AEP 5: The Euclidean algorithm and modular inverses

Overview

In this AEP, you'll learn how to use the Extended Euclidean Algorithm to solve modular equations of the form $ab \% n = 1$ and explore the applications of this idea to cryptography.

Learning Targets associated with this AEP:

- A.3: I can compute `a % b` given integers `a` and `b` and perform arithmetic mod n.

Remember, AEPs do not have fixed deadlines; simply work on this item until you are ready to submit it. But remember the **Two Items Per Week Rule.**

Technology Background

No particular tech skills needed for this AEP.

AEP Description and Tasks

What this AEP is about

In AEP 3, we learned about the **greatest common divisor** of two positive integers and how to use the **Euclidean Algorithm** to find it efficiently. We also learned that we can use the **Extended Eulidean Algorithm** to write the GCD of any two positive integers as a combination of those two integers. In AEP 5, we are going to explore how these ideas can be used to solve certain kinds of equations involving the modulus operator, which then becomes an important tool in breaking certain kinds of codes.

> **This AEP requires that you be familiar with the Euclidean Algorithm and Extended Euclidean Algorithm from AEP 3.** While *completing* AEP 3 is not strictly a requirement for AEP 5, fluency with these two algorithms is.

In your Algebra 1 class back in middle school or high school, you learned how to solve basic equations involving multiplication, like $3x = 1$. It's simple — just divide both sides by 3 to get $x = 1/3$. What if we wanted to extend this idea to equations involving the modulus operator, like this one?

$$3x \% 7 = 1$$

This is significantly harder, because *the value of x must be an integer*. That means we can't "divide by 3"

because doing so would yield a non-integer result:

$$x \% 7 = 1/3$$

But that doesn't make sense because $1/3$ isn't an integer. Instead, we need to find an *integer* x that, when substituted in, yields a true statement. When the modulus is small (like here, where it's 7) we can do this through a brute-force search pretty easily, starting at 1:

Value of x	**Value of** $3x$	**Value of** $3x \% 7$
1	3	3
2	6	6
3	9	2
4	12	5
5	15	1

Having found an integer x such that $3x \% 7 = 1$ — namely $x = 5$ — we can stop because we've solved the equation. There are actually multiple solutions to this equation; $x = 12$ is another ($3 \times 12 = 36$ and $36 \% 7 = 1$), so are $x = 19, 26, 33, \ldots$ — any value of x that is congruent to 5 modulo 7, will work. Because there are infinitely many solutions, we will just refer to the smallest positive solution as "the" solution.

In algebra, we use a -1 exponent to denote a reciprocal, for example $3^{-1} = 1/3$. Note that $3 \times 1/3 = 1$. We will use that negative 1 exponent to mean something similar here: In the situation we just described, we would say that $3^{-1} \% 7 = 5$ since $(3 \times 5) \% 7 = 1$. The number 5 "acts like" the fraction 1/3 when looking at things mod 7.

Another example: $4^{-1} \% 13 = 10$, because look what happens when you multiply 4 times 10:

$$(4 \times 10) \% 13 = 40 \% 13 = 1$$

But notice that for some moduli, the simple equation we started with may be impossible to solve. For example, if we were given the equation $3x \% 6 = 1$ instead, then look what happens:

Value of x	**Value of** $3x$	**Value of** $3x \% 6$
1	3	3
2	6	0
3	9	3
4	12	0
5	15	3

...and so on. The value of $3x \% 6$ will just alternate between 0 and 3, because $3x$ is always either a multiple of 6 (which happens when x is even) or it's 3 plus a multiple of 6 (which happens when x is odd). $3x \% 6$ never evaluates to 1. So $3x \% 6 = 1$ *has no solution*; and we would say $3^{-1} \% 6$ *does not exist*.

Tasks for this AEP

1. Find all of the following values and show your reasoning. If a value doesn't exist, say so (no explanation needed, but make sure you are correct!).

   a) $5^{-1} \% 17$
   b) $13^{-1} \% 22$
   c) $11^{-1} \% 22$
   d) $21^{-1} \% 26$
   e) $4^{-1} \% 26$
   f) $17^{-1} \% 50$
   g) $8^{-1} \% 50$

2. Look at your data from the first question and any additional data you might generate through additional examples, and look at the values of a and n when $a^{-1} \% n$ exists. What is the value of $\gcd(a, n)$ in those situations? Use your observation to fill in the blank with a conjecture:

If a, n are integers, then $a^{-1} \% n$ exists if $\gcd(a, n)$ _____.

Now let's think about how we might find $a^{-1} \% n$ more efficiently than with a brute-force search.

4. Let $a = 92$ and $n = 777$. Use the Euclidean Algorithm to show that $\gcd(a, n) = 1$, and then use the Extended Euclidean Algorithm to find integers x and y such that $92x + 777y = 1$. Be sure to show all your work here.

5. Take the x you found in the previous problem and let $x' = x \% 777$. Show (similarly to how you did this in the first problem) that $x' = 92^{-1} \% 777$.

6. Repeat the idea from tasks 4 and 5 to calculate $1717^{-1} \% 202020$.

7. Based on your previous items, write out an algorithm (in regular English, not in code) on how to calculate $a^{-1} \% n$ for any positive integers a, n. Include conditions under which this number will fail to exist and therefore the algorithm would immediately stop.

8. Finally, we're going to connect this to give a hint to a solution for a problem on *another* AEP. Suppose n, e, and d are positive integers and define $M = \frac{ed-1}{n}$.

   a) Show that $ed + (-M)n = 1$. Make your reasoning clear.
   b) Based on this fact, what can you conclude about the integers e and d? Why?
   c) How might the answer to part (b) give you a way to quickly and efficiently compute d if you were given the values of e and n?

Assignment Expectations and Grading Criteria

> **Note: The wording on these expectations has changed in places. Please read carefully**.

AEPs are graded using the "EMRN" rubric found in the syllabus. Please note, it is the case with all AEP's that **your grade is primarily based on your explanations and writing, and only secondarily on the precision and correctness of your computations.** Correct computations with insufficient explanation will need to be revised and may receive an "N" grade.

Also, **significant incompleteness will result in a grade of "N".** This includes the following:

- **Giving answers with no explanations.** As mentioned above, you are being graded on explanations and writing, not so much on answers. Submissions that contain items where there is an answer with no explanation or insufficient explanation, will be graded "N" and returned without comment.
- Leaving items blank (even accidentally)
- Leaving large gaps in computations (skipping important steps)
- Giving only partial attempts at tasks (for example, working down to a certain point in a solution and then stopping because you need help)

A grade of E or M requires all of the following to be met:

- All work needs to be shown *and* your thought processes clearly expressed in all of the tasks of the assignment. The results also need to be correct.
- All the information needed for an "outsider" to understand your work needs to be self-contained within the work. **The reader should not have to do any work to fill in gaps.**
- Explanations must be given in clearly written and grammatically correct English. Multiple instances of failure to capitalize beginnings of sentences, subject-verb agreement, misuse of punctuation, etc. will result in a grade of R or N.
- Some simple mistakes in calculations are allowed, but significant errors and those that lead to incorrect explanations will probably result in a grade or R or N.

There are some additional formatting requirements in the "Submitting your work" section below.

A grade of "E" is given if all of the above expectations are met, and the work is of superior quality in terms of the clarity of explanations and work, appearance of the writeup, and precision of the mathematics.

Submitting your work

AEP submissions must be typewritten and saved as either a PDF or MS Word file. No part of your submission may involve handwriting; work that is submitted that contains handwriting will be graded N and returned without feedback. This includes electronic handwritten documents, for example using a stylus and a note-taking app. To type up your work, you can use MS Word or Google Docs (both of which have equation editors for mathematical notation) or any other computer-based math typesetting tool. Just make sure you save your work as a Word document or PDF (no `.odt`, `.rtf`, or other file extensions are

allowed).

When you have your work typed up, double-check it for neatness, correctness, and clarity. Then, go to Blackboard, then **Assignments**, then **AEP**, then **AEP 5**. Clicking on the text "AEP 5" will take you to a place on Blackboard where you can upload your work. All grading and revisions of labs are done entirely on Blackboard. **Do not email your work to the professor** – only Blackboard submissions are accepted.

Getting Help

Please note that according to the syllabus, for AEP's **"no interactions at all with another person or with unauthorized sources on the internet is allowed."** Violations of this rule include *any* consultation with other students or former students, including Math Center tutors; using work from another student or former student; submitting the problem set to an online help site such as Chegg or Coursehero; or asking for help in an online forum. All such violations will be treated as academic dishonesty and will result in a grade of "N" and being banned from revising the work.

You **may** ask me (Talbert) for help on this assignment in the form of **specific mathematical or technical questions**. If I cannot answer a question because it would give too much away, I'll tell you so. **However please note: I will not "look over your work" before you submit it to give you feedback on the overall submission**; the expectations are clearly laid out above, so just follow those directions and submit your best work, and you'll be allowed to revise it if needed.

You can ask technology related questions to anyone at any time. For example if you need help with Desmos, or with figuring out how to type up your work, there are no restrictions on that. I recommend the `#tech` channel on Campuswire so that you'll reach a large audience.