Transition to Advanced Mathematics

Practically Perfect Proofs

Fall 2022 **Subhadip Chowdhury** **Math 215**

§A. Introduction

Over the course of the semester, each student will receive about ten problems whose solutions involve crafting coherent, convincing, and mathematically correct arguments, also known as *proofs*. These problems are sometimes difficult and always require careful thought, lots of attention, and lots of time to think and make mistakes.

You will need to submit a formal, correct, professionally-typeset solution (a P^3 or Practically Perfect Proof) for these and each will go through a revision process. The first time you submit your P^3, you will receive a provisional grade and feedback on your work, and may choose to resubmit the assignment.

Note that only the last submission will be counted for your score. *Thus it is possible to receive a lower grade on the final draft than the provisional grade on your first draft on the same problem,* if you make changes to your solution that lower its overall quality.

- This is an **independent** assignment that you should view as a take home examination. You may not discuss the problems with anyone except me. This means you cannot talk to other students about your solutions (or even which problems you are choosing to work on), nor can you ask for help from the TA or other professors, nor from any person in an online setting. *Violation of this policy is grounds for failure of the course.*

- You may **not** refer to any sources other than the lecture notes and textbook for this course. This includes a prohibition against looking things up on the Internet unless you are directed specifically to do so in the context of a problem. If you think that you need some background material or a definition from another source then you may ask me for permission, and if granted then you may look up the necessary material and include it with a footnote in your proof. *Violation of this policy is grounds for failure of the course.*

The first P^3 assignment consisting of two problems will start around week five, and new problems will be assigned on a weekly basis until about two/three weeks before the end of the semester. Part of the purpose of these P^3 assignments is to give you the opportunity to improve your mathematical writing and writing skills in general. All P^3 assignments must be typeset in LaTeX, which will provide you several opportunities to learn this skill before your final EP.

§B. P^3 Grading:

The intended audience for proofs written in this course is your classmates, and you should write with them in mind. Figuring out how to prove something is often difficult and involves scratch work and experimentation. However, in addition to being logically correct, the proof that you ultimately write and turn in should be neat and easy for your readers to follow. The entire point of writing a proof is to **communicate to others** the truth of the statement you are proving. **Each proof will be graded according to the following rubric.**

E	Excellent work, no real complaints. Communication is clear and complete.
M	Understanding of the concepts is evident and the argument is mostly correct, but it's missing some formal details, has LaTeX issues, or is not as clearly communicated as I would like.
R	There are hints of partial progress, but there is a major misstep in the mathematics or it is especially poorly written.
N	Some ideas in the right direction, but did not really get there. Arguments are fragmentary or have significant omissions.

The graded proofs are a chance for me to give you some feedback and for you to understand how your writing is progressing. If you are getting a lot of '**R**'s and '**N**'s on a particular topic or proof technique, then that is an indication that you should practice that topic or technique more or come see me for some clarification.

§C. Frequently Asked Questions

Following are some (asked and anticipated) questions about this assignment. You should read all of this carefully and follow the instructions accordingly.

- **What other requirements are there for my P^3 Problems?**

  The solution for each problem must be written using complete sentences and according to the "Mathematical Writing Practices" appendix from the lecture notes. It must be typeset, well organized, and easy to read. Proper grammar, proper sentence and paragraph structure, and correct spelling are necessities. *Submissions that do not adhere to these basic requirements will receive a draft score of 'N'.*

- **What happens if I submit an incorrect or incomplete solution?**

  When you submit a draft within the first deadline, I will return your problem and indicate if it is finished and ready for final version or if it needs more work. While provisional grades are given as a guide, there is no penalty for a low grade *until the final draft is submitted*.

- **Can I work with someone else or use sources other than the textbook or my class notes?**

  No. No collaboration is permitted. See the first page. One of the primary goals of Math 215 is that you acquire deep personal understanding of proof techniques and the ability to read and write proofs. Being able to do so independently is essential, and thus this project is an independent endeavor.

- **Can I come to your office hours for help?**

  Yes! You are welcome (and encouraged) at any time during office hours to discuss questions on the P^3 assignments (or any other aspect of the course). If my stated times do not suit your schedule, please request an appointment (ideally, at least 24 hours in advance). There is only one requirement for you when you come to seek help: **do not come empty-handed**. By this I mean that you should not come unprepared saying that you *"have no idea where to start."* Part of learning to write proofs is thinking of possible ways to start, even if those ways turn out to be wrong. When you have chosen a problem to work on, start your scratch work with a list of things that you know which seem like they might be related. Write down what you know and what you need to show, and see if any of your ideas help with even a small part of this task. If you come to office hours without having seriously undertaken the basic groundwork on solving a P^3 problem, I will defer meeting with you until a later time when you've had a chance to do so.

The actual problems start on the next page. Check back weekly for new problems.

§D. P^3 Assignment 1

Question 1

Prove that if a and b are two positive integers, then

$$a^2(b+1)+b^2(a+1) \geq 4ab.$$

Hint: This can be proved directly using some algebraic manipulations.

Question 2

Let $a, b, c \in \mathbb{Z}$. Prove that if $a^2+b^2=c^2$, then abc is even.

Hint: Do a proof by cases. What's the minimum number of cases you need?

Question 3

Suppose that a and b are natural numbers such that $a^2=b^3$. Prove that if $4 \mid b$, then $8 \mid a$.

> **Warning:** Be very careful with this proof. Here's a wrong proof for example:
>
> Since $4 \mid b$, we can write $b=4k$ for some $k \in \mathbb{Z}$. Then $a^2=b^3=64k^3 \implies a=8\sqrt{k^3}=8m$. Hence $8 \mid a$.
>
> What's wrong with this argument?

LaTeX tips

- Use the LaTeX template from the P3 tab in Moodle.
- The command for writing $a \mid b$ is

```
$a \mid b$
```

Writing `$a|b$` using the | key gives $a|b$, which doesn't have the correct spacing.

Continued on the next page →

§E. P^3 Assignment 2

Question 4

Suppose n is a natural number and let p be the smallest prime divisor of n. Show that if $p > \sqrt[3]{n}$, then $\dfrac{n}{p}$ can not be a composite number.

> **Hint:** Do a proof by contradiction. What is the definition of a composite number? How can you use the fact that p is the **smallest** prime divisor?

Question 5

This is going to be a five-part problem. The first two parts are in this assignment, the next three parts will be in future assignments.

Although we have not yet proved the following lemma in class, we need it for this problem, so you may use the following result without proof.

Lemma: If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

Part I. Use the lemma to prove the following proposition known as the cancellation law:

Cancellation Law: If $ax \equiv ay \pmod{m}$ and $\gcd(a,m) = 1$, then $x \equiv y \pmod{m}$.

Part II. Suppose $m \in \mathbb{N}$. The function φ, known as Euler's totient function, is defined as follows. Let $\mathcal{S}$ denote the set

$$\mathcal{S}_m = \{k : 1 \le k \le m \text{ and } \gcd(k,m) = 1\}.$$

Then we define

$$\varphi(m) = \text{Cardinality of the set } \mathcal{S}_m.$$

For example, if $m = 15$, then the set in consideration is $\mathcal{S}_{15} = \{1,2,4,7,8,11,13,14\}$. Hence $\varphi(15) = 8$.

Since the cardinality of $\mathcal{S}_m$ is $\varphi(m)$, we can write the set $\mathcal{S}_m$ in roster form as follows

$$\mathcal{S}_m = \left\{a_1, a_2, a_3, \ldots, a_{\varphi(m)}\right\}.$$

Prove the following proposition:

Proposition: Suppose $x \in \mathbb{Z}$ such that $\gcd(x,m) = 1$. Prove that if $a_i \in \mathcal{S}_m$, then $\gcd(xa_i, m) = 1$.

LaTeX tips

- The command for writing $\sqrt[3]{n}$ is `$ \sqrt[3]{n} $`
- The command for writing $a \equiv b \pmod{n}$ is `$ a \equiv b \pmod{n} $`
- There is a built-in command in LaTeX for gcd. Include the 'backslash' as follows `$ \gcd (a,b) $` to get $\gcd(a,b)$ that uses upright letters instead of slanted letters.

Continued on the next page →

§F. P^3 Assignment 3

Question 6

We are continuing the proof from question 5.

Part III. **Proposition:** Suppose $x \in \mathbb{Z}$ such that $\gcd(x, m) = 1$. Prove that if $a_i \in \mathcal{S}_m$, then we can find a $a_j \in \mathcal{S}_m$ such that $xa_i \equiv a_j \pmod{m}$.

Question 7

One of the famous mathematicians of the 17th century was Pierre de Fermat (1601-1665). Fermat made an assertion that for each natural number n with $n \geq 3$, there are no natural numbers a, b, and c for which $a^n + b^n = c^n$. This assertion was discovered in a margin of one of Fermat's books after his death, but Fermat provided no proof. He did, however, state that he had discovered *a truly remarkable proof but the margin did not contain enough room for the proof!*[*]

This assertion became known as **Fermat's Last Theorem** but it more properly should have been called Fermat's Last *Conjecture*. Despite the efforts of mathematicians, this "theorem" remained unproved until Andrew Wiles, a British mathematician, first announced a proof in June of 1993. However, it was soon recognized that this proof had a serious gap, but a corrected version of the proof was published by Wiles again in 1995. Wiles' proof uses many concepts and techniques that were unknown at the time of Fermat and is well beyond what we can cover in this course. Instead, your goal is to explore and prove the following proposition, which is a (very) special case of Fermat's Last Theorem.

Proposition: There do not exist prime numbers a, b, and c such that $a^3 + b^3 = c^3$.

Although Fermat's Last Theorem immediately implies this proposition is true, **you are being asked to use a proof by contradiction to prove this proposition.** Here is an **outline of the proof** for your benefit:

First use the fact that 2 is the only even prime number and use the following three cases: (1) $a = b = 2$; (2) a and b are both odd; and (3) one of a and b is odd and the other one is 2.

Case 1. Show that the case where $a = b = 2$ leads to a contradiction and hence, this case is not possible.

Case 2. Show that the case where a and b are both odd leads to a contradiction and hence, this case is not possible.

Case 3. We now know that one of a or b must be equal to 2. Assume that $b = 2$ (why can we do this?) and substitute into the equation $b^3 = c^3 - a^3$ and use the factorization formula $c^3 - a^3 = (c-a)(c^2 + ac + a^2)$. Use this to obtain a contradiction.

> **Note:** Write a single complete proof of the proposition. **Do not treat this as three separate questions.** Use correct conjunctions and other logical connectors as necessary.

Continued on the next page →

[*] "Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet." (Nagell 1951, p. 252).

§G. P^3 Assignment 4

Question 8

This is a continuation of question 5.

Part IV. We are using the same notations for $x, a_i, \varphi(m)$ etc. from question 5. Prove the following lemmas:

(a) **Lemma:** Let $x \in \mathbb{Z}$ such that $\gcd(x,m) = 1$. For every $1 \leq i \leq \varphi(m)$, there exists a **unique** j with $1 \leq j \leq \varphi(m)$ such that $xa_i \equiv a_j \pmod{m}$.

> **Hint:** The existence part has been already proven in part III. We just need to prove the uniqueness part here.

(b) **Lemma:** Let $1 \leq i, j, k, l \leq \varphi(m)$. If $xa_i \equiv a_j \pmod{m}$ and $xa_k \equiv a_l \pmod{m}$ and $a_i \neq a_k$, then $a_j \neq a_l$.

> **Hint:** You might need to use the result from part I.

Part V. Combine the lemmas from parts I, II, III and IV to prove the following:

Theorem: Let $m \in \mathbb{N}$ and $x \in \mathbb{Z}$ with $\gcd(x,m) = 1$. Then $x^{\varphi(m)} \equiv 1 \pmod{m}$.

> **Hint:** You need to use the result from question 2029(a) in the lecture notes.

Question 9

Let n be a natural number. Prove that there exist **unique** natural numbers a and b such that $n = 2^{a-1}(2b-1)$.

> **Hint:** This is a two-part question. Here's an outline. You need to flesh it out with more details.
>
> To prove existence, first prove that if $n \in \mathbb{N}$, then we can find an odd natural number q and a nonnegative integer p such that $n = 2^p q$. Continue your argument from there to show the existence of a and b as required.
>
> To prove uniqueness, argue by contradiction. If $2^{a_1-1}(2b_1 - 1) = 2^{a_2-1}(2b_2 - 1)$, there are three cases to consider: $a_1 > a_2, a_1 < a_2$, and $a_1 = a_2$. Two of these cases lead to a contradiction.

Continued on the next page →

§H. P^3 Assignment 5

Question 10

Using mathematical induction prove the following proposition.

Proposition: The sum of the cubes of any three consecutive natural numbers is a multiple of 9.

Note: This proposition can be proved by other means, but I am asking you to prove it by induction.

> **Hint:** How would you algebraically denote three consecutive natural numbers? First, restate the proposition in the form $(\forall n \in \mathbb{N})P(n)$.

Question 11

The **Lucas numbers** are a sequence of natural numbers $L_1, L_2, L_3, \ldots, L_n, \ldots$, which are defined recursively as follows:

- $L_1 = 1$ and $L_2 = 3$, and
- $L_{n+2} = L_{n+1} + L_n$ for each natural number n.

We already have defined the Fibonacci numbers in the lecture notes. From the definitions of the Fibonacci numbers and the Lucas numbers, we see that:

- The first ten Fibonacci numbers are: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55$.
- The first ten Lucas numbers are: $1, 3, 4, 7, 11, 18, 29, 47, 76, 123$.

Prove the following proposition: (You can use the definitions of Fibonacci numbers and Lucas numbers directly in your proof.)

Proposition: Let $F_1, F_2, \ldots, F_n, \ldots$ be the sequence of Fibonacci numbers and let $L_1, L_2, \ldots, L_n, \ldots$ be the sequence of Lucas numbers. Then for each natural number n with $n \geq 3$, we have

$$L_n = F_{n+2} - F_{n-2}.$$

Continued on the next page →

§I. P^3 Assignment 6

Question 12

The Archimedean Property of $\mathbb{N}$ can be stated as follows.

Theorem I.1: Archimedean Property of Natural Numbers

Let x be a real number. Then there exists a natural number greater than x.

Using logical symbols, this reads $(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})(n > x)$. An equivalent way to state this would be $(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})\left(\frac{1}{n} < \frac{1}{x}\right)$. You can use either form of this result without proof to prove the following following.

Proposition: $$\bigcup_{n\in\mathbb{N}}\left[3+\frac{1}{n}, 5-\frac{1}{n}\right] = (3,5).$$

Hint: The proof will be in two steps. First, pick an element of the set on the left side and show it is in the set on the right. Next, pick an element from the right-hand side, and show that it is an element of the left side. Each step might be a different proof technique. Only one of the directions needs to use the Archimedean property mentioned above.

Question 13

We will start with an example to explain what's going on in this problem. Let $A = \{u, v, w, x, y, z\}$. The relation

$$\begin{aligned} R =&\{(u,u),(u,v),(u,w),(v,u),(v,v),(v,w),(w,u),(w,v),(w,w),\\ &(x,x),(x,y),(y,x),(y,y),(z,z)\}\end{aligned}$$

defined on A is an example of an equivalence relation. In particular, $[u] = [v] = [w] = \{u, v, w\}, [x] = [y] = \{x, y\}$ and $[z] = \{z\}$.

So $|[u]| = |[v]| = |[w]| = 3$ and $|[x]| = |[y]| = 2$, while $|[z]| = 1$. Therefore, $|[u]|+|[v]|+|[w]|+|[x]|+|[y]|+|[z]| = 14$

Now prove the following proposition for the general case:

Proposition: Let $A = \{a_1, a_2, \ldots, a_n\}$ be an n-element set and let R be an equivalence relation defined on A. Prove that $\sum_{i=1}^{n} |[a_i]|$ is even if and only if n is even.

Note: Observe that

Hint: There are a couple of different ways to prove this. Here's one possible way: suppose there are k equivalence classes. Let $n_1, n_2, \ldots, n_k$ be the cardinalities of each equivalence class respectively. Can you express the given sum in terms of $n_1, n_2, \ldots, n_k$? How is n related to the n_i's?

End of document.