Midterm 1 Review Problems

Due: Never

All homeworks are due at 12:55 PM on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit.

Problem 1

Suppose A and B are sets. For each of the following, either prove the statement using the element method, or give a counterexample.

a. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

b. $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$

c. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ if and only if $A \subseteq B$

Solution

a. **Proof:** Let $X \in \mathcal{P}(A \cap B)$. Then $X \subseteq A \cap B$. So for all $x \in X$, $x \in A \cap B$. For each $x \in X$, since $x \in A \cap B$, $x \in A$. Therefore $X \subseteq A$. By the same reasoning $X \subseteq B$. So $X \in \mathcal{P}(A)$, and $X \in \mathcal{P}(B)$. Therefore $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

   Conversely, let $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Then $X \subseteq A$ and $X \subseteq B$. So for every $x \in X$, both $x \in A$ and $x \in B$; this implies $x \in A \cap B$. So $X \subseteq A \cap B$. Therefore, $X \in \mathcal{P}(A \cap B)$. $\square$

b. **Counterexample:** Let $A = \{1\}$ and $B = \{2\}$, so $A \setminus B = \{1\}$. Then $\mathcal{P}(A \setminus B) = \{\varnothing, \{1\}\}$. On the other hand, $\mathcal{P}(A) = \{\varnothing, \{1\}\}$ and $\mathcal{P}(B) = \{\varnothing, \{2\}\}$, so $\mathcal{P}(A) \setminus \mathcal{P}(B) = \{\{1\}\}$. In particular, $\varnothing$ is in $\mathcal{P}(A \setminus B)$ but not in $\mathcal{P}(A) \setminus \mathcal{P}(B)$, so the two sets are not equal.

c. **Proof:** For each direction, we use a proof by element method.

   First, assume $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Suppose that $a \in A$. Then the one-element set $\{a\}$ is a subset of A, so $\{a\} \in \mathcal{P}(A)$. But then, since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, it follows that $\{a\} \in \mathcal{P}(B)$. This means that $\{a\} \subseteq B$, hence $a \in B$.

Now assume $A \subseteq B$. Suppose that $X \in \mathcal{P}(A)$, i.e. $X \subseteq A$. Then for all $x \in X$, $x \in A$, and since $A \subseteq B$, $x \in B$. So $X \subseteq B$, i.e. $X \in \mathcal{P}(B)$. $\square$

Problem 2

Let S be a set with cardinality n. Prove using a bijection that the number of subsets of S of size k is equal to the number of subsets of size $n - k$.

Solution

We define a function f from the subsets of S of size k to the subsets of S of size $n - k$ by:

$$f(A) = S - A$$

Note that f is total, as the set difference of $S - A$ is well-defined for any A. Additionally, note that $S - A$ always produces a subset of S of size $n - k$ since S has cardinality n, A has cardinality k, and A is a subset of S.

We proceed to show that f is a bijective function by showing that it is injective and surjective:

- f is injective

  Proof. Assume for the sake of contradiction that f is not injective. Then, there exist some k-cardinality subsets A and B of S such that $A \neq B$ and $f(A) = f(B)$. Because $A \neq B$, without loss of generality we can say that there must be some element $x \in S$ such that $x \in A$ and $x \notin B$.

  Thus, $x \notin S - A$, since $x \in A$, and $x \in S - B$, since $x \in S$ and $x \notin B$. By the definition of f, this gives us $f(A) = S - A \neq S - B = f(B)$, but this contradicts our assumption that $f(A) = f(B)$. Thus, it cannot be that f is not injective, and it must be that f is injective. $\square$

- f is surjective

  Proof. Consider an arbitrary $n - k$ element subset B of S. Then, $S - B$ is an $n - (n - k) = k$ element subset of S, since S has cardinality n and $B \subseteq S$.

Consider $f(S - B)$. For any element $x \in S$,

$$\begin{aligned} x \in f(S-B) &\iff x \in S - (S - B) \\ &\iff x \in S \text{ and } x \notin S - B \\ &\iff x \in S \text{ and } x \in B \\ &\iff x \in B \end{aligned}$$

Thus, $f(S - B) = B$, and we have shown that for any output in the codomain of f it is possible to construct an input in f's domain that maps to the given output. By definition, f is surjective. □

Because f is a total functon that is both injective and surjective, it is bijective. Thus, the cardinality of its domain is equal to the cardinality of its codomain, and the number of k element subsets of S is equal to the number of $n-k$ element subsets of S.

Problem 3

a. Prove that provided two bijections $f : Q \to R$ and $g : R \to Q$, their composition, $f \circ g$, is a bijection for any non-empty sets Q, R. The composition is defined as $f \circ g(x) = f(g(x))$ for any $x \in R$.

b. Applying an arbitrary function repeatedly to some initial value is called an *iterated map*. Let f be a bijection $f : R \to R$.

Let g_n be a function $g_n : R \to R$ that applies f n times where $n \geq 1$.

That is, $g_n(x) = f(f(f(\ldots f(x)\ldots)))$ where f is applied n times.

Prove that g_n is a bijection using induction.

Solution

a. *Proof.* We will now prove that $f \circ g$ is a bijection from $R \to R$, by showing it is both injective and surjective.

Injective Assume for the sake of contradiction $x, y \in R$ s.t. $x \neq y, f \circ g(x) = f \circ g(y)$. Because f is a bijection, each element of the domain maps to exactly one element of the codomain. Therefore, if $f \circ g(x) = f \circ g(y)$, then $g(x) = g(y)$. By the same reasoning, if $g(x) = g(y)$, then $x = y$. However, we previously assumed that x and y were distinct. Thus, we have reached a contradiction, proving injectivity.

Surjective Assume for the sake of contradiction that there exists an element $y \in R$ that is not mapped to by $f \circ g$.

By definition, g is surjective. Thus, because Q and R are nonempty, there must $\exists q \in Q$ s.t. $g(q) = y$. Similarly, because f is surjective and $g(q) \in R$, $\exists r \in Rs.t.f(g(q)) = y$.

Therefore, we have reached a contradiction because we have found a $r \in R$ s.t. $f \circ g(r) = y$ Thus, because all values in R are mapped to, $f \circ g$ is surjective.

Because $f \circ g$ is both injective and surjective, $f \circ g$ is a bijection. □

b. *Proof.* We will now prove that g_n is a bijection by induction on n. Let $P(i)$ be the property that g_i is a bijection.

Base case By defintion, g_1 is equivalent to $f(x)$. Because $f(x)$ is by definition a bijection from $\mathbb{R} \to \mathbb{R}$, $P(1)$ is true.

Inductive Step Assume $P(k)$ holds for some positive integer k. We must now prove that P(k + 1) holds.

By definition, $g_{k+1} = f(g_k)$. Because f is a bijection and g_k is a bijection, g_{k+1} is a composition of two bijections. Therefore, as proven in part a, g_{k+1} must also be a bijection.

Hence, because $P(1)$ is true and for all k and $P(k)$ implies $P(k+1)$, $P(n)$ is true for all $n \geq 1$ by induction. □

Problem 4

Let R be an equivalence relation on A, where $|A| = n$.

a. What is the minimum size of R, in terms of n? Justify why you can achieve this size and why no smaller size can be achieved.

b. What is the maximum size of R, in terms of n? Justify why you can achieve this size and why no larger size can be achieved.

c. Suppose n is even. What can you say about the parity of $|R|$? Justify your response.

d. Suppose n is odd. What can you say about the parity of $|R|$? Justify your response.

Solution

a. An equivalence relation must be reflexive, symmetric, and transitive. Going through these properties, we will determine what at minimum needs to be in a relation for it to be an equivalence relation.

For a relation to be reflexive, each element of A must be related to itself. Let L be a relation that satisfies this property and contains no other ordered pairs, $L = \{(a, a) \mid a \in A\}$. This would make $|L| = |A|$.

To satisfy symmetry, for each ordered pair $(a, b) \in R$, (b, a) must be an element of R. Choose an arbitrary ordered pair from the relation L defined above. Because of how L is defined, this ordered pair must be of the form (a, a) for some $a \in A$. So, the reverse of this ordered pair, (a, a), is the same as the original, so it is also in L. Thus, L is symmetric.

To satisfy transitivity, for each pair of ordered pairs $(a, b), (b, c) \in R$, (a, c) is R. Just as before, an arbitrary ordered pair from L will be of the form (a, a) for some $a \in A$. If we choose another ordered pair from L such that a is an element of the ordered pair, this can only be (a, a). As $(a, a) \in L$, L is transitive.

Therefore, as L is reflexive, symmetric, and transitive, it must be an equivalence relation. Since removing an element of L would make it no longer satisfy reflexivity and thus no longer be an equivalence relation, L must be the smallest possible equivalence relation on A. $|L| = n$, as stated above, so the minimum size of any equivalence relation on A is n.

b. Let L be the largest possible relation on A, in which each element of A is related to each element of A. This makes L the Cartesian product $A \times A$.

Now, we must check whether this is already an equivalence relation or if we would need to remove ordered pairs to make it one.

As every element of A is related to every element of A, it must be the case that each element of A is related to itself, so L satisfies reflexivity.

Let $(a, b) \in L$ for some arbitrary elements $a, b \in A$. Based on the definition of L, we know that it is also true that $(b, a) \in L$, so L satisfies symmetry.

Finally, let $(a, b),\ (b, c) \in L$ for some arbitrary elements $a, b, c \in A$. Based on the definition of L, we know that $(a, c) \in L$, so L satisfies transitivity.

Thus, as L is reflexive, symmetric, and transitive, L is an equivalence relation. So, the largest possible relation on A is an equivalence relation.

As $L = A \times A$, $|L| = |A \times A| = n * n = n^2$. Therefore, the maximum size of an equivalence relation on A is n^2.

c. As shown in part a, R must minimally have size n when each element is related just to itself. Starting from this relation, consider what happens when we add a new ordered pair (a, b) for some elements $a, b \in R$. To satisfy symmetry, we must also add the ordered pair (b, a). Therefore, when we add to an equivalence relation, we have to do so in **pairs** of ordered pairs.

Note that this is also true when we consider transitivity. If we have to add to the relation to satisfy transitivity, we will be adding two ordered pairs. For instance, if $(a, b), (b, c) \in R$ and we must add (a, c), then to maintain symmetry we must also add (c, a).

So, the size of the relation must be $n + 2m$, where m is some nonnegative integer, as we start from a relation of size n and add some even number of ordered pairs.

We will now prove that the sum of two even integers in an even integer. Let $x, y \in \mathbb{Z}$, so $2x$ and $2y$ are some arbitrary even integers. Consider the sum $2x + 2y$. This can be factored as $2(x + y)$. Because the sum of two integers is an integer and x and y are both integers, $x + y$ is an integer. So, $2(x + y)$ is an even integer. Therefore, we have shown that the sum of any two even integers is also an even integer.

As n is even and $2m$ is even, $n + 2m$ will be even. Thus, we know that $|R|$ must be even.

d. Just as in part c, the size of the relation must be $n + 2m$, where m is some nonnegative integer. However, unlike in part c, n is now odd.

We will now prove that the sum of an even integer and an odd integer is an odd integer. Let $x, y \in \mathbb{Z}$, so $2x$ is an arbitrary even integer and $2y + 1$ is an arbitrary odd integer. Consider the sum $2x + 2y + 1$. This can be rewritten as $2(x + y) + 1$. By the same reasoning as in part c, $2(x + y)$ is an even integer, which makes $2(x + y) + 1$ an odd integer. Therefore, we have shown that the sum of an even integer and an odd integer is an odd integer.

As n is odd and $2m$ is even, $n + 2m$ will be odd. Thus, we know that $|R|$ must be odd.

Problem 5

Suppose you have a stack of n pancakes of different sizes on a plate and a spatula. Further suppose that you can place your spatula under any of the n pancakes and flip the stack of pancakes above your spatula upside-down. In other words, one flip

will reverse the order of the pancakes from the top of the stack of pancakes to your spatula.

a. Describe an algorithm (procedure) to sort the n pancakes from largest at the bottom to smallest at the top using at most $2n$ flips.

b. Use induction to prove the correctness of your algorithm, namely that it will in fact sort the pancakes in at most $2n$ flips.

Solution

a. The algorithm is to always find the largest pancake, put your spatula underneath it, and flip the stack above this pancake so its order is reversed, putting the largest pancake on top. Then, place your spatula directly above the place in the stack that you want to put this top pancake (for the very first, largest pancake, this would be directly below the entire stack, right above the plate). Then flip the whole stack above this point so the top pancake is right above the place where the spatula was. This places the pancake in its correct position. After this, proceed recursively on all but the pancakes already sorted.

b. Proof is by induction:

Base case: The base case is $n = 1$, a stack containing a single pancake. We can sort a stack of one pancake in 0 flips, which is fewer than $2n = 2(1) = 2$, because a stack of one pancake is already sorted. Thus the base case is satisfied.

Inductive hypothesis: Assume that we can sort a stack of k pancakes in at most $2k$ flips.

Inductive step: We are given a stack of $k + 1$ pancakes. First we find the largest pancake, flip it to the top, then flip the whole stack so the largest pancake is on the bottom. This takes 2 flips. Now, the largest pancake is on the bottom. Therefore, we only need to sort the remaining k pancakes above the largest one, which we have already moved to the bottom. By the inductive hypothesis, this can be done in at most $2k$ flips. Therefore, the total number of flips to sort the whole stack of $k+1$ pancakes is $2+2k = 2(k+1)$, as needed.

Conclusion: Since we can sort a stack of one pancake in at most 2 flips, and assuming we can sort a stack of k pancakes in at most $2k$ flips implies we can sort a stack of $k + 1$ pancakes in at most $2(k + 1)$ flips, we have proven the claim for stacks of pancakes of size n, for all n greater than or equal to 1.

Problem 6

Prove that if $4 \mid n-3$, then $8 \mid n^2-1$.

Solution

Factor $n^2-1=(n+1)(n-1)=(n-3+4)(n-3+2)$. Using $(n-3)=4k$ for $k \in \mathbb{Z}$, expand and get $(n-3+4)(n-3+2)=16k^2+24k+8=8(2k^2+3k+1)$, which is divisible by 8.

Problem 7

For $m \in \mathbb{Z}$, define the relation R_m on $M=\{1,\ldots,m-1\}$ by

$\{(x,y) \mid \exists a,b \in \mathbb{Z}^+,$ such that x^a and y^b have the same remainder when divided by $m\}$.

Prove that $\forall m \in \mathbb{Z}^+, R_m$ is an equivalence relation.

Solution

a. In order to show that R_m is an equivalence relation, we must show reflexivity, symmetry, and transitivity.

   Reflexivity - Let $x \in M$ and $a=b=1$. Then, we can say that $x^1 \equiv x^1 \pmod{m}$. Thus, $\forall x \in M$, $(x,x) \in R_m$.

   Symmetry - Let $(x,y) \in R_m$, then we know that $\exists a,b \in \mathbb{Z}^+$ *s.t.* $x^a \equiv y^b \pmod{m}$. This implies that $y^b \equiv x^a \pmod{m}$, which satisfies the conditions of the relation. Therefore, R_m is symmetric.

   Transitivity - Let $(x,y),(y,z) \in R_m$, then we can say that $\exists a,b,c,d \in \mathbb{Z}^+$ *s.t.* $x^a \equiv y^b \pmod{m}$ and $y^c \equiv z^d \pmod{m}$.

   If we raise both terms in the first congruence to the power c and both terms in the second conqruence to the power b, then we get $x^{ac} \equiv y^{bc} \pmod{m}$ AND $y^{bc} \equiv z^{db} \pmod{m}$. Thus, $x^{ac} \equiv z^{bd} \pmod{m}$.

   We've shown reflexivity, symmetry, and transitivity for R_m, and we've done so using properties of modular arithmetic that hold for all $m \in \mathbb{Z}^+$, so we can conclude that R_m is an equivalence relation.

b. If m is prime, then we know that $\forall x \in M$, $x^{m-1} \equiv 1 \pmod{m}$. This means that $\forall (x,y) \in M \times M$, $x^{m-1} \equiv y^{m-1} \equiv 1 \pmod{m}$. So, if we choose $a=b=$

$m-1$, then any $(x, y) \in M \times M$ is in R_M.

Since we know that $R_m \subseteq M \times M$ by definition of relations and that $M \times M \subseteq R_m$ by the above, we can conclude that $R_m = M \times M$.

Problem 8

For $a, n \in \mathbb{Z}^+$, prove the following identity by induction on n:

$$(a+1)^n \equiv an + 1 \pmod{a^2} \tag{1}$$

Solution

Let $P(k)$ be a predicate that is true if $(a+1)^k \equiv ak + 1 \pmod{a^2}$, and false otherwise.

Base Case: For $n = 1$, we have that $(a+1)^1 \equiv a(1) + 1 \pmod{a^2}$. Both sides of the congruence equal $a + 1$, so both sides are congruent mod a^2.

Inductive Hypothesis: Assume that $P(k)$ is true, for some $k \geq 1$. That is, assume that $(a+1)^k \equiv ak + 1 \pmod{a^2}$.

Inductive Step: We want to show that $(a+1)^{k+1} \equiv a(k+1) + 1 \pmod{a^2}$.

We have assumed that $(a+1)^k \equiv ak + 1 \pmod{a^2}$, so multiplying both sides by $a + 1$ gives us:

$$(a+1)(a+1)^k \equiv (a+1)(ak+1) \pmod{a^2} \tag{2}$$
$$\implies (a+1)^{k+1} \equiv a^2k + a + ak + 1 \pmod{a^2} \tag{3}$$
$$\implies (a+1)^{k+1} \equiv a + ak + 1 \pmod{a^2} \tag{4}$$
$$\implies (a+1)^{k+1} \equiv a(k+1) + 1 \pmod{a^2} \tag{5}$$

, where we can go from (2) to (3) because $a^2k \equiv 0 \pmod{a^2}$. This is what we wanted to show.

Conclusion: Thus, since $P(1)$ holds, and since $P(k) \implies P(k+1)$ for all positive integers $k \geq 1$, we must have that $(a+1)^n \equiv an + 1 \pmod{a^2}$ for all positive integers n.

Problem 9

We say integer a is divisible by integer b if there exists an integer m such that $a = bm$.

a. For a three-digit number ABC, where A, B, and C are the digits, prove that ABC is divisible by 7 if and only if $AB - (2 \cdot C)$ is divisible by 7. AB is a two-digit number with digits A and B.

   For example: The number 511 is divisible by 7 because $51 - 2(1) = 49$, which is divisible by 7.

b. Let's look at another type of integer that's divisible by 7. For digits A, B, and C, consider the function $\textsc{Repeat}(ABC) = ABCABC$, mapping three-digit integers to six-digit integers. For example, $\textsc{Repeat}(123) = 123123$ and $\textsc{Repeat}(442) = 442442$. (A digit is an integer between 0 and 9, inclusive.)

   Prove that for any three digits X, Y, and Z, $7 \mid \textsc{Repeat}(XYZ)$.

Solution

a. We can approach this problem from both directions.

- We want to show that if ABC is divisible by 7, then $AB - (2 \cdot C)$ is divisible by 7 as well. Assume that $ABC \equiv 0 \pmod 7$.

$$\begin{aligned} ABC \equiv 0 \pmod 7 &\Rightarrow (10 \cdot AB) + C \equiv 0 \pmod 7 \\ &\Rightarrow (3 \cdot AB) + C \equiv 0 \pmod 7 \\ &\Rightarrow 3 \cdot ((3 \cdot AB) + C) \equiv 0 \pmod 7 \\ &\Rightarrow (9 \cdot AB) + (3 \cdot C) \equiv 0 \pmod 7 \\ &\Rightarrow [(10 \cdot AB) + C] - [(9 \cdot AB) + (3 \cdot C)] \equiv 0 \pmod 7 \\ &\Rightarrow AB - (2 \cdot C) \equiv 0 \pmod 7 \end{aligned}$$

  Thus, we've shown that ABC being divisible by 7 implies that $AB-(2\cdot C)$ is also divisible by 7.

- Now, we want to show if $AB - (2 \cdot C)$ is divisible by 7, then ABC is also divisible by 7. Assume that $AB - (2 \cdot C) \equiv 0 \pmod 7$.

$$\begin{aligned} AB - (2 \cdot C) \equiv 0 \pmod 7 &\Rightarrow AB + (5 \cdot C) \equiv 0 \pmod 7 \\ &\Rightarrow (10 \cdot AB) + (50 \cdot C) \equiv 0 \pmod 7 \end{aligned}$$

$$\Rightarrow (10 \cdot AB) + C \equiv 0 \pmod 7$$
$$\Rightarrow ABC \equiv 0 \pmod 7$$

Thus, $AB - (2 \cdot C)$ being divisible by 7 implies that ABC is divisble by 7 as well. We've shown that ABC is divisible by 7 *if and only if* $AB - (2 \cdot C)$ is divisible by 7.

b. To prove this, note that any integer in the form $XYZXYZ$ is divisible by 1001 ($XYZXYZ = 1001 \times XYZ$). $7 \mid 1001$ because $1001 = 7 \times 143$, and therefore, $7 \mid XYZXYZ$.

Problem 10

Let m be an integer with exactly three factors: 1, p, and m, where $1 < p < m$.

a. Prove that p is prime.

b. Prove that $m = p^2$.

c. Imagine a series of n doors (numbered 1 through n), each of which is initially closed. A line of n people (also numbered 1 through n) walk past the doors, opening or closing them in the following manner: person i toggles[1] every door numbered with a multiple of i. Prove that, once every person is done, door d is open if and only if d is a perfect square.

Solution

Part a

Suppose $k|p$. Then, since $p|m$, we know $k|m$. However, k cannot be m, since $p < m$, so $k = 1$ or $k = p$. Thus, any factor of p is 1 or p itself, and thus p is prime.

Part b

Since $p|m$, we know $m = pk$ for some $k \in \mathbb{Z}$. This also means $k|m$, and so $k \in \{1, p, m\}$. We see $p \times 1 = p < m$, so $k \neq 1$; we further see $p \times m > m$ (since $p > 1$), so $k \neq m$. This means $k = p$, and so $m = p^2$.

[1] That is, opens the door if it is closed, or closes it if it is open.

Part c

We will first prove that a number $n \in \mathbb{Z}^+$ has an odd number of positive factors iff n is a perfect square.

Let $M_1 = \{m_1 : m_1 | n \text{ and } m_1^2 < n\}$, and let $M_2 = \{m_2 : m_2 | n \text{ and } m_2^2 > n\}$. In words, M_1 is the set of factors of n less than $\sqrt{n}$, and M_2 is the set of factors of n greater than $\sqrt{n}$.

Then, we can construct a bijection $f : M_1 \leftrightarrow M_2$ where $(m_1, m_2) \in f$ iff $m_1 m_2 = n$. We first see that f is a total function: for any given $m_1 \in M_1$, since m_1 is a factor of f, there is exactly one $m_2 \in \mathbb{Z}$ such that $m_1 m_2 = n$; further, this means m_2 is a factor of n, and it must be that $m_2^2 > n$ (or else $m_1^2 < n$ and $m_2^2 \leq n$, which implies $m_1 m_2 < n$); this means $m_2 \in M_2$, as needed.

We next show that f is injective: if $m_1 m_2 = n$ and $m_1' m_2 = n$, then $m_1 m_2 = m_1' m_2$, so $m_1 = m_1'$ and we have shown injectivity.

Lastly, we show f is surjective: if $m_2 \in M_2$, then there is some $m_1 \in \mathbb{Z}$ such that $m_1 m_2 = n$; further, this means m_1 is a factor of n, and it must be that $m_1^2 < n$ (or else $m_1^2 \geq n$ and $m_2^2 > n$, which implies $m_1 m_2 > n$); this means $m_1 \in M_1$, and since $m_1 m_2 = n$, we have $(m_1, m_2) \in f$, as needed.

We must then consider two possible cases: n is a perfect square, and n is not a perfect square.

n is a perfect square This means $n = k^2$ for some $k \in \mathbb{Z}$. Then, if we let F_n be the factors of n, $F_n = M_1 \cup \{k\} \cup M_2$ (we can see this is exhaustive by the definitions of M_1 and M_2), and M_1, M_2, and k are all disjoint (by the construction of M_1 and M_2). Further, we have shown $|M_1| = |M_2|$, so $|F| = 1 + 2|M_1|$, which means $|F|$ is odd.

n is not a perfect square This means that $\sqrt{n}$ is not an integer (and thus not a factor of n). Then, if we let F_n be the factors of n, $F_n = M_1 \cup M_2$. Again, these are exhaustive and disjoint by construction, and $|M_1| = |M_2|$, so $|F| = 2|M_1|$, meaning $|F|$ is even.

Now, we return to the original problem. Door d is toggled by person i iff $i|d$ (and each of those people toggles it exactly once). This means the number of times door d is toggled is the number of factors of d. We have shown that this means door d is toggled an odd number of times if d is a perfect square, and an even number of times if d is not a perfect square. Since each door starts closed, and it ends up open iff it has been toggled an odd number of times, we can then conclude that door d ends up open iff d is a perfect square.