Homework 1

Due Tuesday, September 7

In this assignment you will implement some of the important algorithms we discussed in class, and test them out on some big numbers. You will also have your first written homework, where you will fill in the proofs of results discussed in class.

Implementation Part

1. Let's begin with finding the greatest common divisors of two numbers the slow way. This will also serve as a programming warmup. You can use the functions later in the list to call earlier ones; Jupyter notebooks allow you to call functions from previous cells as long as that cell has been run.

   (a) Write a function `divides(a,b)` which takes as input two integers $a, b \in \mathbb{Z}$ and returns `true` if $a|b$ and `false` otherwise.

   (b) Write a function `getDivisors(a)` which takes as input an integer $a \in \mathbb{Z}$ and returns a complete list `[d1,d2,...]` of positive divisors of a. (You can do this in a steps, but if you're clever you can do this in $\sqrt{a}$ steps).

   (c) Write a function `getCommonDivisors(a,b)` which takes as input two integers $a, b \in \mathbb{Z}$ and returns a complete list of their common divisors.

   (d) Write a function `findGCDSlow(a,b)` which takes as input two integer integers $a, b \in \mathbb{Z}$ and returns their greatest common divisor, using the function `getCommonDivisors(a,b)` from part (c).

2. To find the greatest common divisor the fast way, we will need the Euclidean Algorithm. This is done by iterating long division.

   (a) Write a function `divisionWithRemainder(a,b)` which does long division of a by b. In particular, it will return a list `[q,r]` where $q, r \in \mathbb{Z}$ and $a = bq + r$ for $0 \leq r < b$. (You prove in the written part that q and r are unique. Hint: the modulus operator `%` may be helpful here).

   (b) Write a function `findGCDFast(a,b)` which implements the Euclidean Algorithm to return the greatest common divisor of two integers $a, b \in \mathbb{Z}$. *Make sure it runs both if $a \leq b$ and $a \geq b$!* (We described this algorithm in detail in the 9/1 lecture, and it is also described in Theorem 1.7 in the [HPS]).

3. Given $a, b \in \mathbb{Z}$, the Euclidean algorithm not only gave an efficient way to compute $\gcd(a, b)$, it also provided a way to find the greatest commond divisor as an integer linear combination of a and b. That is, to find $u, v \in \mathbb{Z}$ such that $\gcd(a, b) = au + bv$.

   Write a function `extendedGCD(a,b)` which returns a list `[g,u,v]` where $g = \gcd(a, b)$ and $u, v \in \mathbb{Z}$ such that $au + bv = g$. Do this following the method we described in class (and Theorem 1.11 in [HPS]). (**Hint:** One could do this without storing divisions with remainder by adjusting `findGCDFast(a,b)` to add a step in each division computing the remainder in terms of a and b. This would only require you to remember the 2 previous remainders at every given time, and would only involve minor adjustments to 2(b). If you get stuck a complete outline is given in [HPS Exercise 1.12]).

4. Test out `findGCDSlow`,`findGCDFast`, and `extendedGCD` on the following pairs (a, b) and check they all agree. (**Note:** `findGCDSlow` may stop working once the numbers get big, if you need to cancel it that's fine).

   (a) $(527, 1258)$

   (b) $(1056, 228)$

   (c) $(163961, 167181)$

   (d) $(3892394, 239847)$

   (e) $(32715482947251, 649917361940562)$

   (f) $(579936928948733343289619283592157 76, 375993729939672871359928438912)$

Written Part

5. Let $a, b, c \in \mathbb{Z}$.

   (a) Suppose $a|b$ and $b|c$. Prove $a|c$

   (b) Suppose $a|b$ and $b|a$. Prove $a = \pm b$.

   (c) Suppose $a|b$ and $a|c$. Prove $a|(b + c)$ and $a|(b - c)$.

6. In this exercise we prove the existence and uniqueness of division with remainder. Let $a, b \in \mathbb{Z}$, and suppose that $b \neq 0$. We start with existence.

   (a) We begin by considering the set of numbers $a - bq$ as q varies over the integers. Prove that the set
   $$S = \{a - bq : q \in \mathbb{Z}\},$$
   has at least one nonnegative element.

   (b) Let r be the minimal nonnegative element of S. Show that $0 \leq r < |b|$.

   (c) Use (b) to conclude that $a = bq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$. This proves existence.

   (d) Show that the division with remainder from part (c) is unique. That is, suppose there are $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that
   $$a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2.$$
   Suppose further that $0 \leq r_i < |b|$ for $i = 1, 2$. Then show $q_1 = q_2$ and $r_1 = r_2$.

7. Fix two integers a and b. The extended Euclidean algorithm shows the greatest common divisor of a and b is an integral linear combination of a and b. In this exercise we prove a partial converse to this statement.

   (a) Show that $\gcd(a, b)$ divides $au + bv$ for any $u, v \in \mathbb{Z}$.

   (b) Using part (a), prove that a and b are coprime if and only if there are $u, v \in \mathbb{Z}$ such that $au + bv = 1$. Give an example to show that u and v need not be unique.

   (c) Suppose (u_1, v_1) and (u_2, v_2) are two solutions to $au + bv = 1$. Show that a divides $v_2 - v_1$ and that b divides $u_2 - u_1$. Even stronger, show that there is in fact some $k \in \mathbb{Z}$ so that $v_2 = v_1 - ka$ and $u_2 = u_1 + kb$ (for the same k).

8. In this exercise we prove the algebraic consistency of modular arithmetic. Let m be a positive integer, and fix integers a, a', b, b' satisfying

$$\begin{aligned} a &\equiv a' \mod m \\ b &\equiv b' \mod m. \end{aligned}$$

Prove that the following congruences hold.

(a) $a + b \equiv a' + b' \mod m$.

(b) $a - b \equiv a' - b' \mod m$.

(c) $ab \equiv a'b' \mod m$.

9. Let's get a little practice with modular algebra. You're welcome to make use of a Jupyter notebook to help you in these calculations.

(a) What is 4^{-1} modulo 15?

(b) Solve $4x = 11 \mod 15$ for x. Give a value of x that lives in $\mathbb{Z}/15\mathbb{Z}$.

(c) What is 35^{-1} modulo 573?

(d) Solve $35x + 112 = 375 \mod 573$ for x. Give a value of x that lives in $\mathbb{Z}/573\mathbb{Z}$.