

1.2 Problems NS-2

Topic of this homework:

Prime numbers, greatest common divisors, the continued fraction algorithm

Prime numbers

Problem # 1: *Every integer may be written as a product of primes.*

– 1.1: *Write the numbers 1,000,000, 1,000,004, and 999,999 in the form $N = \prod_k \pi_k^{\beta_k}$.*

Hint: Use Matlab/Octave to find the prime factors.

Ans:

– 1.2: *Give a generalized formula for the natural logarithm of a number $\ln(N)$ in terms of its primes π_k and their multiplicities β_k . Express your answer as a sum of terms.*

Ans:

Problem # 2: *Using the computer*

– 2.1: *Explain why the following brief Matlab/Octave program returns the prime numbers π_k between 1 and 100.*

```
n=2:100;  
k = isprime(n);  
n(k)
```

Ans:

– 2.2: How many primes are there between 2 and $N = 100$?

Ans:

Problem # 3: Prime numbers may be identified using a sieve (see Fig. ??).

– 3.1: By hand, complete the sieve of Eratosthenes for $n = 1, \dots, 49$. Circle each prime p , then cross out each number that is a multiple of p .

Ans:

– 3.2: What is the largest number you need to consider before only primes remain?

Ans:

– 3.3: Generalize: For $n = 1, \dots, N$, what is the largest number you need to consider before only the primes remain?

Ans:

– 3.4: Write each of these numbers as a product of primes: 22, 30, 34, 43, 44, 48, 49. **Ans:**

– 3.5: Find the largest prime $\pi_k \leq 100$. Do not use Matlab/Octave other than to check your answer. Hint: Write the numbers starting with 100 and count backward: 100, 99, 98, 97, Cross off the even numbers, leaving 99, 97, 95, Pull out a factor (only one is necessary to show that it is not prime).

Ans:

– 3.6: Find the largest prime $\pi_k \leq 1000$. Do not use Matlab/Octave other than to check your answer.

Ans:

– 3.7: Explain why $\pi_k^{-s} = e^{-s \ln \pi_k}$.

Ans:

Greatest common divisors

Consider using the Euclidean algorithm to find the greatest common divisor (GCD; the largest common prime factor) of two numbers. Note that this algorithm may be performed using one of two methods:

Method	Division	Subtraction
On each iteration...	$a_{i+1} = b_i$ $b_{i+1} = a_i - b_i \cdot \text{floor}(a_i/b_i)$	$a_{i+1} = \max(a_i, b_i) - \min(a_i, b_i)$ $b_{i+1} = \min(a_i, b_i)$
Terminates when...	$b = 0$ (GCD = a)	$b = 0$ (GCD = a)

The division method (Eq. 2.1, Sec. 2.1.2, Ch. 2) is preferred because the subtraction method is much slower.

Problem # 4: Understanding the Euclidean algorithm (GCD)

– 4.1: Use the Octave/Matlab command `factor` to find the prime factors of $a = 85$ and $b = 15$.

Ans:

– 4.2: What is the greatest common prime factor of $a = 85$ and $b = 15$?

Ans:

– 4.3: By hand, perform the Euclidean algorithm for $a = 85$ and $b = 15$.

Ans:

– 4.4: By hand, perform the Euclidean algorithm for $a = 75$ and $b = 25$. Is the result a prime number?

Ans:

– 4.5: Consider the first step of the GCD division algorithm when $a < b$ (e.g., $a = 25$ and $b = 75$). What happens to a and b in the first step? Does it matter if you begin the algorithm with $a < b$ rather than $b < a$?

Ans:

– 4.6: Describe in your own words how the GCD algorithm works. Try the algorithm using numbers that have already been divided into factors (e.g., $a = 5 \cdot 3$ and $b = 7 \cdot 3$).

Ans:

– 4.7: Find the GCD of $2 \cdot \pi_{25}$ and $3 \cdot \pi_{25}$.

Ans: .

Problem # 5: Coprimes

– 5.1: Define the term coprime.

Ans:

– 5.2: How can the Euclidean algorithm be used to identify coprimes?

Ans:

– 5.3: Give at least one application of the Euclidean algorithm.

Ans:

– 5.4: Write a Matlab function, function $x = \text{my_gcd}(a, b)$, that uses the Euclidean algorithm to find the GCD of any two inputs a and b . Test your function on the (a, b) combinations from the previous problem. Include a printout (or hand-write) your algorithm to turn in.

Hints and advice:

- Don't give your variables the same names as Matlab functions! Since `gcd` is an existing Matlab/Octave function, if you use it as a variable or function name, you won't be able to use `gcd` to check your `gcd()` function. Try `clear all` to recover from this problem.
- Try using a “while” loop for this exercise (see Matlab documentation for help).
- You may need to use some temporary variables for a and b in order to perform the algorithm.

Ans:

Algebraic generalization of the GCD (Euclidean) algorithm

Problem # 6: In this problem we are looking for integer solutions $(m, n) \in \mathbb{Z}$ to the equations $ma + nb = \gcd(a, b)$ and $ma + nb = 0$ given positive integers $(a, b) \in \mathbb{Z}^+$.

Note that this requires that either m or n be negative. These solutions may be found using the Euclidean algorithm only if (a, b) are coprime ($a \perp b$). Note that integer (whole number) polynomial relations such as these are known as *Diophantine equations*. Such equations (e.g., $ma + nb = 0$) are linear Diophantine equations, possibly the simplest form of such relations.

Example: $\gcd(2, 3) = 1$: For $(a, b) = (2, 3)$, the result is

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \underbrace{\begin{bmatrix} -1 & 1 \\ 3 & -2 \end{bmatrix}}_{\substack{m \\ n}} \begin{bmatrix} 2 \\ 3 \end{bmatrix}.$$

Thus from the above equation we find the solution (m, n) to the integer equation

$$2m + 3n = \gcd(2, 3) = 1;$$

namely, $(m, n) = (-1, 1)$ (i.e., $-2 + 3 = 1$). There is also a second solution $(3, -2)$ (i.e., $3 \cdot 2 - 2 \cdot 3 = 0$) that represents the terminating condition. Thus these two solutions are a pair and the solution exists only if (a, b) are coprime ($a \perp b$).

Subtraction method: This method is more complicated than the division algorithm because at each stage we must check whether $a < b$. Define

$$\begin{bmatrix} a_0 \\ b_0 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where Q sets $a_{i+1} = a_i - b_i$ and $b_{i+1} = b_i$ assuming $a_i > b_i$, and S is a swap matrix that swaps a_i and b_i if $a_i < b_i$. Using these matrices, we implement the algorithm by assigning

$$\begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} = Q \begin{bmatrix} a_i \\ b_i \end{bmatrix} \text{ for } a_i > b_i, \quad \begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} = QS \begin{bmatrix} a_i \\ b_i \end{bmatrix} \text{ for } a_i < b_i.$$

The result of this method is a cascade of Q and S matrices. For $(a, b) = (2, 3)$, the result is

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}}_Q \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_S \underbrace{\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}}_Q \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_S \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \underbrace{\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}}_{\substack{m \\ n}} \begin{bmatrix} 2 \\ 3 \end{bmatrix}.$$

Thus we find two solutions (m, n) to the integer equation $2m + 3n = \gcd(2, 3) = 1$.

– 6.1: By inspection, find at least one integer pair (m, n) that satisfies $12m + 15n = 3$.

Ans:

– 6.2: Using matrix methods for the Euclidean algorithm, find integer pairs (m, n) that satisfy $12m + 15n = 3$ and $12m + 15n = 0$. Show your work!!!

Ans:

– 6.3: Does the equation $12m + 15n = 1$ have integer solutions for n and m ? Why or why not?

Ans:

Problem # 7: Matrix approach:

It can be difficult to keep track of the a 's and b 's when the algorithm has many steps. We need an alternative way to run the Euclidean algorithm using matrix algebra. Matrix methods provide a more transparent approach to the operations on (a, b) . Thus the Euclidean algorithm can be classified in terms of standard matrix operations. Write out the indirect matrix approach discussed at the end of Sec. ?? (Eq. ??).

Ans:

Continued fractions

Problem # 8: Here we explore the continued fraction algorithm (CFA), discussed in Sec. ??.

In its simplest form, the CFA starts with a real number, which we denote as $\alpha \in \mathbb{R}$. Let us work with an irrational real number, $\pi \in \mathbb{I}$, as an example because its CFA representation will be infinitely long. We can represent the CFA coefficients α as a vector of integers $n_k, k = 1, 2, \dots, \infty$:

$$\begin{aligned}\alpha &= [n_1; n_2, n_3, n_4, \dots] \\ &= n_1 + \frac{1}{n_2 + \frac{1}{n_3 + \frac{1}{n_4 + \dots}}}\end{aligned}$$

As discussed in Sec. ?? (p. ??), the CFA is recursive, with three steps per iteration. For $\alpha_1 = \pi, n_1 = 3, r_1 = \pi - 3$, and $\alpha_2 \equiv 1/r_1$.

$$\begin{aligned}\alpha_2 &= 1/0.1416 = 7.0625 \dots \\ \alpha_1 &= n_1 + \frac{1}{\alpha_2} = n_1 + \frac{1}{n_2 + \frac{1}{\alpha_3}} = \dots\end{aligned}$$

In terms of a Matlab/Octave script,

```

alpha0 = pi;
K=10;
n=zeros(1,K); alpha=zeros(1,K);
alpha(1)=alpha0;

for k=2:K %k=1 to K
n(k)=round(alpha(k-1));
%n(k)=fix(alpha(k-1));
alpha(k)= 1/(alpha(k-1)-n(k));
%disp([fix(k), round(n(k)), alpha(k)]); pause(1)
end
disp([n; alpha]);
%Now compare this to matlab's rat() function
rat(alpha0,1e-20)

```

– 8.1: *By hand (you may use Matlab/Octave as a calculator), find the first three values of n_k for $\alpha = e^\pi$.*

Ans:

– 8.2: *For the preceding question, what is the error (remainder) when you truncate the continued fraction after n_1, \dots, n_3 ? Give the absolute value of the error and the percentage error relative to the original α .*

Ans:

– 8.3: *Use the Matlab/Octave program provided to find the first 10 values of n_k for $\alpha = e^\pi$, and verify your result using the Matlab/Octave command `rat()`.*

Ans:

– 8.4: *Discuss the similarities and differences between the Euclidean algorithm and the CFA.*

Ans:

– 8.5: *Extra Credit: Show that the CFA is the inverse operation of the GCD (i.e., the CFA is the GCD run in reverse). (Hint: see Sec. ??.)*

Ans:

Continued fraction algorithm (CFA) (8 pts)

Problem # 9: CFA of ratios of large primes

– 9.1: *Starting from the primes below 10^6 , form the CFA of π_j/π_k with $j = 78498$ and $k < j$.*

Ans:

– 9.2: *Look at other ratios of prime numbers and look for a pattern in the CFA of the ratios of large primes. What is the most obvious conclusion? **Ans:***

– 9.3: *(4pts) Expand $23/7$ as a continued fraction. Express your answer in bracket notation (e.g., $\pi = [3., 7, 16, \dots]$). Show your work. **Ans:***

– 9.4: *(2pts) Can $\sqrt{2}$ be represented as a finite continued fraction? Why or why not? **Ans:***

– 9.5: (2pts) What is the CFA for $\sqrt{2} - 1$?

Hint: $\sqrt{2} + 1 = \frac{1}{\sqrt{2} - 1} = [2; 2, 2, 2, \dots].$

Ans:

– 9.6: Find the CFA for $1 + \sqrt{3}$

Ans:

– 9.7: Show that

$$\frac{1}{1 - \sqrt{a}} = a^{\frac{11}{2}} + a^{\frac{9}{2}} + a^{\frac{7}{2}} + a^{\frac{5}{2}} + a^{\frac{3}{2}} + \sqrt{a} + a^5 + a^4 + a^3 + a^2 + a + 1 = 1 - a^6$$

syms a,b

b= taylor(1/(1-sqrt(a)))

simplify((1-sqrt(a))*b) = 1-a^6

Use symbolic analysis to show this, then explain. **Ans:**