3.6 (a) $1+2+\cdots+m = m(m+1)/2$ (i)

We know $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

$$= \frac{n\cdot(n-1)\cdot(n-2)\cdots(n-k+1)}{k\cdot(k-1)\,(k-2)\cdots 1} \quad \text{(ii)}$$

We should specify k and n make sure (i) = (ii)

It can be easily derived that $k=2$, since

$$2\cdot(2-1) = 2$$

If $k=2$, the numerator of (ii) becomes

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

To guarantee $m\cdot(m+1) = n\cdot(n-1)$ we should have

$$n = m+1$$

Therefore $1+2+\cdots n = \frac{n(n+1)}{2} = \binom{n+1}{2}$

(b)

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5}
\end{array}$$

Assume $n=4$. we have

$1+2+3+4 = 10 = \binom{n+1}{2} = \binom{5}{2}$

As the Pascal's triangle shows, we can easily prove the above argument is true.

3.8. (a) $4^2 = (1+1+1+1)^2$

$$= \binom{2}{2,0,0,0} 1^2 1^0 1^0 1^0 + \binom{2}{0,2,0,0} 1^0 1^2 1^0 1^0 + \binom{2}{0,0,2,0} 1^0 1^0 1^2 1^0 +$$

$$\binom{2}{0,0,0,2} 1^0 1^0 1^0 1^2 + \binom{2}{1,1,0,0} 1^1 1^1 1^0 1^0 + \binom{2}{1,0,1,0} 1^1 1^0 1^1 1^0 + \binom{2}{1,0,0,1} 1^1 1^0 1^0 1^1 +$$

$$\binom{2}{0,1,1,0} 1^0 1^1 1^1 1^0 + \binom{2}{0,1,0,1} 1^0 1^1 1^0 1^1 + \binom{2}{0,0,1,1} 1^0 1^0 1^1 1^1$$

$$= 1+1+1+1+2+2+2+2+2+2 = 16$$

(b) $4^2 = (2+1+1)^2$

$$= \binom{2}{2,0,0} 2^2 1^0 1^0 + \binom{2}{0,2,0} 2^0 1^2 1^0 + \binom{2}{0,0,2} 2^0 1^0 1^2 +$$

$$\binom{2}{1,0,1} 2^1 1^0 1^1 + \binom{2}{0,1,1} 2^0 1^1 1^1 + \binom{2}{1,1,0} 2^1 1^1 1^0$$

$$= 4 + 1 + 1 + 2\cdot 2 + 2\cdot 1 + 2\cdot 2$$

$$= 4 + 1 + 1 + 4 + 2 + 4$$

$$= 16$$

3.11. Based on the definition of birthday attack (P.61)

We know $n = 2^b$ and $k \approx \sqrt{n}$

| b. | n. | k | time |
|---|---|---|---|
| 32 | $2^{32}$ | $2^{16}$ | $2^{16}/10^{15} = 6.5\times10^{-11}$ s |
| 64 | $2^{64}$ | $2^{32}$ | $2^{32}/10^{15} = 4.3\times10^{-6}$ s |
| 128 | $2^{128}$ | $2^{64}$ | $2^{64}/10^{15} = 1.8\times10^{4}$ s $\approx$ 5 hours |
| 256 | $2^{256}$ | $2^{128}$ | $2^{128}/10^{15} = 3.4\times10^{23}$ s $\approx 10^{16}$ years |

Morover, we know one million computers can generate

$10^6 \cdot 10^9 = 10^{15}$ contracts per seconds.

Therefore, time $= k/10^{15}$

3.14 $n = 669$. using the approximation (13.18)

$$q(k) \approx \exp\left(-\frac{k(k-1)}{2n}\right) < 0.5$$

We can find that when $k = 31$.

$$\exp\left(-\frac{31\times30}{2\times669}\right) = 0.4990 < 0.5$$

Therefore. 31 people need to be in a room for it to be likely at least two of them have the same birthday on Mars.

3.21. (a). Based on differential calculus, we have

$$f'(x) = \frac{\partial f(x)}{\partial x} = \frac{\partial(x - \log(1+x))}{\partial x}$$

$$= \frac{\partial x}{\partial x} - \frac{\partial[\log(1+x)]}{\partial x}$$

$$= 1 - \frac{1}{1+x}$$

Let $f'(x) = 0$, we have $1 - \frac{1}{1+x} = 0 \Rightarrow x = 0$

Therefore $x = 0$ is a possible minimum of $f(x)$

(b) $f(0) = 0 - \log(1+x) = 0$

$$f(1) = 1 - \log(1+1) = \log e - \log(2)$$

$$= \log\left(\frac{e}{2}\right)$$

Since $e/2 > 1$, $\log\left(\frac{e}{2}\right) > 0$

Therefore $f(1) > 0 = f(0)$, $x = 0$ is a minimum.

3.22. (a) Let's consider the complementary event $A$:

how many people are required for it to be likely that no one has the same birthday as you do?

Assuming there are $k$ people, the probability of one person has different birthday as yours is $\frac{364}{365}$

Therefore $P(A) = \left(\frac{364}{365}\right)^k \geq 0.5$

We can derive that $k \cdot \log\left(\frac{364}{365}\right) \geq \log\frac{1}{2}$

Such that $k \leq \log\frac{1}{2} / \log\left(\frac{364}{365}\right)$

$k \leq 252.7$

Therefore, we require 253 people to satisfy that it to be likely that someone has the same birthday as yours, namely. $P(\bar{A}) = 1 - \left(\frac{364}{365}\right)^k \geq 0.5$

(b) We know $P(A) = \left(\frac{364}{365}\right)^k$

$$q(k) = \frac{(365)_k}{(365)^k} \quad (P_{58}.\ \text{Formula } 3.16)$$

3.28 (a). Chose one number Via throwing a dice,

this event has 6 outcomes.

Divide the five dice into one group including all the five dice : $\binom{5}{5} = 1$

A: all five dice showing the same number has $(6)_1 \binom{5}{5} = 6$ cases

$P(A) = \frac{6}{6^5}$

(b) Divide the five dice into two groups, one group has 4 dice and another one has 1 dice.

$\binom{5}{4\ 1} = \frac{5!}{4!\,1!} = 5$

Choosing two orderd numbers via throwing two dice has $(6)_2 = 6 \cdot 5 = 30$ outcomes

$P(B) = \frac{(6)_2 \binom{5}{4\ 1}}{6^5} = \frac{150}{300}$

(c) Similiar as (b)

$P(C) = \frac{(6)_2 \binom{5}{3\ 2}}{6^5} = \frac{300}{6^5}$

(d) Divide the five dice into three groups. one group has 3 dice, one group has 1 dice. and the last group has 1 dice. We have $\binom{5}{3\ 1.1}$ cases

Choosing one number via throwing a dice has 6 outcomes

Choosing two numbers from the left 5 numbers has $\binom{5}{2}$ outcomes.

Therefore, we have $\binom{6}{1}\cdot\binom{5}{2}$ outcomes.

$$P(D) = \frac{\binom{6}{1}\binom{5}{2}\binom{5}{3.1.1}}{6^5} = \frac{6\cdot 10\cdot 20}{6^5} = \frac{1200}{6^5}$$

In particular, the two numbers chosen from the left 5 numbers do not in an order way. For example

$6\ 6\ 6\ \underline{2}\ \underline{3}$
$6\ 6\ 6\ \underline{3}\ \underline{2}$ are the same outcome for the event in this question.

(e) Similiarly, we have $P(E) = \frac{\binom{6}{1}\binom{5}{2}\binom{5}{2.2\ 1}}{6^5}$

$$= \frac{6.\ 10.\ 30}{6^5} = \frac{1800}{6^5}$$

(f) Since we have 5 dice, we don't need separate the dice any more. Therefore

$$P(F) = \frac{\binom{6}{1}\binom{5}{1}\binom{4}{1}\binom{3}{1}\binom{2}{1}}{6^5} = \frac{6\cdot5\cdot4\cdot3\cdot2}{6^5} = \frac{720}{6^5}$$

(g). The missing part is two dice show one number and the left 3 dice show 3 different numbers

$$P(G) = \frac{\binom{6}{1}\binom{5}{3}\binom{5}{2,1,1,1}}{6^5} = \frac{6\cdot10\cdot60}{6^5}$$

$$= \frac{3600}{6^5}$$

We can find that

$$P(A) + P(B) + P(C) + P(D) + P(E) + P(F) + P(G)$$

$$= \frac{6 + 150 + 300 + 1200 + 1800 + 720 + 3600}{6^5}$$

$$= 1$$

3.34 $\Pr[\text{blackjack}] = \dfrac{\binom{4}{1}\binom{16}{1}}{\binom{52}{2}} =$ **64/1326 = 32/663**

3.35 (a) $\Pr[\text{three of a kind}] = \dfrac{\binom{13}{1}\binom{4}{3}}{\binom{52}{3}} = \dfrac{52}{\binom{52}{3}}$

(b) $\Pr[\text{a pair and one other card}] = \dfrac{(13)_2\binom{4}{2}\binom{4}{1}\binom{44}{0}}{\binom{52}{3}} = \dfrac{3744}{\binom{52}{3}}$

(c) $\Pr[\text{three cards of different rank}] = \dfrac{\binom{13}{3}\binom{4}{1}\binom{4}{1}\binom{4}{1}\binom{40}{0}}{\binom{52}{3}} = \dfrac{18304}{\binom{52}{3}}$

(d) $52 + 3744 + 18304 = 22100$

$\binom{52}{3} = 22100$

Therefore the tree probabilities above sum to 1

## Solution to Problem 3.44

a) The first wire can be placed in $\binom{26}{2}$ ways. The second wire can be placed in $\binom{24}{2}$ ways, etc. The wires are interchangeable. There are $k!$ orderings of the wires. Thus, the number of ways $k$ wires can be placed is

$$\frac{\prod_{m=0}^{k-1}\binom{26-2m}{2}}{k!}$$

For $k = 10$, the number of ways is $1.51 \times 10^{14}$.

b) Take the inputs in order from A to Z. Input A can be connected to 26 possible outputs. Input B can then be connected to 25 possible outputs. Continuing this pattern, the number of possible rotors is $26! = 4.03 \times 10^{26}$.

c) Since the rotors were different, three rotors could be built in $26!(26!-1)(26!-2) = 6.56 \times 10^{79}$ ways.

d) Each rotor could be placed in one of 26 positions. Therefore the three rotors could be placed in $26^3 = 17576$ ways.

e) The left rotor's ring could be placed in 26 positions. The middle rotor's ring could be placed in 26 positions. Therefore, the two rotors could be placed in $26^2 = 676$ ways.

f) Using the plugboard solution for $k = 13$, the number of reflectors is

$$\frac{\prod_{m=0}^{12}\binom{26-2m}{2}}{13!} = 7.91 \times 10^{12}$$

g) The total number of Enigma configurations with $k = 10$ wires is

$$26!(26!-1)(26!-2)26^3 26^2 \frac{\prod_{m=0}^{9}\binom{26-2m}{2}}{10!}\frac{\prod_{m=0}^{12}\binom{26-2m}{2}}{13!} = 9.31 \times 10^{113}$$

This is a very large number, approximately $2^{378}$, large even for today's cryptosystems.

h) Since order mattered, three rotors can be placed in $5 \cdot 4 \cdot 3 = 60$ ways.

i) After learning the wiring of the rotors and the wiring of the plugboard, the number of unknown configurations was reduced to

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 26^2 \cdot 1.51 \times 10^{14} = 1.08 \times 10^{23}$$

j) After capturing the Enigma machines, the number of unknown configurations was reduced by a factor of approximately $10^{90}$. The number of remaining configurations, $10^{23}$, was a much more manageable number. Capturing Enigma machines was extremely important.