Math 251

Definitions and Results

This document includes the principal definitions and theorems that are introduced and proved in class. In solving problems, you may refer to these definitions and results by the numbers here.

These are also the definitions that you should use when creating proofs; if you want to use a different definition, you will need to prove (or quote a theorem) which says that they are equivalent.

Obviously, if a homework problem asks you to prove one of these results, you may not cite the result (or any later result which depends on it), in your answer.

You may use any earlier homework problem to help solve a later homework problem, if you think it will help.

1 Definitions and Theorems

You may assume that basic facts about equations and inequalities can be stated without proof. Just make sure that your calculations are correct!

Definition 1.1
An integer is called ***even*** *if it is divisible by 2.*

Definition 1.2
Let a and b be integers. We say that a is ***divisible*** *by b if there is an integer n such that $a = bn$. We also say that b* ***divides*** *a, or b is a* ***factor*** *of a, or b is a* ***divisor*** *of a. We denote this symbolically by $b \mid a$.*

Definition 1.3
An integer a is called ***odd*** *if there is some integer n such that $a = 2n + 1$.*

Definition 1.4
An integer p is called ***prime*** *if $p > 1$ and the only positive divisors of p are 1 and p.*

Definition 1.5
An integer a is called ***composite*** *if there is some integer n such that $1 < n < a$ and $n \mid a$.*

Theorem 1.1 (Pythagoras' Theorem)
Let a and b be the lengths of the legs of a right-angle triangle, and let c be the length of the hypotenuse. Then

$$a^2 + b^2 = c^2.$$

2 Proof and Counterexamples

Proposition 2.1
The sum of two even integers is even.

Proposition 2.2
Let a, b and c be integers. If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proposition 2.3
Let a be an integer. Then a is even if and only if $a+1$ is odd.

Proposition 2.4
Let a, b, c and d be integers. If $a \mid b$, $b \mid c$ and $c \mid d$ then $a \mid d$.

Proposition 2.5
Let x be an integer. If $x > 1$ then $x^3 + 1$ is composite.

3 Boolean Algebra

Definition 3.1
*A **Boolean variable** is a quantity which takes one of the values $\boldsymbol{T}$ or $\boldsymbol{F}$.*

*Given two boolean variables x and y, we define the Boolean operations **and** $\wedge$, **or** $\vee$, **not** $\neg$, **implication** $\Rightarrow$, **reverse implication** $\Leftarrow$, **double implication** $\Leftrightarrow$, **xor** $\veebar$ and **nand** $\barwedge$ using the following tables:*

x	y	$x \wedge y$	$x \vee y$	$x \Rightarrow y$	$x \Leftarrow y$	$x \Leftrightarrow y$	$x \veebar y$	$x \barwedge y$
T	***T***	***T***	***T***	***T***	***T***	***T***	***F***	***F***
T	***F***	***F***	***T***	***F***	***T***	***F***	***T***	***F***
F	***T***	***F***	***T***	***T***	***F***	***F***	***T***	***F***
F	***F***	***F***	***F***	***T***	***T***	***T***	***F***	***T***

x	$\neg x$
T	***F***
F	***T***

Theorem 3.1
Let x, y and z be Boolean variables. Then:

(i) $x \wedge y = y \wedge x$ *and* $x \vee y = y \vee x$ *(commutative rules).*

(ii) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ *and* $(x \vee y) \vee z = x \vee (y \vee z)$ *(associative rules).*

(iii) $\neg(\neg x) = x$ *(double negation rule)*

(iv) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ *and* $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ *(distributive rules).*

(v) $x \wedge x = x$ and $x \vee x = x$ *(idempotent rules).*

(vi) $x \wedge \boldsymbol{T} = x$ *and* $x \vee \boldsymbol{F} = x$ *(identity elements).*

(vii) $x \wedge \boldsymbol{F} = \boldsymbol{F}$ and $x \vee \boldsymbol{T} = \boldsymbol{T}$.

(viii) $x \wedge (\neg x) = \boldsymbol{F}$ and $x \vee (\neg x) = \boldsymbol{T}$.

(ix) $x \wedge (x \vee y) = x$ *and* $x \vee (x \wedge y) = x$ *(absorption rules).*

(x) $\neg(x \wedge y) = (\neg x) \vee (\neg y)$ *and* $\neg(x \vee y) = (\neg x) \wedge (\neg y)$ *(DeMorgan's laws).*

(xi) $x \Rightarrow y = (\neg x) \vee y$.

(xii) $x \Rightarrow y = (\neg y) \Rightarrow (\neg x)$ *(contrapositive rule).*

(xiii) $x \Leftrightarrow y = (x \Rightarrow y) \wedge (y \Rightarrow x)$.

Note: Bender and Williamson uses $\sim$ for $\neg$.

4 Sets

Definition 4.1
*A **set** is an unordered, repetition-free collection of mathematical objects. The objects in a set are called its **elements**. If x is an element of the set S, we write $x \in S$.*

*The number of elements in a set S is called its **cardinality** or **size**, denoted $|S|$. A set is called **finite** if its cardinality is an integer, otherwise it is called **infinite**.*

*The set with no elements is called the **empty set**, denoted* $\{\}$ or $\emptyset$.

*It is often convenient to restrict the set of mathematical objects that we are considering to a particular **universe** of objects. The set of all objects in the universe is the **universal set** usually denoted U.*

*Two sets are **equal** if they have exactly the same elements.*

Proposition 4.1
Let A and B be sets. Then $A = B$ if and only if $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$.

Definition 4.2
Let A and B be sets. We say A is a subset of B if every element of A is an element of B. We write $A \subseteq B$.

*If $A \subseteq B$ and $A \neq B$, we say that A is a **proper** subset of B, and write $A \subset B$.*

*The **power set** of A is the set of all subsets of A, denoted $\mathcal{P}(A)$ or 2^A.*

Proposition 4.2
If A is a set, then $\emptyset \subseteq A$.

Proposition 4.3
Let A be a set. Then $x \in A$ if and only if $\{x\} \subseteq A$.

Proposition 4.4
Let A and B be sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Theorem 4.5
Let A be a finite set. Then

$$|\mathcal{P}(A)| = 2^{|A|}.$$

Definition 4.3
*A **predicate** P on a set D is a rule which associates each element $x \in D$ with precisely one of the values $\boldsymbol{T}$ or $\boldsymbol{F}$, denoted $P(x)$. (ie. P is a function from D to $\{\boldsymbol{T}, \boldsymbol{F}\}$.)*

Given two predicates P and Q, we can perform Boolean algebra operations to produce new predicates: $(P \wedge Q)(x) = P(x) \wedge Q(x)$, $(P \vee Q)(x) = P(x) \vee Q(x)$ and $(\neg P)(x) = \neg(P(x))$.

Given a predicate P on a set D, we write

$$\{x \in D : P(x)\}$$

for the set of all $x \in D$ such that $P(x)$ is $\boldsymbol{T}$. If D is a universal set U we will simply write

$$\{x : P(x)\}.$$

Definition 4.4
If D is a set and P is a predicate on D, the statement "for all $x \in D$, $P(x)$," written

$$\forall\ x \in D, P(x),$$

is $\boldsymbol{T}$ if $P(x)$ has constant value $\boldsymbol{T}$.

The statement "there exists $x \in D$ such that $P(x)$", written

$$\exists\ x \in D, P(x)$$

is $\boldsymbol{T}$ if $P(x)$ does not have constant value $\boldsymbol{F}$.

The statement "there exists a unique $x \in D$ such that $P(x)$", written

$$\exists!\ x \in D, P(x)$$

is $\boldsymbol{T}$ if $P(x)$ is $\boldsymbol{F}$ except for precisely one x where it is $\boldsymbol{T}$.

Proposition 4.6
Let P be a predicate on D and X a subset of D. Then:

(i) $\neg(\forall\ x \in D, P(x))$ *is logically equivalent to* $\exists\ x \in D, \neg(P(x))$.

(ii) $\neg(\exists\ x \in D, P(x))$ *is logically equivalent to* $\forall\ x \in D, \neg(P(x))$.

(iii) $\forall\ x \in D, P(x) \wedge Q(x)$ *is logically equivalent to* $(\forall\ x \in D, P(x)) \wedge (\forall\ x \in D, Q(x))$.

(iv) $\exists\ x \in D, P(x) \vee Q(x)$ *is logically equivalent to* $(\exists\ x \in D, P(x)) \vee (\exists\ x \in D, Q(x))$.

(v) $\forall\ x \in X, P(x)$ *is logically equivalent to* $\forall\ x \in D, (x \in X) \Rightarrow P(x)$

(vi) $\exists\ x \in X, P(x)$ *is logically equivalent to* $\exists\ x \in D, (x \in X) \wedge P(x)$.

(vii) $(\forall\ x \in \emptyset, P(x)) = \boldsymbol{T}$

(viii) $(\exists\ x \in \emptyset, P(x)) = \boldsymbol{F}$.

Proposition 4.7
Let P be a predicate on a set D, and let X be a subset of D. Then

$$\{x \in D : (x \in X) \wedge P(x)\} = \{x \in X : P(x)\}$$

and in particular

$$\{x : x \in X\} = X.$$

Proposition 4.8
Let X and Y be sets and P a predicate on X and Y. Then

(i) $\forall\ x \in X, \forall\ y \in Y, P(x,y)$ *is logically equivalent to* $\forall\ y \in Y, \forall\ x \in X, P(x,y)$.

(ii) $\exists\ x \in X, \exists\ y \in Y, P(x,y)$ *is logically equivalent to* $\exists\ y \in Y, \exists\ x \in X, P(x,y)$.

It is customary to combine repeated quantifiers into one:

This...	...means this
$\forall\ x \in X, y \in Y, P(x,y)$	$\forall\ x \in X, \forall\ y \in Y, P(x,y)$
$\forall\ x, y \in X, P(x,y)$	$\forall\ x \in X, \forall\ y \in X, P(x,y)$
$\exists\ x \in X, y \in Y, P(x,y)$	$\exists\ x \in X, \exists\ y \in Y, P(x,y)$
$\exists\ x, y \in X, P(x,y)$	$\exists\ x \in X, \exists\ y \in X, P(x,y)$

5 Set Operations

Definition 5.1
Let X and Y be sets. Then we define the ***intersection*** *of X and Y to be the set*

$$X \cap Y = \{x : (x \in X) \wedge (x \in Y)\}.$$

We define the ***union*** *of X and Y to be the set*

$$X \cup Y = \{x : (x \in X) \vee (x \in Y)\}.$$

We say X and Y are ***disjoint*** *if $X \cap Y = \emptyset$.*
The ***set difference*** *of X and Y is*

$$X \setminus Y = \{x \in X : x \notin Y\}.$$

The ***symmetric difference*** *of X and Y is*

$$X \bigtriangleup Y = \{x : (x \in X) \veebar (y \in Y)\} = (X \setminus Y) \cup (Y \setminus X).$$

If U is some universe of objects we are considering, the complement of a set X is

$$X^c = U \setminus X = \{x : x \notin X\}.$$

Theorem 5.1
Let X, Y and Z be sets in some universe of objects U. Then:

(i) $X \cap Y = Y \cap X$ *and* $X \cup Y = Y \cup X$ *(commutative rules).*

(ii) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ *and* $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ *(associative rules).*

(iii) $(X^c)^c = X$

(iv) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ *and* $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ *(distributive rules).*

(v) $X \cap X = X$ *and* $X \cup X = X$ *(idempotent rules).*

(vi) $X \cap U = X$ *and* $X \cup \emptyset = X$ *(identity element).*

(vii) $X \cap \emptyset = \emptyset$ *and* $X \cup U = U$.

(viii) $X \cap X^c = \emptyset$ *and* $X \cup X^c = U$.

(ix) $X \cap (X \cup Y) = X$ *and* $X \cup (X \cap Y) = X$ *(absorption rules).*

(x) $(X \cap Y)^c = X^c \cup Y^c$ *and* $(X \cup Y)^c = X^c \cap Y^c$ *(DeMorgan's rules for complements).*

(xi) $U^c = \emptyset$ *and* $\emptyset^c = U$.

(xii) $X \subseteq Y$ *if and only if* $Y^c \subseteq X^c$.

(xiii) $X \setminus Y = X \cap Y^c$.

(xiv) $X \setminus (Y \setminus X) = X$.

(xv) $X \cap (Y \setminus X) = \emptyset$ *and* $X \cup (Y \setminus X) = X \cup Y$.

(xvi) $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$ *and* $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$ *(DeMorgan's rules for set difference).*

(xvii) $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$.

Not the similarities between this theorem and Theorem 3.1.

Theorem 5.2
If X and Y are finite sets, then

$$|X| + |Y| = |X \cup Y| + |X \cap Y|.$$

Corollary 5.3
If X and Y are finite disjoint sets, then

$$|X| + |Y| = |X \cup Y|.$$

Proposition 5.4
If X and Y are sets and P is a predicate on $X \cup Y$, then

(i) $\forall\, x \in X \cup Y, P(x)$ *is logically equivalent to* $(\forall\, x \in X, P(x)) \wedge (\forall\, x \in Y, P(x))$.

(ii) $\exists\, x \in X \cup Y, P(x)$ *is logically equivalent to* $(\exists\, x \in X, P(x)) \vee (\exists\, x \in Y, P(x))$

6 Contrapositive, Contradiction and Induction

A **contrapositive proof** of "If A then B" is a proof of the statement "If not B then not A." This proof method works because $x \Rightarrow y$ is logically equivalent to $(\neg y) \Rightarrow (\neg x)$ (Theorem 3.1(xii)).

A **proof by contradiction** (or **reductio ad absurdum**) of "If A then B" is a proof that assumes that both A and (not B) are true and then shows that this situation is impossible. This proof method works because $x \Rightarrow y$ is logically equivalent to $x \wedge (\neg y) = \mathbf{F}$.

The **Well-Ordering Principle** says that any non-empty subset of the natural numbers has a least element. Symbolically: $\forall\, X \subseteq \mathbb{N}$, $X \neq \emptyset$, $\exists\, x \in X$, $\forall\, y \in X$, $x \leq y$.

A **proof by smallest counterexample** of "For all $n \in \mathbb{N}$, $P(n)$" proceeds by assuming that the set $X = \{n : \neg P(n)\}$ of counterexamples is not empty and so has a smallest element by the well-odering principle. We verify that this smallest element is not 1. We let n be this smallest element and then proceed to obtain a contradiction, either by showing that there is a smaller counterexample, or alternatively, by showing $x \notin X$. This implies that X is empty.

The **Principle of Mathematical Induction** says that if P is a predicate on $\mathbb{N}$ such that $P(1)$ is true, and if $P(n)$ is true, so is $P(n+1)$, then $P(n)$ is true for all natural numbers. Symbolically: $(P(1) \wedge (\forall\, n \in \mathbb{N},\, P(n) \implies P(n+1)) \implies (\forall\, n \in \mathbb{N},\, P(n))$.

A **proof by induction** of "For all $n \in \mathbb{N}$, $P(n)$" proceeds by first proving $P(1)$, then assuming $P(n)$ and using it to prove $P(n+1)$. We can then cite the principle of mathematical induction to conclude that $P(n)$ is true for all $n \in \mathbb{N}$.

Proposition 6.1
Let $a \in \mathbb{N}$. Then a is even or odd, and cannot be both.

Corollary 6.2
Let $a \in \mathbb{Z}$. Then a is even or odd, and cannot be both.

7 Lists and Cartesian Products

Definition 7.1
*A **list** (or **sequence** or **word**) is an ordered collection of objects. The objects in a list are called the **elements** of the list. A list with elements a_1, a_2, ... etc. is denoted $(a_1, a_2, \ldots)$.*

*The **length** of a list is the number of elements in the list (including repetitions). The **empty list** is the list () of length 0.*

*Two lists are **equal** if they have the same length, and have the same elements in corresponding positions.*

*An n**-tuple** is a list of length n.*

Definition 7.2
*Let n and k be integers with $0 \leq k \leq n$. The **falling factorial** $(n)_k$ is the quantity*

$$(n)_k = \begin{cases} n(n-1)(n-2)\cdots(n-k+1), & k > 0, \\ 1, & k = 0. \end{cases}$$

*If n is a positive integer, we define the **factorial** of n to be the quantity*

$$n! = (n)_n = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1.$$

We define $0! = (0)_0 = 1$.

Theorem 7.1 (Multiplication Principle)
The number of k-tuples for which there are n_1 choices for the first element, n_2 choices for the second element, etc. is

$$n_1 n_2 \cdots n_k.$$

Corollary 7.2
The number of k-tuples whose elements are chosen from a pool of n possible elements is n^k if repetition is allowed, and $(n)_k$ if repetition is forbidden.

Definition 7.3
*Let X_1, X_2, ... X_n be a collection of sets. The **Cartesian product** of the sets is the set of all n-tuples $(x_1, x_2, \ldots, x_n)$ such that $x_k \in X_k$ for all $k = 1, \ldots, n$. In symbols,*

$$X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) : \forall\, k \in \{1, 2, \ldots, n\}, x_k \in X_k\}.$$

If X is a set, we define

$$X^n = \underbrace{X \times X \times \cdots \times X}_{n \text{ times}}.$$

Corollary 7.3
Let X_1, X_2, $\dots X_n$ be a collection of finite sets. Then

$$|X_1 \times X_2 \times \cdot \times X_n| = |X_1||X_2| \cdots |X_n|.$$

If X is a finite set, then

$$|X^n| = |X|^n.$$

8 Relations and Functions

Definition 8.1
*A **relation** R is a set of 2-tuples. If $(a, b) \in R$, we write $a\,R\,b$ and if $(a, b) \notin R$ we write $a \not R\, b$. The **domain** of a relation is the set $\{a : \exists\ b, aRb\}$ and the **range** of a relation is the set $\{b : \exists\ a, aRb\}$.*

*The **inverse relation** of a relation R is the relation*

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

That is $b\,R^{-1}\,a$ if and only if $a\,R\,b$

*Let A and B be a sets. We say that R is a **relation between A and B** if $R \subseteq A \times B$. We say that a relation R is a **relation on** A if $R \subseteq A^2$.*

Let R be a relation on a set A. We say that a relation R on A is:

*(i) **reflexive** if a is always related to itself, symbolically: $\forall\ a \in A, a\,R\,a$.*

*(ii) **irreflexive** if a is never related to itself, symbolically: $\forall\ a \in A, a \not R\ a$.*

*(iii) **symmetric** if whenever $a\,R\,b$, you have $b\,R\,a$, symbolically $\forall\ a, b \in A, a\,R\,b \Rightarrow b\,R\,a$.*

*(iv) **antisymmetric** if whenever aRb and bRa then $a = b$, symbolically $\forall\ a, b \in A, (aRb) \wedge (bRa) \Rightarrow (a = b)$.*

*(v) **total** if for every a and b, $a\,R\,b$ or ba, symbolically: $\forall\ a, b \in A, (a\,R\,b) \vee (b\,R\,a)$.*

*(vi) **transitive** if whenever $a\,R\,b$ and $b\,R\,c$, then $a\,R\,c$, symbolically: $\forall a, b, c \in A, (a\,R\,b) \wedge (b\,R\,c) \Rightarrow (a\,R\,c)$.*

Definition 8.2
*Let $\sim$ be a relation on a set A. We say that $\sim$ is an **equivalence relation** if $\sim$ is reflexive, symmetric and transitive.*

Definition 8.3
*Let $\preceq$ be a relation on a set A. We say that $\preceq$ is a **preorder** if $\preceq$ is reflexive and transitive. We say that $\preceq$ is a **partial order** if it is a preorder which is also antisymmetric. We say that $\preceq$ is a **total order** if it is a partial order which is also total.*

Definition 8.4
*Let f a relation between two sets A and B. We say f is a **function** if for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$. It is customary to write $f(a) = b$ when $(a, b) \in f$ if f is a function.*

The set A is the ***domain*** *of f and B is the* ***codomain*** *of f. We express the idea that f is a function with domain A and codomain B by writing $f : A \to B$.*

A function $f : A \to B$ is ***surjective*** *or* ***onto*** *if for all $b \in B$ there is some $a \in A$ such that $b = f(a)$.*

A function $f : A \to B$ is ***injective*** *or* ***one-to-one*** *if whenever $f(a_1) = f(a_2)$ then $a_1 = a_2$.*

A function is ***bijective*** *if it is both injective and surjective.*

Theorem 8.1
Let $f : A \to B$. Then f is bijective if and only if the inverse relation f^{-1} is a function.

Definition 8.5
If $f : A \to B$ and $X \subseteq B$, we let

$$f^{-1}(X) = \{a \in A : f(a) \in X\}.$$

9 Equivalence Classes and Partitions

Definition 9.1
Let $\sim$ be an equivalence relation on a set X. If $x \in X$ then the ***equivalence class*** *of x is the set*

$$[x] = \{y \in X : x \sim y\}.$$

If there is some confusion possible about the equivalence relation being used, we will write $[x]_\sim = [x]$.

Proposition 9.1
Let $\sim$ be an equivalence relation on a set X. Then

(i) Let $x \in X$. Then $x \in [x]$.

(ii) Let $x,\, y \in X$. Then $x \sim y$ if and only if $[x] = [y]$.

(iii) Let $x,\, y,\, a \in X$. If $x,\, y \in [a]$ then $x \sim y$.

(iv) If $[x] \cap [y] \neq \emptyset$ then $[x] = [y]$.

Definition 9.2
Let X be a set. A ***partition*** *$\mathcal{P}$ of X is a set of non-empty subsets of X which are pairwise disjoint, and whose union is X.*

The sets in $\mathcal{P}$ are called the ***parts*** *of the partition.*

Corollary 9.2
Let $\sim$ be an equivalence relation on a set X. Then the set of equivalence classes, denoted $X/\sim$, is a partition.

Theorem 9.3
Let $\mathcal{P}$ be a partition of a set X. Then the relation $x \overset{\mathcal{P}}{\equiv} y$ if x and y are in the same part of $\mathcal{P}$ (ie. there is some $P \in \mathcal{P}$ such that $x,\, y \in P$) is an equivalence relation.

Furthermore, the equivalence classes of this equivalence relation are precisely the parts of $\mathcal{P}$.

10 Combinatorics

Theorem 10.1 (Multiplication Principle)
The number of lists of length k where the mth element is chosen from a set of n_m choices is

$$n_1 n_2 \cdots n_m \cdots n_k.$$

Corollary 10.2
If X_1, X_2, ..., X_k are finite sets, then

$$|X_1 \times X_2 \times \cdots \times X_k| = |X_1||X_2| \cdots |X_k|.$$

If X is a finite set, then

$$|X^k| = |X|^k.$$

Definition 10.1
*Let n and k be natural numbers. Then we define the **falling factorial** of n and k to be*

$$(n)_k = n(n-1) \cdots (n-k+1).$$

In addition, we define $(0)_k = 0$, $(n)_0 = 1$ and $(0)_0 = 1$.

*The **factorial** of n is*

$$n! = n(n-1) \cdots (3)(2)(1) = (n)_n,$$

and

$$0! = (0)_0 = 1.$$

Corollary 10.3
Let X be a finite set. The number of k-tuples of elements of X, where no element is repeated, is

$$(|X|)_k.$$

Proposition 10.4
Let $\mathcal{P} = \{P_1, P_2, \ldots, P_m\}$ be a partition of a finite set X. Then

$$|X| = |P_1| + |P_2| + \cdots + |P_m|.$$

Corollary 10.5
Let $\mathcal{P}$ be a partition of a finite set X such that every part has the same size. Then

$$|\mathcal{P}| = |X|/|P|$$

for any part $P \in \mathcal{P}$.

Corollary 10.6
Let $\sim$ be an equivalence relation on a finite set X such that every equivalence class has the same size. Then the number of equivalence classes is

$$|X/\sim| = |X|/|[x]|$$

for any $x \in X$.

Proposition 10.7
Let X be a finite set with $|X| = n$. Then the number of subsets of size k is

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

Definition 10.2
A multiset is a collection of mathematical objects where repetition is allowed but order does not matter. The order of an element of a multiset is the number of times it occurs in the multiset. The cardinality of a multiset is the sum of the orders of its elements.

Given a collection of n objects, the number of multisets of size k that can be formed from those n objects is denoted by

$$\left(\!\!\binom{n}{k}\!\!\right).$$

Proposition 10.8

$$\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k} = \frac{(n+k-1)!}{(n-1)!k!}.$$

Proposition 10.9 (Inclusion-exclusion Principle)
If A_1, A_2, $\ldots A_n$ are finite sets, then

$$\begin{aligned}\left|\bigcup_{k=1}^{n} A_k\right| =& \sum_{k=1}^{n} |A_k| \\ &- \sum_{k_1=1}^{n-1} \sum_{k_2=k_1+1}^{n} |A_{k_1} \cap A_{k_2}| \\ &+ \sum_{k_1=1}^{n-2} \sum_{k_2=k_1+1}^{n-1} \sum_{k_3=k_2+1}^{n} |A_{k_1} \cap A_{k_2} \cap A_{k_3}| \\ &- \cdots \\ &\quad\vdots \\ &+ (-1)^{j-1} \sum_{k_1=1}^{n-j+1} \sum_{k_2=k_1+1}^{n-j+2} \cdots \sum_{k_j=k_{j-1}+1}^{n} |A_{k_1} \cap A_{k_2} \cap \cdots \cap A_{k_j}| \\ &\quad\vdots \\ &+ (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|\end{aligned}$$

or, more concisely,

$$\left|\bigcup_{k=1}^{n} A_k\right| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=j}} \left|\bigcap_{k \in S} A_k\right|$$

Proposition 10.10
If $f : A \to B$ then:

(i) *if f is surjective then $|A| \geq |B|$.*

(ii) *if f is injective then $|A| \leq |B|$.*

(iii) *if f is bijective then $|A| = |B|$.*

Proposition 10.11 (Pigeonhole Principle)
If $f : A \to B$ is such that every $b \in B$ has no more than n elements $a \in A$ such that $f(a) = b$, then $|B| \leq |A|n$.

Equivalently, if $|B| \geq |A|n + 1$ then there is some b such that there are at least $n + 1$ elements $a \in A$ such that $f(a) = b$.

11 Number Theory

Theorem 11.1
Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then there are unique numbers q, $r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Definition 11.1
We call q the ***quotient*** *and r the* ***remainder*** *or* ***modulus*** *of a divided by b. We define*

$$a \operatorname{div} b = q \qquad \textit{and} \qquad a \mod b = r.$$

Definition 11.2
For $n \in \mathbb{N}$, we define $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. We define addition and multiplcation for $\mathbb{Z}_n$ by

$$a + b = (a + b) \mod n \qquad \textit{and} \qquad a \times b = (a \times b) \mod n.$$

Proposition 11.2
For $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n$ there is a unique element $b \in \mathbb{Z}_n$ such that $a + b = 0$ in $\mathbb{Z}_n$. We call b the ***additive inverse*** *of a, usually written $-a$.*

We define subtraction in $\mathbb{Z}_n$ by $a - b = a + (-b) = (a - b) \mod n$.