CS 70 Discrete Mathematics and Probability Theory
Spring 2020 HW 4

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.

Solution:

(a) Let $x = 7a+3$ and $y = 5a+2$. We want to show that $\gcd(x,y) = 1$, i.e. x and y are coprime. We use the subtractive form of Euclid's Algorithm.

$$\begin{aligned}
\gcd(x,y) &= \gcd(7a+3, 5a+2) \\
&= \gcd(5a+2, 7a+3-(5a+2)) \\
&= \gcd(5a+2, 2a+1) \\
&= \gcd(2a+1, 5a+2-2(2a+1)) \\
&= \gcd(2a+1, a) \\
&= \gcd(a, 2a+1-2a) \\
&= \gcd(a,1) = 1.
\end{aligned}$$

So $\gcd(7a+3, 5a+2) = 1$. Hence, $7a+3$ and $5a+2$ are coprime.

(b) According to Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$ where $gcd(a,p) = 1$. So $3^{10} \equiv 1 \pmod{11}$. Then,

$$3^{48} = \left(3^{10}\right)^4 \cdot 3^8 \equiv (1) \cdot 3^8 = \left(3^2\right)^4 \equiv (-2)^4 = 16 \equiv 5 \pmod{11}.$$

Alternatively,

$$3^{48} = \left(3^{10}\right)^4 \cdot 3^8 \equiv (1) \cdot 3^8 = \left(3^4\right)^2 \equiv (81)^2 \equiv (4)^2 = 16 \equiv 5 \pmod{11}.$$

Thus, $3^{48} \equiv 5 \pmod{11}$.

(c)

$$x^2 + x \equiv 2 \pmod{4} \Rightarrow x^2 + x - 2 \equiv (x+2)(x-1) \equiv 0 \pmod{4}.$$

So we have two possible solutions for x:

$$\begin{aligned} x+2 \equiv 0 \pmod{4} &\Rightarrow \quad x \equiv 2 \pmod{4}, \\ x-1 \equiv 0 \pmod{4} &\Rightarrow \quad x \equiv 1 \pmod{4}. \end{aligned}$$

Hence, the solution is $x \equiv 2 \pmod{4}$ or $x \equiv 1 \pmod{4}$.

Note that it is not possible to set $(x+2) = 2$ and $(x-1) = 2$ in order to have $(x+2)(x-1) = 4 \equiv 0 \pmod{4}$ since we should have $x = 0$ and $x = 3$ at the same time which is a contradiction.

(d) Fermat's little theorem states that if p is a prime number, then for any integer x, where $gcd(x,p) = 1$, $x^{p-1} = 1 \pmod{p}$. So

$$x^6 \equiv 1 \pmod{6}.$$

So

$$\begin{aligned} 17x^{12} + 5x^7 - 14x^{40} &\equiv 3\left(x^6\right)^2 + 5x^6 \cdot x - 0 \cdot x^{40} \pmod{7} \\ &\equiv 3 + 5x \equiv 6 \pmod{7}. \end{aligned}$$

$$\Rightarrow 5x \equiv 6 - 3 \equiv 3 \pmod{7}.$$

Now since gcd(5,7)=1, 5 has a (unique) inverse mod 7, and since $5 \times 3 = 15 \equiv 1 \pmod{7}$ the inverse is 3. We multiply both sides of $5x \equiv 3 \pmod{7}$ by 3.

$$x \equiv 9 \equiv 2 \pmod{7}.$$

(e) We know $a + 4c \equiv 2b \pmod{21}$. To simplify we write:

$$100a + 10b + c = 100a + 5(2b) + c \pmod{21}.$$

We can replace $2b$ from the assumption in the question:

$$100a + 5(a+4c) + c = 105a + 21c = 21(5a+c) \equiv 0 \pmod{21}.$$

Hence,

$$100a + 10b + c \equiv 0 \pmod{21}.$$

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).

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

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?

Solution:

(a) Let $\text{GCD}(x,y)$ be the GCD of positive integers x and y. If $x = y$, then obviously

$$\text{GCD}(x,y) = \text{GCD}(x,x) = x$$

Euclid's insight was to observe that, if $x > y$, then

$$\text{GCD}(x,y) = \text{GCD}(x-y,y)$$

So the subtractive form of the recursive GCD as learned from the lecture is:

```
gcd(x, y)
        if(y > x) return gcd(y, x)
        else if(x = y) return x
        else return gcd(y, x-y)
```

We can write this iteratively using a while loop as follows:

```
gcd(x, y)
        while(x != y)
          if(x > y) x = x-y
          else y = y-x
        return x
```

Now for EGCD, we learned from the lecture that the subtractive form of the recursive EGCD algorithm is

```
egcd(x, y)
          if(y > x)
            (d', a', b') = egcd(y, x)
            return (d', b', a')
          else if(x = y)
            return (x, 1, 0)
          else
            (d', a', b') = egcd(x-y, y)
            return (d', a', b'-a')
```

To write this iteratively we do the following: Initially, we have x and y as our inputs. Assume x' and y' are the reduced values of x and y after a few subtraction in GCD. So

$$\begin{aligned} x' &= ax+by, \\ y' &= cx+dy. \end{aligned}$$

So $\text{GCD}(x,y) = \text{GCD}(x',y')$.
If $x' > y'$ can continue reducing this to

$$\begin{aligned} x' = x'-y' = (a-c)x+(b-d)y, \\ y' = cx+dy. \end{aligned}$$

and if not

$$\begin{aligned} x' = ax+by, \\ y' = y'-x' = (c-a)x+(d-b)y. \end{aligned}$$

This is repeated until $x' = y'$. Then, $\text{GCD}(x,y) = \text{GCD}(x',y') = x'$ and the corresponding coefficients are coefficnet for $\text{GCD}(x,y) = mx+ny$.
The algorithm starts with

$$\begin{aligned} x' = ax+by \Rightarrow a = 1, \quad b = 0, \\ y' = ax+cd \Rightarrow c = 0, \quad d = 1. \end{aligned}$$

so we have

```
egcd(x, y)
          x' = x, y' = y
          a = 1, b = 0
          c = 0, d = 1
          div = x', m = a, n = b
          while(x' != y')
           if(x' > y')
             x' = x'-y'
             a = a-c, b = b-d
             div = x', m = a, n = b
           else
             y' = y'-x'
             c = c-a, d = d-b
             div= y', m = c, n = d
          return div, m, n
```

(b) Initially we have $x = 54$ and $y = 17$, so

`x' = 54, y' = 17, a = 1, b = 0, c = 1, d = 0`

iteration 1:

`x' = 3, y' = 17, a = 1, b = -3, c = 0, d = 1`

iteration 2:

`x' = 3, y' = 2, a = 1, b = -3, c = -5, d = 16`

iteration 3:

`x' = 1, y' = 2, a = 6, b = -19, c = -5, d = 16`

iteration 3:

`x' = 1, y' = 1, a = 6, b = -19, c = -11, d = 35`

So we can return either

`(div = x' = 1, m = a = 6, n = b = -19)` or

`(div = y' = 1, m = c = -11, n = d = 35)`.

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.

   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 $180^\circ(n-2)$ — 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.

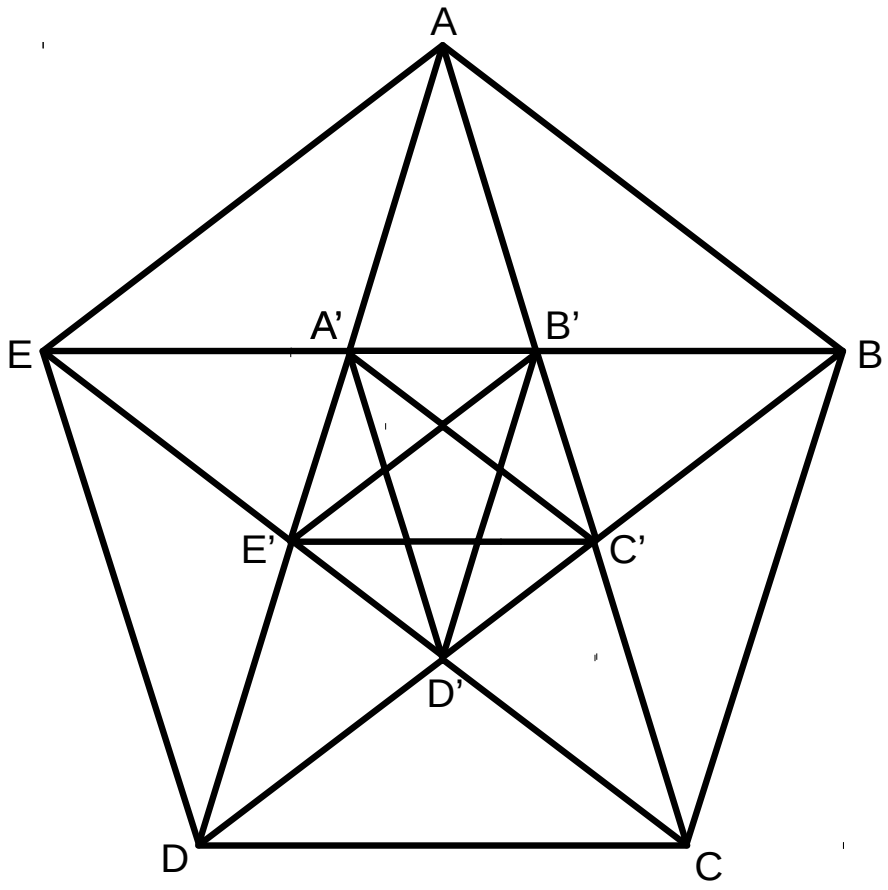


Figure 1: Regular pentagon

- 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', ..., 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?*

Solution:

1. Let us enumerate the argument calls to GCD: $(a_0, b_0), (a_1, b_1), (a_2, b_2), \ldots$ where $a_0 = a$ and $b_0 = b$. By definition, the algorithm terminates if and only if there exists some n such that $b_n = 0$.

   Suppose a and b are commensurable. Let $g > 0; x, y \in \mathbb{N}$ such that $a = xg$ and $b = yg$. Let $(x_0, y_0), (x_1, y_1), \ldots$ the sequence of argument calls to GCD for the integral inputs (x, y). We will show by induction that we can rewrite the sequence (a_i, b_i) as:

   $$(a_i, b_i) = (x_i g, y_i g)$$

   This would prove that $\text{GCD}(a, b)$ terminates. Indeed, we know that $\text{GCD}(x, y)$ terminates, so there exists some n such that $y_n = 0$, thus $b_n = 0$ and $\text{GCD}(a, b)$ terminates.

   The proof by induction is straightforward, except that we have to make sure that we do not overflow past the termination n such that $y_n = 0$. The induction hypothesis is:

   $$H_i := i \leq n \Rightarrow (a_i, b_i) = (x_i g, y_i g)$$

   H_0 holds by definition. Suppose H_i holds and $i \leq n - 1$. We have:

   $$\begin{aligned}(a_{i+1}, b_{i+1}) &= (b_i, a_i - \lfloor a_i / b_i \rfloor b_i) \\ &= (y_i g, x_i g - \lfloor (x_i g)/(y_i g) \rfloor y_i g) \\ &= (y_i g, (x_i - \lfloor x_i / y_i \rfloor y_i) g) \\ &= (x_{i+1} g, y_{i+1} g)\end{aligned}$$

which concludes our proof.

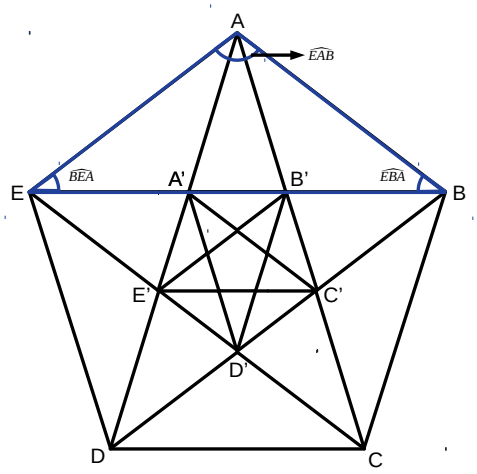


Figure 2: Interior angles of triangle EAB

2. Because all interior angles are equal, $\widehat{EAB} = 540^\circ/5 = 108^\circ$. Since $EA = AB$, EAB is an isosceles triangle, and $\widehat{BEA} = \widehat{EBA} = (180^\circ - 108^\circ)/2 = 36^\circ$. See Figure 2.

   $A'AB'$ is an isosceles triangle:

   By symmetry, EAB, ABC, BCD, CDE, and DEA are all congruent triangles, thus $\widehat{CAB} = \widehat{DAE} = \widehat{EBA} = 36^\circ$. (See Figure 3 for illustration.)

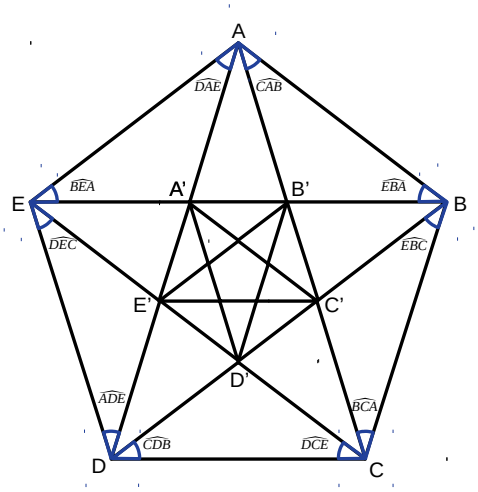


Figure 3: The inside angles

Also

- $\widehat{A'AB'} = \widehat{EAB} - \widehat{DAE} - \widehat{CAB} = 108^\circ - 36^\circ - 36^\circ = 36^\circ$.
- $\widehat{EA'A} = 180^\circ - 36^\circ - 36^\circ = 108^\circ$.
- $\widehat{AB'B} = 180^\circ - 36^\circ - 36^\circ = 108^\circ$.
- $\widehat{AA'B'} = 180^\circ - 108^\circ = 72^\circ$.

- $\widehat{AB'A'} = 180^\circ - 108^\circ = 72^\circ$.

Since $\widehat{AA'B'} = \widehat{AB'A'}$, $A'AB'$ is an isosceles triangle.

EAB' is an isosceles triangle:

Since $\widehat{EAB'} = \widehat{EAA'} + \widehat{A'AB'} = 36^\circ + 36^\circ = 72^\circ = \widehat{A'B'A}$, EAB' is also an isosceles triangle.

Now consider the triangle $EE'B'$:

- By symmetry, $\widehat{E'EB'} = \widehat{A'AB'} = 36^\circ$
- $\widehat{E'A'B'} = \widehat{EA'A} = 108^\circ$
- By symmetry, $\widehat{EE'A'}$ and $\widehat{A'AB'}$ are congruent triangles and $E'A' = A'B'$.
- Since, $E'A' = A'B'$, $\widehat{A'E'B'} = \widehat{A'B'E'} = (180^\circ - 108^\circ)/2 = 36^\circ$. Since $\widehat{E'EB'} = \widehat{E'B'E}$, $EE'B'$ is an isosceles triangle.

3. Interior angles: We already showed that $\widehat{E'A'B'} = 108^\circ$ in the previous part, and by the symmetry argument, $\widehat{A'B'C'} = \widehat{B'C'D'} = \widehat{C'D'E'} = \widehat{D'E'A'} = \widehat{E'A'B'} = 108^\circ$.

   Since $A'AB', B'BC', C'CD', D'DE'$, and $E'EA'$ are all congruent triangles, $E'A' = A'B' = B'C' = C'D' = D'E'$.

   Since $\widehat{A'B'C'} = \widehat{B'C'D'} = \widehat{C'D'E'} = \widehat{D'E'A'} = \widehat{E'A'B'}$ and $E'A' = A'B' = B'C' = C'D' = D'E'$, then $A'B'C'D'E'$ is a regular pentagon.

4. Since EAB' is an isosceles triangle, $EA = EB'$. So

$$\text{GCD}(EA, EB) = \text{GCD}(EB', EB)$$

5. Since $EB > EB'$, we use Euclid's algorithm:

$$\text{GCD}(EB', EB) = \text{GCD}(EB', EB - EB').$$

   But from Figure 3 we know that $EB - EB' = B'B$. So

$$\text{GCD}(EB', EB) = \text{GCD}(EB', EB - EB') = \text{GCD}(EB', B'B).$$

6. Since $EA'E'$ and $BB'C'$ are congruent (Figure 3) we have $B'B = EA'$. SO

$$\text{GCD}(EB', B'B) = \text{GCD}(EB', EA').$$

7. Since $EB' > EA'$, we use Euclid's algorithm:

$$\text{GCD}(EB', EB) = \text{GCD}(EB' - EA', EA').$$

   But from Figure 3 we know that $EB' - EA' = A'B'$. So

$$\text{GCD}(EB', EA') = \text{GCD}(EB' - EA', EA') = \text{GCD}(A'B', EA').$$

8. Since $EA'E'$ is an isoceles triangle (Figure 3) we have $EA' = EA'$. So

$$\text{GCD}(A'B', EA') = \text{GCD}(A'B', EE').$$

9. Since $EE'B'$ is an isoceles triangle (Figure 3) we have $EE' = E'B'$. So

$$\text{GCD}(A'B', EE') = \text{GCD}(A'B', E'B').$$

10. By the contrapositive of question 1, to show that EB and EA are incommensurable, it suffices to show that $\text{GCD}(EB, EA)$ does not terminate.

    From previous parts we conclude that

$$\text{GCD}(EA, EB) = \text{GCD}(A'B', E'B').$$

    Here we pause for a moment. We started by asking what is the GCD of the side of the pentagon and its chord, and two euclidean algorithm steps later, we are asked the exact same question, only on the smaller pentagon $A'B'C'D'E'$. Now, all the reasoning that applied in the previous two GCD steps can also apply in the next two GCD steps, only to go from $A'B'C'D'E'$ to the immediately smaller pentagram contained in it. This process will repeat to infinity, always considering smaller and smaller pentagons, without ever reaching a case where the size of the pentagon side is 0. Thus, $\text{GCD}(EB, EA)$ does not terminate, and EB and EA are incommensurable.

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.

Solution:

Given x, consider the set T defined as $\{xy^{-1} \pmod p : y \in S\}$. Note that the set T has the same cardinality as S, because for $y_1 \neq y_2 \pmod p$, we have $xy_1^{-1} \neq xy_2^{-1} \pmod p$ (if not, we can multiply both sides by x^{-1}, and take the inverse to get a contradiction).

Therefore, the sets S and T must have a non-empty intersection. So there must be $y_1, y_2 \in S$ such that $xy_1^{-1} = y_2 \pmod p$. But this means that $x \equiv y_1 y_2 \pmod p$.

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.

Solution:

(a) The earliest AC Transit bus Joel can take is at 7:11am, from which he can transfer to BART immediately after he gets off the bus at 7:21am.

Let the x^{th} bus (zero-based) be the bus Joel can take with zero transfer time, and let the y^{th} train (zero-based) be the train that he will connect to. Taking the time the BART starts running (4:25am) as a reference point, let t be the time in minutes from 4:25am to the transfer time to the y^{th} train [1]. Figure 4 shows the timeline.

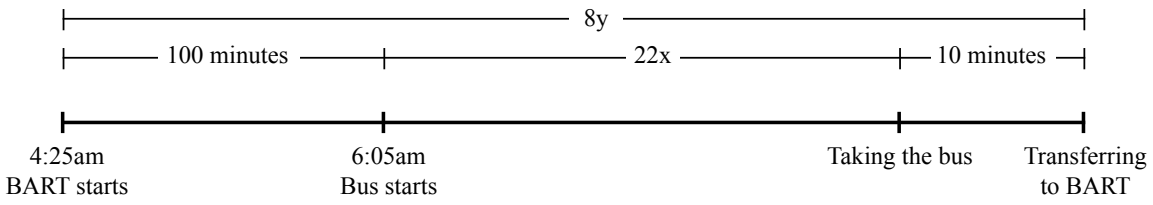


Figure 4: Timeline

From the timeline, we see the relation between x, y, and t,

$$\begin{aligned} t = 100 + 22x + 10 &= 8y \\ 8y - 22x &= 110 \\ 4y - 11x &= 55 \end{aligned} \tag{1}$$

We modulo both sides of Equation (1) with 11 to eliminate x,

$$\begin{aligned} &\text{Left-hand side: } (4y - 11x) \equiv 4y, \pmod{11}, \\ &\text{Right-hand side: } 55 \equiv 0 \pmod{11}, \end{aligned}$$

and form a congruence,

$$4y \equiv 0 \pmod{11}. \tag{2}$$

[1] Using any other time as a reference point works too, i.e., midnight, 7:00am (and find the BART departure after 7:00am), etc.

Since 3 is the multiplicative inverse of 4 modulo 11. Multiplying both sides of the congruence (2) by 3 gives us y,

$$\begin{aligned} 3 \cdot 4y &\equiv 3 \cdot 0 \pmod{11} \\ y &\equiv 0 \pmod{11}, \\ y &\in \{\ldots, 0, 11, 22, 33, \ldots\}. \end{aligned}$$

Since the bus hasn't started running when the 0^{th} and 11^{th} trains run, the 22^{th} train is the first train to connect to. The 22^{th} train departs at 4:25am + 8(22) minutes = 4:25am + 2:56 hours = 7:21am. The bus that arrives the BART station at 7:21am departs Joel's home stop at 7:21am - 10 minutes = 7:11am.

(b) The first AC Transit bus Joel can take is at 11:35am, from which he can connect to BART at 11:45am, and then Muni bus at 12:18pm. This is the only bus of the day that he can avoid waiting for both transfers.

From part a, we know that the soonest time Joel can arrive the San Francisco BART station is 7:21am + 33 minutes = 7:54am, and that he can choose to arrive every 88 minutes after that, since it is the interval AC Transit bus and BART coincides again. Let x be the number of times this 88-minute interval occurs after 7:54am (x starts from 0), and y^{th} bus (zero-based) be the Muni bus that Joel can transfer to with zero transfer time. Taking the time the Muni bus starts running (7:12am) as a reference point, let t be the time in minutes from 7:12am to the transfer time from BART to the y^{th} Muni bus. Figure 5 shows the timeline.

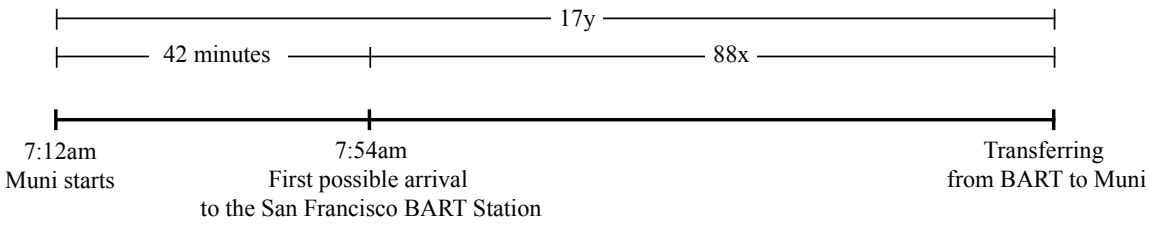


Figure 5: Timeline

Again, we write a relation between x, y, and t.

$$\begin{aligned} t &= 42 + 88x = 17y \\ 17y - 88x &= 42 \end{aligned} \tag{3}$$

The rest is quite similar to part a.

We modulo both sides of Equation (3) with 88 to eliminate x and form a congruence,

$$17y \equiv 42 \pmod{88}. \tag{4}$$

We have $17 \times 5 = 85 \equiv -3 \pmod{88}$. Let's mutiply both sides by 5:

$$-3y \equiv 210 \equiv 34 \pmod{88}. \tag{5}$$

We have $3 \times 29 = 87 \equiv -1 \pmod{88}$. Let's mutiply both sides by 29:

$$y \equiv 34 \times 29 = 986 \equiv 18 \pmod{88}, \tag{6}$$
$$y \in \{\ldots, -70, 18, 106, \ldots\}. \tag{7}$$

The first Muni bus Joel can take with zero transfer time is the 18^{th} Muni bus at 7:12am + 17(18) minutes = 7:12am + 5:06 hours = 12:18pm. Subtracting the 33 minutes BART transit time, the BART departure time is 12:18pm - 33 minutes = 11:45am. Subtracting the 10 minutes AC Transit travel time, the AC Transit bus departure time is 11:45am - 10 minutes = 11:35am.

Because the Least Common Multiple of 88 and 17 is $88 \times 17 = 1496$, it will take 1,496 minutes = 24 hours 56 minutes for all three buses and BART to coincide again. Since all services stop just before midnight and restart at their respective times the next day, all three buses and BART coincide only once a day, and what we found is the only bus Joel can take that day. □

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)

Solution:

(a) This problem mirrors the proof of Fermat's Little Theorem, except now we work with the set $\{m_1, m_2, \cdots, m_{\phi(n)}\}$.

Since m_i and a are both coprime to n, so is $a \cdot m_i$. Suppose $a \cdot m_i$ shared a common factor with n, and WLOG, assume that it is a prime p. Then, either $p|a$ or $p|m_i$. In either case, p is a common factor between n and one of a or m_i, contradiction.

We now prove that f is injective. Suppose we have $f(x) = f(y)$, so $ax \equiv ay \pmod{n}$. Since a has a multiplicative inverse $\pmod{n}$, we see $x \equiv y \pmod{n}$, thus showing that f is injective.

We continue to show that f is surjective. Take any y that is relatively prime to n. Then, we see that $f(a^{-1}y) \equiv y \pmod{n}$, so therefore, there is an x such that $f(x) = y$. Furthermore, $a^{-1}y \pmod{n}$ is relatively prime to n, since we are multiplying two numbers that are relatively prime to n.

(b) Since both sets have the same elements, just in different orders, multiplying them together gives

$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv am_1 \cdot am_2 \cdot \ldots \cdot am_{\phi(n)} \pmod{n}$$

and factoring out the a terms,

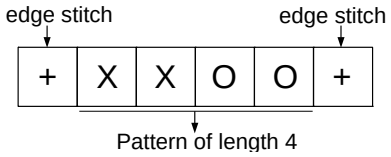
$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv a^{\phi(n)} \left(m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)}\right) \pmod{n}.$$

Thus we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

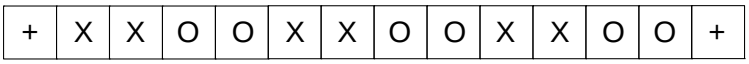
7 Celebrate and Remember Textiles

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.**

Solution: Let x be the number of stitches we need to cast on. Using the Chinese Remainder Theorem, we can write the following system of congruences:

$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 2 \pmod 5. \end{aligned}$$

We have $M = 7 \cdot 4 \cdot 5 = 140$, $r_1 = 4$, $m_1 = 7$, $b_1 = M/m_1 = 4 \cdot 5 = 20$, $r_2 = 3$, $m_2 = 4$, $b_2 = M/m_2 = 7 \cdot 5 = 35$, and $r_3 = 2$, $m_3 = 5$, $b_3 = M/m_3 = 7 \cdot 4 = 28$. We need to solve for the multiplicative inverse of b_i modulo m_i for $i \in \{1,2,3\}$:

$$\begin{aligned} b_1 a_1 &\equiv 1 \pmod{m_1} \\ 20 a_1 &\equiv 1 \pmod 7 \\ 6 a_1 &\equiv 1 \pmod 7 \\ \rightarrow a_1 &= 6, \end{aligned}$$

$$\begin{aligned} b_2 a_2 &\equiv 1 \pmod{m_2} \\ 35 a_2 &\equiv 1 \pmod 4 \\ 3 a_2 &\equiv 1 \pmod 4 \\ \rightarrow a_2 &= 3, \end{aligned}$$

and

$$\begin{aligned} b_3 a_3 &\equiv 1 \pmod{m_3} \\ 28 a_3 &\equiv 1 \pmod 5 \\ 3 a_3 &\equiv 1 \pmod 5 \\ \rightarrow a_3 &= 2. \end{aligned}$$

Therefore,

$$\begin{aligned} x &\equiv 6 \cdot 20 \cdot 4 + 2 \cdot 35 \cdot 3 + 2 \cdot 28 \cdot 2 \pmod{140} \\ &\equiv 102 \pmod{140}, \end{aligned}$$

so the smallest x that satisfies all three congruences is 102. Therefore we should cast on 102 stitches in order to be able to knit all three patterns into the 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.**

Solution: Assume we have two numbers $a = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$ and $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$. These numbers can be writen as:

$$a = \sum_{i=1}^{n} a_i v_i \pmod N, \quad b = \sum_{i=1}^{n} b_i v_i \pmod N,$$

for

$$N = \prod_{j=1}^{n} m_j, \quad v_i = \left(\prod_{j \neq i} m_j^{-1} \pmod{m_i} \right) \prod_{j \neq i} m_j,$$

as we learn from the lecture.

(a) We want to show that

$$a + b \pmod N = \left[\sum_{i=1}^{n} (a \pmod{m_i} + b \pmod{m_i}) v_i \right] \pmod N.$$

Starting from the left hand side we have

$$\begin{aligned} a + b \pmod N &= \sum_{i=1}^{n} a_i v_i + \sum_{i=1}^{n} b_i v_i \pmod N \\ &= \sum_{i=1}^{n} (a_i + b_i) v_i \pmod N \\ &= \left[\sum_{i=1}^{n} (a \pmod{m_i} + b \pmod{m_i}) v_i \right] \pmod N. \end{aligned}$$

□

(b) We want to show that

$$a \cdot b \pmod N = \left[\sum_{i=1}^{n} (a \pmod{m_i}) \cdot b \pmod{m_i}) v_i\right] \pmod N,$$

The left hands side can be expanded as

$$\begin{aligned} a \cdot b \pmod N &= \sum_{i=1}^{n} a_i v_i \cdot \sum_{j=1}^{n} b_j v_j \pmod N \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j v_i v_j \pmod N. \end{aligned}$$

We know that

$$\begin{aligned} v_i v_j &\equiv 0 \pmod N, i \neq j, \\ v_i v_i &\equiv v_i \pmod N. \end{aligned}$$

So this eliminates all the terms with $v_i v_j$ where $i \neq j$. So we only have a summation over the index i.

$$\begin{aligned} a \cdot b \pmod N &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j v_i v_j \pmod N \\ &= \sum_{i=1}^{n} a_i b_i v_i v_i \pmod N \\ &= \sum_{i=1}^{n} (a_i b_i) v_i \pmod N \\ &= \left[\sum_{i=1}^{n} (a \pmod{m_i}) \cdot b \pmod{m_i}) v_i\right] \pmod N. \qquad \square \end{aligned}$$

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 $p_1, \cdots, p_k$.

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

Solution: For $x \in S_N$, x is not divisible by every prime $p_1, \cdots, p_k$. So $x = z_i \pmod{p_i}, z_i \neq 0$.

There are $p_i - 1$ possible values for each z_i and we know from CRT there is a unique value mod N that satisfies this system of equations. So the total number of tickets is $\prod_{i=1}^{k} (p_i - 1)$.

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.

Solution:

Let $n \in \mathbb{N}$. We begin by breaking down 42 into prime factors: $42 = 7 \times 3 \times 2$. Since 7, 3, and 2 are prime, we can apply Fermat's Little Theorem, which says that $a^p \equiv a \pmod{p}$, to get the congruences

$$n^7 \equiv n \pmod{7}, \tag{8}$$
$$n^3 \equiv n \pmod{3}, \quad \text{and} \tag{9}$$
$$n^2 \equiv n \pmod{2}. \tag{10}$$

Now, let's take (9) and multiply it by $n^3 \cdot n$. This gives us

$$n^7 \equiv n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \pmod{3},$$

and since by (9), $n^3 \equiv n \pmod{3}$, this gives

$$n^7 \equiv n \pmod{3}.$$

Similarly, we take (10) and multiply by $n^2 \cdot n^2 \cdot n$ to get

$$n^7 \equiv n^2 \cdot n^2 \cdot n^2 \cdot n \equiv n^4 \pmod{2}.$$

Notice that $n^4 \equiv n^2 \cdot n^2 \equiv n \cdot n \equiv n^2 \pmod{2}$, and by (10) $n^2 \equiv n \pmod{2}$, so we have

$$n^7 \equiv n \pmod{2}.$$

Thus,

$$n^7 \equiv n \pmod{7}, \tag{11}$$
$$n^7 \equiv n \pmod{3}, \quad \text{and} \tag{12}$$
$$n^7 \equiv n \pmod{2}. \tag{13}$$

Let $x = n^7 - n$. By the Chinese Remainder Theorem, the system of congruences

$$x \equiv 0 \pmod{7}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 0 \pmod{2}$$

has a unique solution modulo $2 \cdot 3 \cdot 7 = 42$, and this unique solution is $x \equiv 0 \pmod{42}$. So, we have that $n^7 - n \equiv 0 \pmod{42}$, which means $n^7 - n$ is divisible by 42.

11 Make Your Own Question

You must make your own question on this week's material and solve it.

12 Homework Process and Study Group

You must describe your homework process and study group in order to receive credit for this question.