Some number-theoretic problems

This document gives more detailed discussions of numbers 3, 4, 8, 11 in the original document.

3. A variation on Euclid's proof

Euclid's famous proof of the infinity of primes involves taking the primes "so far" and producing a new one. We formalise this procedure, starting from an arbitrary prime. Any such start gives an infinite sequence of primes.

> Let p_1 be a prime number. For every n, let p_{n+1} be the smallest prime divisor of $p_1 \cdots p_n + 1$.

We always see the prime 2 at the first or second stage: if p_1 is odd, then $p_1 + 1$ is even, and 2 is its smallest prime divisor. What about the prime 3? If p_1 is congruent to 1 (mod 3), then $2p_1 + 1$ is divisible by 3, and so the prime 3 occurs at step 3. Otherwise, the situation is more problematic.

- Is it true that, for every n, there is a prime p_1 for which none of the first n terms of the sequence is equal to 3?
- Is there a prime p_1 for which no term of the sequence is equal to 3?

4. Approximation from below

Let n be a positive integer and a a positive real number. It is easy to show that there is a positive real number b (depending on n and a) with the property that, for any positive integers $x_1, \ldots, x_n$,

$$\text{if } \frac{1}{x_1} + \cdots + \frac{1}{x_n} < a, \text{ then } \frac{1}{x_1} + \cdots + \frac{1}{x_n} \leq a - b.$$

If a is an integer, find an explicit lower bound for b in terms of n and a.

This problem arose in a problem I worked on concerning permutation groups; in the end I found a different approach so this problem remained unsolved.

8. A determinant problem

This problem is due to Robin Chapman. It has been verified for a range of primes by computation, but a general proof is lacking.

Let p be a prime congruent to 3 (mod 4), and let $r = (p+1)/2$. Let $\left(\frac{x}{p}\right)$ denote the *Legendre symbol* (taking the values $+1$, -1, or 0 according as x is congruent to a nonzero square, a non-square, or zero (mod p). Show that the $r \times r$ matrix with (i, j) entry $\left(\frac{j-i}{p}\right)$ has determinant 1.

11. A universal sequence from the primes

A zero-one sequence is called *universal* if every finite zero-one sequence occurs as a (consecutive) subsequence of it. This concept arises in various places. For example, a random zero-one sequence is universal with probability 1; and a sequence is universal if and only if the graph whose vertex set is the integers, two vertices i and j adjacent if and only if the $|j-i|$th term of the sequence is 1, is isomorphic to the famous Erdős–Rényi *random graph*.

Since primes appear to behave "randomly", and there is a construction of the random graph from the primes using congruence mod 4, it is natural to ask the following question.

Let s be the sequence whose nth term is 0 if the nth odd prime is congruent to 1 (mod 4), and to 1 if the nth odd prime is congruent to 3 (mod 4). Is s universal?

It is hoped that recent advances in the study of prime numbers such as the *Green–Tao theorem* may give tools to study this problem.