Stuff $\pmod p$

1. Let $p = 4k + 3$ be a prime number. Find the number of different residues modulo p of $(x^2 + y^2)^2$, where $\gcd(x, p) = \gcd(y, p) = 1$.

2. Let both p and $2p + 1$ be primes. There are a total of $2p + 1$ balls in two boxes, and neither is empty. Each step, one is allowed to move exactly half the balls in one box to the other box. Let k be any positive integer less than $2p + 1$. Prove that there is a stage such that there are exactly k balls in one of the boxes.

3. Let p be an odd prime and let
$$f(x) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) x^{i-1}.$$
   (a) Prove that f is divisible by $x - 1$ but not by $(x - 1)^2$ if and only if $p \equiv 3 \pmod 4$.
   (b) Prove that if $p \equiv 5 \pmod 8$ then f is divisible by $(x - 1)^2$ and not by $(x - 1)^3$.

4. Find all odd primes p such that both of the numbers
$$n_1 = 1 + p + p^2 + \cdots + p^{p-2} + p^{p-1} \qquad \text{and} \qquad n_2 = 1 - p + p^2 - \cdots - p^{p-2} + p^{p-1}$$
are primes.

5. Find all surjective functions $f : \mathbb{N} \to \mathbb{N}$ such that for every $m, n \in \mathbb{N}$ and every prime p, the number $f(m + n)$ is divisible by p if and only if $f(m) + f(n)$ is divisible by p. (Here $\mathbb{N}$ denotes the set of all positive integers.)

6. Let p be a prime such that $p = k \cdot 2^n + 1$, where k is odd, $k > 1$. Suppose that p divides Fermat number $2^{2^m} + 1$ for some integer m with $m \le n - 2$. Prove that $k^{2^{n-1}}$ is congruent to 1 modulo p.

7. Let $\{x_n\}_{n=1}^{\infty}$ be a sequence with $x_1 = 2$, $x_2 = 12$, and $x_{n+2} = 6x_{n+1} - x_n$ for every positive integer n. Let p be an odd prime, and let q be a prime divisor of x_p. Prove that if $q > 3$, then $q \ge 2p - 1$.

8. Let p be a prime, and let k be an integer greater than 2. There are integers $a_1, a_2, \ldots, a_k$ such that p divides neither a_i $(1 \le i \le k)$ nor $a_i - a_j$ $(1 \le i < j \le k)$. Denote by S the set
$$\{n | 1 \le n \le p - 1, (na_1)_p < (na_2)_p) < \cdots < (na_k)_p\},$$
where $(b)_p$ denotes the remainder when b is divided by p. Prove that S contains less than $\frac{2p}{k+1}$ elements.

9. Let $p > 2$ be a prime number, and let $S = \{0, 1, \ldots, p-1\}$. Determine the number of 6-tuples $(x_1, x_2, x_3, x_4, x_5, x_6)$ with $x_i \in S, 1 \leq i \leq 6$, such that

$$x_1^2 + x_2^2 + x_3^3 \equiv x_4^2 + x_5^2 + x_6^2 \pmod{p}.$$

10. Given a finite set P of prime numbers, prove that there exists a positive integer x which is representable in the form $x = a^p + b^p$ (with $a, b \in \mathbb{N}$) for each $p \in P$, but not representable in that form for any $p \notin P$.

11. Let $p > 2$ be a prime and let a, b, c, d be integers not divisile by p, such that

$$\left\{\frac{ra}{p}\right\} + \left\{\frac{rb}{p}\right\} + \left\{\frac{rc}{p}\right\} + \left\{\frac{rd}{p}\right\} = 2$$

for any integer r not divisible by p. Prove that at least two of the numbers $a+b$, $a+c$, $a+d$, $b+c$, $b+d$, $c+d$ are divisible by p. Here, for real numbers x $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of x.

12. Let m be a given positive integer.

    (a) Prove that there exists an integer N_1 such that for every prime p greater than N_1, there are m consecutive positive integers each of which is congruent to the square of an integer modulo p.

    (b) Prove that there exists an integer N_2 such that for every prime p greater than N_2, there are m consecutive positive integers each of which is not congruent to a square of an integer modulo p.

13. Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions with the properties:

    (a) g is surjective;

    (b) $2f(n)^2 = n^2 + g(n)^2$ for all positive integers n;

    (c) $|f(n) - n| \leq 2004\sqrt{n}$ for all n.

    Prove that there are infinitely many $n \in \mathbb{N}$ with $f(n) = n$.

14. Find all positive integers $n > 1$ for which there exists a unique integer a with $0 < a \leq n!$ such that $a^n + 1$ is divisible by $n!$.

15. Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

16. Let f be a polynomial with integer coefficients, and let p be a prime such that $f(0) = 0$, $f(1) = 1$, and $f(k)$ is congruent to either 0 or 1 modulo p for all positive integers k. Show that the degree of f is at least $p - 1$.

17. Find all integer solutions of the equation

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

18. Find all ordered triples of primes (p, q, r) such that

$$p | q^r + 1, \quad q | r^p + 1, \quad r | p^q + 1.$$