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.

(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.)

(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.

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 $b \equiv 0 \bmod d$.

(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).

(c) Solve for x: $77x \equiv 35 \bmod 42$.

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.

(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 1. 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.)*

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

(d) 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.

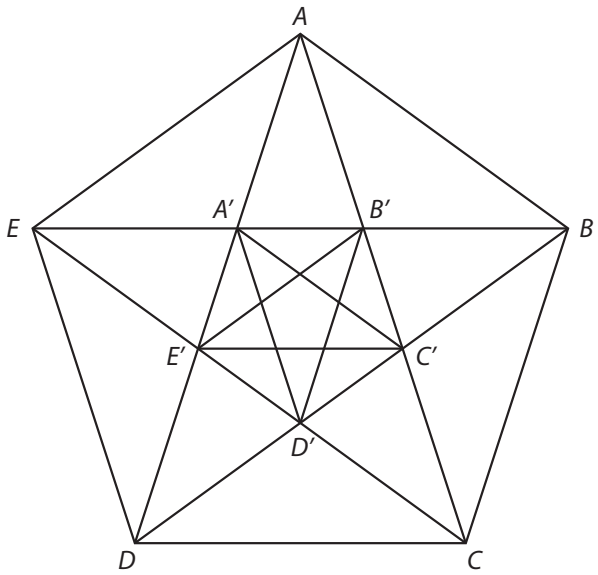

Figure 1: Regular pentagon

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

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

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

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

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

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

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

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

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

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

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

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

15. Midterm question 13

Re-do midterm question 13.

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?