EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Homework 4

This homework is due September 29, 2014, at 12:00 noon.

1. Modular Arithmetic Lab

In Python, you can perform many common modular arithmetic operations. For example, the modular reduction operator is represented by the % operator (e.g. `7 % 2` returns 1). In this week's Virtual Lab, we will explore a few basic modular arithmetic and primality testing algorithms, as well as how to implement them in Python.

Please download the IPython starter code from Piazza or the course webpage, and answer the following questions.

(a) Implement the function `mod_exp`, which takes three parameters x, y, and m, and computes (x^y) mod m using *repeated squaring*. Do NOT use Python's built-in `pow` function.

(b) Implement the function `gcd`, which takes a pair of natural numbers x, y, and computes their greatest common divisor.

(c) Implement the `egcd` function, which takes a pair of natural numbers $x >= y$, and returns a triple of integers (d, a, b) such that $d = gcd(x, y) = ax + by$.

Use the function `egcd` to find the positive inverse of 117 mod 103, of 17947 mod 222, and of 1812647 mod 1234567.

The answers are 81, 19, and 710348, respectively.

(d) Implement the function `is_prime`, which checks if a positive number x is a prime number. A naive implementation would be fine here; we'll look at more efficient implementations in later questions.

(e) The Sieve of Eratosthenes is a simple, ancient algorithm for finding all prime numbers up to any given limit. It does so by iteratively marking as composite (i.e. not prime) the multiples of each prime, starting with the multiples of 2.

Implement the function `sieve`, which takes a positive integer n, and returns a list of all primes less than or equal to n. A sample execution of the algorithm is given in the code skeleton.

Reminder: When you finish, don't forget to convert the notebook to pdf and merge it with your written homework. Please also zip the `ipynb` file and submit it as `hw4.zip`.

2. 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). 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. (Please do not find the answer by listing all the schedules.)

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 1 shows the timeline.

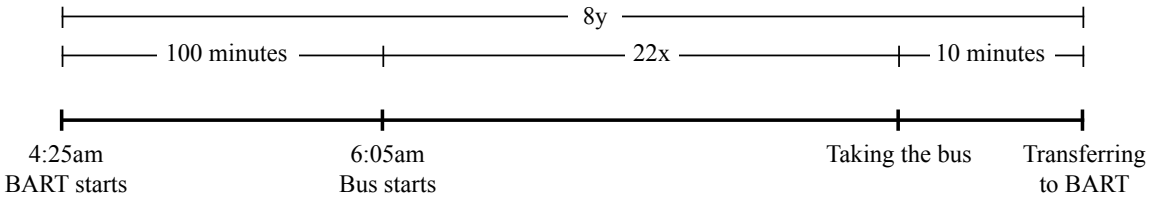

Figure 1: Timeline

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 can use the Extended Euclid's algorithm to solve for $x, y \in \mathbb{Z}$ in Equation (1), starting with finding the GCD of 11 and 4 with the Euclid's algorithm.

$$11 = 4(2) + 3 \tag{2}$$
$$4 = 3(1) + 1 \tag{3}$$
$$3 = 1(3) + 0 \tag{4}$$

Equation (4) tells us that $\gcd(11,4) = 1$. Working our way back up, we rearrange Equation (3) to write 1 as a linear combination of 3 and 4,

$$\begin{aligned} 1 &= 4 - 3(1) \\ 1 &= 4 - (11 - 4(2))(1) \qquad \text{[Substituted 3 with values from Equation (2)]} \\ 1 &= 4 - 11 + 4(2) \\ 1 &= 4(3) - 11 \end{aligned} \tag{5}$$

Now we have solved a very similar equation to Equation(1), $4a - 11b = 1$, where a and b are both integers. How can we use this to solve Equation (1)? We will present two ways to do so.

1st Approach: Multiplying Equation (5) by 55,

$$\begin{aligned} 55(4(3) - 11) &= 55 \\ 4(165) - 11(55) &= 55 \end{aligned}$$

We have found one possible $(x,y) = (165,55)$! But will that give the first transfer time of the day? Notice that once the bus and train coincides, they will coincide again every 88 minutes. (Because 88

[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.

is the Least Common Multiple[2] of 22 and 8.) In other words, every 4^{th} bus will coincide again with every 11^{th} train. Therefore, we know that the 55^{th} bus and the 165^{th} train are not the first ones Joel can take, since the $55-4=51^{\text{st}}$ bus and $165-11=154^{\text{th}}$ bus apparently coincides too. Mathematically,

$$\begin{aligned} 4(165)-11(55) &= 55 \\ 11(4)-4(11)+4(165)-11(55) &= 55 \quad [11(4)-4(11)=0] \\ 4(165-11)-11(55-4) &= 55 \\ 4(154)-11(51) &= 55 \end{aligned}$$

Doing this 13 times gives us the first bus and train that coincide (one more time and we'll get a bus that hasn't started running),

$$\begin{aligned} 4(165)-11(55) &= 55 \\ 13(11(4)-4(11))+4(165)-11(55) &= 55 \quad [13(11(4)-4(11))=0] \\ 11(52)-4(143)+4(165)-11(55) &= 55 \\ 4(165-143)-11(55-52) &= 55 \\ 4(22)-11(3) &= 55 \end{aligned} \tag{6}$$

Therefore, the 3^{rd} and the 22^{th} train are the first bus and train Joel can take with no transfer time. The 3^{rd} bus departs at 6:05am + 22(3) minutes = 6:05am + 1:06 hours = 7:11am. The 22^{th} train departs at 4:25am + 8(22) minutes = 4:25am + 2:56 hours = 7:21am. □

2nd Approach: Variable elimination. We modulo both sides of Equation (1) with 11 to eliminate x,

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

and form a congruence,

$$4y \equiv 0 \pmod{11}. \tag{7}$$

From Equation (5), 3 is the multiplicative inverse of 4 modulo 11. Multiplying both sides of the congruence (7) with 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.

(This approach is convenient, but it has a pitfall. Because we eliminate x completely, we wouldn't know when no solution exists unless we explicitly check if the set of y's we found gives valid x's.) □

[2]Read more at `http://en.wikipedia.org/wiki/Least_common_multiple`

(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.

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 2 shows the timeline.

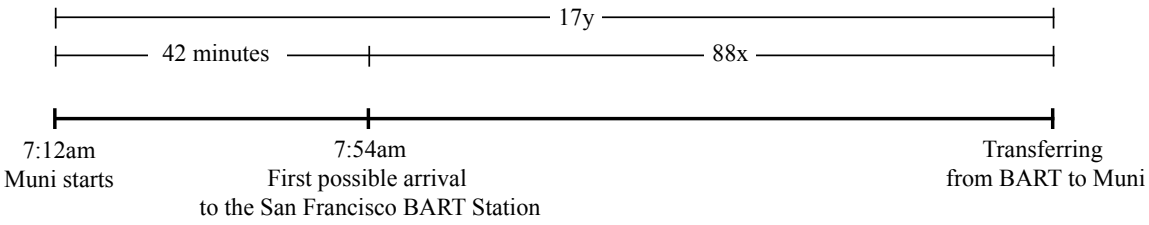

Figure 2: Timeline

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

$$t = 42 + 88x = 17y$$
$$17y - 88x = 42 \tag{8}$$

The rest is quite similar to part (a). We find the GCD of 88 and 17 with the Euclid's algorithm, and then run the Extended Euclid's algorithm to express it interms of linear combination of 88 and 17.

$$88 = 17(5) + 3 \tag{9}$$
$$17 = 3(5) + 2 \tag{10}$$
$$3 = 2(1) + 1 \tag{11}$$
$$2 = 1(2) + 0 \tag{12}$$

Equation (12) tells us that gcd(88,17)=1. Working our way back up, we rearrange Equation (11) to

write 1 as a linear combination of 3 and 2,

$$
\begin{aligned}
1 &= 3 - 2(1) \\
1 &= 3 - (17 - 3(5))(1) && \text{[Substituted 2 with values from Equation (10)]} \\
1 &= 3 - 17 + 3(5) \\
1 &= 3(6) - 17 \\
1 &= (88 - 17(5))(6) - 17 && \text{[Substituted 3 with values from Equation (9)]} \\
1 &= 88(6) - 17(30) - 17 \\
1 &= 88(6) - 17(31) && (13)
\end{aligned}
$$

Similarly, we will show two approaches to use Equation (13) to solve Equation (8).

1st Approach: Multiplying both sides of Equation (13) with 42,

$$
\begin{aligned}
42(88(6) - 17(31)) &= 42 \\
88(252) - 17(1302) &= 42.
\end{aligned}
$$

According to Equation (8), we have $x = -252$ and $y = -1302$. Since 88 and 17 are relatively primes, we can get to the next pair of x and y by adding 17 to x and 88 to y at a time. Doing this 15 times gives us the first valid $x, y \geq 0$,

$$
\begin{aligned}
15(17(88) - 88(17)) + 88(252) - 17(1302) &= 42 \quad [15(17(88) - 88(17)) = 0] \\
17(1320) - 88(255) + 88(252) - 17(1302) &= 42 \\
88(252 - 255) - 17(1302 - 1320) &= 42 \\
17(18) - 88(3) &= 42 \qquad (14)
\end{aligned}
$$

Comparing Equation (14) to Equation (8), we get $x = 3$ and $y = 18$.

2nd Approach: Variable elimination. We modulo both sides of Equation (1) with 88 to eliminate x and form a congruence,

$$17y \equiv 42 \pmod{88}. \qquad (15)$$

From Equation (13),

$$
\begin{aligned}
88(6) - 17(31) &= 1 \\
17(31) - 88(6) &= -1 \\
17(31) \bmod 88 &= -1 \qquad (16)
\end{aligned}
$$

Multiplying both sides of the congruence (15) with 31 gives us y,

$$
\begin{aligned}
31 \cdot 17y &\equiv 31 \cdot 42 \pmod{88} \\
-y &\equiv 1302 \pmod{88} && \text{[From Equation (16)]} \\
y &\equiv -70 \pmod{88}, \\
y &\in \{\ldots, -70, 18, 106, \ldots\}.
\end{aligned}
$$

From either approach, the first Muni bus Joel can take with zero transfer time is the 18^{th} 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. □

3. Solution for $ax \equiv b \bmod m$

In the lecture notes, we proved that when $gcd(m,a) = 1$, a has a unique multiplicative inverse, or equivalently $ax \equiv 1 \bmod m$ has exactly one solution x (modulo m). The proof of the unique multiplicative inverse (theorem 5.2) actually proved that when $gcd(m,a) = 1$, the solution of $ax \equiv b \bmod m$ with unknown variable x is unique. Now let's consider the case where $gcd(m,a) > 1$ and see why there is no unique solution in this case. Let's consider the general solution of $ax \equiv b \bmod m$ with $gcd(m,a) > 1$.

(a) Let $gcd(m,a) = d$. Prove that $ax \equiv b \bmod m$ has a solution (that is, there exists an x that satisfies this equation) if and only if $b \equiv 0 \bmod d$.

Necessary condition ($ax \equiv b \bmod m$ has a solution $\implies b \equiv 0 \bmod d$):
If $ax \equiv b \bmod m$ has a solution, we can write $ax = my + b$ for some $x, y \in \mathbb{Z}$.
Since d is the greatest common divisor of m and a, we know that $d|a$ and $d|m$. Therefore d divides $ax - my = b$, or equivalently, $b \equiv 0 \bmod d$.

Sufficient condition ($b \equiv 0 \bmod d \implies ax \equiv b \bmod m$ has a solution):
Consider the congruent equation $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d}$. Since $gcd(m,a) = d$, we know that $gcd(\frac{m}{d}, \frac{a}{d}) = 1$.
Therefore $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d}$ has a solution, or equivalently, $\exists x, y \in \mathbb{Z}$, such that $\frac{a}{d}x = \frac{m}{d}y + \frac{b}{d}$.
$\implies ax = my + b$.
$\implies x$ is a solution for $ax \equiv b \bmod m$.

Another proof for $b \equiv 0 \bmod d \implies ax \equiv b \bmod m$ has a solution:
If $d|b$, we can write $b = kd$ for some $k \in \mathbb{Z}$. Since $gcd(m,a) = d$, $\exists w, y \in \mathbb{Z}$, such that $aw + my = d$.
Multiplying both sides by k, we get $kaw + kmy = kd = b$. So

$$akw + mky \equiv b \bmod m$$
$$akw \equiv b \bmod m$$

Then kw is a solution of $ax \equiv b \bmod m$.

(b) Let $gcd(m,a) = d$. Assume $b \equiv 0 \bmod d$. Prove that $ax \equiv b \bmod m$ has exactly d solutions (modulo m).

From the proof of sufficient condition in part(a), we have shown that if x satisfies $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d}$, then x also satisfies $ax \equiv b \bmod m$. How about the reverse?
If x satisfies $ax \equiv b \bmod m$, then

$$ax = my + b \text{ for some } y \in \mathbb{Z}$$
$$\implies \frac{a}{d}x = \frac{m}{d}y + \frac{b}{d}$$
$$\implies x \text{ satisfies } \frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$$

We conclude the above proof as the following Lemma:
Lemma: $\forall x \in \mathbb{Z}$, x satisfies $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$ if and only if x satisfies $ax \equiv b \mod m$.

Let x_0 be the unique solution (modulo $\frac{m}{d}$) of $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$, denoting as $x \equiv x_0 \mod \frac{m}{d}$. Any $x \in \mathbb{Z}$ that satisfies $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$ must be of the form $x = x_0 + k\frac{m}{d}$ for some $k \in \mathbb{Z}$.
By the above Lemma, any $x \in \mathbb{Z}$ that satisfies $ax \equiv b \mod m$ will also be of the form $x = x_0 + k\frac{m}{d}$. Now we will show that there are only d distinct solutions (modulo m) for $ax \equiv b \mod m$ among $x = x_0 + k\frac{m}{d}$ $\forall k \in \mathbb{Z}$.
Two solutions, $x_1 = x_0 + k_1\frac{m}{d}$ and $x_2 = x_0 + k_2\frac{m}{d}$, are the same in modulo m if and only if

$$\begin{aligned} x_0 + k_1\frac{m}{d} \equiv x_0 + k_2\frac{m}{d} \mod m &\iff (k_1 - k_2)\frac{m}{d} \equiv 0 \mod m \\ &\iff (k_1 - k_2)\frac{m}{d} = qm \text{ for some } q \in \mathbb{Z} \\ &\iff (k_1 - k_2)m = qmd \\ &\iff k_1 - k_2 = qd \end{aligned}$$

The above argument proved that two solutions with the form of $x = x_0 + k\frac{m}{d}$ are equal $\mod m$ if and only if $k_1 \equiv k_2 \mod d$. Without loss of generality, we can construct solutions by letting $k \in \{0, 1, ..., d-1\}$. To be very specific, the d distinct solutions of $ax \equiv b \mod m$ are

$$x \equiv x_0 + k\frac{m}{d} \mod m, \quad k = 0, 1, ..., d-1$$

(c) Solve for x: $77x \equiv 35 \mod 42$.
Since $gcd(77, 42) = 7$ and $35 \equiv 0 \mod 7$, we can find a unique solution from $\frac{77}{7}x \equiv \frac{35}{7} \mod \frac{42}{7}$:

$$\begin{aligned} 11x &\equiv 5 \mod 6 \\ -1x &\equiv -1 \mod 6 \quad \text{(because } 11 \equiv -1 \mod 6 \text{ and } 5 \equiv -1 \mod 6\text{)} \\ x &\equiv 1 \mod 6 \end{aligned}$$

The solution of $\frac{77}{7}x \equiv \frac{35}{7} \mod \frac{42}{7}$ is $x \equiv 1 \mod 6$. Based on part(b), the solutions of $77x \equiv 35 \mod 42$ are

$$x \equiv 1 + 6k \mod 42, \quad k = 0, 1, ..., 6$$

4. Pentagons, Pentagrams, and Pythagoreans: a high-school 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 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 pillar of Pythagoras teaching was that any two segment lengths are commensurable.

(a) 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:

i. If $b = 0$ then return a.
ii. 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.

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.

(b) 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 3. Given that the sum of the interior angles of a pentagon is 540°, prove that $EA < EB$. *(Hint: You might find the Law of Sines useful.)*

Because all interior angles are equal, $\widehat{EAB} = 540°/5 = 108°$. Since $EA = AB$, EAB is an isosceles triangle, and $\widehat{BEA} = \widehat{EBA} = (180° - 108°)/2 = 36°$. See Figure 4. According to the Law of Sines,

$$\begin{aligned}
\frac{EA}{\sin \widehat{EBA}} &= \frac{EB}{\sin \widehat{EAB}} \\
\frac{EA}{EB} &= \frac{\sin \widehat{EBA}}{\sin \widehat{EAB}}
\end{aligned}$$

Since $\dfrac{\widehat{EBA}}{\widehat{EAB}} = \dfrac{36°}{108°} < 1$, $\dfrac{\sin \widehat{EBA}}{\sin \widehat{EAB}} < 1$, and thus,

$$\begin{aligned}
\frac{EA}{EB} &= \frac{\sin \widehat{EBA}}{\sin \widehat{EAB}} < 1 \\
EA &< EB
\end{aligned}$$

□

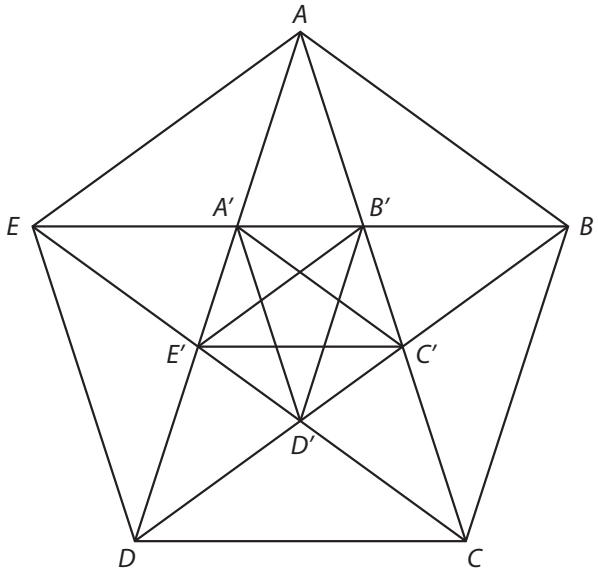

Figure 3: Regular pentagon

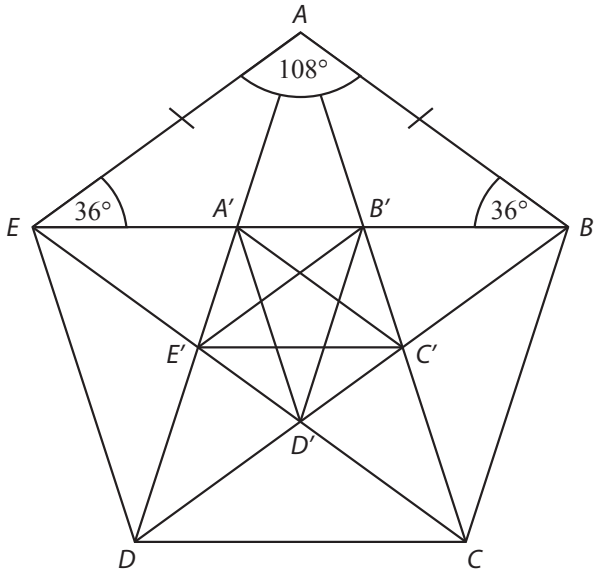

Figure 4: Interior angles of triangle EAB

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

By symmetry, EAB, ABC, BCD, CDE, and DEA are all congruent triangles, thus $\widehat{CAB} = \widehat{DAE} = \widehat{EBA} = 36°$. (See Figure 5 for illustration.)

Continuing to calculate angles from the previous part,

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

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

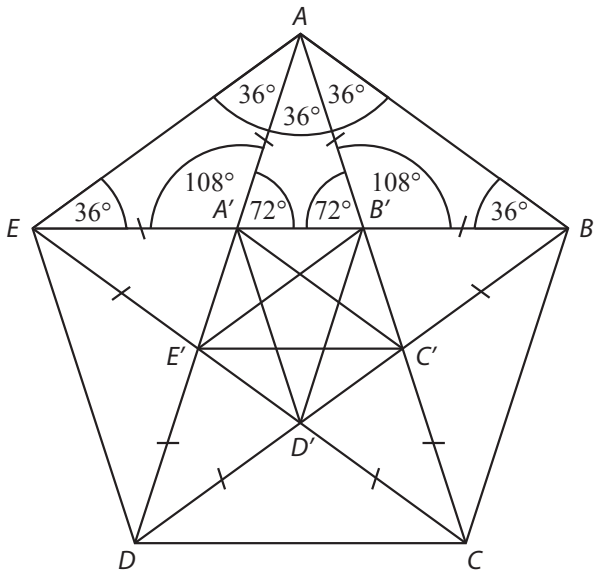

Figure 5: The inside angles

Next, since $\widehat{EAB'} = \widehat{EAA'} + \widehat{A'AB'} = 36° + 36° = 72° = \widehat{A'B'A}$, EAB' is also an isosceles triangle.

Now consider triangle $EE'B'$.

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

(d) Let $A', \ldots, E'$ be the intersection points of the chords as in Figure 3. 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.

Interior angles: We already showed that $E'A'B' = 108°$ in the previous part, and by the symmetry argument, $A'B'C' = B'C'D' = C'D'E' = D'E'A' = E'A'B' = 108°$.

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

(e) Express $E'A'$ and $E'B'$ separately in terms of EA and EB.

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

$$\begin{aligned} E'A' = A'B' &= EB' - EA' \\ &= EB' - (EB - EB') \\ &= 2EB' - EB \\ &= 2EA - EB \end{aligned}$$

From part (c), $E'B' = E'E$ because $EE'B'$ is an isoscele triangle.

$$E'B' = E'E = EA' = B'B = EB - EB' = EB - EA.$$

(f) Using the previous elements, show that EB and EA are incommensurable. (In modern terms, we would say that EB/EA is irrational.)

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 ($EB > EA$ by question 2).

As $EA > 0$, $EB - EA > 0$ and $EB - 2EA < 0$ by question 4, the next call to GCD is with arguments $(EA, EB - EA) = (EA, E'B')$. As $E'B' > 0$, $EA - E'B' = 2EA - EB > 0$ and $EA - 2E'B' = 3EA - 2EB < 0$ the next call is $\text{GCD}(E'B', E'A')$.

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.

5. **Midterm question 3**
   Re-do midterm question 3.

   Solution will be posted separately

6. **Midterm question 4**
   Re-do midterm question 4.

   Solution will be posted separately

7. **Midterm question 5**
   Re-do midterm question 5.

   Solution will be posted separately

8. **Midterm question 6**
   Re-do midterm question 6.

   Solution will be posted separately

9. **Midterm question 7**
   Re-do midterm question 7.

   Solution will be posted separately

10. **Midterm question 8**
    Re-do midterm question 8.

    Solution will be posted separately

11. **Midterm question 9**
    Re-do midterm question 9.

    Solution will be posted separately

12. **Midterm question 10**
    Re-do midterm question 10.

    Solution will be posted separately

13. **Midterm question 11**
    Re-do midterm question 11.

    Solution will be posted separately

14. **Midterm question 12**
    Re-do midterm question 12.

    Solution will be posted separately

15. **Midterm question 13**
    Re-do midterm question 13.

    Solution will be posted separately

16. **Write your own problem**
    Write your own problem related to this week's material and solve it. You may still work in groups to brainstorm problems, but each student should submit a unique problem. What is the problem? How to formulate it? How to solve it? What is the solution?