

# 151 Excellent Exam 2 Review

soumilm, vchowdha

## Midterm 2

## 1 Things to Know

### 1.1 Induction

#### 1. General proof template:

☺ **Setup:** State what  $P(n)$  is explicitly. These are super easy points on the exam. Don't forget to use quotation marks and to quantify  $n$  **outside** of  $P(n)$ .

☺ **Base Case(s):** Explicitly state and prove your base cases. These should be very short proofs.  
Note: *It is possible to need multiple base cases in a weak induction proof!*

#### ☺ **Induction Step:**

👤 In weak induction, you assume  $p(n)$  for some  $n \geq n_l$ , where  $n_l$  is your last base case and you want to prove  $p(n+1)$

👤 In strong induction, you assume  $p(k)$  for all  $n_0 \leq k \leq n$  for some  $n \geq n_l$  where  $n_0$  is the first base case and  $n_l$  is the last base case and again want to show  $p(n+1)$ . Be careful with the quantification of  $n$  and  $k$  here!

💀 Going back to the domino analogy, you show that for any domino after and including the last base case domino, if all previous dominoes fell, then the next one will fall too

👤 Remember that you are proving an *implication* - a common mistake is to assume  $p(n+1)$  and show a true statement, but this doesn't work

👤 For more mistakes and other useful tips, go to Parmita's Ponderings from the course website

### 1.2 Relations

#### 1. Definitions

☺ A **relation** on a set  $S$  is a subset of  $S \times S$

☺ Types of relations:

👤 A relation  $R$  on  $S$  is an **equivalence relation** iff it satisfies these three properties:

💀 Reflexivity:  $x R x \quad \forall x \in S$

💀 Symmetry:  $x R y \implies y R x \quad \forall x, y \in S$

💀 Transitivity:  $x R y \wedge y R z \implies x R z \quad \forall x, y, z \in S$

👤 A relation  $R$  on  $S$  is an **order relation** iff it satisfies these three properties:

💀 Reflexivity

💀 Antisymmetry:  $x R y \wedge y R x \implies x = y \quad \forall x, y \in S$

💀 Transitivity

☺ The **equivalence class** of  $x \in S$  under some equivalence relation  $\sim$  on  $S$  is defined as the set of all  $y \in S$  such that  $x \sim y$

#### 2. The set of all equivalence classes for some relation $R$ on set $S$ forms a partition of the set $S$

Note: *This is a pretty useful proof to review and/or try yourself*

## 1.3 Number Theory

### 1.3.1 Not Modular Arithmetic

#### 1. Divisors

- ☺ Let  $a, b \in \mathbb{Z}$ . Then,  $b \mid a$  iff  $a = bk$  for some  $k \in \mathbb{Z}$
- ☺ Let  $a, b \in \mathbb{Z}$ . Then,  $d$  is the **greatest common divisor** of  $a$  and  $b$  iff:
  - 🔔  $d \mid a$
  - 🔔  $d \mid b$
  - 🔔  $\forall d' \in \mathbb{Z}, d' \mid a \wedge d' \mid b \implies d' \mid d$

Note: Be especially careful about showing the last point. A very common mistake is to use the “greatest” part of the gcd to make claims about the relative sizes of  $d, a, b$ . While this is true, it doesn’t follow from the definitions and doesn’t always hold.

- ☺  $a$  and  $b$  are **relatively coprime** iff  $\gcd(a, b) = 1$
- ☺ **Euclid’s Lemma**: Let  $a, b, c \in \mathbb{Z}$ . If  $a$  and  $b$  are coprime and  $a \mid bc$ , then  $a \mid c$ .

#### 2. Linear Diophantine Equations

- ☺ A **linear diophantine equation** is an equation of the following form  $ax + by = c$ , where  $a, b, x, y, c \in \mathbb{Z}$  and the goal is to find  $x, y$ .
- ☺ Theorem behind the **Euclidean Algorithm**: Let  $a, b, q, r \in \mathbb{Z}$  and suppose  $a = bq + r$ . Then,  $\gcd(a, b) = \gcd(b, r)$ .
- ☺ Make sure to know how to do the Euclidean algorithm and extended Euclidean algorithm. Common mistakes:
  - 🔔 Messing up arithmetic - double check your work at each step
  - 🔔 In the back substitution part of the extended Euclidean algorithm, simplify at each step instead of waiting till the end. This will make you less likely to make arithmetic errors
- ☺ **Bezout’s Lemma**: Let  $a, b, c \in \mathbb{Z}$ . Then,  $ax + by = c$  has a solution  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  iff  $\gcd(a, b) \mid c$
- ☺ Given a solution  $(x_0, y_0)$  to an LDE  $ax + by = c$ ,

$$x = x_0 + k \left( \frac{b}{\gcd(a, b)} \right), y = y_0 - k \left( \frac{a}{\gcd(a, b)} \right)$$

is another solution, for some  $k \in \mathbb{Z}$

#### 3. Primes

- ☺ Let  $p \in \mathbb{Z}$ . Then  $p$  is **prime** iff  $p \mid ab \implies p \mid a \vee p \mid b \forall a, b \in \mathbb{Z}$  and  $p$  is not a unit and not zero.
- ☺ Let  $a \in \mathbb{Z}$ . Then,  $a$  is **irreducible** iff  $a$  is a nonzero non-unit and for all  $m, n \in \mathbb{Z}, a = mn \implies m$  or  $n$  is a unit.
- ☺ Know how to prove  $p$  is prime  $\iff p$  is irreducible.
- ☺ Another useful proof to review is the induction step of the unique prime factorization theorem.

### 1.3.2 Modular Arithmetic

#### 1. The three definitions of $a \equiv b \pmod{n}$ :

- ☺  $n \mid (a - b)$
- ☺  $a = nk + b$  for some  $k \in \mathbb{Z}$
- ☺  $a$  and  $b$  leave the same remainder when divided by  $n$  (assume  $n$  is not zero)

Note: Exercise: verify that the three properties are indeed equivalent

## 2. Congruence modulo $n$ is an equivalence relation

- ☺ Verify the three properties (should be straightforward using the definitions)
- ☺ Be careful not to confuse the modular congruence defined here with the `mod` operator used in many programming languages - when we talk about mods, we're talking about a different notion of *equality*, not an operation

## 3. Things you can do with mods

- ☺ Add congruent statements i.e. if  $a \equiv_n b$  and  $c \equiv_n d$ , then  $a + c \equiv_n b + d$
- ☺ Multiply congruent statements i.e. if  $a \equiv_n b$  and  $c \equiv_n d$ , then  $ab \equiv_n cd$
- ☺ Substitute a value for something it is congruent to (does not hold if the number is an exponent):  
 $a \equiv_n b$  and  $a \equiv_n c$  implies  $c \equiv_n b$  (note this just holds because of transitivity)
- ☺ Raise both sides of a congruent statement to the *same* power
- ☺ Multiply by the multiplicative inverse (see below for why dividing isn't a thing)

## 4. Common modular arithmetic things you'll have to do and useful theorems

- ☺ To solve for the multiplicative inverse of  $k$  modulo  $n$ , you need to find  $u \in \mathbb{Z}$  such that  $ku \equiv 1 \pmod n$ . This can be done by solving  $ku + jn = 1$  via the extended Euclidean algorithm (note we used the second definition of modular congruence here).
- ☺ **Fermat's Little Theorem:** If  $p$  is prime and  $\gcd(a, p) = 1$ , then  $a^p \equiv a \pmod p$ . This also means  $a^{p-1} \equiv 1 \pmod p$ .
- ☺ **Wilson's Theorem:** If  $p$  is prime, then  $(p-1)! \equiv -1 \pmod p$

## 5. Why you shouldn't divide in modular arithmetic - *by Annie N.*

So, let's say I give you the following statement:

$$n \mid x(a - b) \text{ where } a, b, x \in \mathbb{Z}$$

Would you ever think to just jump straight to  $n \mid (a - b)$ ?

You shouldn't, because  $n$  and  $x$  might share common factors that  $n$  and  $(a - b)$  might not.

But let's work with this statement a little more.

If  $n \mid x(a - b)$  we can distribute the  $x$  and see  $n \mid ax - bx$ .

Applying the definition of mods we can see  $ax \equiv bx \pmod n$

And we've already said that we it wouldn't make sense to divide  $x$ , so we shouldn't magically be able to divide now!

As a quick aside, think about what conditions you would need on  $x$  and  $n$  for it to make sense to say  $n \mid (a - b)$ . You should notice that these are precisely the conditions we need to have a multiplicative inverse!

## 2 Problems

We've put together a bunch of problems for you to use for review. I'd recommend sitting down and solving them without looking at the solutions. Remember, you can be terser and provide less justification (but not *no* justification) on the midterm than you would on a typical homework. Also in general, these problems are **not** necessarily representative of exam problems, but rather meant to test your conceptual understanding of a wide range of topics. Good luck!

### 2.1 Induction

1. Show that  $\forall n \in \mathbb{N}, \sum_{i=0}^n i^2 = \frac{n(n+1)(2n+1)}{6}$
2. Show that if  $n \in \mathbb{N}$  and  $x, y \geq 0$ , then  $(\frac{x+y}{2})^n \leq \frac{x^n + y^n}{2}$ .
3. Let  $\langle a \rangle$  be a sequence such that  $a_1 = 2$  and  $a_2 = 8$  and  $a_n = 4(a_{n-1} - a_{n-2})$  for  $n \geq 3$ . Find and prove a closed form formula for  $a_n$ .
4. Consider a game played as follows: We have two ghosts and two piles of with  $m$  and  $n$  pumpkins. Ghosts take turns drawing between 1 and 3 pumpkins from a single pile. A ghost loses when there are no pumpkins left to draw. Show that the second ghost has a winning strategy iff  $4 \mid m - n$ .
5. Prove using induction that  $6 \mid n^3 + 5n$  for all  $n \in \mathbb{N}$ .

### 2.2 Relations

6. Define a relation  $R$  on  $\mathcal{P}(\mathbb{N})$  by  $X \sim Y$  if  $\exists$  a bijection  $X \rightarrow Y$ . Show that this is an equivalence relation. Determine the equivalence class of  $\emptyset$  and of  $\{1, 2, 3, 4, 5\}$  under this relation.
7. Say  $\langle a_n \rangle$  and  $\langle b_n \rangle$  are two sequences of naturals. Define a relation  $R$  on it as follows:  $(a_n, b_n) \in R$  if they differ in finitely many positions (i.e. the set  $\{i \in \mathbb{N} \text{ s.t. } a_i \neq b_i\}$  is finite). Show that  $R$  is an equivalence relation.
8. Let  $S$  be the union of disjoint sets  $A_1 \dots A_k$ . Let  $\sim$  be the relation on  $S$  such that  $x \sim y$  iff  $x$  and  $y$  are in the same set  $A_i$  for  $i \in [k]$ . Prove that  $\sim$  is an equivalence relation. Is  $\sim$  still an equivalence relation if we do not require the  $A_i$ 's to be disjoint?

### 2.3 Number Theory

#### 2.3.1 Not Modular Arithmetic

9. Find all solutions  $x, y \in \mathbb{Z} \times \mathbb{Z}$  (if they exist) to  $60x + 42y = 102$ .
10. Suppose  $\gcd(a, b) = 1$ . Find (with proof)  $\gcd(a^2, b^2)$  (you can write it as an expression of  $a$  and  $b$  if necessary, but do not use the gcd operator).
11. Let  $\overline{abc}$  be a 3-digit number written in base-10 (i.e.  $\overline{abc} = 100a + 10b + c$ ). Prove that the 6-digit number  $\overline{abcabc}$  has at least three distinct prime factors.
12. A natural number is *perfect* if all its positive factors except for itself add up to the number itself. Prove that if  $2^n - 1$  is prime, then  $2^{n-1}(2^n - 1)$  is perfect.

#### 2.3.2 Modular Arithmetic

13. Compute  $(20!)^{228} \bmod 23$ .
14. Prove *without* induction that  $6 \mid n^3 + 5n$  for all  $n \in \mathbb{N}$ .
15. We say a sequence of 5 naturals  $(a_1, a_2, a_3, a_4, a_5)$  is "good" if  $\forall i \in [4], a_{i+1} - a_i = 6$  and every  $a_i$  is prime. Show that the only good sequence is  $(5, 11, 17, 23, 29)$ . (Hint: Consider  $a_i \bmod 5$ ).

### 3 Solutions

Note: These are the complete solutions to the problems. Once again, we don't expect this much detail on the exam.

#### 3.1 Induction

**Problem 1** Show that  $\forall n \in \mathbb{N}, \sum_{i=0}^n i^2 = \frac{n(n+1)(2n+1)}{6}$ .

**Solution:**

Let  $p(n) = “\sum_{i=0}^n i^2 = \frac{n(n+1)(2n+1)}{6}”$ .

Base Case:  $n = 0$ . Then,  $\sum_{i=0}^0 i^2 = 0 = \frac{0(0+1)(2 \cdot 0 + 1)}{6}$ .

Induction Step: Let  $n \in \mathbb{N}$  and assume  $p(n)$  is true. We want to show  $p(n+1)$  is true.

$$\begin{aligned}
 \sum_{i=0}^{n+1} i^2 &= (n+1)^2 + \sum_{i=0}^n i^2 && \text{split up sum} \\
 &= (n+1)^2 + \frac{n(n+1)(2n+1)}{6} && \text{IH} \\
 &= \frac{6(n+1)^2 + n(n+1)(2n+1)}{6} && \text{combine fracs} \\
 &= \frac{(n+1)(6(n+1) + n(2n+1))}{6} && \text{factoring} \\
 &= \frac{(n+1)(6n+6+2n^2+n)}{6} && \text{expanding} \\
 &= \frac{(n+1)(2n^2+7n+6)}{6} && \text{simplifying} \\
 &= \frac{(n+1)(2n+3)(n+2)}{6} && \text{factoring} \\
 &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}
 \end{aligned}$$

So,  $p(n+1)$  is true and thus by PMI,  $p(n)$  is true for all  $n \in \mathbb{N}$ .



**Problem 2** Show that if  $n \in \mathbb{N}$  and  $x, y \geq 0$ , then  $(\frac{x+y}{2})^n \leq \frac{x^n+y^n}{2}$ .

**Solution:**

Let  $p(n) = “(\frac{x+y}{2})^n \leq \frac{x^n+y^n}{2}”$  for some  $x, y \geq 0$ .

Base Case:  $n = 0$

Then,  $(\frac{x+y}{2})^0 = 1 \leq \frac{x^0+y^0}{2} = \frac{1+1}{2} = 1$ .

Induction Step: Let  $n \in \mathbb{N}$  and assume  $p(n)$ . We want to show  $p(n+1)$ .

$$\begin{aligned}
\left(\frac{x+y}{2}\right)^{n+1} &= \left(\frac{x+y}{2}\right) \left(\frac{x+y}{2}\right)^n \\
&\leq \left(\frac{x+y}{2}\right) \left(\frac{x^n+y^n}{2}\right) && \text{IH} \\
&= \frac{x^{n+1}+y^{n+1}+x^ny+xy^n}{4} \\
&= \frac{x^{n+1}+y^{n+1}}{2} + \frac{x^ny+xy^n-x^{n+1}-y^{n+1}}{4} && \text{splitting up fractions} \\
&\leq \frac{x^{n+1}+y^{n+1}}{2}
\end{aligned}$$

The last line is true because  $x^ny+y^nx-x^{n+1}-y^{n+1}=x^n(y-x)+y^n(x-y)=(x^n-y^n)(y-x)$ . If  $x \geq y$ , then  $y-x \leq 0$  and  $x^n-y^n \geq 0$ . Otherwise, if  $y > x$ , then  $y^n > x^n$ , so  $x^n-y^n < 0$  and  $y-x > 0$ . In either case,  $(x^n-y^n)(y-x) \leq 0$ . ☺

**Problem 3** Let  $\langle a \rangle$  be a sequence such that  $a_1 = 2$  and  $a_2 = 8$  and  $a_n = 4(a_{n-1} - a_{n-2})$  for  $n \geq 3$ . Find and prove a closed form formula for  $a_n$ .

**Solution:**

We claim that  $a_n = n2^n$  for all  $n \geq 1$ . Let  $p(n) = "a_n = n2^n"$ .

Base Case:

- $n = 1$ : Then,  $a_1 = 2 = (2^1)(1)$ .
- $n = 2$ : Then,  $a_2 = 8 = (2^2)(2)$

Induction Step: Let  $n \geq 2$  and suppose  $1 \leq k \leq n$ ,  $p(k)$  is true. We want to show  $p(n+1)$  is true.

$$\begin{aligned}
a_{n+1} &= 4(a_n - a_{n-1}) && \text{def of recurrence} \\
&= 4(n2^n - (n-1)2^{n-1}) && \text{IH} \\
&= 2n2^{n+1} - (n-1)2^{n+1} && \text{distributing} \\
&= (2n - (n-1))2^{n+1} && \text{factoring} \\
&= (n+1)2^{n+1}
\end{aligned}$$

Thus  $p(n+1)$  is true so by SPMI  $p(n)$  is true for all  $n \geq 1$ . ☺

**Problem 4** Consider a game played as follows: We have two ghosts and two piles of with  $m$  and  $n$  pumpkins. Ghosts take turns drawing between 1 and 3 pumpkins from a single pile. A ghost loses when there are no pumpkins left to draw. Show that the second ghost has a winning strategy iff  $4 \mid m-n$ .

**Solution:**

Let  $p(k) = "if there are a total of  $k$  pumpkins, the second ghost has a winning strategy  $\iff 4 \mid m-n"$$

In other words, we are inducting on  $k = m+n$

Base Cases:

$k = 0$ . Then  $m = n = 0$ , and so the second ghost automatically wins. Since  $4 \mid m-n = 0-0$ , we have that  $p(0)$  holds.

$k = 1$ . Then  $m = 1$  and  $n = 0$  or vice versa. In either case, the first ghost can take all the pumpkins from the nonempty pile. Since  $4 \nmid m-n$  in these cases,  $p(1)$  holds.

$k = 2$ . Then either  $m = n = 1$  or  $m = 2, n = 0$  or  $m = 0, n = 2$ . In the first case, the first ghost must draw the last pumpkin from one of the two piles, allowing the second ghost to take the last remaining pumpkin and win. Then  $4 \mid m - n$  and  $p(2)$  holds since the second ghost always wins. In the second or third case, the first ghost can take both the remaining pumpkins. Since  $4 \nmid m - n$  and the second ghost cannot win,  $p(2)$  holds in this case too.

$k = 3$ : Then WLOG  $m \geq n$ . So, either  $m = 3, n = 0$  or  $m = 2, n = 1$ . In the first case, the first ghost can take all three pumpkins from their pile and therefore win. In the second case, the first ghost can take one pumpkin from the second ghost's pile, forcing the second ghost to take one from one pile and leave another nonempty. Then, the first ghost can take the last pumpkin and win. So, since  $4 \nmid m - n$  and the second ghost cannot win,  $p(3)$  holds too.

Inductive Step: Suppose that  $\forall i \leq k, p(i)$  holds ( $k \geq 4$ ). We want to show that  $p(k + 1)$  holds. Consider the game with  $k + 1$  pumpkins split across the two piles. We want to show that whatever the first ghost plays, the second ghost can make a move that leaves it in a winning position.

Suppose  $4 \mid m - n$ .

Suppose the first ghost draws  $j$  pumpkins. WLOG it draws these from the first pile.

If the first pile has at least  $4 - j$  pumpkins left, the second ghost can draw  $4 - j$  pumpkins from it. (Note:  $j \in \{1, 2, 3\} \implies 4 - j \in \{1, 2, 3\}$ , so this is a legal move.) Then, over the course of these two moves, one pile lost four pumpkins and the other pile stayed the same. Then  $m - n$  goes up or down by 4, and so  $4 \mid m - n$  still. Since there are now  $k - 4$  pumpkins, we have that the second ghost can win from here (by IH). Then, the second ghost can win from the game state starting with  $k$  pumpkins.

If there are not  $4 - j$  pumpkins left, the second ghost can draw  $j$  pumpkins from the second pile. Then  $m - n$  stays the same but  $m + n$  decreases. Then, by the IH, the second ghost can win.

Note that it is impossible for the first pile to have fewer than  $4 - j$  pumpkins, and the second pile to have fewer than  $j$  pumpkins (since then  $k < 4 - j + j = 4$ , and we took  $k > 4$ ). Hence in either of the above two situations the move described for the second player *is* valid.

Now suppose  $4 \nmid m - n$ .

Say  $m - n \equiv a \pmod{4}$ , with  $a \in \{1, 2, 3\}$ . Then the first ghost can take  $a$  pumpkins from the first pile (the one with  $m$  pumpkins). This would bring  $m - n$  to  $0 \mid 4$ , and from this game state, the second ghost would be the first to go. Then, by the IH, the first ghost can always win, and the second ghost will lose.

Hence, the second ghost can win  $\iff 4 \mid m - n$ .



**Problem 5** Prove using induction that  $6 \mid n^3 + 5n$  for all  $n \in \mathbb{N}$ .

**Solution:**


Let  $p(n) = "6 \mid n^3 + 5n"$  for  $n \in \mathbb{N}$ .

Base Case:  $n = 0$ . Since  $n^3 + 5n = 0$ , and  $6 \mid 0$ , we have that  $6 \mid n^3 + 5n$ .

Induction Step: Let  $n \in \mathbb{N}$  and suppose  $p(n)$  is true (in particular, say  $n^3 + 5n = 6k, k \in \mathbb{Z}$ ). We want to show  $p(n + 1)$  is true.

First, note that  $n^2 + n$  is even. We can show this by casing on the parity of  $n$ : if  $n$  is even,  $n^2$  and  $n$  are both even; if  $n$  is odd  $n^2$  and  $n$  are both odd. In either case,  $n^2 + n$  is even. Then, let  $n^2 + n = 2m$

$$\begin{aligned}
& (n+1)^3 + 5(n+1) \\
&= (n^3 + 3n^2 + 3n + 1) + (5n + 5) && \text{expanding} \\
&= (n^3 + 5n) + 3(n^2 + n) + 6 && \text{rearranging and factoring} \\
&= 6k + 3(n^2 + n) + 6 && \text{by IH} \\
&= 6k + 3(2m) + 6 && \text{by the note above} \\
&= 6(k + m + 1) && \text{factoring}
\end{aligned}$$

Then  $6 \mid (n+1)^3 + 5(n+1)$ . Hence  $p(n+1)$  holds. 

### 3.2 Relations

**Problem 6** Define a relation  $R$  on  $\mathcal{P}(\mathbb{N})$  by  $X \sim Y$  if  $\exists$  a bijection  $X \rightarrow Y$ . Show that this is an equivalence relation. Determine the equivalence class of  $\emptyset$  and of  $\{1, 2, 3, 4, 5\}$  under this relation.


**Solution:**

We show three properties:

Reflexive: Given any set  $X \subseteq \mathbb{N}$ , we know the function  $f(n) = n$  is a bijection  $X \rightarrow X$ . Hence  $X \sim X$ .

Symmetric: Suppose  $X \sim Y$ . WTS  $Y \sim X$ . Let  $f : X \rightarrow Y$  be a bijection. Then, let  $g : Y \rightarrow X$  be the two-sided inverse of  $f$ . Note that  $f$  is then a two-sided inverse of  $g$ , and hence  $g$  is bijective. Then  $\exists$  a bijection  $Y \rightarrow X$ , and so  $Y \sim X$ .

Transitive: Suppose  $X \sim Y$  and  $Y \sim Z$ . In particular, let  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be bijections. Note then that  $gf : X \rightarrow Z$  is also bijective ( $f^{-1}g^{-1}$  is a two-sided inverse for  $gf$ ). Then,  $X \sim Z$ .

The equivalence class of  $\emptyset$  is simply  $\{\emptyset\}$ , while the equivalence class of  $\{1, 2, 3, 4, 5\}$  is  $\{X \subseteq \mathbb{N} \text{ s.t. } |X| = 5\}$  

**Problem 7** Say  $\langle a_n \rangle$  and  $\langle b_n \rangle$  are two sequences of naturals. Define a relation  $R$  on it as follows:  $(a_n, b_n) \in R$  if they differ in finitely many positions (i.e. the set  $\{i \in \mathbb{N} \text{ s.t. } a_i \neq b_i\}$  is finite). Show that  $R$  is an equivalence relation.

**Solution:**

*Notation*: We use  $S_{ab}$  to denote  $\{i \in \mathbb{N} \text{ s.t. } a_i \neq b_i\}$ .

We prove three properties:

Reflexive: Clearly,  $(a_n, a_n) \in R$ , since  $S_{aa} = \emptyset$ , which is finite.

Symmetric: Suppose  $(a_n, b_n) \in R$ . Then  $S_{ab}$  is finite. However, note that  $S_{ab} = S_{ba}$  since  $a_i \neq b_i \iff b_i \neq a_i$ . Then  $S_{ba}$  is also finite.

Transitive: Suppose  $(a_n, b_n) \in R$  and  $(b_n, c_n) \in R$ . We wish to show that  $(a_n, c_n) \in R$ . To do this, I claim  $S_{ac} \subseteq S_{ab} \cup S_{bc}$ . Once we prove this claim, it will show that  $|S_{ac}| \leq |S_{ab}| + |S_{bc}|$ , and so  $S_{ac}$  must be finite (and therefore  $(a_n, c_n) \in R$ ). All that remains then is to prove the claim.

Let  $i \in S_{ac}$ . In particular,  $a_i \neq c_i$ . We want to show  $i \in S_{ab}$  or  $i \in S_{bc}$ . In particular, we want to show  $a_i \neq b_i$  or  $b_i \neq c_i$ . We do this by casework:

*Case 1*:  $a_i \neq b_i$ . Then  $i \in S_{ab}$ , and we are done.



Case 2:  $a_i = b_i$ . We know that  $a_i \neq c_i$ , and since  $a_i = b_i$ , we have that  $b_i \neq c_i$ . Then  $i \in S_{bc}$ .

Hence, the claim is true, and hence  $S_{ac}$  is finite. Therefore  $(a_n, c_n) \in R$



Note: The transitivity step is a little non-intuitive, so let me try and explain the reasoning. The idea is that we can figure out where  $a$  and  $c$  differ by checking where  $a$  and  $b$  differ and where  $b$  and  $c$  differ.  $a$  and  $c$  cannot differ in some position if  $a$  and  $b$  agree on that position and  $b$  and  $c$  also agree at that position. Since there are only finitely many positions where  $a$  and  $b$  differ, and finitely many positions where  $b$  and  $c$  differ, we have that  $a$  and  $c$  can only differ in finitely many positions.

**Problem 8** Let  $S$  be the union of disjoint sets  $A_1 \dots A_k$ . Let  $\sim$  be the relation on  $S$  such that  $x \sim y \iff x$  and  $y$  are in the same set  $A_i$  for  $i \in [k]$ . Prove that  $\sim$  is an equivalence relation. Is  $\sim$  still an equivalence relation if we do not require the  $A_i$ 's to be disjoint?

**Solution:**

We show the same three properties as always:

Reflexive: Say  $x \in S$ . WTS  $x \sim x$ . But this is clear, since  $x$  and  $x$  are clearly from the same  $A_i$ .

Symmetric: Say  $x \sim y$ . WTS  $y \sim x$ . We know from the definition of  $\sim$  that  $\exists A_i$  with  $x, y \in A_i$ . But then, by definition,  $y \sim x$ .

Transitive: Say  $x \sim y$  and  $y \sim z$ . We know then that  $\exists A_i$  with  $x, y \in A_i$  and  $\exists A_j$  with  $y, z \in A_j$ . Note that  $A_i$  must then equal  $A_j$ , since  $y$  is in both (if  $A_i \neq A_j$ , they would be disjoint, so  $A_i \cap A_j = \emptyset$ , which is not possible since  $y \in A_i \cap A_j$ ). Then  $z \in A_i$ . Since  $x \in A_i$  as well, we have that  $x \sim z$ .

Note that transitivity does not hold if we do not require our  $A_i$ 's to be distinct. For example, let  $S = A_1 \cup A_2$ , with  $A_1 = \{0, 1\}$  and  $A_2 = \{1, 2\}$ . Then  $0 \sim 1$  and  $1 \sim 2$  but  $0 \not\sim 2$ .



Note: What this question is essentially saying is that given any set  $S$  that can be partitioned into a bunch of  $A_i$ 's, we can define an equivalence relation on  $S$  such that the  $A_i$ 's are the equivalence classes. Convince yourself that this follows from the definition of  $\sim$  and equivalence classes.

### 3.3 Number Theory

#### 3.3.1 Not Modular Arithmetic 🐞 🐞

**Problem 9** Find all solutions  $x, y \in \mathbb{Z} \times \mathbb{Z}$  (if they exist) to  $60x + 42y = 102$ .

**Solution:**

First, we find  $\gcd(60, 42)$  to see if any solutions exist at all:

$$\begin{aligned} & \gcd(60, 42) \\ &= \gcd(18, 42) \\ &= \gcd(18, 6) \\ &= \gcd(0, 6) \\ &= 6 \end{aligned}$$

Since  $6 \mid 102$ , we see that there is indeed a solution. We then back-substitute:

$$\begin{aligned} 6 &= 42 - 2 \cdot 18 \\ 18 &= 60 - 42 \\ \implies 6 &= 42 - 2(60 - 42) \\ &= -2(60) + 3(42) \end{aligned}$$

Then  $(-2) \cdot 60 + 3 \cdot 42 = 6$ . Multiplying by 17, we have that  $(-34) \cdot 60 + (51) \cdot 42 = 102$ . Then, let  $x_0 = -34$  and  $y_0 = 51$ . We have that all the solutions to  $60x + 42y = 102$  are:

$$\begin{aligned} x &= x_0 + k \frac{42}{\gcd(60, 42)} \\ y &= y_0 - k \frac{60}{\gcd(60, 42)} \end{aligned}$$

Plugging in the relevant values, we have that  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  satisfies  $60x + 42y \iff$

$$\begin{aligned} x &= -34 + 7k \\ y &= 51 - 10k \end{aligned}$$

for some  $k \in \mathbb{Z}$



**Problem 10** Suppose  $\gcd(a, b) = 1$ . Find (with proof)  $\gcd(a^2, b^2)$  (you can write it as an expression of  $a$  and  $b$  if necessary, but do not use the gcd operator).

**Solution:**

Claim:  $\gcd(a^2, b^2) = 1$ . Since  $1 \mid a^2, b^2$ , we need only prove that  $n \mid a^2 \wedge n \mid b^2 \implies n \mid 1$ . In particular, we need to show that no natural greater than 1 is a factor of both  $a^2$  and  $b^2$ .

AFSOC  $\exists n > 1$  with  $n \mid a^2$  and  $n \mid b^2$ . Consider any prime factor  $p$  of  $n$  (we know such a  $p$  must exist, since  $n$  can be factored into primes). Since  $p \mid n$ , we have that  $p \mid a^2$  and  $p \mid b^2$ . Since  $p \mid a^2$ ,  $p \mid a$  (we know  $p \mid xy \implies p \mid x$  or  $p \mid y$ ; take  $x = y = a$ ). Similarly,  $p \mid b$ . But then  $p \mid \gcd(a, b) = 1$ . Since  $p$  is a prime ( $p > 1$ ), this is a contradiction.

Hence, the only common factors of  $a^2$  and  $b^2$  are  $\pm 1$ , and so  $\gcd(a^2, b^2) = 1$ .



**Problem 11** Let  $\overline{abc}$  be a 3-digit number written in base-10 (i.e.  $\overline{abc} = 100a + 10b + c$ ). Prove that the 6-digit number  $\overline{abcabc}$  has at least three distinct prime factors.

**Solution:**

Consider  $\overline{abcabc}$ . This is equal to  $10^5a + 10^4b + 10^3c + 10^2a + 10b + c = 10^3(10^2a + 10b + c) + (10^2a + 10b + c) = 1000 \cdot \overline{abc} + \overline{abc} = 1001 \cdot \overline{abc}$ .

We note that  $1001 = 7 \cdot 11 \cdot 13$ . Then  $7, 11, 13 \mid 1001\overline{abc} = \overline{abcabc}$ . We then have that  $\overline{abcabc}$  has at least three prime factors - 7, 11 and 13.



**Problem 12** A natural number is perfect if all its positive factors except for itself add up to the number itself. Prove that if  $2^n - 1$  is prime, then  $2^{n-1}(2^n - 1)$  is perfect.

**Solution:**

Let  $p = 2^n - 1$ . We have that the only positive factors of  $p$  are 1 and  $p$ . From this, it follows that if  $m \mid 2^{n-1}p$ ,  $m$  is of the form  $2^k$  or  $2^k p$ , where  $0 \leq k \leq n-1$ . (To see this, case on whether  $p \mid m$ . If  $p \mid m$ , we have that  $(m/p) \mid 2^{n-1}$ , so  $(m/p) = 2^k$ . If  $p \nmid m$ , we have that  $m \mid 2^{n-1}$  by Euclid's lemma.)

So then our positive factors of  $2^{n-1}(2^n - 1)$  are  $\{1, 2, 2^2, \dots, 2^{n-1}, p, 2p, 2^2p, \dots, 2^{n-1}p\}$ . We sum up all of these except the last one.

Note that  $1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1 = p$ , using the formula for a geometric series. Also  $p + 2p + \dots + 2^{n-2}p$  (we exclude the last term) is  $p(2^{n-1} - 1)$ , again since this is a geometric series.

Adding these terms together, we have that the sum of all the positive factors of  $2^{n-1}p$  except itself add up to  $p + p(2^{n-1} - 1) = 2^{n-1}p$ . Then,  $2^{n-1}p$  is a perfect number. 😊

Note: Primes of the form  $2^n - 1$  are called Mersenne primes, and Euclid conjectured that  $n$  is a perfect number  $\iff n = \frac{q(q+1)}{2}$ , where  $q$  is a Mersenne prime. The above proof is the backwards direction, but the forwards direction is slightly trickier to prove. In particular, nobody knows a proof yet (though we have not found a counterexample either). However, Euler did prove that every even perfect number must be of the above form.

### 3.3.2 Modular Arithmetic ♪♪

**Problem 13** Compute  $(20!)^{228} \bmod 23$ .

**Solution:**

First we find  $20! \bmod 23$ :

Note that  $22 \cdot 21 \cdot (20!) \equiv_{23} 22! \equiv_{23} -1$  by Wilson's Theorem. Since  $22 \equiv_{23} -1$  and  $21 \equiv_{23} -2$ , we have that  $(-1)(-2)(20!) \equiv_{23} 2 \cdot 20! \equiv_{23} -1$ . Multiplying both sides by 12, we have that  $12 \cdot 2 \cdot (20!) \equiv_{23} -12 \equiv_{23} 11$ . But  $12 \cdot 2 \equiv_{23} 1$ , so we have that  $20! \equiv_{23} 11$ .

Now, we compute  $11^{228} \bmod 23$ , noting that  $(20!)^{228} \equiv_{23} 11^{228}$ . Note that  $11^{22} \equiv 1$  by Fermat's little theorem. Then  $11^{228} \equiv_{23} 11^{22 \cdot 10 + 8} \equiv_{23} (11^{22})^{10} \cdot 11^8 \equiv_{23} 11^8 \equiv_{23}$ . We have that  $11^2 \equiv_{23} 121 \equiv_{23} 6$ . Then  $11^4 \equiv_{23} 6^2 \equiv_{23} 36 \equiv_{23} 13$ . Then  $11^8 \equiv_{23} 13^2 \equiv_{23} 169 \equiv_{23} 8$ .

Then,  $(20!)^{228} \equiv_{23} 8$ . 😊

**Problem 14** Prove without induction that  $6 \mid n^3 + 5n$  for all  $n \in \mathbb{N}$ .

**Solution:**

Let  $n \in \mathbb{N}$  be arbitrary. We then show two things: that  $2 \mid n^3 + 5n$  and  $3 \mid n^3 + 5n$ .

Part 1: We know  $n$  is either odd or even. If  $n$  is even, then  $n^3 + 5n \equiv_2 0^3 + 5 \cdot 0 \equiv_2 0 + 0 \equiv_2 0$ . If  $n$  is odd (i.e.  $n \equiv_2 1$ ). Then  $n^3 + 5n \equiv_2 1^3 + 5 \cdot 1 \equiv_2 1 + 5 \equiv_2 6 \equiv_2 0$ . In either case, we have that  $n^3 + 5n \equiv_2 0$ , so  $2 \mid n^3 + 5n$ .

Part 2: We case on the congruence class of  $n \bmod 3$ . We can rewrite  $n^3 + 5n$  as  $n(n^2 + 5)$ . Note that  $n \equiv_3 0$  or  $n \not\equiv_3 0$ , in which case  $n^2 \equiv_3 1$ . In the first case, we see that  $n^3 + 5n \equiv_3 0$ . In the second case, we have that  $n^2 + 5 \equiv_3 6 \equiv_3 0$ , so  $3 \mid n^2 + 5 \implies 3 \mid n(n^2 + 5)$ . In either case,  $3 \mid n^3 + 5n$ .

Hence,  $6 \mid n^3 + 5n$ . 😊

**Problem 15** We say a sequence of 5 naturals  $(a_1, a_2, a_3, a_4, a_5)$  is "good" if  $\forall i \in [4], a_{i+1} - a_i = 6$  and every  $a_i$  is prime. Show that the only good sequence is  $(5, 11, 17, 23, 29)$ .

(Hint: Consider  $a_i \bmod 5$ ).

**Solution:**

Say  $(a_1, a_2, a_3, a_4, a_5)$  is a good sequence. Since  $a_{i+1} = 6 + a_i$ , we have that  $a_{i+1} \equiv_5 1 + a_i$ . Then, note that  $a_i \equiv_5 (i - 1) + a_1$ . In particular, this means that  $a_1, a_2, a_3, a_4, a_5$  are all in different equivalence classes  $\bmod 5$ . But since there are only 5 equivalence classes  $\bmod 5$ , we have that some  $a_k \equiv 0 \bmod 5$ . But since  $a_k$  must be prime, we have that  $a_k = 5$ . Since all the  $a_i$ 's are non-negative, we have that  $k$  must be 1 (otherwise  $a_1$  is at most 6 less than 5, which is a contradiction). Then we have that if  $(a_1, a_2, a_3, a_4, a_5)$  is

a good sequence, it must be  $(5, 11, 17, 23, 29)$  (using the property that adjacent numbers differ by 6). Note that this is an implication, we need to still verify that the sequence provided is indeed a “good” sequence. However, since all the numbers in the sequence are prime, we see that it is indeed a good sequence. 😊