UNIVERSITY COLLEGE DUBLIN
School of Mathematical Sciences
Mathematical Enrichment Class, 9 February 2013
Professor Gary McGuire

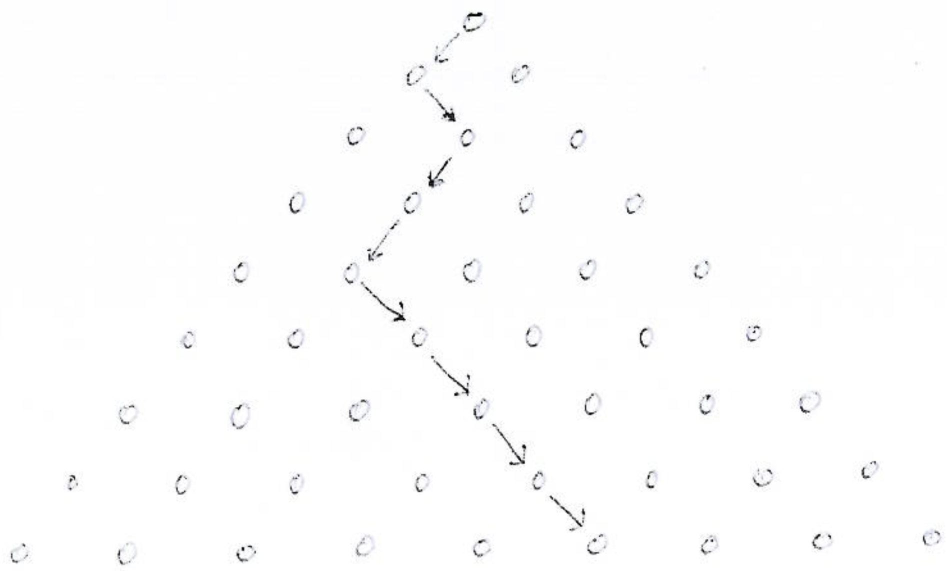
See website `www.ucd.ie/mathsciences` and click on Events and Outreach or go to `www.irmo.ie` and follow link to UCD.

1. Suppose a hacker can check 1000 passwords in one second.

How many possible passwords are there with three characters? How long will it take a hacker to check them all?

How about with eight characters? xu4dP&B(

2. How many paths are there from the top circle to any lower circle?



3. What are the chances of winning the lotto?

We can choose from

26	small letters
26	capital letters
10	digits
10	others (say)
72	

A password with two characters has $72 \times 72 = 72^2$ possibilities

$72^2 = 5184$

So it takes 5·184 seconds to try them all.

With three characters, $72^3 = 373\,248$ passwords.

About 6 minutes.

With four characters, $72^4 = 26873856$

About 7½ hours.

With eight characters, $72^8 = 722204136308736$

$\approx 7.2 \times 10^{14}$

About 10^{11} seconds

8.35×10^6 days

22,900 years.

Long passwords are much more secure

72^8 = number of ways to choose 8 characters from 72 where order matters, and they do not need to be distinct.

The number of ways of choosing k from n, where order matters and they are not distinct, is

$$n^k$$

$$\begin{array}{ccccc} A & B & A & & \\ \_\_ & \_\_ & \_\_ & \cdots & \_\_ \\ 1 & 2 & 3 & & k \end{array}$$

(n choices for each place)

If the choices must be distinct, then

$$\begin{array}{ccccc} \_\_ & \_\_ & \_\_ & \cdots & \_\_ \\ 1 & 2 & 3 & & k \\ n & n-1 & n-2 & & \\ \text{choices} & \text{choices} & \text{choices} & & \end{array}$$

$n(n-1)(n-2)\cdots(n-k+1)$ ways of choosing k from n (order matters, choices distinct)

Suppose $k=n$.

$$n(n-1)(n-2)(n-3)\cdots(3)(2)(1) \text{ ways of ordering } n \text{ things.}$$

$$\parallel$$

$$n!$$

e.g. $n=3$

123
132
213
231
312
321

$3! = (3)(2)(1) = 6$

How many ways are there of choosing a captain and vice-captain from a team of 11 people?

$11 \cdot 10 = 110$

In how many ways can you re-arrange the letters of the word RANDOM ?

$$6! = (6)(5)(4)(3)(2)(1)$$
$$= 720$$

What about SCHOOL ?

$$\frac{1}{2} 6!$$

What about CARAVAN ?

NVAACAR

$$\frac{7!}{3!}$$

Consider a set with n elements.

How many subsets of size k are there?

$n = 1$

$k=0$	$k=1$
1	1

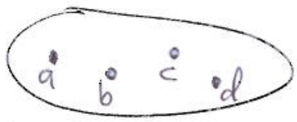
$n = 2$

$k=0$	$k=1$	$k=2$
1	2	1

$n = 3$

$k=0$	$k=1$	$k=2$	$k=3$
1	3	3	1

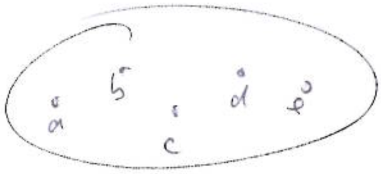
$n=4$



$k=0$	$k=1$	$k=2$	$k=3$	$k=4$
1	4	6	4	1

ab bc abc
ac bd abd
ad cd acd
bcd

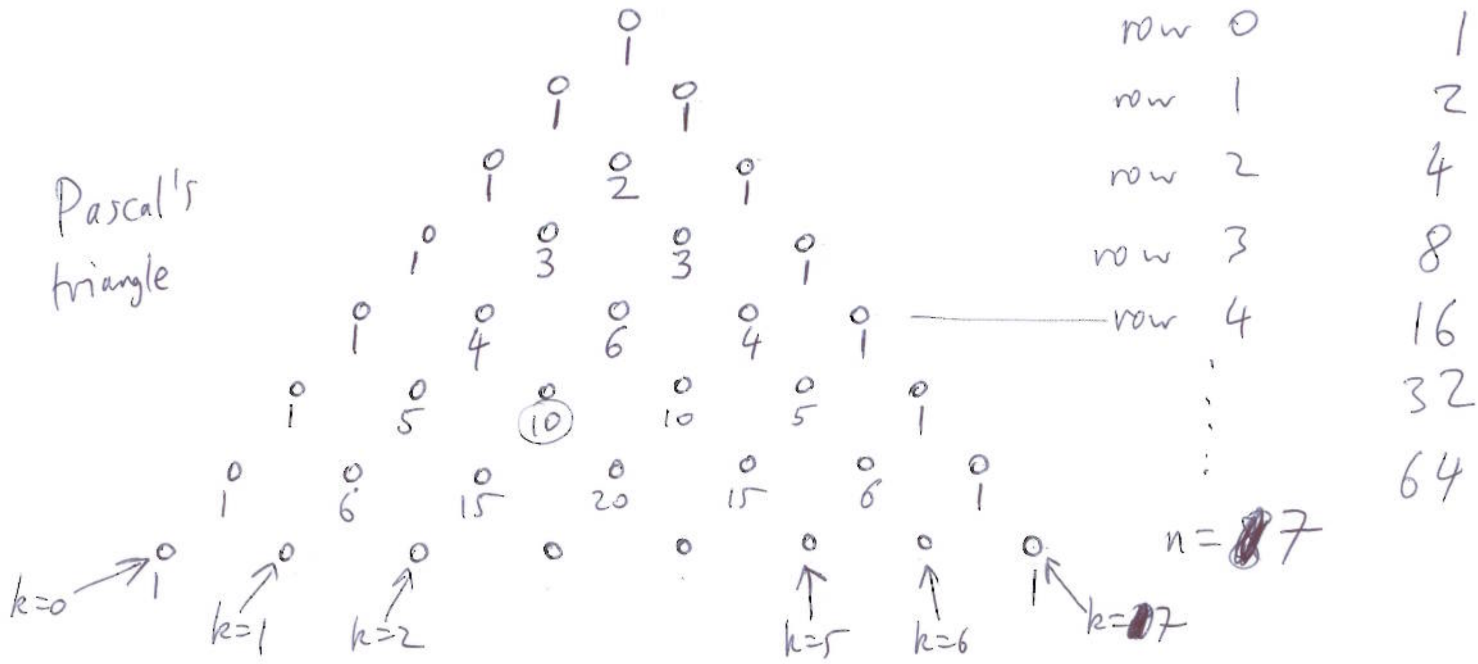
$n=5$



1 5 10 10 5 1

ab

$\binom{n}{k}$ = number of ways of choosing k from n, where order does not matter, repetition not allowed (choices are distinct)



Let $\binom{n}{k}$ denote the number of paths from the top to the k-th circle in the n-th row.

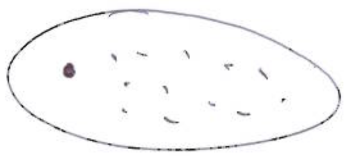
$$\binom{n}{k} = \binom{n}{n-k}$$ symmetry

① $$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

② $$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

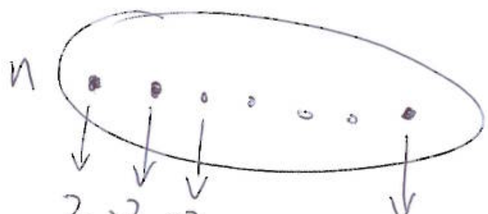
---

①



$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}.$$

②



$$2 \cdot 2 \cdot 2 \cdots\cdots \cdot 2 = 2^n$$

Total number of subsets