CS 487/687 / CM 730: Assignment #1 Due: Wed Feb 1, 2023 at 11:59pm

Submission Instructions: Submit your solutions for each question to Crowdmark before the due date and time. Questions 1.(b), 3.(a), 3.(d) require some Maple coding. Your solution to these question parts should be in the form of two **plain text** files comprised of Maple commands. The files should be named `LastnameA1Q1.mpl` and `LastnameA1Q3.mpl`. (One file per question, not one file per question part.) Your submission to Crowdmark for the questions that involve Maple coding should include the result of executing the Maple commands, i.e., the plain text file `fileout` produced by running

```
maple < LastnameInput.mpl > fileout
```

Also email the files `LastnameA1Q1.mpl` and `LastnameA1Q3.mpl` to the course account by the due date and time.

1. (Continued fractions) Let K be a field, and $f_1, \ldots, f_\ell \in \mathsf{K}$. Then

$$f_1 + \cfrac{1}{f_2 + \cfrac{1}{\cdots \cfrac{}{f_{\ell-1} + \cfrac{1}{f_\ell}}}}$$

is the *continued fraction*, denoted by $C(f_1, \ldots, f_\ell)$. Now assume R is a Euclidean Domain and K its field of fractions. For $(r_0, r_1) \in \mathsf{R}^2$, let $q_i \in \mathsf{R}$, for $1 \le i \le \ell$, be the quotients in the extended Euclidean algorithm.

   (a) Show that
$$\frac{r_0}{r_1} = C(q_1, \ldots, q_l).$$

   (b) A convenient way to represent the continued fraction expansion is as a list $[q_1, q_2, \ldots, q_l]$. Write a Maple procedure to compute the continued fraction expansion of two polynomials in $\mathbb{Q}[x]$. Run your algorithm on $r_0 = x^{20}$ and $r_1 = x^{19} + 2x^{18} + x \in \mathbb{Q}[x]$.

2. Suppose you are given as input a polynomial $f \in \mathsf{R}[y]$ of degree n, together with a matrix $A \in \mathsf{R}[x]^{n \times n}$ filled with polynomials bounded in degree by $d > 0$.

   (a) Assuming the naive cost model, derive the cost of computing $f(A)$ using Horner's scheme. *Note:* You are counting ring operations from R, and your cost estimates should be in terms of the input parameters n and d.

   (b) Assuming the naive cost model, derive the cost of computing $f(A)$ using the baby-steps/giant-steps approach of Patterson and Stockmeyer.

   (c) Now assume Karatsuba is used for the polynomial multiplication, and derive the cost of computing $f(A)$ using the baby-steps/giant-steps approach.

3. (Binary GCD Algorithm) Consider the following recipe to compute the GCD of two positive integers.

   Algorithm:

   ```
   Input: $a, b \in \mathbb{Z}_{>0}$
   Output: $\gcd(a,b) \in \mathbb{Z}_{>0}$
   1. if $a = b$ then return $a$;
   2. if both $a$ and $b$ are even then return $2\ \gcd(a/2, b/2)$;
   3. if exactly one number is even, say $a$, then return $\gcd(a/2, b)$;
   4. if both $a$ and $b$ are odd, with, say $a > b$, then return $\gcd((a-b)/2, b)$;
   ```

   (a) Implement the above algorithm in Maple (call it `binarygcd`) and demonstrate it on the pairs $(34,21)$, $(136,51)$, $(481,325)$, $(8771,3206)$.

   (b) Prove the algorithm works correctly. Use induction (you figure out what to base the induction on).

   (c) Find a good upper bound on the recursion depth, and use this to prove a running time of $O(\ell^2)$ bit operations on inputs of size l (that is, $\lg a, \lg b \leq \ell$).

   (d) Modify the algorithm so that it additionally computes $s, t \in \mathbb{Z}$ such that $sa + tb = \gcd(a,b)$. Give your answer in the form of a Maple function called `ebinarygcd` and test it on the pairs from part (a).

4. Let R be a ring (commutative, with 1) and $f, g \in \mathsf{R}[x,y]$ (polynomials in the two variables x and y). Assume that f and g have degrees less than m in y and n in x. Let $h = f \cdot g$ be the product of f and g.

   (a) Viewing f and g as polynomials in x with coefficients from $\mathsf{R}[y]$, bound the cost of operations in R to compute h assuming the classical school method for univariate polynomial multiplication.

   (b) Now bound the number of operations from R to compute h when Karatsuba's algorithm is used.