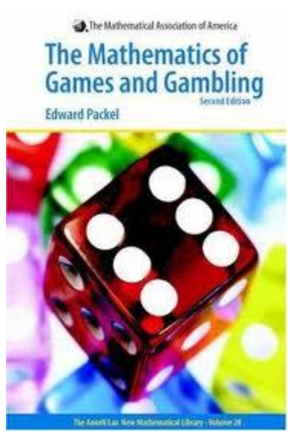


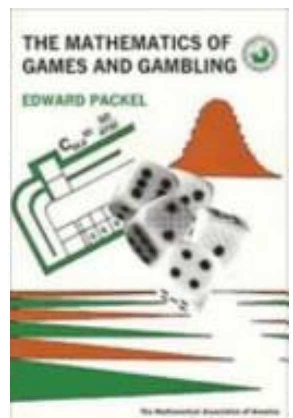
Fun Books…

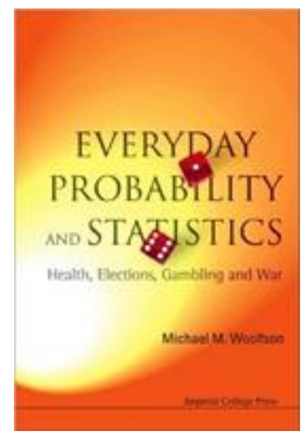

Poker Math
That Matters
Owen Gaines


THE MATHEMATICS OF
POKER


Richard A. Epstein
SECOND EDITION
The Theory of
GAMBLING AND
STATISTICAL LOGIC

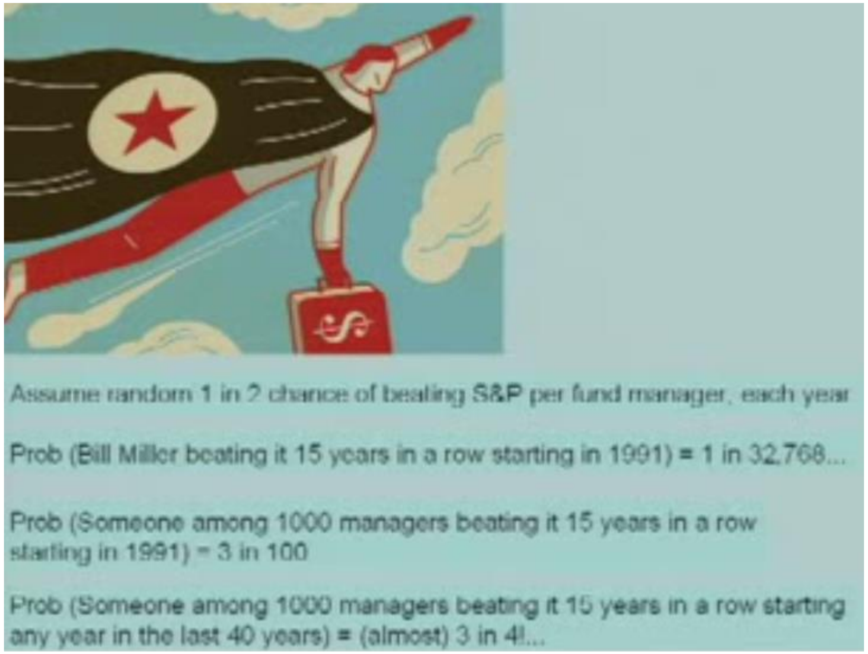

The Mathematical Association of America
The Mathematics of
Games and Gambling
Second Edition
Edward Packel


THE MATHEMATICS OF
GAMES AND GAMBLING
EDWARD PACKEL


EVERYDAY
PROBABILITY
AND STATISTICS
Health, Elections, Gambling and War
Michael M. Woolfson

Exercise from Mlodinow's talk

- At 10:14 into the video, Mlodinow shows three probabilities.
- Can you derive the first two?



- http://www.youtube.com/watch?v=F0sLuRsu1Do
- [Mlodinow, 2008, p. 180-181]