# 1 Counting

### Useful formulas.

$$a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}$$
$$a + (a + d) + \cdots + (a + nd) = \frac{(n+1)(a + a + nd)}{2}$$
$${}^nP_k = \frac{n!}{(n-k)!}$$
$$\binom{n}{k} = {}^nC_k = \frac{n!}{k!(n-k)!}$$
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

# 2 Graphing

### Definitions.

**Tree.** graph with no cycle, **Leaf.** vertex with degree 1.
**Weight of graph.** sum of weights of all its edges.
**Spanning tree.** subgraph that is a tree and contains *all* vertices of original graph.

### Theorems.

**Degree Theorem.**In any graph, sum of degrees = 2× no. edges.
**Leaf Lemma.** Every tree with $\geq 2$ vertices has $\geq 2$ leaves (deg1 vertices).
**Tree Theorem.** Every tree with $n$ vertices has exactly $n - 1$ edges.
**Euler Walk Theorem I.** A connected graph contains a closed Euler walk iff every vertex has an even degree.
<u>directed version.</u> iff for every vertex the no. arrows in = no. arrows out.
**Euler Walk Theorem II.** A connected graph contains an open Euler walk iff
(i) start/end vertices have odd degree; and
(ii) all other vertices have even degree.
<u>directed version.</u> iff
(i) for start vertex, no. arrows out exactly one more than no. arrows in;
(ii) for end vertex, no. arrows in exactly one more than no. arrows out;
(iii) for all other vertices no. arrows in = no. arrows out.

### Prim's Algorithm

1. Choose any vertex to initalise tree.
2. Grow the tree by one edge: of all edges that connect to vertices not yet in tree, find one with minimum-weight and add it in tree.
3. Repeat step 2 until tree spans.

### Finding Euler circuit.

1. Check all vertices are even.
2. Construct any cycle.
3. If there's still remaining unused edges, construct cycle with those and combine the cycles.
4. Repeat step 3 until all edges used.

### Chinese Postman Problem (Choosing edges to repeat)

1. Enumerate all pairings of odd vertices.
2. For each pair, find paths that join the vertices with minimum weight.
3. Use the set of pairings which sum of weights is minimised.
4. Walk the edges found above twice.

**Vertex colouring** If graph $G$ contains a complete graph on $n$ vertices, then $\chi(G) \geq n$.
Upper bound. Arrange degrees in decreasing order, place integers $1, 2, 3, \ldots$ below the degrees until you reach integer $k$ such that $k + 1 > d_{k+1}$, then $\chi(G) \leq k + 1$.

# 3 Clocking

**Congruence properties** If $a \equiv b \pmod{m}$, then I can

- add multiples of modulo $m$ to any side
- multiply by integers
- exponentiate both sides with positive powers only
- two congruences with the same modulo can be added/multiplied with each other

### Calendrical Knowledge

YYYY is a leap year iff

- it is not a century year and divisible by 4 (1996); or
- it is a century year and divisible by 400 (2000).

Calendar (mod 7)

| Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | 28/29 | 31 | 30 | 31 | 30 | 31 | 31 | 30 | 31 | 30 | 31 |
| 3 | 0/1 | 3 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 2 | 3 |

## 4 Coding

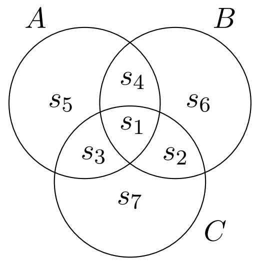
**Binary representation.** Divide by 2 and write it **right-to-left**.

| bin | oct | hex | bin | hex |
|---|---|---|---|---|
| 0 | 0 | 0 | 1000 | 8 |
| 1 | 1 | 1 | 1001 | 9 |
| 10 | 2 | 2 | 1010 | A |
| 11 | 3 | 3 | 1011 | B |
| 100 | 4 | 4 | 1100 | C |
| 101 | 5 | 5 | 1101 | D |
| 110 | 6 | 6 | 1110 | E |
| 111 | 7 | 7 | 1111 | F |

**Modulo 37 encoding and ECC.** 0-9 becomes 0-9 and _(space) is 36, and

| sym | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| num | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| sym | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| num | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

**Weighted sum** $w = 1(\text{last char}) + 2(\text{second last char}) + \cdots + n(\text{first char})$, and for modulo 37 encoding, append a checksum char such that $w \equiv 0 \pmod{37}$.




**ISBN.** 10 digits, X in last digit means 10, and a valid ISBN will have $w \equiv 0 \pmod{11}$.

**Hamming $(7,4)$ and $(8,4)$ Codes.** Every circle has even parity. In $(8,4)$, $s_8$ keeps total parity even.

## 5 Cryptography

**Affine Cryptosystems** with modulo $n$, $(a,b)$ is the encryption key
encrypt: $y \equiv ax + b \pmod{n}$
decrypt: $y \equiv a'x - a'b \pmod{n}$ where $a'$ is $a$ inverse modulo $n$.

**Finding modulo Inverse.** Use Euclid $a = qd + r$, $\gcd(a,d) = \gcd(d,r)$.

**Modular exponentiation.** Finding $a^n \pmod{m}$. Express $n$ as multiples(usually binary), then split $a^n$ and find remainder for each term.

**RSA.** $p, q$ are 2 primes, $n = pq$, $k$ is an integer that has an inverse $\pmod{(p-1)(q-1)}$.

- Let $P$ be a chunk of plaintext such that $0 \le P < n$.
- $j$ is inverse of $k$ mod $(p-1)(q-1)$, $kj \equiv 1 \pmod{(p-1)(q-1)}$
- Public key is $(n, k)$. Private key is $(j)$.
- Procedure encrypt: $C \equiv P^k \pmod{n}$.
- Procedure decrypt: $P \equiv C^j \pmod{n}$.

## 6 Chancing

**Probability.** With event $E$ and sample space $S$, $\mathbb{P}(E) = \dfrac{|E|}{|S|}$.

**Independence.** characterising property: $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$ where $A, B$ are events.

**Conditional Probability.** $\mathbb{P}(A \mid B) = \dfrac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$.

**Binomial distribution.** For $n$ independent events each with probability $p$,

$$X \sim B(n,p) \iff \mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k} \text{ and } \mathbb{E}[X] = np$$

**Expectation.** $\mathbb{E}[X] = \sum_x x \cdot \mathbb{P}(X = x)$ iterated through all possible values for $x$.

Expectation is linear so suppose total winnings $X = X_1 + \cdots + X_k$, then

$$\mathbb{E}[X] = \mathbb{E}[X_1] + \cdots + \mathbb{E}[X_k].$$

**Poisson Distribution** For Binomial distribution with large $N$ and moderate $\mathbb{E}[X] = c = Np$, then

$$\mathbb{P}(X = k) \approx \frac{e^{-c} c^k}{k!}$$