Problem 1

Let $H = \{1, 5, 9, 13, \dots\}$ be the set of all positive integers in the form $4k + 1$.

a. Show that the set H is closed under multiplication.

b. List all numbers in H that are less than 150 and *not* Hilbert primes.

c. Show that every number in H has a factorization into Hilbert primes.

d. Show that H does **not** have (a) unique factorization by finding two different factorization(s) of 693 into Hilbert primes.

e. What is the smallest number in H with two different factorizations into Hilbert primes?

a. Let $a, b \in H$. Then $a = 4k + 1$ and $b = 4j + 1$ for some $k, l \in \mathbb{Z}$.

$$a \cdot b$$

$$\begin{aligned} &= (4k + 1)(4j + 1) \\ &= 16kj + 4k + 4j + 1 \\ &= 4(4kj + k + j) + 1 \end{aligned}$$

This is the form of a Hilbert number, thus H is closed under multiplication.

b. Hilbert primes < 150 are $1, 5, 13, \dots, 149$ or $H_0, H_1, H_2, \dots H_{37}$. Since they are not primes, each H_i is in the form $(4k+1)(4j+1)$ for some $k, j \in \mathbb{Z}$ such that $4k+1 > 1$ and $4j+1 < H_i$. Let $k \le j$. We can iterate through all possibilities of k and j to find non primes < 150. Doing so, we get 9 such numbers: $25, 45, 65, 81, 85, 105, 117, 125, 145$.

c. We will use strong induction.
Base Case: $H_0 = 1$. Since 1 is a Hilbert prime, it factors into itself. Thus, the base case is true.
Inductive Hypothesis: Assume that H_k has a factorization into Hilbert primes for all n and some k such that $0 \le n < k$. There are two cases for H_{k+1}: either it is a Hilbert prime or it is not.
Case 1: If H_{k+1} is a Hilbert prime. Then $H_{k+1} = H_0 \cdot H_{k+1}$. Thus, it has a factorization into Hilbert primes.
Case 2: If H_{k+1} is not a Hilbert prime, then $H_{k+1} = H_j \cdot H_i$ for some $j, i \in \mathbb{N}$, such that H_j and H_i are not 1 or H_{k+1}. By the inductive hypothesis, H_j and H_i have factorization into Hilbert primes. Thus, H_{k+1} has a factorization into Hilbert primes.
By strong induction, we have shown that for every $a \in H$, H_a factorizes into Hilbert primes.

d. $693 = 3^2 \cdot 7 \cdot 11$. From this we can see that $693 = H_5 \cdot H_8$ and $693 = H_2 \cdot H_{19}$. When we check, we see that $H_5, H_2, H_8,$ and $H_{19} < 150$ and are not part of the list of non-Hilbert-primes that we found. So, they are Hilbert primes. Thus, 693 has two different factorization into Hilbert primes, meaning that numbers in H do not necessarily have unique factorization.

e. Let there be $k \in \mathbb{N}$ such that H_k has two different factorizations into Hilbert primes. Since we are looking for the smallest k, we can say $H_k = H_a \cdot H_b$ and $H_k = H_c \cdot H_d$ for some $a, b, c, d \in \mathbb{N}$ such that $H_a, H_b, H_c,$ and H_d are Hilbert primes and distinct. Since $H_k = H_k$, $H_a \cdot H_b$ and $H_c \cdot H_d$ must have the same prime factorization. For them to be different Hilbert factorizations, we must arrange the factors differently. Obviously, H_a or H_b must be greater than 1 or there can't be two factorizations. Furthermore, at least one of H_a and H_b must be non-prime as it would factor to $H_0 \cdot H_k = H_a \cdot H_b$ - not distinct. We can iterate through all the possibilities, setting 693 as a baseline since we already know that that has two Hilbert prime factorizations.

a	b	H_a	H_b	$H_a \cdot H_b$
1	2	5	9	45
1	6	5	25	125
1	8	5	33	165
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2	12	9	49	441
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
5	5	21	21	441
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

By doing such, we find that smallest number in H with two different factorizations into Hilbert primes is 441.

Problem 2

Consider the polynomial $p(x) = x^7 + 2x^6 + Ax^5 + Bx^3 + Cx^2 - 4x + 1$ with all integer coefficients. Suppose you learn that $A + B + C = 3$. Show that $p(x)$ cannot have rational roots.

By the rational root theorem, all roots r of $p(x)$ must be in the form $\frac{s}{t}$ where $s|a_0$ and $t|a_n$. $a_0 = a_n = 1$. The only integers that divide 1 are 1 and -1. Thus, $\frac{s}{t} = \pm 1$. We are given $A + B + C = 3$. If $p(1)$ or $p(-1)$ are roots, they will equal 1. Let us test both cases.

$$\begin{aligned} p(1) &= 1^7 + 2(1)^6 + A(1)^5 + B(1)^3 + C(1)^2 - 4(1) + 1 \\ &= 1 + 2 + A + B + C - 4 + 1 \\ &= A + B + C \end{aligned}$$

Obviously, $3 \neq 0$, so 1 is not a root.

$$\begin{aligned} p(-1) &= (-1)^7 + 2(-1)^6 + A(-1)^5 + B(-1)^3 + C(-1)^2 - 4(-1) + 1 \\ &= -1 + 2 - A - B + C + 4 + 1 \\ &= -A - B + C + 6 \end{aligned}$$

$$-A - B + C = 6$$

Adding $A + B + C = 3$ and $-A - B + C = 6$ gives $2C = 9 \Rightarrow C = \frac{9}{2}$. However, this is not possible as C is defined as an integer. Thus. -1 is not a root. Therefore, $p(x)$ does not have rational roots.

Problem 3

Compute (412, 600) and find m and n so that $412m + 600n = (412, 600)$.

We will utilize the extended Euclidean algorithm.

q	r	m	n
	600	0	1
1	412	1	0
2	188	-1	1
5	36	3	-2
4	8	-16	11
2	4	67	-46

Thus, $(412, 600) = 4$. $m = 67 - 150t$ and $n = -46 + 103t$ for some $t \in \mathbb{Z}$.

Problem 4

Calculate $(840, 595, 476)$.

We will first compute $(840, 595)$ to some d, then compute $(d, 476)$ to get $(840, 595, 476)$.

q	r
	840
1	595
2	245
2	105
2	35
3	0

Thus, $(840, 595) = 35$. Now, we will compute $(35, 476)$.

q	r
	476
13	35
1	21
1	14
1	7
2	0

Thus, $(35, 476) = 7$. Therefore, $(840, 595, 476) = 7$.

Problem 5

Search (on the web, in books, etc.) for an easy-to-state, easy-to-understand conjecture in number theory that has still not been proven. State the conjecture below.

The Erdős–Straus Conjecture, formulated in 1948, states that for all $n \in \mathbb{N}, n \geq 2$, there exists $x, y, z \in \mathbb{N}$ such that

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

That is, the number $\frac{4}{n}$ can be expressed as the sum of three unit fractions. So far, it has been verified up to $n \leq 10^{17}$. Interestingly, it also seems to work when you allow negative unit fractions.