CS 22 — Spring 2020 **Review Session 1**

1 Disclaimer

The TAs do not know what is on the midterm. The following is our guide for what we believe will be helpful in preparation. Additionally, the example proofs we provide in this review guide may be informal, or stripped to their bare bones. They strive to convey an idea, but are not necessarily paragons of perfect proofs. We suggest looking at the website or the homework solutions for completely polished proofs.

2 Proof Techniques

2.1 Direct Proof

Given statements ⇒ conclusion.

Claim: The product of two odd numbers is odd,
What we know: An odd number $n = 2k + 1$ for some $k \in \mathbb{Z}$.

$$(2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2\underbrace{(2ab + a + b)}_{k \in \mathbb{Z}} + 1 = 2k + 1.$$

2.2 Contradiction

Say we have some proposition T that we are tyring to prove. Here is how we can prove it by contradiction:

1. Assume T is not true.
2. Given T is false, use a direct proof to obtain a contradiction.
3. Since T being false leads us to a contradiction, T must be true.

Often T is of the form "If p then q." In this case, assume that p is true and q is false to reach a contradiction. Often, this contradiction will be of the form "If p is true and q is false then p is false. This is a contradiction as p cannot both be true and false.

For example

$$\text{If } \underbrace{n^2 \text{ is even}}_{p} \text{ then } \underbrace{n \text{ is even.}}_{q}$$

Proof. Assume for sake of contradiction that n^2 is even but n is odd. Since n is odd, $n = 2k + 1$ for some $k \in \mathbb{Z}$.
So $n^2 = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2m + 1$.

Where $m = 2k^2 + 2k$.

Since m is an integer, n^2 is odd. This is a contradiction since n^2 is even, and therefore if n^2 is even then n must also be even. □

Consider a set $A = \{a_1, ..., a_n\}$ with cardinality n.

Consider $f : P(A) \to \{0,1\}^n$ where $f(X) = s_1 s_2 ... s_n$ and $s_i = 1$ if $x_i \in X$ and $s_i = 0$ if $x_i \notin X$.

Claim: If $f(X_1) = f(X_2)$ then $X_1 = X_2$.

Proof. Assume for sake of contradiction that $f(X_1) = f(X_2)$ but $X_1 \neq X_2$. Since $X_1 \neq X_2$, there must be some element in one set but not the other. Assume without loss of generality that $a_i \in X_1$ and $a_i \notin X_2$. Then $f(X_1)$ will have a 1 at position i but $f(X_2)$ will have a 0 at position i. This is a contradiction as we began by assuming that $f(X_1) = f(X_2)$. □

Idea: Can you see how this could have been done as a direct proof?

2.3 Proof by Cases

Claim: There exists x, y irrational such that x^y is rational.

Proof. Consider $z = \sqrt{2}^{\sqrt{2}}$.

Case 1: z is rational. Let $x = y = \sqrt{2}$ then we are done.

Case 2: z is irrational. Then let $x = z$ and $y = \sqrt{2}$ and we get

$$\sqrt{2}^{\sqrt{2}*\sqrt{2}} = \sqrt{2}^2 = 2$$

□

2.4 Counterexample

Counterexamples help us prove that something is not true.

For example, suppose Kristy makes the claim that if xy is rational then x and y are rational.

Kareem can disprove her claim by coming up with a counterexample. For example, if $x = \sqrt{2}$ and $y = \sqrt{2}$, then $xy = 2$, which is rational.

However, you **cannot** prove a claim by showing one example of it. Kareem has not proven that x and y are irrational, he has just shown that they are not always rational.

For example, the claim "all CS22 students like donuts" can be disproved by finding a

student who does not like donuts. Finding this counterexample, however, will not prove that no students like donuts.

Claim: $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$

Proof. Consider $A = \{1\}$ and $B = \{2\}$.
Then $\{1, 2\} \in \mathcal{P}(A \cup B)$ but $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$. □

2.5 Proof by Element Method

How do you prove that $A = B$? First show that $A \subseteq B$ and then you show that $B \subseteq A$. If every element in A is also an element in B and every element in B is also an element of A, then A must equal B.

To show that $A \subseteq B$ you consider an arbitrary element in A and show it is also in B.

Claim: $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

Proof.

$$\begin{aligned} & x \in \mathcal{P}(A \cap B) \\ \iff & x \subseteq A \cap B \\ \iff & x \subseteq A \text{ and } x \subseteq B \\ \iff & x \in \mathcal{P}(A) \text{ and } x \in \mathcal{P}(B) \\ \iff & x \in \mathcal{P}(A) \cap \mathcal{P}(B) \end{aligned}$$

□

2.6 Bijective Proof

Example provided later. (Put together proofs for injectivity and surjectivity further down in this sheet, and then add conclusion.)

2.7 Bidirectional Proof

If a claim is of the form "A if and only if B," you must prove both "if A, then B" and "if B, then A"

2.8 Inductive Proof

More detail later.

3 Sets and Notation

A set is a collection of objects without order or repetition.

3.1 Membership vs. Subsets

If an object s is a member of a set S, we say $s \in S$. If a set T is a subset of a set S, we write $T \subseteq S$. This means that every member of T is also a member of S.

a. A is any set. Which of the following is **always true**?

   i. $A \subseteq A$ - T

   ii. $\{\} \subseteq A$ - T

   iii. $\{\} \in A$ - F

b. A is any set and $\mathcal{P}(A)$ is the set of all subsets of A. Which of the following is **always true**?

   i. $A \in \mathcal{P}(A)$ - T

   ii. $A \subseteq \mathcal{P}(A)$ - F

   iii. $\emptyset \in \mathcal{P}(A)$ - T

   iv. $\emptyset \subseteq \mathcal{P}(A)$ - T

   v. $\{A, \emptyset\} \subseteq \mathcal{P}(A)$ - T

c. S is the set of students in CS22. B is the set of students at Brown. Duncan is a student in CS22. Which of the following is **always true**?

   i. $S \subseteq B$ - T

   ii. Duncan $\subseteq S$ - F

   iii. Duncan $\in S$ - T

   iv. $\{\text{Duncan}\} \subseteq B$ - T

3.2 Set Operations

The union $A \cup B$ of two sets A and B is the set of all elements that are in A or B.

The intersection $A \cap B$ of two sets A and B is the set of all elements that are in A *and* B.

The set difference $B - A$ of two sets A and B is the set of all elements that are in B, but that are not in A.

The complement $\overline{A}$ of a set A is the set of all elements that are *not* in A (where "all elements" refers to all elements in some universal set U.)

The cardinality $|A|$ of a set A is the number of elements of A. Remember that sets have no duplicates!

3.3 Power Sets

The *power set* of a set S, denoted $\mathcal{P}(S)$ is the set of all subsets of S. The power set of S has cardinality $2^{|S|}$. We proved this last result by noticing that there are the same number of subsets of a set of size n as there are binary strings of length n (see the sample bijective proof on the website).

3.4 Product

The product of two sets A and B, denoted $A \times B$, is the set of all ordered pairs (a, b) for $a \in A$, $b \in B$. The product of a single set, A, is the set of all ordered pairs (a, a) where $a \in A$.

4 Relations

4.1 Relation on $A \times B$ vs. Relation on A

A *relation* R on the sets A and B is a subset of the Cartesian product $A \times B$. A relation R on the set A is a subset of the Cartesian product $A \times A$.

Always remember to specify the set(s) on which the relation is defined!

4.2 Notation

aRb and $(a, b) \in R$ are both compact ways of saying the same thing: a is related to b in R.

Remember that a relation is a set of ordered pairs, not a description of the way elements are linked. For example, the following is a relation on $\mathbb{Z}$:

$$R = \{(x, y) \mid x \leq y\}.$$

However, "$\leq$" is not a relation.

4.3 Reflexivity

A relation R on A is *reflexive* if for all $a \in A, (a, a) \in R$. In other words, a relation is reflexive if *every element* in the set A is related to itself in R. This is why it's important

to specify a set when talking about a relation: you can't tell if a relation is reflexive if you don't know which elements have to be related to themselves (and every element must be!)

4.4 Symmetry and Transitivity

A relation R on A is *symmetric* if for all $a, b \in A$, the following holds: **if** $(a, b) \in R$, **then** $(b, a) \in R$.

A relation R on A is *transitive* if for all $a, b, c \in A$, the following holds: **if** $(a, b) \in R$ and $(b, c) \in R$, **then** $(a, c) \in R$. Remember that a, b, and c do not need to be different elements.

It's important to note that the definitions of symmetry and transitivity are phrased as if-then statements. A relation is symmetric/transitive *unless* it violates the appropriate if-then condition. To violate the condition, you must simultaneously satisfy the if-clause, and violate the then-clause.

Consider the following example of a relation that is not transitive: the order pairs $(1, 2)$ and $(2, 1)$ are in the relation (this satisfies the if-clause of the transitivity definition) but there is no pair $(1, 1)$ in the relation (this violates the then-clause.) As another illustrative example: any empty relation is both symmetric and transitive, as there are no ordered pairs in the empty relation to satisfy the if-clause of either definition.

4.5 Equivalence Relation

An *equivalence relation* is a relation that is reflexive, symmetric, and transitive.

4.6 Equivalence Classes

Let R be an equivalence relation on A. Then the *equivalence class* of $a \in A$ is defined as

$$[a]_R := \{x \mid x \in A, (x, a) \in R\}.$$

Note that a is not unique (unless it is the only element in its equivalence class.) Rather, any element in the same equivalent class can serve equally well as the representative for the class.

An equivalence relation splits a set into equivalences classes. In other words, it forms a partition of the set.

A *partition* of a set A is a collection of nonempty subsets $B_1, \ldots, B_k$ of A such that

1. $B_1 \cup \cdots \cup B_k = A$, and
2. $B_i \cap B_j = \emptyset \quad \forall i, j$ where $i \neq j$.

4.7 Examples

Consider the set B of all students at Brown. For each of the following relations on B, state if they are reflexive, symmetric, or transitive. If they are an equivalence relation then list the equivalence classes.

i. Two students are related if they are the same age (e.g. 21).

   Reflexive, symmetric, and transitive. Therefore equivalence relation. equivalence classes are students of each age.

ii. s_1 and s_2 are students and $(s_1, s_2) \in R$ if s_1 is younger than s_2.

   Transitive but not reflexive or symmetric.

iii. Two students are related if they are studying anthropology.

   Symmetric and transitive but not reflexive

iv. Two students are related if they go to Brown.

   Reflexive, symmetric, and transitive. Therefore equivalence relation. One equivalence class which consists of all students at Brown.

Let $A = \{1, 2, 3\}$. Consider the following relations on $\mathcal{P}(A)$. State if they are reflexive, symmetric, or transitive. If they are an equivalence relation then list the equivalence classes.

i. $(S_1, S_2) \in R$ if $|S_1| = |S_2|$.

   Reflexive, symmetric, and transitive. Therefore equivalence relation. equivalence classes are sets of each size.

ii. $(S_1, S_2) \in R$ if $S_1 \subseteq S_2$.

   Reflexive and transitive but not symmetric.

iii. $(S_1, S_2) \in R$ if S_1 and S_2 share an element.

   Symmetric, but neither reflexive (suppose $S_1 = S_2 = \emptyset$) nor transitive.

5 Functions

5.1 Formal Definition

A *function* $f : A \to B$ is a relation on A and B with the following property: for every $a \in A$ there exists exactly one pair (a, b) in the relation, where $b \in B$.

We call A the domain and B the codomain.

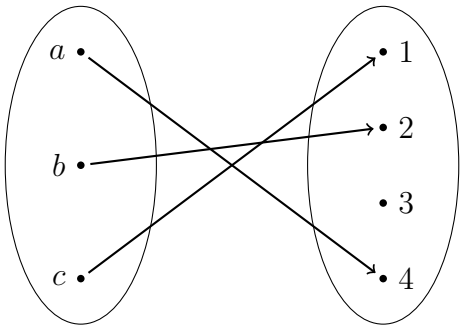
It's important to note that a function is characterized not only by the "rule" that maps inputs to outputs, but also by the domain and codomain.

Additionally, we call the set of all $b \in B$ such that there exists $a \in A$ where $f(a) = b$ the *image* of f. In other words, the image is the set of all elements mapped to by f.

5.2 Injectivity

A function is injective if for all $b \in B$, there exists at most one $a \in A$ such that $f(a) = b$. In other words, no two distinct elements map to the same thing! Another way to think about this: if you give me an element in the image of the function, I can tell you without a doubt which element mapped to it. Why? Because there won't be more than one element that maps to it.

If a function $f : A \to B$ is injective, we know that $|A| \leq |B|$. This is because every element in A needs some unmatched element in B, so B needs to have at least as many elements as A!



There are two ways to prove that a function is injective:

1. Consider two arbitrary distinct elements in the domain. Show that they must map to distinct outputs.

   Proof. Consider the function $f : \mathbb{Z} \to \mathbb{E}$ (where $\mathbb{E}$ is the set of even integers) defined by $f(x) = 2x$. Consider distinct elements $a, b \in \mathbb{Z}$. Assume for the sake of contradiction that $f(a) = f(b)$. Note that $f(a) = 2a$ and $f(b) = 2b$, which means $2a = 2b$. But $2a \neq 2b$ since $a \neq b$. Thus $f(a) \neq f(b)$, meaning

that f is injective. □

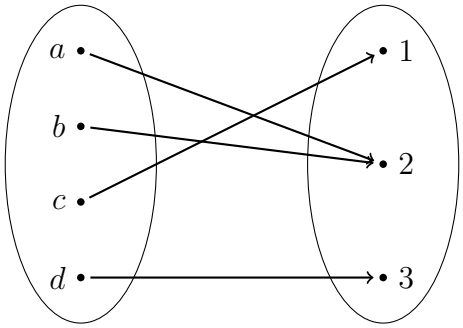
2. Consider two equal elements in the image of f (say, $f(a)$ and $f(b)$.) Show that $a = b$.

Proof. Consider the function $f : \mathbb{Z} \to \mathbb{E}$ defined by $f(x) = 2x$. Consider $f(a)$ and $f(b)$ in the image of f, where $f(a) = f(b)$. Note that $f(a) = 2a$ and $f(b) = 2b$. Thus, $2a = 2b$, meaning that $a = b$. This proves injectivity. □

5.3 Surjectivity

A function is surjective if for all $b \in B$, there exists at *least* one $a \in A$ such that $f(a) = b$. In other words, no element in the codomain gets left behind: there is always some element that maps to it. Equivalently, a function is surjective if the image of the function is the entire codomain.

If a function $f : A \to B$ is surjective, we know that $|A| \geq |B|$. This is because every element in B needs some element in A to map to it, so A needs to have at least as many elements as B.



To prove that a function is surjective, consider an arbitrary element in the codomain, and construct the specific element in the domain that maps to it.

Proof. Consider the function $f : \mathbb{Z} \to \mathbb{E}$ defined by $f(x) = 2x$. Consider an arbitrary element in the codomain b. Since b is even, $b = 2a$ for some $a \in \mathbb{Z}$. By definition of f, $f(a) = 2a = b$, and so we've found the element that maps to b. This proves surjectivity. □

5.4 Bijectivity

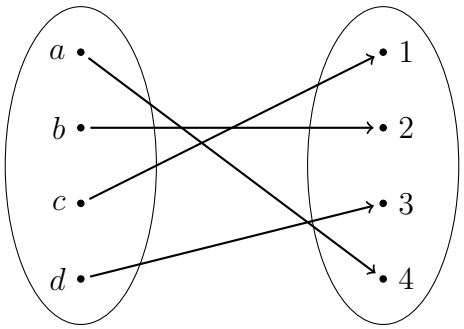
A bijection is a function that is both injective and surjective. Thus, to prove that a function is a bijection, prove that it is injective and surjective.

If we combine our results from injectivity and surjectivity, we know that the cardinality of the domain must be less than or equal to that of the codomain (by injectivity),

and that the cardinality of the domain must be greater than or equal to that of the domain (by surjectivity.) Thus, the cardinalities of the two sets must be equal. This is a powerful result:

There exists a bijection between two sets if and only if they have equal cardinality.

Thus, to prove that the sizes of two sets are equal, it suffices to prove that there exists a biejction between them.



5.5 Intuition and Examples

For each of the following, state if it is a function, injections, surjection, or neither.

(a) $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2$

A function but not injective or surjective.

(b) $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ where $f(x) = x^2$. $\mathbb{Z}^+$ denotes the positive integers.

Injection.

(c) $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = \sqrt{x}$.

Not a function.

(d) f : First Year Students at Brown $\to$ First Year Dorms at Brown where f(student) = the dorm that the student lives in.

Surjection.

(e) f : Students at Brown $\to$ Banner IDs of current Students where f(student) = the banner ID of student.

Bijection.

(f) f : People in the World $\to \{0, 1\}$ where f(person) $= 1$ if they are Prof. Littman and 0 otherwise.

Surjection.

(g) f : Library at Brown $\to \mathbb{Z}$ where $f(\text{Library})$ = number of books in the library.
Injection.

(h) $f : S \to \mathcal{P}(S)$ where $f(S) = \{S\}$.
Injection.

(i) $f : \mathcal{P}(\{1, 2, 4\}) \to \{0, 1, 2, 3\}$ where $f(X) = |X|$.
Surjection.

6 Induction

6.1 Example 1: Template and Weak Induction

Idea: If you are stuck on an induction problem on the exam, start by writing out the inductive hypothesis and the structure of the proof. You will receive partial credit for this and it will also help you think of how to proceed.

Idea: Often the inductive step is a direct proof using the inductive hypothesis. This is not always the case, sometimes you might have to use ***different cases*** *or even* ***contradiction***

We will first provide a review of the template for an inductive proof and provide an example.

For example, say we are trying to prove that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ is true for all $n \in \mathbb{N}$.

1. Define the predicate $P(n)$.
   Let $P(n)$ be the predicate that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.
2. Show that the base case is true.
   We will first show $P(0)$ is true. $\sum_{i=0}^{0} i = 0$ and $\frac{0(0+1)}{2} = 0$ so they are equal as needed.
3. Assume the inductive hypothesis is true. If you are using stardard induction then you will assume $P(k)$ is true for some integer k. If you are using strong induction then you will assume $P(i)$ is true for all $i \leq k$. Either way, you should specify that k is some integer greater than or equal to your greatest base case.
   Assume $P(k)$ is true for some arbitrary integer $k \geq 0$.
4. Show that $P(k + 1)$ is true given the inductive hypothesis.

We will now show that $\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

We know that $\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + (k+1)$.

By our inductive hypothesis $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$.

Therefore

$$\begin{aligned}\sum_{i=0}^{k+1} i &= \left(\sum_{i=0}^{k} i\right) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}\end{aligned}$$

as needed. □

5. Conclude the proof.

   Therefore, as $P(0)$ *is true and* $P(k)$ *implies* $P(k+1)$ *for all* $k \in \mathbb{Z}$, $k \geq 0$, $P(n)$ *is true for all nonnegative integers* n.

6.2 Example 2: Strong Induction

Define the sequence S as follows: $S_1 = 1$, $S_2 = 3$, $S_n = S_{n-1} * S_{n-2}$ for integers $n \geq 2$. Prove that S_n is odd for all positive integers n.

Proof. Let $P(n)$ be the predicate that S_n is odd.

Base Cases: $S_1 = 1$ and $S_2 = 3$, which are both odd, so $P(1)$ and $P(2)$ are both true.

Inductive Hypothesis: For some arbitrary integer $k \geq 2$, assume for all positive integers $i \leq k$ that $P(i)$ is true. That is, assume S_1 through S_k are odd.

Inductive Step: Consider S_{k+1}. As $k \geq 2$, $S_{k+1} = S_k * S_{k-1}$. By the inductive hypothesis, S_k and S_{k-1} are both odd. As we proved in section 2.1, the product of two odd numbers is odd, so S_{k+1} is odd. Therefore, $P(k+1)$ is true.

Conclusion: Thus, as $P(1)$ and $P(2)$ are true and for any positive integer k, $P(1)$,...,$P(k)$ imply $P(k+1)$, $P(n)$ is true for all positive integers n, so all terms in the sequence are odd. □

7 Number Theory

7.1 Definitions

Definition 1: We say that a *divides* b, denoted $a \mid b$, when $b = ka$ for some $k \in \mathbb{Z}$.

Definition 2: We say that a is *congruent* to b mod m, denoted $a \equiv b \pmod{m}$, if $m \mid (b - a)$. Another way to say this is that $a = b + km$ for some $k \in \mathbb{Z}$. Yet another way to say this: a and b have the same remainder upon division by m. Take a moment to convince yourself that these statements are equivalent.

7.2 Properties of Congruence Relations:

For $a, b \in \mathbb{Z}$, if $a \equiv b \mod m$, then

- $a + c \equiv b + c \mod m$ for $c \in \mathbb{Z}$
- $ac \equiv bc \pmod{m}$ for $c \in \mathbb{Z}$
- $a^n \equiv b^n \mod m$ for $n \in \mathbb{Z}^+$

If we also have $c \equiv d \pmod{m}$, then

- $a + c \equiv b + d \mod m$
- $ac \equiv bd \mod m$

7.3 GCD

The greatest common denominator of a and b is the largest positive integer which divides both a and b. To find the gcd of two numbers, we can run the Euclidean algorithm.

Theorom 1: For any $a, b \in \mathbb{Z}$ there exists $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$. In words, we say that a and b can be written as a linear combination of their gcd.

Theorem 2: An integer is a linear combination of a and b if and only if it is a multiple of their gcd.

7.4 Multiplicative Inverse

Consider the particular congruence

$$ax \equiv 1 \pmod{m}.$$

If this equation has a solution, then we know we can find some integer x which, when multiplied by a, yields $1 \pmod{m}$. We define this integer to be the *multiplicative*

inverse of $a \pmod m$, and we denote it a^{-1}. If a multiplicative inverse exists $\pmod m$, then when working $\pmod m$, we can "divide" by a—that is, we can multiply two sides of a congruence by a^{-1}, cancelling a from both sides.

When does a multiplicative inverse exist? According to the above Theorem 2: a^{-1} exists if and only if $\gcd(a, m)$ divides 1 (which is c in this particular congruence.) For something to divide 1, it must itself be 1. Thus, a^{-1} exists $\pmod m$ if and only if $\gcd(a, m) = 1$, that is, if and only if a and m are relatively prime.

How do we find the multiplicative inverse? We can run the Euclidean algorithm and then backtrack to obtain the multiplicative inverse (gcdcombo).

7.5 Fermat's little Theorem

If p is prime and does not divide $a \in \mathbb{Z}$ then

$$a^{p-1} \equiv 1 \pmod p.$$

This means a^{p-2} is a multiplicative inverse for $a \bmod p$.

7.6 Euler's Totient Function

The totient function of n is a count of how many positive integers less than or equal to n are relatively prime to it. For any prime p, $\phi(p) = p - 1$.

If m and a are relatively prime, then

$$a^{\phi(m)} \equiv 1 \pmod m.$$

This means $a^{\phi(m)-1}$ is a multiplicative inverse for $a \bmod m$. Fermat's little theorem is just a special case of this rule.

7.7 Example Problems

1. Prove that if $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a + c \equiv b + d \pmod m$

   Proof. $a \equiv b \pmod m$, $c \equiv d \pmod m \implies m|(a - b)$ and $m|(c - d)$ so $a - b = mk$ and $c - d = mj$ for some integers k and j. Adding these two equations, $a - b + c - d = mk + mj$ means $(a + c) - (b + d) = (k + j)m$. Integers are closed under addition so $k + j$ is an integer, $m|((a + c) - (b + d))$ and $a + c \equiv b + d \pmod m$ □

2. Compute the multiplicative inverse of 8 mod 27 with the Euclidean algorithm

and the Euler-Fermat method.
$27 = 8 * 3 + 3$
$8 = 3 * 2 + 2$
$3 = 2 * 1 + 1$
Backtracking:
$2 = 8 - 3 * 2$ so $1 = 3 - (8 - 3 * 2) = 3 * 3 - 8$
$3 = 27 - 8 * 3$ so $1 = 3 * (27 - 8 * 3) - 8$
$1 = 3 * 27 - 10 * 8$
So -10 is a multiplicative inverse of 8 mod 27. The only numbers less or equal to than 27 not relatively prime to it are the multiples of 3, which there 9 of. $27 - 9 = 18$, so. A multiplicative inverse of 8 mod 27 is then $8^{18-1} = 8^{17}$