p	q	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Order of operations:

$\sim$ not — Performed first

$\wedge$ and, $\vee$ or — Coequal in order

$\to$ if-then/implies, $\leftrightarrow$ if and only if — Coequal in order — Performed last

Theorem 2.1.1 Logical Equivalences			
Given any statement variables *p*, *q* and *r*, a tautology **true** and a contradiction **false**:			
1	Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2	Associative laws (same connector)	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3	Distributive laws (2 diff connectors)	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4	Identity laws	$p \wedge$ **true** $\equiv p$	$p \vee$ **false** $\equiv p$
5	Negation laws	$p \vee \sim p \equiv$ **true**	$p \wedge \sim p \equiv$ **false**
6	Double negative law	$\sim(\sim p) \equiv p$	
7	Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
8	Universal bound laws	$p \vee$ **true** $\equiv$ **true**	$p \wedge$ **false** $\equiv$ **false**
9	De Morgan's laws	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10	Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11	Negation of **true** and **false**	$\sim$**true** $\equiv$ **false**	$\sim$**false** $\equiv$ **true**

Conditional Statements	
Implication Law	$p \to q \equiv \boldsymbol{\sim p \vee q}$
	$\boldsymbol{\sim(p \to q) \equiv p \wedge \sim q}$
Contrapositive	$p \to q \equiv \sim q \to \sim p$
	$\forall x \in D\ (P(x) \to Q(x)) \equiv \forall x \in D\ (\sim Q(x) \to \sim P(x))$
Converse and Inverse of p → q	$q \to p \equiv \sim p \to \sim q$ (converse) (inverse)

	$p \to q$ is NOT $\equiv q \to p$
	$\forall x \in D\ (Q(x) \to P(x)) \equiv \forall x \in D\ (\sim P(x) \to \sim Q(x))$
Sufficient Condition (*r* is a sufficient condition for *s*, *r* only if *s*)	r → s
	$\forall x\ (r(x) \to s(x))$
Necessary Condition	s → r
	$\forall x\ (s(x) \to r(x))$
	~r → ~s (contrapositive)
	$\forall x\ (\sim r(x) \to \sim s(x))$

Universal Condition Statement	$\forall\ x\ (P(x) \to Q(x)) \equiv P(x) \Rightarrow Q(x)$ [every element in the truth set of P(x) is in the truth set of Q(x)]
	$\forall x\ (P(x) \leftrightarrow Q(x)) \equiv P(x) \Leftrightarrow Q(x)$ [identical truth sets]
Equivalent form of universal statement	$\boldsymbol{\forall\ x \in U\ (P(x) \to Q(x)) \equiv \forall x \in D,\ Q(x)}$
	$\forall\ x \in D,\ Q(x) \equiv Q(x_1) \wedge Q(x_2) \wedge \ldots \wedge Q(x_n)$
Equivalent form of existential statement	**$\exists\ x$ s.t. $(P(x) \wedge Q(x)) \equiv \exists\ x \in D$ s.t. $Q(x)$,** where D is the set of all x for which $P(x)$ is true
	$\exists\ x \in D,\ Q(x) \equiv Q(x_1) \vee Q(x_2) \vee \ldots \vee Q(x_n)$
Vacuously True (True by default)	$\forall\ x \in D\ (P(x) \to Q(x))$ iff $P(x)$ is false for every x in D. $\forall\ a \in X,\ P(a)$ is vacuously true if X is an empty set.
Find an element in y that works for that particular x	$\forall\ x \in D, \exists\ y \in E$ such that $P(x,y)$ $\sim(\forall\ x \in D, \exists\ y \in E$ such that $P(x,y)) \equiv \exists\ x \in D$ such that $\forall\ y \in E, \sim P(x,y)$
Find the particular x that will work on all y	$\exists\ x \in D$ such that $\forall\ y \in E,\ P(x,y)$ $\sim(\exists\ x \in D$ such that $\forall\ y \in E,\ P(x,y)) \equiv \forall x \in D, \exists y \in E$ such that $\sim P(x,y)$
The rule of universal instantiation	If some property is true of *everything* in the set, then it is true of *any particular* thing in the set.

Theorem 5.3.5 Set Identities

Identity Laws	$A \cup \varnothing = A$	$A \cap U = A$
Universal Bound Laws	$A \cup U = U$	$A \cap \varnothing = \varnothing$
Idempotent Laws	$A \cup A = A$	$A \cap A = A$
Double Complement Law	$\overline{(\overline{A})} = A$	
Commutative Laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
De Morgan's Laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Absorption Laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complement Laws	$A \cup \overline{A} = U$	$A \cap \overline{A} = \varnothing$
Set Difference Law	$A \setminus B = A \cap \overline{B}$	
	$\overline{\varnothing} = U$	$\overline{U} = \varnothing$

One of De Morgan's Laws. Work in the universal set U. For all sets A, B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Rules of inference			
Modus Ponens **(Universal Modus Ponens)**	$p \to q$ p • q		$\forall x\ (P(x) \to Q(x))$ *$P(a)$ for a particular a* • $Q(a)$
Modus Tollens **(Universal Modus Tollens)**	$p \to q$ $\sim q$ • $\sim p$		$\forall x, (P(x) \to Q(x))$ $\sim Q(a)$ for a particular a • $\sim P(a)$
Generalization	p • $p \vee q$	q • $p \vee q$	
Specialization	$p \wedge q$ • p	$p \wedge q$ • q	
Conjunction	p q • $p \wedge q$		
Elimination	$p \vee q$ $\sim q$ • p	$p \vee q$ $\sim p$ • q	
Transitivity	$p \to q$ $q \to r$ • $p \to r$		
Proof by Division Into Cases	$p \vee q$ $p \to r$ $q \to r$ • r		
Contradiction Rule	$\sim p \to$ **false** • p		

Algorithm	Examples
Algorithm 8.3.8 (for finding base-b representations). 1. input $n \in \mathbb{Z}^+$ 2. $q := n$ 3. $\ell := 0$ 4. while $q \neq 0$ do 5. $a_\ell := q \underline{\mathrm{mod}}\, b$ 6. $q := q \underline{\mathrm{div}}\, b$ 7. $\ell := \ell + 1$ 8. end do 9. output $(a_{\ell-1}a_{\ell-2}\dots a_1a_0)_b$	**Example 8.3.9.** $(b, n) = (8, 1511)$ $\begin{array}{r\|l} 8 & 1511 \\ 8 & 188 \;-\; 7 \;\to a_0 \\ 8 & 23 \;-\; 4 \;\to a_1 \\ 8 & 2 \;-\; 7 \;\to a_2 \\ & 0 \;-\; 2 \;\to a_3 \end{array}$ So $1511 = (2747)_8$. **Example 8.3.10.** $(b, n) = (16, 1511)$ $\begin{array}{r\|l} 16 & 1511 \\ 16 & 94 \;-\; 7 \;\to a_0 \\ 16 & 5 \;-\; 14 = \mathrm{E} \;\to a_1 \\ & 0 \;-\; 5 \;\to a_2 \end{array}$ So $1511 = (5\mathrm{E}7)_{16}$.

Algorithm 8.4.8 (Euclidean Algorithm).

```
input m, n ∈ ℤ⁺ with m ⩾ n > 0
x := m
y := n
while y ≠ 0 do
    r := x mod y
    x := y
    y := r
end do
output x
```

Example 8.4.9. To find $\gcd(1076, 414)$:

$$\begin{array}{ccccc} x & & y & & r \\ \downarrow & & \downarrow & & \downarrow \\ 1076 & \underline{\text{mod}} & 414 & = & 248 \\ 414 & \underline{\text{mod}} & 248 & = & 166 \\ 248 & \underline{\text{mod}} & 166 & = & 82 \\ 166 & \underline{\text{mod}} & 82 & = & 2 \\ 82 & \underline{\text{mod}} & 2 & = & 0 \\ \hline \multicolumn{5}{c}{\therefore\ \gcd(1076, 414) = 2} \end{array}$$

Example 8.6.21. Find a multiplicative inverse of 7 modulo 12.

Solution. Apply the Euclidean Algorithm:

$$\begin{array}{lcll} 12 \,\underline{\text{mod}}\, 7 = 5 & \leftarrow\text{--} & 5 = 12 - 7 \times 1 & (1) \\ 7 \,\underline{\text{mod}}\, 5 = 2 & \leftarrow\text{--} & 2 = \ 7 - 5 \times 1 & (2) \\ 5 \,\underline{\text{mod}}\, 2 = 1 & \leftarrow\text{--} & 1 = \ 5 - 2 \times 2 & (3) \\ 2 \,\underline{\text{mod}}\, 1 = 0 & & & \end{array}$$

Hence

$$\begin{aligned} \gcd(12, 7) = 1 &= 5 - 2 \times 2 && \text{by (3);} \\ &= 5 - (7 - 5 \times 1) \times 2 && \text{by (2);} \\ &= 7 \times (-2) + 5 \times 3 && \\ &= 7 \times (-2) + (12 - 7 \times 1) \times 3 && \text{by (1);} \\ &= 12 \times 3 + 7 \times (-5) && \\ &\equiv 7 \times (-5) \pmod{12}. && \end{aligned}$$

Hence -5 is a multiplicative inverse of 7 modulo 12. In view of Proposition 8.6.16(2), this implies $7, 19, 31, \ldots$ are all multiplicative inverses of 7 modulo 12.

To solve the equation
ax ≡ c (mod n), where gcd(a, n) = 1.

(1) Check if gcd(a, n) = 1
- If yes → proceed to steps 2&3
- If no→ no solution (proof see tut 7 Q10)

(Tut 7 Q10)
1. Let $x \in \mathbb{Z}$ such that $4x \equiv 6 \pmod{48}$.
2. Use Lemma 8.6.2 to get $k \in \mathbb{Z}$ such that $4x = 48k + 6$.
3. Note that 6 is an integer linear combination of 4 and 48 (as $6 = 4x + 48(-k)$).
4. Therefore, $\gcd(4, 48) \mid 6$. (by Tut 7 Q6: Let $a, b \in \mathbb{Z}$ with $a \neq 0$ *or* $b \neq 0$. Prove that an integer n is an integer linear combination of a and b if and only if $\gcd(a, b) \mid n$.)
5. However, we know $\gcd(4,48) = 4$ and $4 \nmid 6$ (by lemma 8.1.5 as $6/4 = 1.5 \notin \mathbb{Z}$) which is the required contradiction.

<u>#2</u>
1. Let $x \in \mathbb{Z}$ such that $4x \equiv 6 \pmod{48}$.
2. Use Lemma 8.6.2 to get $k \in \mathbb{Z}$ such that $4x = 48k + 6$.
3. Then $x = 12k + \frac{3}{2}$.
4. Therefore, $x - 12k = \frac{3}{2}$.
5. LHS is an integer but RHS is not, which is the required contradiction.

(2) Find a multiplicative inverse b of a modulo n.
- This can be done either by trial and error, or
- by using the Euclidean Algorithm as in the proofs of Bezout's Lemma and Theorem 8.6.19.

(3) The solution is x ≡ bc (mod n).

Example 8.6.24. To solve $7x \equiv 2 \pmod{12}$:

(1) We know from Example 8.6.21 that -5 is a multiplicative inverse of 7 modulo 12.

(2) The solution is

$$\begin{aligned} x &\equiv -5 \times 2 \pmod{12} \\ &= -10 \\ &\equiv 2 \pmod{12}. \end{aligned}$$

<u>Remark:</u> derived from Corollary 8.6.23. Let n ∈ Z +. Suppose a, b, c ∈ Z, where b is a multiplicative inverse of a modulo n. Then ax ≡ c (mod n) ⇔ x ≡ bc (mod n).

Example 8.6.25. Solve $26x \equiv 9 \pmod{35}$.

Solution. Apply the Euclidean Algorithm:

$$\begin{array}{lcl} 35 \,\underline{\text{mod}}\, 26 = 9 & \leftarrow\text{--} & 9 = 35 - 26 \times 1 \quad (1) \\ 26 \,\underline{\text{mod}}\, 9 = 8 & \leftarrow\text{--} & 8 = 26 - 9 \times 2 \quad (2) \\ 9 \,\underline{\text{mod}}\, 8 = 1 & \leftarrow\text{--} & 1 = 9 - 8 \times 1 \quad (3) \\ 8 \,\underline{\text{mod}}\, 1 = 0 & & \end{array}$$

Hence

$$\begin{aligned} \gcd(35, 26) = 1 &= 9 - 8 \times 1 && \text{by (3);} \\ &= 9 - (26 - 9 \times 2) \times 1 && \text{by (2);} \\ &= 26 \times (-1) + 9 \times 3 \\ &= 26 \times (-1) + (35 - 26 \times 1) \times 3 && \text{by (1);} \\ &= 35 \times 3 + 26 \times (-4) \\ &\equiv 26 \times (-4) \pmod{35}. \end{aligned}$$

Hence -4 is a multiplicative inverse of 26 modulo 35. Thus the solution to the congruence equation is

$$\begin{aligned} x &\equiv -4 \times 9 \pmod{35} \\ &= -36 \\ &\equiv 34 \pmod{35}. \end{aligned}$$

Algorithm 10.7.1 Kruskal

Input: G [a connected weighted graph with n vertices]

Algorithm:

1. Initialize T to have all the vertices of G and no edges.
2. Let E be the set of all edges of G, and let $m = 0$.
3. While ($m < n - 1$)
   - 3a. Find an edge e in E of least weight.
   - 3b. Delete e from E.
   - 3c. If addition of e to the edge set of T does not produce a circuit, then add e to the edge set of T and set $m = m + 1$

   End while

Output: T [T is a minimum spanning tree for G]

- If some edges have the same weight as others, more than one minimum spanning tree can occur as output.
- To make the output unique, the edges of the graph can be placed in an array and edges having the same weight can be added in the order they appear in the array.

	Edge considered	Wt	Action taken
1	→ Chi – Mil	74	added
2	→ Lou – Cin	83	added
3	→ Lou – Nas	151	added
4	→ Cin – Det	230	added
5	→ StL – Lou	242	added
6	→ StL – Chi	262	added
7	→ Chi – Lou	269	not added
8	→ Lou – Det	306	not added
9	→ Lou – Mil	348	not added
10	→ Min – Chi	355	added

Total weight = 1397

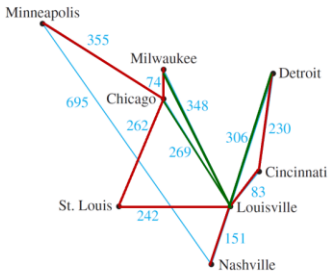


Figure 10.7.4

Algorithm 10.7.2 Prim

Input: G [a connected weighted graph with n vertices]

Algorithm:

1. Pick a vertex v of G and let T be the graph with this vertex only.
2. Let V be the set of all vertices of G except v.
3. For $i = 1$ to $n - 1$
   - 3a. Find an edge e of G such that (1) e connects T to one of the vertices in V, and (2) e has the least weight of all edges connecting T to a vertex in V. Let w be the endpoint of e that is in V.
   - 3b. Add e and w to the edge and vertex sets of T, and delete w from V.

Output: T [T is a minimum spanning tree for G]

	Vertex added	Edge added	Weight
0	Minneapolis		
1	Chicago	Min – Chi	355
2	Milwaukee	Chi – Mil	74
3	St. Louis	Chi – StL	262
4	Louisville	StL – Lou	242
5	Cincinnati	Lou – Cin	83
6	Nashville	Lou – Nas	151
7	Detroit	Cin – Det	230

Total weight = 1397

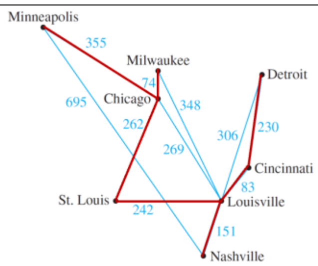


Figure 10.7.6

Formula	
No. of elements	Let m, n ϵ Z and $m \le n$, then there are $n - m + 1$ integers from m to n inclusive.
Equally likely probability of an event E in a finite sample space S	$P(E) = \dfrac{\text{The no. of outcomes in } E}{\text{The total no. of outcomes in } S} = \dfrac{\lvert E \rvert}{\lvert S \rvert}$

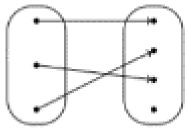
Probability Axioms	Let S be a sample space. A probability function P from the set of all events in S to the set of real numbers satisfies the following axioms: For all events A and B in S, 1. $0 \le P(A) \le 1$ 2. $P(\emptyset) = 0$ and $P(S) = 1$ 3. If A and B are disjoint ($A \cap B = \emptyset$), then $P(A \cup B) = P(A) + P(B)$
Probability of the Complement	$P(\bar{A}) = 1 - P(A)$
Probability of a Union	$P(A \cup B) = P(A) + P(B) - P(A \cap B)$.
Addition/Sum Rule	Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$. Then $\lvert A\rvert = \lvert A_1\rvert + \lvert A_2\rvert + \ldots + \lvert A_k\rvert$
The Difference Rule	If A is a finite set and $B \subseteq A$, then $\lvert A \setminus B\rvert = \lvert A\rvert - \lvert B\rvert$
The Inclusion/Exclusion Rule	If A, B, and C are any finite sets, then $\lvert A \cup B\rvert = \lvert A\rvert + \lvert B\rvert - \lvert A \cap B\rvert$ and $\lvert A \cup B \cup C\rvert = \lvert A\rvert + \lvert B\rvert + \lvert C\rvert - \lvert A \cap B\rvert - \lvert A \cap C\rvert - \lvert B \cap C\rvert + \lvert A \cap B \cap C\rvert$
Permutations	$n!$
r-permutation	$P(n,r) = n(n-1)(n-2)\ldots(n-r+1) = \frac{n!}{(n-r)!}$
Permutations with repetition	$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}$ $= \frac{n!}{n_1!\,n_2!\,n_3!\cdots n_k!}$
r-combination	$\binom{n}{r} = \frac{P(n,\ r)}{r!} = \frac{n!}{r!\,(n-r)!}$
Combinations with repetition	This equals the number of ways r objects can be selected from n categories of objects with repetitions allowed. $\binom{\boldsymbol{r+n-1}}{\boldsymbol{r}}$

	Order Matters	**Order Does Not Matter**
Repetition Is Allowed	n^k	$\binom{k+n-1}{k}$
Repetition Is Not Allowed	$P(n, k)$	$\binom{n}{k}$

Pascal's Formula	Let n and r be positive integers, $r \le n$. Then $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$
Binomial Theorem	Given any real numbers a and b and any non-negative integer n, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ $= a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n$
Expected Value	$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \cdots + a_n p_n$

Linearity of Expectation	For random variables X and Y, $$E[X+Y]=E[X]+E[Y]$$ For random variables $X_1, X_2, \cdots, X_n$ and constants $c_1, c_2, \cdots, c_n$, $$E\left[\sum_{i=1}^{n} c_i \cdot X_i\right]=\sum_{i=1}^{n}(c_i \cdot E[X_i])$$
Conditional Probability	Let A and B be events in a sample space S. If $P(A) \neq 0$, then the **conditional probability of B given A**, denoted $P(B\|A)$, is $$P(B\|A)=\frac{P(A \cap B)}{P(A)}$$ $$P(A \cap B)=P(B\|A) \cdot P(A)$$ $$P(A)=\frac{P(A \cap B)}{P(B\|A)}$$
Bayes' Theorem	Suppose that a sample space S is a union of mutually disjoint events B_1, B_2, B_3, …, B_n. Suppose A is an event in S, and suppose A and all the B_i have non-zero probabilities. If k is an integer with $1 \leq k \leq n$, then $$P(B_k\|A)=\frac{P(A\|B_k) \cdot P(B_k)}{P(A\|B_1) \cdot P(B_1)+P(A\|B_2) \cdot P(B_2)+\cdots+P(A\|B_n) \cdot P(B_n)}$$
Independent Events	If A and B are events in a sample space S, then A and B are **independent**, if and only if, $$P(A \cap B) = P(A) \cdot P(B)$$
Pairwise Independent and Mutually Independent	Let A, B and C be events in a sample space S. A, B and C are **pairwise independent**, if and only if, they satisfy conditions 1 – 3 below. They are **mutually independent** if, and only if, they satisfy all four conditions below. 1. $P(A \cap B) = P(A) \cdot P(B)$ 2. $P(A \cap C) = P(A) \cdot P(C)$ 3. $P(B \cap C) = P(B) \cdot P(C)$ 4. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$
Euler's formula	For a connected planar simple graph $G = (V, E)$ with $e = \|E\|$ and $v = \|V\|$, if we let f be the number of faces, then $f = e - v + 2$.
Full BT Theorem	If T is a full binary tree with k internal vertices, then T has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices (leaves).
Height of a BT & no. of vertices	Height is the highest level (root is level 0). For non-negative integers h, if T is any binary tree with height h and t terminal vertices (leaves), then $t \leq 2^h$ Equivalently, $\log_2 t \leq h$

Commonly used definitions and theorems	
Sets	
Theorem 5.2.4.	(No. of elements in a Power Set) If a set X has n ($n \geq 0$) elements, then $\wp(X)$ has 2^n elements.
Function	

Terminology 6.1.18	Well-defined function	A function is well-defined if its definition ensures that every element of the domain is assigned exactly one element of the codomain. 
Definition 6.1.22	Composite Function $g \circ f$ (composed with or circle)	Let $f : A \to B$ and $g : B \to C$. Then $g \circ f : A \to C$ such that for every $x \in A$, • $(g \circ f)(x) = g(f(x))$ • For $g \circ f$ to be well-defined, the codomain of f must equal the domain of g
Definition 6.2.5	Surjection, Injection, Bijection (bijective function)	Let $f : A \to B$. (1) f is surjective or onto if $\forall y \in B\ \exists x \in A\ (y = f(x))$. (2) f is injective or one-to-one if $\forall x, x' \in A\ (f(x) = f(x') \Rightarrow x = x')$ (3) f is bijective if it is both surjective and injective, i.e., $\forall y \in B\ \exists! x \in A\ (y = f(x))$. • A function is surjective if and only if its codomain is equal to its range • A function $f : A \to B$ is not surjective if and only if $\exists y \in B\ \forall x \in A\ (y \neq f(x))$. • A function $f : A \to B$ is not injective if and only if $\exists x, x' \in A\ (f(x) = f(x') \wedge x \neq x')$
Definition 6.2.13	Inverse	Let $f : A \to B$. Then $g : B \to A$ is an inverse of f if • $\forall x \in A\ \forall y \in B\ (y = f(x) \Leftrightarrow x = g(y))$
Theorem 6.2.17	A function $f : A \to B$ is bijective if and only if it has an inverse.	
Note to self	Remember to consider the negative values of y in the codomain to determine if the function is surjective. (not surjective as negative values have no preimages) E.g. $f(x) = x^2$ or $f(x) = \|x\|$	
	Induction	

1. Prove by induction that for all $n \in \mathbb{Z}_{\geqslant 1}$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1).$$

Solution.

1. For each $n \in \mathbb{Z}_{\geqslant 1}$, let $P(n)$ be the proposition

$$\text{“ } 1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1) \text{ ”}.$$

2. (Base step) $P(1)$ is true because $1^2 = 1 = \frac{1}{6} \times 1 \times (1+1) \times (2 \times 1 + 1)$.
3. (Induction step)
   3.1. Let $k \in \mathbb{Z}_{\geqslant 1}$ such that $P(k)$ is true, i.e., that

$$\text{“ } 1^2 + 2^2 + \cdots + k^2 = \frac{1}{6} k(k+1)(2k+1) \text{ ”}.$$

   3.2. Then $1^2 + 2^2 + \cdots + k^2 + (k+1)^2$
   3.3. $= \frac{1}{6} k(k+1)(2k+1) + (k+1)^2$ by the induction hypothesis;
   3.4. $= \frac{1}{6}(k+1)\big(k(2k+1) + 6(k+1)\big)$
   3.5. $= \frac{1}{6}(k+1)(2k^2 + 7k + 6)$
   3.6. $= \frac{1}{6}(k+1)(k+2)(2k+3)$
   3.7. $= \frac{1}{6}(k+1)\big((k+1)+1\big)\big(2(k+1)+1\big)$.
   3.8. Thus $P(k+1)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 1}\ P(n)$ is true by MI.

5. Prove by induction that

$$\forall n \in \mathbb{Z}_{\geqslant 8}\ \exists x, y \in \mathbb{Z}_{\geqslant 0}\ (n = 3x + 5y).$$

(As a consequence, any integer-valued transaction over 8 dollars can be carried out using only 3-dollar and 5-dollar coins.)

Solution.

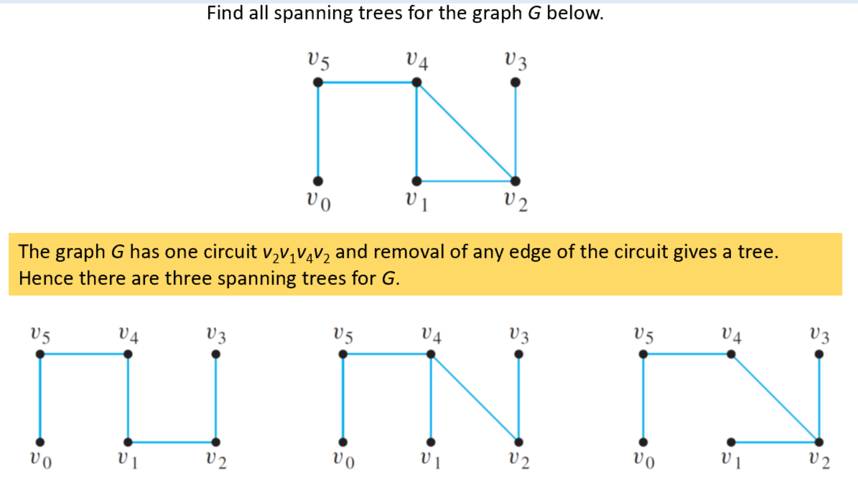
1. For each $n \in \mathbb{Z}_{\geqslant 8}$, let $P(n)$ be the proposition “ $\exists x, y \in \mathbb{Z}_{\geqslant 0}\ (n = 3x + 5y)$ ”.
2. (Base step) $P(8)$ is true because $8 = 3 \times 1 + 5 \times 1$.
3. (Induction step)
   3.1. Let $k \in \mathbb{Z}_{\geqslant 8}$ such that $P(k)$ is true.
   3.2. Find $x, y \in \mathbb{Z}_{\geqslant 0}$ such that $k = 3x + 5y$.
   3.3. Case 1: $y > 0$.
      3.3.1. Then $k + 1 = (3x + 5y) + 1$ by the choice of x, y;
      3.3.2. $= 3(x+2) + 5(y-1)$ where $x + 2 \in \mathbb{Z}_{\geqslant 0}$.
      3.3.3. As $y > 0$, we know $y - 1 \in \mathbb{Z}_{\geqslant 0}$.
      3.3.4. So $P(k+1)$ is true.
   3.4. Case 2: $y = 0$.
      3.4.1. Then $k = 3x + 3 \times 0 = 3x$
      3.4.2. $\therefore\ x = k/3 \geqslant 8/3$ as $k \geqslant 8$;
      3.4.3. $\therefore\ x \geqslant \lceil 8/3 \rceil = 3$ as $x \in \mathbb{Z}$.
      3.4.4. Thus $k + 1 = 3x + 1 = 3(x-3) + 5 \times 2$, where $x - 3 \in \mathbb{Z}_{\geqslant 0}$.
      3.4.5. So $P(k+1)$ is true.
   3.5. Thus $P(k+1)$ is true in all cases.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 1}\ P(n)$ is true by MI. □

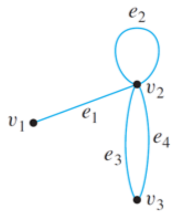
Alternative solution.

1. For each $n \in \mathbb{Z}_{\geqslant 0}$, let $P(n)$ be the proposition “ $\exists x, y \in \mathbb{Z}_{\geqslant 0}\ (n + 8 = 3x + 5y)$ ”.
2. (Base step)
   2.1. $P(0)$ is true because $0 + 8 = 8 = 3 \times 1 + 5 \times 1$.
   2.2. $P(1)$ is true because $1 + 8 = 9 = 3 \times 3 + 5 \times 0$.
   2.3. $P(2)$ is true because $2 + 8 = 10 = 3 \times 0 + 5 \times 2$.
3. (Induction step)
   3.1. Let $k \in \mathbb{Z}_{\geqslant 0}$ such that $P(0), P(1), \ldots, P(k+2)$ is true.
   3.2. Apply $P(k)$ to find $x, y \in \mathbb{Z}_{\geqslant 0}$ such that $k + 8 = 3x + 5y$.
   3.3. Then $(k+3) + 8 = (k+8) + 3$
   3.4. $= (3x + 5y) + 3$ by the choice of x, y;
   3.5. $= 3(x+1) + 5y$ where $x + 1, y \in \mathbb{Z}_{\geqslant 0}$.
   3.6. Thus $P(k+3)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 0}\ P(n)$ is true by Strong MI. □

Number Theory		
Definition 8.1.1	divides $d \mid n$	Let n, d ∈ Z. Then d is said to divide n if • **n = dk for some k ∈ Z.** • $d \mid n$ for "d divides n", and $d \nmid n$ for "d does not divide n".
Proposition 8.1.10	Let d, n ∈ Z. If d | n and n ≠ 0, then |d| ≤ |n|.	
Lemma 8.1.14	(Closure Lemma (non-standard name)). Let a, b, d, m, n ∈ Z. If d | m and d | n, then d | am + bn.	
Theorem 8.1.16	(Division Theorem). For all n ∈ Z and d ∈ Z +, there exist unique q, r ∈ Z such that n = dq + r and 0 ≤ r < d.	
Corollary 8.1.22	Let n ∈ Z. Then n is either even or odd, but not both.	
Tut 7 Q6	Let $a, b \in \mathbb{Z}$ with $a \neq 0$ *or* $b \neq 0$. Prove that an integer n is an integer linear combination of a and b if and only if $\gcd(a, b) \mid n$.	
Definition 8.4.1.	Let m, n ∈ Z. (1) A common divisor of m and n is divisor of both m and n. (2) The greatest common divisor of m and n is denoted gcd(m, n) Hence, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$.	
8.5.2.	(Bezout's Lemma). Let m, n ∈ Z with n ≠ 0. Then gcd(m, n) is an integer linear combination of m and n.	
Lemma 8.6.2.	(alternative definitions of congruence). The following are equivalent for all a, b ∈ Z and all n ∈ Z + (i) a ≡ b (mod n). (ii) a = nk + b for some k ∈ Z. (iii) n | (a − b).	
Lemma 8.6.5.	Let a, b, c ∈ Z and n ∈ Z +. (1) (Reflexivity) a ≡ a (mod n). (2) (Symmetry) If a ≡ b (mod n), then b ≡ a (mod n). (3) (Transitivity) If a ≡ b (mod n) and b ≡ c (mod n), then a ≡ c (mod n).	
Definition 8.6.18	Two integers a, n are coprime if gcd(a, n) = 1.	
Theorem 8.6.19.	Let a ∈ Z and n ∈ Z +. Then a has a multiplicative inverse modulo n if and only if a and n are coprime	
Relations		
Definition 9.2.2.	Reflexive, Symmetric, Transitive (combine 3 properties to get equivalence relation)	Let A be a set and R be a relation on A. (1) R is reflexive if ∀x ∈ A (x R x). (2) R is symmetric if ∀x, y ∈ A (x R y ⇒ y R x). (3) R is transitive if ∀x, y, z ∈ A (x R y ∧ y R z ⇒ x R z). Note: • It is wrong to say that "a is reflexive", "b is reflexive", "c is not reflexive". • We either say the relation R is reflexive or not reflexive. • We don't say an element of A is reflexive or not reflexive. Reflexivity, symmetry and transitivity are properties of relations, not individual elements of A.

Definition 9.2.10.	Equivalence Class $[x]_R$ or simply $[x]$	Let A be a set and R be an equivalence relation on A. For each x ∈ A, the equivalence class of x with respect to R, denoted $[x]_R$, is defined by $[x]_R = \{y \in A: x \mathrel{R} y\}$. • Define $A/R = \{[x]_R: x \in A\}$. **Example 9.2.12.** Fix $n \in \mathbb{Z}^+$. The congruence-mod-n relation R_n on $\mathbb{Z}$ is an equivalence relation. The equivalence classes are of the form $$[x] = \{y \in \mathbb{Z} : x \equiv y \pmod n\} = \{x + nk : k \in \mathbb{Z}\},$$ where $x \in \mathbb{Z}$. So $\mathbb{Z}/R_n = \{\{x + nk : k \in \mathbb{Z}\} : x \in \mathbb{Z}\} = \{[0], [1], \ldots, [n-1]\}$. If $n = 2$, then there are two equivalence classes: $$\{2k : k \in \mathbb{Z}\} \quad \text{and} \quad \{2k+1 : k \in \mathbb{Z}\}.$$
Definition 9.3.1.	Partition (C)	A partition of a set A is a set C of nonempty subsets of A such that **(≥ 1)** ∀x ∈ A ∃S ∈ C (x ∈ S); and **(≤ 1)** ∀x ∈ A ∀S, S' ∈ C (x ∈ S ∧ x ∈ S' ⇒ S = S') Elements of a partition are called components of the partition. e.g. The set A = {1, 2, 3} has the following partitions: • {{1}, {2}, {3}}, • {{1}, {2, 3}}, • {{2}, {1, 3}}, • {{3}, {1, 2}}, • {{1, 2, 3}} e.g. The congruence-mod-2 relation gives rise to the following partition of Z {{2k : k ∈ Z}, {2k + 1 : k ∈ Z}}
Definition 9.4.1.	Partial order ⪯ ≺ (for x ⪯ y ∧ x ≠ y.)	Let A be a set and R be a relation on A. (1) R is antisymmetric if ∀x, y ∈ A (x R y ∧ y R x ⇒ x = y). (2) R is a (non-strict) partial order if R is reflexive, antisymmetric, and transitive. (3) Suppose R is a partial order. Let x, y ∈ A. Then x, y are comparable (under R) if x R y or y R x. (4) R is a (non-strict) total order if R is a partial order and ∀x, y ∈ A (x R y ∨ y R x). (connex) <u>Note 9.4.2.</u> A total order is always a partial order <u>Note:</u> "divides" relation on integers is a partial order
	Counting and Probability	
Theorem 5.3.12 (Epp)	(Inclusion–Exclusion Principle). For all finite sets A, B |A ∪ B| = |A| + |B| − |A ∩ B|.	
Pigeonhole Principle (PHP)	A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain.	
Generalized PHP	• For any function *f* from a finite set *X* with *n* elements to a finite set *Y* with *m* elements and for any positive integer *k*, if $k < n/m$, then there is some $y \in Y$ such that *y* is the image of at least $k + 1$ distinct elements of *X*.	

	• (Contrapositive) For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each $y \in Y$, $f^{-1}(\{y\})$ has at most k elements, then X has at most km elements; in other words, $n \le km$.
Graphs and Trees	
Edges	$$Max\ no.of\ edges = \binom{n}{2} = \frac{n(n-1)}{2}$$
No. of simple graphs	$$No.of\ simple\ graphs\ on\ n\ vertices = 2^{\binom{n}{2}} = 2^{\frac{n(n-1)}{2}}$$
Spanning Tree	A **spanning tree** for a graph G is a subgraph of G that contains every vertex of G and is a tree. (tut 11 Q8) The number of spanning trees in a complete graph K_n is n^{n-2}. 
Theorem 10.1.1.	(The Handshake Theorem) If the vertices of G are $v_1, v_2, \ldots, v_n$, where $n \ge 0$, then the total degree of G $= \deg(v_1) + \deg(v_2) + \ldots + \deg(v_n)$ $= 2 \times$ (the number of edges of G).
Theorem 10.2.4.	(combining 10.2.2. and 10.2.3.) A graph G has an Euler circuit iff G is connected and every vertex of G has positive even degree.
Corollary 10.2.5	Let G be a graph, and let v and w be two distinct vertices of G. There is an Euler trail from v to w if and only if G is connected, v and w have odd degree, and all other vertices of G have positive even degree.
Proposition 10.2.6.	If a graph G has a Hamiltonian circuit, then G has a subgraph H with the following properties: 1. H contains every vertex of G. 2. H is connected. 3. H has the same number of edges as vertices. Every vertex of H has degree 2.
10.3.2.	If G is a graph with vertices $v_1, v_2, \ldots, v_m$ and **A** is the adjacency matrix of G, then for each positive integer n and for all integers $i, j = 1, 2, \ldots, m$, the ij-th entry of $\mathbf{A}^n$ = the number of walks of length n from v_i to v_j.

	Consider the adjacency matrix A of the graph *G*. $\mathbf{A} = \begin{array}{cc} & \begin{matrix} v_1 & v_2 & v_3 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \end{matrix} & \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \end{array}.$  Compute $\mathbf{A}^2$: $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 6 & 2 \\ 2 & 2 & 4 \end{bmatrix}.$ Note that the entry in row 2 and column 2 is 6, which equals the number of walks of length 2 from v_2 to v_2. To compute a_{22}, you multiply row 2 of A with column 2 of A to obtain a sum of three terms: $\begin{bmatrix} 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} = 1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2.$
Theorem 10.5.2.	Any tree with n vertices ($n > 0$) has $n - 1$ edges.