CS 70 Discrete Mathematics and Probability Theory
Spring 2020 HW 4

Due: Fri, 2/21 11:59 PM
Grace period until Sun 2/23 11:59 PM

1 Modular Arithmetic Problems

In each case show your work and justify your answers.

(a) For natural numbers a, show that $7a+3$ and $5a+2$ are coprime.

(b) What is $3^{48} \pmod{11}$?

(c) Solve $x^2+x \equiv 2 \pmod{4}$.

- Rewrite the expression as $(x+a)(x+b) \equiv 0 \pmod{4}$.
- Argue why $x+2 = 2q_1$ and $x-1 = 2q_2$ for integers q_1 and q_2, which gives

$$(x+2)(x-1) = 4q_1q_2 \equiv 0 \pmod{4},$$

cannot be a solution.
- Consider the solutions for $x+a \equiv 0 \pmod{4}$ and $x+b \equiv 0 \pmod{4}$. Then, determine the solutions of the original equation.

(d) If $17x^{12}+5x^7-14x^{40} \equiv 6 \pmod{7}$, find x.

- Simplify the coefficients of all terms with x^m.
- Use Fermat's little theorem to simplify all terms containing x^m.

(e) If $a+4c \equiv 2b \pmod{21}$, simplify $100a+10b+c \pmod{21}$.
(HINT: Replace b in $100a+10b+c \pmod{21}$ from $a+4c \equiv 2b \pmod{21}$.

In parts (c), (d), and (e) give your solutions as integers mod m.

2 Iterative EGCD

(a) **Convert the subtractive form of the recursive EGCD algorithm into an iterative form involving a while loop.** Your algorithm should involve only a single pass, not a pass up and then a pass down.

(HINT: First do this for the subtractive form of the GCD. Then think about what you want to keep track of as you descend into the EGCD so that you are able to return the desired answer at the end without having to go back up.)

(b) **Show that the subtractive form of your iterative EGCD outputs the correct answer for the following**, (Write the updated values computed by the algorithm after each iteration).

$$gcd(54,17) = 1, \quad egcd(54,17) \to \begin{cases} (d = 1, a = -11, b = 35) \Rightarrow 1 = (-11) \cdot 54 + (35) \cdot 17. \\ \text{or} \\ (d = 1, a = 6, b = -19) \Rightarrow 1 = (6) \cdot 54 + (-19) \cdot 17. \end{cases}$$

Feel free to collect steps together for things that seem repetitive. Do you see now why we teach you the mod form of the EGCD?

3 Pentagons, Pentagrams, and Pythagoreans: a Euclidean geometry proof of the existence of irrational numbers by way of Euclid's Algorithm

According to historical accounts, the pentagram was commonly used as a recognition sign between the Pythagoreans, the members of Pythagoras' school (about 500 BC). In this problem, we will establish a key property of this figure in relation to the Euclidean algorithm, which offers a mathematical perspective on the fascination with this symbol.

Recall that two non-negative real numbers (think of segment lengths) a, b are said to be commensurable if there exists a third real g such that both a and b are some natural multiple of g: $\exists k, k' \in \mathbb{N} : a = kg, b = k'g$. For engineering practices, it is extremely useful to have such a g, as it stands for a common unit of measurement between the two lengths.

A very common belief of the time was that any two segment lengths are commensurable. The Pentagram is believed to be the foundation of one of the first (if not the first) realizations that this is not true — that irrational numbers must exist. This problem asks you to use classical planar geometry to understand this ancient argument. In this problem, you are free to use facts from standard Euclidean geometry without having to prove them.

1. Let us recall the Euclidean algorithm on real non-negative inputs a, b. Without loss of generality, let us assume $a \geq b$. The Euclidean algorithm, which we denote by GCD, goes as follow:

   (a) If $b = 0$ then return a.

   (b) Else return $\text{GCD}(b, a - \lfloor a/b \rfloor b)$ (where $x \mapsto \lfloor x \rfloor$ is the floor function).

   Show that if a and b are commensurable, then the Euclidean algorithm terminates for these inputs.

   (HINT: Use induction to prove this. If you would like, feel free to first understand the above argument in the case of the subtractive version of the Euclidean algorithm.)

2. Let $ABCDE$ be a regular pentagon, meaning $AB = BC = CD = DE = EA$ and $\widehat{EAB} = \widehat{ABC} = \widehat{BCD} = \widehat{CDE} = \widehat{DEA}$; see Figure 1. This figure depicts the pentagram and can be used to walk through a visual geometric argument of irrationality via Euclid's algorithm.

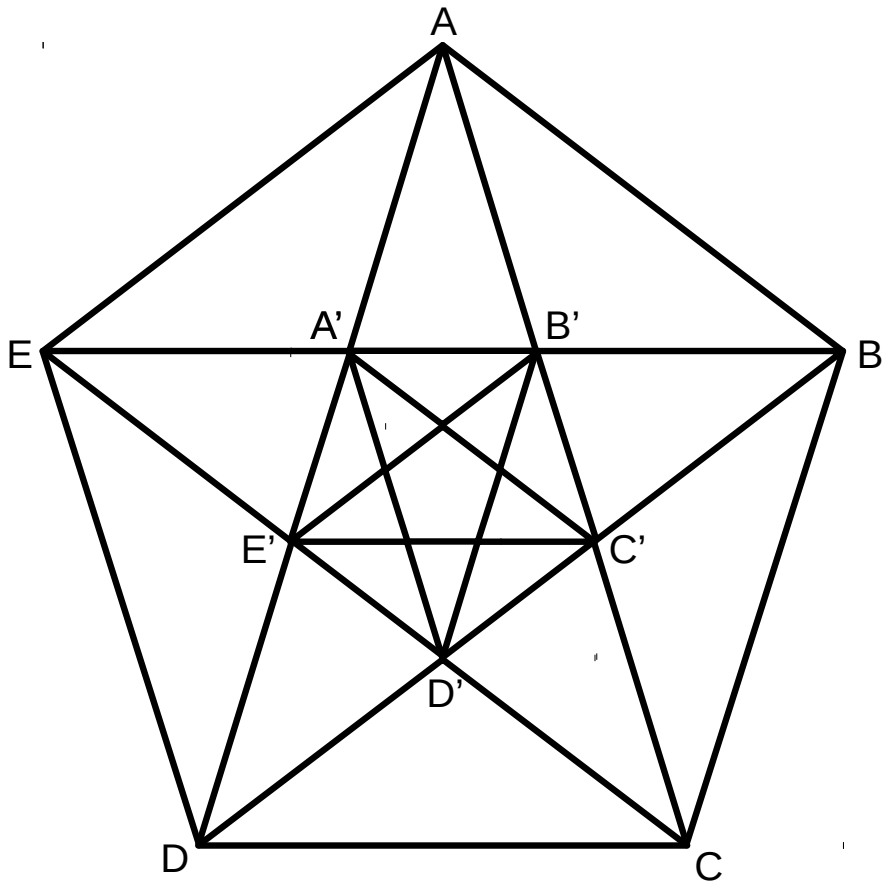


Figure 1: Regular pentagon

For your convenience, we will collect here some facts from classical Euclidean geometry that you might find useful. Feel free to use these without having to prove them.

- The sum of interior angles of a triangle is $180°$. (And in general, the sum of all interior angles of a simple n-sided polygon is $180°(n-2)$ — a fact that can be proven by induction by chopping off triangles.)
- In particular, the sum of the interior angles of a pentagon is $540°$.
- The Law of Sines. For example, the Law of Sines for the triangle EBA tells us that $\frac{EB}{\sin\widehat{EAB}} = \frac{EA}{\sin\widehat{EBA}} = \frac{AB}{\sin\widehat{AEB}}$. This quantitatively expresses the fact that similar triangles (those with the same angles) have sides whose lengths are proportional — it is like the entire triangle has been scaled up or down in size.
- Sufficient evidence for congruence between two triangles in Euclidean geometry can be shown through the following comparisons: 1) SAS (Side-Angle-Side): If two pairs of sides of two triangles are equal in length, and the included angles are equal in measurement, then the triangles are congruent. 2)SSS (Side-Side-Side): If three pairs of sides of two triangles are equal in length, then the triangles are congruent. 3)ASA (Angle-

Side-Angle): If two pairs of angles of two triangles are equal in measurement, and the included sides are equal in length, then the triangles are congruent.

- Symmetry: the regular pentagon is the same if you rotate it to have any corner pointing upwards.
- Parallel lines intersecting another line form equal angles. When two lines cross, the opposite angles formed are equal.
- An isoceles triangle is one that has (at least) two equal sides. By the SAS congruence property above, this also means that it has (at least) two equal internal angles.

The first thing to do is prove a key observation about certain isoceles triangles being in the figure.

Show that $A'AB'$, EAB', and $EE'B'$ are isosceles triangles.

(HINT: Try to find the congruent triangles in the figure in order to find the relation between the angles in $A'AB'$, EAB', and $EE'B'$.)

3. The second key lemma is an observation about the inside of the Pentagram. Let $A', \ldots, E'$ be the intersection points of the chords as in Figure 1.

   Show that $A'B'C'D'E'$ is a regular pentagon, i.e., all interior angles are equal and all sides are equal in length.

4. Now, we begin the main part of the proof. We are essentially executing Euclid's algorithm geometrically.

   Justify this statement: $\mathbf{GCD}(EA, EB) = \mathbf{GCD}(EB', EB)$

   For this part and subsequent parts, you can use either geometry or the correctness of Euclid's algorithm. (You don't have to prove correctness of Euclid's algorithm since you've already done that.) In particular, you can definitely invoke what you've already proved above as needed — there's a reason we put those parts first.

5. **Justify this statement: $\mathbf{GCD}(EB', EB) = \mathbf{GCD}(EB', B'B)$**

6. **Justify this statement: $\mathbf{GCD}(EB', B'B) = \mathbf{GCD}(EB', EA')$**

7. **Justify this statement: $\mathbf{GCD}(EB', EA') = \mathbf{GCD}(A'B', EA')$**

8. **Justify this statement: $\mathbf{GCD}(A'B', EA') = \mathbf{GCD}(A'B', EE')$**

9. **Justify this statement: $\mathbf{GCD}(A'B', EE') = \mathbf{GCD}(A'B', E'B')$**

10. Now, notice that we have found ourselves with a statement that is only in terms of the inner pentagon. Using the previous elements, **argue that EB and EA must be incommensurable.** (In modern terms, we would say that EB/EA is irrational.)

    (HINT: It suffices to show that $GCD(EB, EA)$ does not terminate. What did you see above? Remember, why is the Pentagram considered a symbol of infinite regress?

4 Product of Two

Suppose that $p > 2$ is a prime number and S is a set of numbers between 1 and $p-1$ such that $|S| > p/2$, i.e. $(\forall x \in S)(1 \leq x \leq p-1)$. Prove that any number $1 \leq x \leq p-1$ can be written as the product of two (not necessarily distinct) numbers in S, mod p.

5 Just Can't Wait

Joel lives in Berkeley. He mainly commutes by public transport, i.e., bus and BART. He hates waiting while transferring, and he usually plans his trip so that he can get on his next vehicle immediately after he gets off the previous one (zero transfer time, i.e. if he gets off his previous vehicle at 7:00am he gets on his next vehicle at 7:00am). Tomorrow, Joel needs to take an AC Transit bus from his home stop to the Downtown Berkeley BART station, then take BART into San Francisco.

(a) The bus arrives at Joel's home stop every 22 minutes from 6:05am onwards, and it takes 10 minutes to get to the Downtown Berkeley BART station. The train arrives at the station every 8 minutes from 4:25am onwards. What time is the earliest bus he can take to be able to transfer to the train immediately? Show your work. (Find the answer without listing all the schedules.)

(b) Joel has to take a Muni bus after he gets off the train in San Francisco. The commute time on BART is 33 minutes, and the Muni bus arrives at the San Francisco BART station every 17 minutes from 7:12am onwards. What time is the earliest bus he could take from Berkeley to ensure zero transfer time for both transfers? If all bus/BART services stop just before midnight, is it the only bus he can take that day? Show your work.

6 Euler's Totient Theorem

Euler's Totient Theorem states that, if n and a are coprime,

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

where $\phi(n)$ (known as Euler's Totient Function) is the number of positive integers less than or equal to n which are coprime to n (including 1).

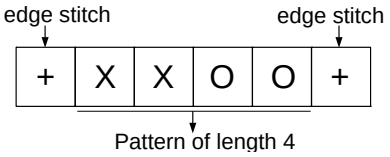
(a) Let the numbers less than n which are coprime to n be $m_1, m_2, \cdots, m_{\phi(n)}$. Argue that $am_1, am_2, \cdots, am_{\phi(n)}$ is a permutation of $m_1, m_2, \cdots, m_{\phi(n)}$. In other words, prove that $f : \{m_1, m_2, ..., m_{\phi(n)}\} \to \{m_1, m_2, ..., m_{\phi(n)}\}$ is a bijection where $f(x) := ax \pmod{n}$.

(b) Prove Euler's Theorem. (Hint: Recall the FLT proof)

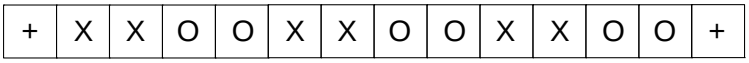
7 Celebrate and Remember Textiles

Mathematics and computing both owe an immense debt to textiles, where many key ideas originated.

Instructions for knitting patterns will tell you to begin by "casting on" the needle some multiple of m plus r, where m is the number of stitches to create one repetition of the pattern and r is the number of stitches needed for the two edges of the piece. For example, in the simple rib stitch pattern below, the repeating pattern is of length $m = 4$, and you need $r = 2$ stitches for the edges.



Thus, to make the final piece wider, you can add as many multiples of the pattern of length 4 as you like; for example, if you want to repeat the pattern 3 times, you need to cast on a total of $3m + r = 3(4) + 2 = 14$ stitches (shown below).



You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements:

- Alternating Link: Multiple of 7, plus 4
- Double Broken Rib: Multiple of 4, plus 2
- Swag: Multiple of 5, plus 2

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns. **Find the smallest number of stitches you need to cast on in order to incorporate all three patterns in your baby blanket.**

8 CRT Coordinates

The Chinese Remainder Theorem is the key to understanding the true structure of modular arithmetic when working mod a composite number.

Consider $m_1, m_2, \ldots, m_n$ pairwise coprime — i.e. no two share any factors. Then $N = \prod_{i=1}^{n} m_i$ is the modulus that we are working in.

The CRT tells us that we can view each number in mod N arithmetic as a vector of sorts — where the i-th coordinate is obtained by modding by m_i. So a number a is represented by $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$ where

$a_i = a \bmod m_i$. The CRT tells us that we have basis elements v_i whose vector representations have a 1 in the i-th position and 0 everywhere else.

You've seen proofs in class for the case of $n = 2$, this problem just asks you to generalize the arguments.

(a) **Prove that we can do addition for numbers mod N by simply doing addition mod m_i in each component for the CRT representation.**

(b) **Prove that we can do multiplication for numbers mod N by simply doing multiplication mod m_i in each component for the CRT representation.**

9 Totient Function

Show that the set $S_N = \{x : gcd(x,N) = 1, 0 \leq x < N\}$ has size $(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$, where N is composed of the distinct prime factors $p_1, \cdots, p_k$.

$$N = p_1^1 p_2^1 \cdots p_k^1$$

10 Fermat's Little Theorem

Fermat's Little Theorem states that for any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

11 Make Your Own Question

Make your own question on this week's material and solve it.

12 Homework Process and Study Group

Citing sources and collaborators are an important part of life, including being a student! We also want to understand what resources you find helpful and how much time homework is taking, so we can change things in the future if possible.

1. **What sources (if any) did you use as you worked through the homework?**
2. **If you worked with someone on this homework, who did you work with?** List names and student ID's. (In case of homework party, you can also just describe the group.)
3. **How did you work on this homework?** (For example, *I first worked by myself for 2 hours, but got stuck on problem 3, so I went to office hours. Then I went to homework party for a few hours, where I finished the homework.*)
4. **Roughly how many total hours did you work on this homework?**