Some number-theoretic problems

These problems are ones I have collected over the years. Here Z_p denotes the ring of integers modulo p, not the ring of p-adic integers.

1. Find all positive integers greater than two which can be written as the sum of two powers of the same prime in three different ways. (I know of only six such integers, none of which has more than three different representations of this form.)

2. It is known that the average number of ways in which a positive integer in the range $[1, \ldots, n]$ can be written as a sum of *consecutive* primes tends to the limit $\log_e 2$ as $n \to \infty$. Is it true that the limiting distribution of the number of representations of this form is Poisson with parameter $\log_e 2$? (This would imply that the density of the set of numbers with no such representation is $1/2$. It would also imply that there exist integers with arbitrarily many such representations. Either of these assertions would be a nice result!)

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

   - 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. 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 $x_1, \ldots, x_n$,

$$\text{if } \frac{1}{x_1} + \cdots + \frac{1}{x_n} < a, \text{ then } c1x_1 + \cdots + \frac{1}{x_n} \leq a - b.$$

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

5. (Donald Preece) R. D. Carmichael defined a *primitive lambda-root* or PLR of n to be an element of $U(n)$ (the group of units modulo n) whose order is equal to the exponent of $U(n)$. It is possible to count

the number of PLRs of n, for any n. Is it possible to count the number of PLRs x having the property that $x-1$ is a unit? In particular, for which n do all (resp. some, none) of the PLRs have this property? (The number can be counted in principle by inclusion-exclusion, but there is unlikely to be a neat formula.)

6. (Patrick Moss) A sequence $(u(n))$ of non-negative integers is said to be *realizable* if there is a set X and a permutation T of X such that $u(n)$ is the number of fixed points of T^n in X. It can be shown indirectly that, if $(u(n))$ is realizable, then so is the sequence $(u(n)^n)$. Find a pair (X', T') realizing this sequence, in terms of the pair (X, T) realizing the original sequence. (This is not likely to be easy. For example, let p be a prime. The constant sequence with value p is realized by the identity permutation of a set of size p. An obvious realization of the sequence (p^n) is (X, T), where X is the algebraic closure of the field with p elements and T is the Frobenius map $T(x) = x^p$.)

7. The *Stirling transform* of a sequence a is the sequence b given by

$$b(n) = \sum_{k=1}^{n} S(n,k)a(k),$$

where $S(n,k)$ are the Stirling numbers of the second kind. What can be said about the asymptotics of a sequence a for which $b(n) \sim c \cdot a(n)$ for some constant $c > 1$? (Many interesting sequences, for example, chains in the partition lattice, zero-one matrices with n ones and no zero rows or columns have this property.)

8. (Robin Chapman) 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.

9. Do there exist infinitely many non-abelian finite simple groups whose order is a prime plus one? (The context is a theorem of Cauchy which states that a primitive permutation group of degree prime plus one is doubly transitive. Neumann, Sims and Wiegold pointed out in 1968 that this is false: if S is a non-abelian finite simple group, then $S \times S$,

acting on S by left and right multiplication, is primitive but not doubly transitive. The first few finite simple groups have order a prime plus one. So the question asks whether this construction gives infinitely many counterexamples to Cauchy's "theorem". Note that this is a number theory question; no group theory is required apart from the known formulae for the orders of the finite simple groups.)

10. (Donald Preece and PJC) Let p be an odd prime, and k an integer at least 3. A *k-AP decomposition mod p* is an arithmetic progression $(a_1, \ldots, a_k)$ consisting of integers not congruent to 0 or 1 mod p such that the group of units of Z_p is the direct product by the cyclic groups generated by the terms of the progression. There are many examples of 3-AP decompositions, but no 4-AP decompositions are known. Do any exist? (or indeed, do k-AP decompositions exist for $k \geq 4$?) (Note: we assume that each cyclic factor has order greater than 1. Without this assumption, the AP $[3528, 1148, 2381, 1]$ mod 3613 is an example.)

11. A zero-one sequence is called *universal* if every finite zero-one sequence occurs as a (consecutive) subsequence of it. 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?

12. (João Araújo and PJC) Characterise the primes p which have the property that there exists an element c of the multiplicative group of Z_p with the property that $\{c, c-1, -1\}$ generates a proper subgroup of the multiplicative group. (Primes congruent to 1 (mod 4) have this property since -1 is a square and there are two consecutive squares. Also primes congruent to 1 (mod 3) have the property: take c to be a primitive 6th root of unity. There are others: the remaining primes less than 1000 with this property are 131, 191, 239, 251, 311, 419, 431 and 491.)