Set

Injectivity:

$(\forall x, y \in A)[f(x) = f(y) \Rightarrow x = y]$

Surjectivity:

$(\forall b \in B)(\exists a \in A)[f(a) = b]$

Bijectivity:

1. Invertible
2. Injective + Surjective
3. Cardinality. I.e.: $|A| = |B|$

Countable:

f: N -> S => S is countable

Mod

1. a|b, a|c => a|(a+c)
2. a|b => a|bc
3. a|b, b|c => a|c
4. a|b, a|c => a|(mb + nc)

$a \bmod m = a+km \bmod m$

$(a \bmod mn) \bmod n = a \bmod n$

$(a+b \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

$(a+b) \bmod m = (a + (b \bmod m)) \bmod m$

$(a+b) \bmod m = ((a \bmod m) + b) \bmod m$

$(a \cdot b) \bmod m = (a \cdot (b \bmod m)) \bmod m$

$(a \cdot b) \bmod m = ((a \bmod m) \cdot b) \bmod m$

Associativity: If a, b, and c belong to $\mathbf{Z}_m$, then

$(a +_m b) +_m c = a +_m (b +_m c)$

$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutativity: If a and b belong to $\mathbf{Z}_m$, then

$a +_m b = b +_m a$

$a \cdot_m b = b \cdot_m a$

Distributivity: If a, b, and c belong to Z_m , then

$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

Associativity:

$(a+b) + c \equiv a + (b+c) \pmod m$

$(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod m$

Commutativity:

$a+b \equiv b+a \pmod m$

$a \cdot b \equiv b \cdot a \pmod m$

Distributivity:

$a(b+c) \equiv ab+ac \pmod m$

If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

$a + c \equiv b + d \pmod m$

$a - c \equiv b - d \pmod m$

$ac \equiv bd \bmod m$

If $a \equiv b \bmod m$, then for any $c \in \mathbf{Z}$,

$a+c \equiv b+c \bmod m$

$a-c \equiv b-c \bmod m$

$ac \equiv bc \pmod m$

GCD

Euclidean Algorithm

$a = bq + r$

gcd(a,b) = gcd(b,r) until r = 0

Fot gcd(a,m) = sa + tm = 1 => tb = 0 (mod m)

$(s \bmod m) \cdot_m a = 1$ => s mod m is inverse of a in Z_m

CRT:

x = a (mod m)
M = product of m_i
$M_i = M / m_i$
$y_i = M_i \pmod{m_i}$
x = (sum of $a_i M_i y_i$) mod M

RSA

(n, e) public key
(p, q) private key
N = pq
E = (p-1)(q-1)

(d) inverse of e
$(de) \equiv 1 \pmod{(p-1)(q-1)}$

$C = x^e \bmod n$
$C^d = (x^e)^d = x^{ed} = x \pmod n$

$a^{p-1} = 1 \pmod p$

Counting

	With repetition	Without repetition
Combinations	${}^{n}C_r = \frac{(n+r-1)!}{r!(n-1)!}$	${}^{n}C_r = \frac{n!}{r!(n-r)!}$
Permutations	${}^{n}P_r = n^r$	${}^{n}P_r = \frac{n!}{(n-r)!}$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

Let n and k be integers with $0 < k < n$. Then,

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

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r} \binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \binom{n}{k}$$

Inclusion-Excludsion

$$|A_1 \cup A_2 \cup \cdots \cup A_n| =$$

$$\sum_{1 \le i \le n} |A_i| - \sum_{1 \le i \le j \le n} |A_i \cap A_j| +$$

$$\sum_{1 \le i \le j \le k \le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$$

$$p(E \cap F) = p(F)p(E|F)$$

The events are mutually independent if

$$p(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_m}) = p(E_{i_1})p(E_{i_2}) \cdots p(E_{i_m})$$

$$p(E|F) = \frac{p(E \cap F)}{p(F)}$$

If X and Y are two independent random variables on a sample space S, then

$$V(X+Y) = V(X) + V(Y)$$

Let X be the number of successes in n independent Bernoulli trials, with probability of success p and probability of failure $q = 1 - p$. Then

$$p(X = k) = b(k{:}\, n, p) = C(n,k)p^k q^{n-k}$$

$$\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} = (p+q)^n = 1$$

$$p(E_1 \cap E_2 \cap \cdots \cap E_n) =$$
$$p(E_1)p(E_2|E_1)p(E_3|E_1 \cap E_2) \cdots p(E_n|E_1 \cap E_2 \cap \cdots \cap E_{n-1})$$

The independence condition can be rewritten as

$$p(E|F) = p(E)$$

Suppose that E and F are events from a sample space S such that $p(E) \neq 0$ and $p(F) \neq 0$. Then:

$$p(F|E) = \frac{p(E|F)p(F)}{p(E|F)p(F) + p(E|\overline{F})p(\overline{F})}$$

Suppose that E is an event from a sample space S and that $F_1, F_2, \ldots, F_n$ are mutually exclusive events such that $\cup_{i=1}^{n} F_i = S$. Assume that $p(E) \neq 0$ and $p(F_i) \neq 0$ for $i = 1, 2, \ldots, n$. Then

$$p(F_j|E) = \frac{p(E|F_j)p(F_j)}{\sum_{i=1}^{n} p(E|F_i)p(F_i)}.$$

$$E(X) = \sum_{x \in S} p(s)X(s) \qquad E(X) = \sum_{r \in X(S)} p(X = r)r$$

$$V(X) = E(X^2) - E(X)^2 = \sum_{s \in S} (X(s) - E(X))^2 p(s) = E\left((X - E(X))^2\right)$$