4400-001 - SPRING 2022 - WEEK 2 (1/18, 1/20)
CHAPTER 1 – THE EUCLIDEAN ALGORITHM

Most of these exercises can be found in Savin - Chapter 1, but have been reorganized below.

Exercise 1 (Required). Euclidean algorithm and continued fractions – computations.

(1) Use the Euclidean algorithm to find the greatest common divisor of:
   (a) 1084 and 412
   (b) 1979 and 531
   (c) 305 and 185
(2) Use the calculations from part (1) to express the following in continued fraction form:
   (a) 1084/412
   (b) 1979/531
   (c) 305/185.
(3) Find all integer solutions of
   (a) $305x + 185y = \gcd(305, 185)$
   (b) $1979x + 531y = \gcd(1979, 531)$
   (c) $15750x + 9150 = \gcd(15750, 9150)$
   (d) $427x + 259y = 13$

Exercise 2 (Required). Continued fractions and rationality

(1) Use the continued fraction algorithm to show $\sqrt{3}$ is not rational. To how many decimal digits does the fourth convergent approximate $\sqrt{3}$?
(2) Use the continued fraction algorithm to show $\sqrt{7}$ is not rational. To how many decimal digits does the fourth convergent approximate $\sqrt{7}$?
(3) Find a number α whose continued fraction expansion is

$$\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}$$

Exercise 3 (Recommended). Some basic divisibility results.

(1) If a, b, c are integers such that $a|b$ and $b|c$, show that $a|c$.
(2) If a, b, c are integers such that $a|b$ and $a|c$, show that $a|(b + c)$.
(3) Let a and b be two integers. Use the fundamental theorem of arithmetic to show that any common divisor of a and b divides $\gcd(a, b)$.
(4) Let a and b be two relatively prime integers (that means $\gcd(a, b) = 1$). Use the fundamental theorem of arithmetic to show that if $a|c$ and $b|c$ then $ab|c$.
(5) Show that $\gcd(ad, bd) = \gcd(a, b)d$.
(6) Let a and b be two positive integers such that $a+b$ is a prime number. Show that $\gcd(a, b) = 1$.

Exercise 4. Least/lowest common multiples. Let a and b be two positive integers. The least/lowest common multiple of a, denoted by $\mathrm{lcm}(a,b)$, is the smallest positive integer m such that both $a|m$ and $b|m$ (this exists by the well-ordering principle; why is the set of all such m non-empty?).

(1) Show that $\mathrm{lcm}(a,b)$ divides any common multiple of a and b. *Hint: if m is a common multiple, use division to write $m = q \cdot \mathrm{lcm}(a,b) + r$ with $0 \le r < \mathrm{lcm}(a,b)$.*
(2) Show that $ab = \gcd(a,b)\mathrm{lcm}(a,b)$. *Hint: do the case $\gcd(a,b) = 1$ first.*
(3) Use the Euclidean algorithm and the formula of (2) to find
   (a) $\mathrm{lcm}(13853, 6951)$
   (b) $\mathrm{lcm}(15750, 9150)$.

Exercise 5. Factoring products of nearby primes. Factorizing numbers in general is hard. But sometimes it's easy, if you know a bit about the shape of the factorization! This is important in cryptography, where security of some algorithms depends on the difficulty of factorization. The following method can break RSA, a cryptosystem we'll learn about later in class, if you aren't careful.

(1) Suppose p and q are odd primes such that $q = p+2$ (such pairs are called *twin primes*[1]). Show that, if $n = pq$, then $n + 1 = (p+1)^2$; in particular, $n+1$ is a square.
(2) 19043 is a product of two primes that differ by two. Use (1) to factor 19043.
(3) More generally, suppose $n = pq$ for any two primes p, q. Show that
$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$
In particular, $n + \left(\frac{p-q}{2}\right)^2$ is square and its square root is $\frac{p+q}{2}$.
(4) The following numbers are products of two nearby primes. Use (3) to factor them (*hint: run through small values of $p-q$ and check whether $n + \left(\frac{p-q}{2}\right)^2$ is a square*).
   (a) 826277
   (b) 3992003
   (c) 1340939

Exercise 6. Fibonacci numbers and the efficiency of the Euclidean algorithm. The Fibonacci numbers are defined by $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \ge 2$.

(1) There is a simple closed formula for f_n in term of the golden ratio $\frac{1+\sqrt{5}}{2}$ and its partner in quadratic crime $\frac{1-\sqrt{5}}{2}$, which we derive now using linear algebra:
   (a) Find a 2×2 matrix A such that for all $n \ge 2$,
$$A\begin{bmatrix} f_{n-1} \\ f_{n-2} \end{bmatrix} = \begin{bmatrix} f_n \\ f_{n-1} \end{bmatrix}$$
   (b) Deduce that
$$A^{n-1}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} f_n \\ f_{n-1} \end{bmatrix}$$
   (c) Find a closed formula for f_n from (b) by diagonalizing the matrix A (i.e. find a basis for $\mathbb{R}^2$ consisting of eigenvectors of A and then express the formula of (b) using this basis).
(2) Read Chapter 1 - Section 4 of Savin (starting on the bottom of p.16); compare part (1) to exercise 1) in that section, and then do exercises 2) and 3) in that section.

[1] A longstanding open problem in number theory, the twin prime conjecture, asks whether there are infinitely many twin primes. In 2013, Yitang Zhang showed that there are infinitely many pairs of primes of the form $p, p+k$ for some value of $k < 70,000,000$, and this was later improved to $k < 246$ by a large online collaboration of mathematicians.