1. Recall the extension of Euclid's algorithm that we discussed in class.

```
1  def extended_Euclid(a,b):
2      """
3      a, b are non-negative integers
4      The function returns (u, v, d) such that d = gcd(a,b)
5      and d = ua + vb
6      """
7
8      if b == 0: return (1, 0, a)
9      (u, v, d) = extended_Euclid(b, a % b)
10     return (v, u - v * (a//b), d)
```

We argued in class that the algorithm correctly returns (u, v, d) as stated in the comment in the beginning of the code. Suppose for a certain input (a, b), where $a > b \geq 1$, the call to extended_Euclid(a, b) executes line 9 a total of t times (where $t \geq 1$). Let the value of (a, b) in the i-th call to extended_Euclid(a, b) be (a_i, b_i); let $(a_0, b_0) = (a, b)$. Let the value (u, v) returned by the i-th call be (u_i, v_i), so that $u_i a_i + v_i b_i = d$; thus $(u_t, v_t) = (1, 0)$. Then, for $i = 1, 2, \ldots, t$, we have

$$\begin{bmatrix} a_{i-1} \\ b_{i-1} \end{bmatrix} = \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_i \\ b_i \end{bmatrix};$$

$$\begin{bmatrix} u_{i-1} & v_{i-1} \end{bmatrix} = \begin{bmatrix} u_i & v_i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix},$$

where q_i is the quotient obtained on dividing a_{i-1} by b_{i-1}.

(a) Show that $|u_i| \leq b_i/d$ and $|v_i| \leq a_i/d$, where $d = \mathsf{gcd}(a, b)$. You may use induction to show that the claim holds for $i - 1$ assuming it holds for i; what is the base case?

(b) Suppose a and b are n-bit integers. Show that the total number of bit operations needed for extended_Euclid(a, b) is $O(n^3)$, assuming that integer division of ℓ-bit integers can be done in using $O(\ell^2)$ bit operations.

2. Consider the following modification to Euclid's algorithm.

```
def modified_Euclid(a,b):
    """
    a, b are non-negative integers
    The function returns (u, v, d) such that d = gcd(a,b)
    and d = ua + vb
    """

    if b == 0: return a
    r = a % b
    if r < b/2:
        return modified_Euclid(b, r)
    else:
        return modified_Euclid(b, b-r)
```

(a) Argue that for integers $a > b > 0$, modified_Euclid(a, b) returns the gcd of a and b.

(b) How many times is modified_Euclid called recursively after modified_Euclid(a, b) is called with Fibonacci numbers $a = F_{t+1}$ and $b = F_t$?

3. Describe an algorithm to determine if a given positive number $N \geq 2$ can be written in the form $N = Q^E$, where Q and E are both integers at least 2. For n-bit numbers N, your algorithm should run in time $O(n^k)$ for some small constant k (fixed independent of n).

4. Suppose x, y and ℓ are n-bit numbers, such that $x > y$. Suppose the binary expansion of the fraction x/y is

$$0.b_0b_1b_2b_3\ldots = \sum_{i\geq 1} b_i 2^{-i},$$

which in general may not terminate. Describe an algorithm to determine b_ℓ, given x, y and ℓ. Your algorithm should run in time $O(n^k)$ for some small constant k (fixed independent of n).

(Due 30 Aug 2023)