Jose Espinosa's Problems in Mathematical Induction

Problems

1. Let p be an odd prime, and let

   $$F(n) = \sum_{k=1}^{p-1} k^{(p-1)n+1} - \frac{n(n-1)}{2} \sum_{k=1}^{p-1} (k^{2p-1} - 3k^2) - \frac{p(p-1)}{2} [(p-1)n+1]$$

   for $n \geq 0$. Prove that $F(n)$ is divisible by p^3 for all $n \geq 0$.

2. Let F_n denote the n^{th} Fibonacci number. Prove that

   $$1 + 2^{2n} + 3^{2n} + 2[(-1)^{F_n} + 1]$$

   is divisible by 7 for all $n \geq 0$.

3. Let F_n denote the n^{th} Fibonacci number. Prove that

   $$2(2^{2n} + 5^{2n} + 6^{2n}) + 3(-1)^{n+1}[(-1)^{F_n} + 1]$$

   is divisible by 13 for all $n \geq 0$.

4. Let p and q be odd primes, such that $p < q$, and $q - 1$ is not divisible by p.

   Let a_1, a_2, $\ldots$, a_m be positive integers such that both $\sum_{i=1}^{m} a_i$ and $\sum_{i=1}^{m} a_i^{kpq}$ are divisible by p^2q^2, for any odd positive integer k. Also, a_i is not divisible by neither p nor q for all i.

   Let

   $$F(n) = \sum_{i=1}^{m} a_i^{(p-1)(q-1)n+1}$$

   for $n \geq 0$. Prove that $F(n)$ is divisible by p^2q^2 for all $n \geq 0$.

5. Let a, b, and c be three positive integers, where $c = a + b$. Let d be an odd factor of $a^2 + b^2 + c^2$. Prove that for all positive integers n:

   (a) $a^{6n-4} + b^{6n-4} + c^{6n-4}$ is divisible by d.

   (b) $a^{6n-2} + b^{6n-2} + c^{6n-2}$ is divisible by d^2.

(c) $a^{2^n} + b^{2^n} + c^{2^n}$ is divisible by d.

(d) $a^{4^n} + b^{4^n} + c^{4^n}$ is divisible by d^2.

6. The function $F(n)$ satisfies $F(1) = 1$, $F(2) = 6$, and $F(n) = F(n-1) + F(n-2)$ for all $n \geq 3$. Prove that for all $n \geq 2$,

   (a) $\sum_{i=1}^{n} F(i)^2 = F(n)F(n+1) - 5$, and

   (b) $F(n)^2 + F(n+1)^2 = F(2n+4) - F(2n-3)$.

7. Let p be a prime of the form $4k+3$. Prove that

$$\sum_{i=1}^{2k+1} i^{2^n}$$

   is divisible by p for all $n \geq 1$.

8. Let p be a prime of the form $4k+1$, where k is odd.

   (a) Consider the quadratic residues modulo p, reduced so that they are between 1 and $p-1$ inclusive. Show that exactly k of these residues are between 1 and $2k$ inclusive.

   (b) Let $a_1, a_2, \ldots, a_k$ be the quadratic residues specified in part (a). Prove that

$$\sum_{i=1}^{k} a_i^{2^n}$$

   is divisible by p for all $n \geq 1$.

9. Prove that for all positive integers n,

$$2^{2n-1} + 4^{2n-1} + 9^{2n-1}$$

   is not a perfect square.

10. Prove that for all positive integers n, $8^{2^n} - 5^{2^n}$ is not a perfect square.

11. Prove that for all integers $n \geq 0$,

$$\begin{aligned} &2(13^{6n+1} + 30^{6n+1} + 100^{6n+1} + 200^{6n+1}) \\ &\quad + 2n(n-2)(13^7 + 30^7 + 100^7 + 200^7) \\ &\quad - n(n-1)(13^{13} + 30^{13} + 100^{13} + 200^{13}) \end{aligned}$$

   is divisible by 7^3.

12. Let f be a function taking the positive integers to the positive integers, and let p be a prime. There exist positive integers c and k such that $f(n+c) - kf(n)$ is divisible by p for all n. Prove that there exists a positive integer b such that $f(n+bc) - f(n)$ is divisible by p for all n.

13. Prove that for all integers $n \geq 0$,

$$1 + 2^{4n+2} + 3^{4n+2} + 4^{4n+2} + 5^{4n+2} + 6^{4n+2}$$

is divisible by 13.

14. Prove that for all integers $n \geq 0$,

$$2(3^{4n+3} + 4^{4n+3}) - 25n^2 + 65n + 68$$

is divisible by 125.

15. Prove that $2^{2^n} + 3^{2^n} + 5^{2^n}$ is divisible by 19 for all positive integers n.

16. Let a be a real number, and let $f(n)$ and $g(n)$ be functions satisfying $f(n) = (a-1)f(n-1) + af(n-2)$ for all $n \geq 3$ and $g(n) = f(n+2) + af(n+1) + (a-1)f(n)$ for all $n \geq 1$. Prove that for all $n \geq 1$,

$$g(n) = (2a-1)a^{n-1}[f(2) + f(1)].$$

17. The function $f(n)$ satisfies $f(1) = f(2) = 1$, and $f(n) = 3[f(n-1) + f(n-2)] + 1$ for all $n \geq 3$. Prove that for all positive integers n, $f(3n) + f(3n+1)$ is divisible by 32.

18. Let p be a prime greater than 5. Prove that for all integers $n \geq 0$,

$$\begin{aligned} &100(2^{(p-1)n+1} - 3^{(p-1)n+1} - 5^{(p-1)n+1} + 6^{(p-1)n+1}) \\ &\quad - n(2^{100(p-1)+1} - 3^{100(p-1)+1} - 5^{100(p-1)+1} + 6^{100(p-1)+1}) \end{aligned}$$

is divisible by p^2.

19. Let p be an odd prime. The function $F(n)$ takes the non-negative integers to the integers, and satisfies $F(n+3) - 3F(n+2) + 3F(n+1) - F(n) \equiv 0 \pmod{p^3}$ for all $n \geq 0$. Prove that for all $n \geq 0$,

$$F(n) \equiv \frac{(n-1)(n-2)}{2} F(0) - n(n-2)F(1) + \frac{n(n-1)}{2} F(2) \pmod{p^3}.$$

20. The function $a(n)$ satisfies $a(1) = a(2) = 1$, and $a(n) = a(n-1) + 2a(n-2) + 1$ for all $n \geq 3$. Prove that for all positive integers n,

$$a(n) = 2^{n-1} - \frac{(-1)^n + 1}{2}.$$

21. Let $n \geq 3$ be a positive integer. Arrange the first n^2 Fibonacci numbers in an $n \times n$ array, spiralling counter-clockwise. For example, for $n = 3$ and $n = 4$, the arrays are:

5	**3**	2
8	1	**1**
13	**21**	34

987	**610**	377	233
5	3	2	144
8	1	1	**89**
13	21	**34**	55

Note that $21 + 1 = 2(8 + 3)$ and $610 + 5 = 5(89 + 34)$. Generalize these results and prove.

22. What happens if we replace Fibonacci numbers by Lucas numbers in the previous problem?

23. Let a and b be positive integers which are relatively prime to each other, and let $p > 3$ be a prime dividing $a^2 + ab + b^2$. Prove that for all integers $n \geq 0$,

$$a^{(p-1)n+4} + b^{(p-1)n+4} + (a+b)^{(p-1)n+4}$$

is divisible by p^2.

24. Let p be a prime of the form $6k + 5$. Prove that

$$\sum_{i=1}^{3k+2} i^{2\cdot 3^n}$$

is divisible by p for all $n \geq 0$.

25. Let F_n denote the n^{th} Fibonacci number. Prove that

$$F_n^2 + F_{n+1}^2 + F_{n+2}^2 + F_{n+3}^2 = 3F_{2n+3}$$

for all $n \geq 0$.

26. Let F_n denote the n^{th} Fibonacci number. Prove that

$$F_{5n+3} + F_{5n+4}^2$$

is divisible by 11 for all $n \geq 0$.

27. Let k be a fixed positive integer and let p be an odd prime, such that $p \geq k$. Let $F(n)$ be a function taking the integers to the integers satisfying

$$\sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} F(n+i) \equiv 0 \pmod{p^k}$$

for all integers n. Prove that if $F(a_0)$, $F(a_1)$, $\ldots$, $F(a_{k-1})$ are all divisible by p^k, where the a_i are all distinct modulo p, then $F(n)$ is divisible by p^k for all n.

28. Let F_n denote the n^{th} Fibonacci number, and for all $n \geq 0$, let $G_n(x)$ be the polynomial $89x^n - F_n x^{11} - F_{n-11}$. Prove that for all $n \geq 0$, $G_n(x)$ is divisible by $x^2 - x - 1$.

29. Let p be a prime of the form $4k+1$. Prove that for all $n \geq 0$,

$$\sum_{i=1}^{2k} i^{4n+2}$$

is divisible by p.

30. Let p be an odd prime. For all integers $n \geq 0$, let

$$F(n) = \sum_{k=1}^{p-1} k^{(p-1)n+1} - \frac{p(p-1)}{2} \cdot [(p-1)n+1],$$

and let $G(n) = 500500F(n) - n(n-1)F(1001)/2$. Prove that $G(n)$ is divisible by p^3 for all $n \geq 0$.

31. Let p be an odd prime, and let 2^k be the greatest power of 2 dividing $p-1$. Let $1 \leq j \leq k$, and let $m = (p-1)/2^j$.

    (a) Show that there exist m values of a, from 1 to $(p-1)/2$ inclusive, such that $a^{2m} \equiv 1 \pmod{p}$.

(b) Let $a_1, a_2, \ldots, a_m$ be the m values in part (a). Show that

$$\sum_{i=1}^{m} a_i^{2n}$$

is divisible by p for all $n \geq 0$, except when n is divisible by m.

32. Prove or disprove the following: Under the assumptions of problem 23, let

$$f(n) = a^{(p-1)n+4} + b^{(p-1)n+4} + (a+b)^{(p-1)n+4}.$$

Then

$$12f(n) \equiv (n-3)(n-4)f(0) \pmod{p^3}.$$

Hints and Solutions

1. We claim that $F(n+3) - 3F(n+2) + 3F(n+1) - F(n) \equiv 0 \pmod{p^3}$ for all $n \geq 0$, and that $F(2) \equiv F(1) \equiv F(0) \equiv 0 \pmod{p^3}$. Then the result follows from induction.

   Let

$$G(n) = \sum_{k=1}^{p-1} k^{(p-1)n+1}, \text{ and}$$

$$H(n) = -\frac{n(n-1)}{2} \sum_{k=1}^{p-1} (k^{2p-1} - 3k^2) - \frac{p(p-1)}{2} [(p-1)n+1],$$

   so $F(n) = G(n) + H(n)$.

   The function $H(n)$ is quadratic in n, so $H(n+3) - 3H(n+2) + 3H(n+1) - H(n) = 0$ for all $n \geq 0$.

   Let k be an integer, $1 \leq k \leq p-1$. Then by Fermat's Little Theorem,

$k^{p-1} - 1 \equiv 0 \pmod{p}$. Cubing this, we get

$$\begin{aligned}
&k^{3(p-1)} - 3k^{2(p-1)} + 3k^{p-1} - 1 \equiv 0 \\
\Rightarrow\ &k^{(p-1)(n+3)+1} - 3k^{(p-1)(n+2)+1} \\
&+3k^{(p-1)(n+1)+1} - k^{(p-1)n+1} \equiv 0 \\
\Rightarrow\ &\sum_{k=1}^{p-1} k^{(p-1)(n+3)+1} - 3\sum_{k-1}^{p-1} k^{(p-1)(n+2)+1} \\
&+3\sum_{k=1}^{p-1} k^{(p-1)(n+1)+1} - \sum_{k=1}^{p-1} k^{(p-1)n+1} \equiv 0 \\
\Rightarrow\ &G(n+3) - 3G(n+2) + 3G(n+1) - 3G(n) \equiv 0 \pmod{p^3}.
\end{aligned}$$

Therefore, $F(n+3) - 3F(n+2) + 3F(n+1) - 3F(n) \equiv 0 \pmod{p^3}$ for all $n \geq 0$.

Now,

$$\begin{aligned}
F(0) &= \sum_{k=1}^{p-1} k - \frac{p(p-1)}{2} = 0, \text{ and} \\
F(2) &= \sum_{k=1}^{p-1} k^{2p-1} - \sum_{k=1}^{p-1} k^{2p-1} + \sum_{k=1}^{p-1} 3k^2 - \frac{p(p-1)(2p-1)}{2} = 0.
\end{aligned}$$

To calculate $F(1)$, as before, let k be an integer, $1 \leq k \leq p-1$. Then by the Binomial Theorem,

$$\begin{aligned}
k^p + (p-k)^p = k^p + p^p - \binom{p}{1} p^{p-1} k + \cdots + (-1)^{p-2} \binom{p}{p-2} p^2 k^{p-1} \\
+ (-1)^{p-1} \binom{p}{p-1} p k^{p-1} + (-1)^p \binom{p}{p} k^p \\
\equiv p^2 k^{p-1} \pmod{p^3}.
\end{aligned}$$

By Fermat's Little Theorem, $k^{p-1} - 1 = pt$ for some integer t. Therefore, $p^2 k^{p-1} = p^2(1+pt) \equiv p^2 \pmod{p^3}$. Summing from $k=1$ to $(p-1)/2$, we obtain

$$\sum_{k=1}^{p-1} k^p \equiv \frac{p-1}{2} \cdot p^2 \pmod{p^3}.$$

Therefore,

$$F(1) = \sum_{k=1}^{p-1} k^p - \frac{p^2(p-1)}{2} \equiv 0 \pmod{p^3}.$$

2. Hint: Prove that the expression has period 6 modulo 7.

3. Hint: Prove that the expression has period 12 modulo 13.

4. Since a_i is relatively prime to both p and q, by Fermat's Little Theorem, $a_i^{(p-1)(q-1)} - 1$ is divisible by pq. Squaring this, we get

$$\begin{aligned} a_i^{2(p-1)(q-1)} - 2a_i^{(p-1)(q-1)} + 1 &\equiv 0 \\ \Rightarrow\ a_i^{(p-1)(q-1)(n+2)+1} - 2a_i^{(p-1)(q-1)(n+1)+1} + a_i^{(p-1)(q-1)n+1} &\equiv 0 \\ \Rightarrow\ \sum_{i=1}^{m} a_i^{(p-1)(q-1)(n+2)+1} - 2\sum_{i=1}^{m} a_i^{(p-1)(q-1)(n+1)+1} & \\ + \sum_{i=1}^{m} a_i^{(p-1)(q-1)n+1} &\equiv 0 \\ \Rightarrow\ F(n+2) - 2F(n+1) + F(n) \equiv 0 \pmod{p^2q^2}. & \end{aligned}$$

Also,

$$F(0) = \sum_{i=1}^{m} a_i \equiv 0 \pmod{p^2q^2}.$$

It is now easy to prove by induction that $F(n) \equiv nF(1) \pmod{p^2q^2}$ for all $n \geq 0$.

Now, p does not divide $p-1$, and p does not divide $q-1$ by definition. Also, q does not divide neither $p-1$ nor $q-1$. Therefore, $(p-1)(q-1)$ is relatively prime to p^2q^2.

By a result in number theory, there exists an n such that $n(p-1)(q-1)+1 \equiv 0 \pmod{p^2q^2}$. For this n, n is clearly relatively prime to p^2q^2. Also, $p-1$ is even, so $n(p-1)(q-1)+1$ is an odd multiple of pq. Therefore, $F(n) \equiv 0 \pmod{p^2q^2}$. However, $F(n) \equiv nF(1) \pmod{p^2q^2}$, and n is relatively prime to p^2q^2. We conclude that $F(1) \equiv 0 \pmod{p^2q^2}$, and hence, that $F(n) \equiv nF(1) \equiv 0 \pmod{p^2q^2}$ for all $n \geq 0$.

5. Let $s_n = a^{2n} + b^{2n} + c^{2n}$ for all n. First, $a^2 + b^2 + c^2 = 2(a^2 + ab + b^2)$, and since d is odd, d divides $a^2 + ab + b^2$. Also,

$$\begin{aligned} a^2b^2 + a^2c^2 + b^2c^2 &= a^2b^2 + (a^2 + b^2)(a + b)^2 \\ &= a^4 + 2a^3b + 3a^2b^2 + 2ab^3 + b^4 \\ &= (a^2 + ab + b^2)^2, \end{aligned}$$

so $a^2b^2 + a^2c^2 + b^2c^2$ is divisible by d^2. Finally, by results on recursions,

$$s_n = (a^2 + b^2 + c^2)s_{n-1} - (a^2b^2 + a^2c^2 + b^2c^2)s_{n-2} + a^2b^2c^2 s_{n-3}$$

for all $n \geq 3$.

(a) Note that $a^{6n-4} + b^{6n-4} + c^{6n-4} = s_{3n-2}$, and

$$s_{3n-2} = (a^2 + b^2 + c^2)s_{3n-3} - (a^2b^2 + a^2c^2 + b^2c^2)s_{3n-4} + a^2b^2c^2 s_{3n-5}$$

for all $n \geq 2$. For $n = 2$, $s_{3n-5} = s_1 = a^2 + b^2 + c^2$, which is divisible by d. Also, $a^2b^2 + a^2c^2 + b^2c^2$ is divisible by d. Hence, by induction, s_{3n-2} is divisible by d for all $n \geq 1$.

(b) Note that $a^{6n-2} + b^{6n-2} + c^{6n-2} = s_{3n-1}$, and

$$s_{3n-1} = (a^2 + b^2 + c^2)s_{3n-2} - (a^2b^2 + a^2c^2 + b^2c^2)s_{3n-3} + a^2b^2c^2 s_{3n-4}$$

for all $n \geq 2$. For $n = 2$, $s_{3n-4} = s_2 = a^4 + b^4 + c^4 = 2a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 2b^4 = 2(a^2 + ab + b^2)^2$, which is divisible by d^2. By part (a), s_{3n-2} is divisible by d. Also, $a^2 + b^2 + c^2$ is divisible by d and $a^2b^2 + a^2c^2 + b^2c^2$ is divisible by d^2. Hence, by induction, s_{3n-1} is divisible by d^2 for all $n \geq 1$.

(c) For all $n \geq 1$, 2^n is even, so 2^n is congruent to 0, 2, or 4 modulo 6. However, congruence to 0 implies divisibility by 3, so 2^n is congruent to 2 or 4. The result then follows from parts (a) and (b).

(d) It is easy to show that $4^n \equiv 4 \pmod{6}$ for all $n \geq 1$. The result then follows from part (b).

6. (a) Hint: Show that for all $k \geq 1$, $F(k)^2 = F(k+1)F(k) - F(k)F(k-1)$. Sum this from $k = 1$ to n.

(b) Let $A(n) = F(n)^2 + F(n+1)^2$ and $B(n) = F(2n+4) - F(2n-3)$ for all $n \geq 2$. Then $A(2) = B(2) = 85$ and $A(3) = B(3) = 218$. We claim that $A(n) - 3A(n-1) + A(n-2) = B(n) - 3B(n-1) + B(n-2) = 0$ for all $n \geq 4$. Then it follows that $A(n) = B(n)$ for all $n \geq 2$.

Now,

$$\begin{aligned}
&A(n) - 3A(n-1) + A(n-2) \\
&= F(n+1)^2 + F(n)^2 - 3F(n)^2 - 3F(n-1)^2 + F(n-1)^2 + F(n-2)^2 \\
&= [F(n) + F(n-1)]^2 - 2F(n)^2 - 2F(n-1)^2 + [F(n) - F(n-1)]^2 \\
&= F(n)^2 + 2F(n)F(n-1) + F(n-1)^2 - 2F(n)^2 - 2F(n-1)^2 \\
&\quad + F(n)^2 - 2F(n)F(n-1) + F(n-1)^2 \\
&= 0.
\end{aligned}$$

Also,

$$\begin{aligned}
&B(n) - 3B(n-1) + B(n-2) \\
&= F(2n+4) - F(2n-3) - 3F(2n+2) + 3F(2n-5) + F(2n) - F(2n-7) \\
&= F(2n+4) - 3F(2n+2) + F(2n) - F(2n-3) + 3F(2n-5) - F(2n-7) \\
&= F(2n+3) + F(2n+2) - 3F(2n+2) + F(2n+2) - F(2n+1) \\
&\quad - F(2n-4) - F(2n-5) + 3F(2n-5) - F(2n-5) + F(2n-6) \\
&= F(2n+3) - F(2n+2) - F(2n+1) - F(2n-4) + F(2n-5) + F(2n-6) \\
&= 0.
\end{aligned}$$

7. We first prove a lemma:

Lemma. For any prime p and positive integer n not divisible by $p-1$,

$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod{p}.$$

Proof. Let s denote the given sum, and let g be a primitive root modulo p. Since n is not divisible by $p-1$, $g^n \not\equiv 1 \pmod{p}$. Therefore,

$$g^n s = \sum_{i=1}^{p-1} (gi)^n \equiv \sum_{i=1}^{p-1} i^n \equiv s \pmod{p},$$

so $(g^n - 1)s \equiv 0 \Rightarrow s \equiv 0 \pmod{p}$. ■

Now, let t denote the sum in the problem, and let u denote

$$\begin{aligned}\sum_{i=1}^{p-1} i^{2^n} &= \sum_{i=1}^{2k+1} i^{2^n} + \sum_{i=2k+2}^{4k+2} i^{2^n} \\ &= \sum_{i=1}^{2k+1} i^{2^n} + \sum_{i=1}^{2k+1} (p-i)^{2^n} \\ &\equiv 2t \pmod{p}.\end{aligned}$$

Since 2^n is not divisible by $p - 1 = 4k + 2 = 2(2k + 1)$, by the Lemma, $u \equiv 0 \pmod{p}$, so $t \equiv 0 \pmod{p}$.

8. (a) Let a be a quadratic residue modulo p, $1 \le a \le p - 1$. We claim that $p - a$ is also a quadratic residue modulo p.

   Since a is a quadratic residue, $a \equiv x^2 \pmod{p}$ for some x. A result in number theory states that there exists a u such that $u^2 \equiv -1 \pmod{p}$. Then $(xu)^2 \equiv -a \equiv p - a \pmod{p}$, so $p - a$ is also a quadratic residue modulo p. Also, if $a \le 2k$, then $p - a \ge 2k + 1$, and vice-versa.

   Now, there are exactly $p - 1 = 4k$ quadratic residues modulo p. Therefore, exactly half must be between 1 and $2k$, and half between $2k + 1$ and $4k$.

   (b) For $k + 1 \le i \le 2k$, let $a_i = p - a_{2k+1-i}$. Then by the solution to part (a), the numbers $a_1, a_2, \ldots, a_{2k}$ represent the quadratic residues modulo p.

   Let s denote the given sum, and let t denote

$$\begin{aligned}\sum_{i=1}^{2k} a_i^{2^n} &= \sum_{i=1}^{k} a_i^{2^n} + \sum_{i=k+1}^{2k} a_i^{2^n} \\ &= \sum_{i=1}^{k} a_i^{2^n} + \sum_{i=1}^{k} (p-a_i)^{2^n} \\ &\equiv 2s \pmod{p}.\end{aligned}$$

As i varies from 1 to $p-1$, i^2 takes on every quadratic residue exactly twice. Therefore,

$$\sum_{i=1}^{p-1} i^{2^{n+1}} = \sum_{i=1}^{p-1} (i^2)^{2^n} \equiv 2\sum_{i=1}^{2k} a_i^{2^n} \equiv 2t \equiv 4s \pmod{p}.$$

Now $p-1=4k$, where k is odd, so it cannot divide 2^{n+1}. Therefore, $4s \equiv 0 \pmod{p}$, which implies that $s \equiv 0 \pmod{p}$.

9. The expression is congruent to $2 \cdot (2^{n-1})^2$ modulo 13. Since 2 is not a square modulo 13, neither is the expression.

10. The expression factors as

$$(8^{2^{n-1}} + 5^{2^{n-1}})(8^{2^{n-2}} + 5^{2^{n-2}}) \cdots (8^2 + 5^2)(8+5)(8-5).$$

The last factor is 3, and all the other factors are congruent to 2 modulo 3. Therefore, the expression has exactly one factor of 3, and cannot be a perfect square.

11. Hint: See the solution to Problem 1. For an alternative approach, see the solution to Problem 14.

12. If k is divisible by p, then it follows that $f(n)$ is also divisible by p for all n, and the result follows trivially, so assume that k is not divisible by p.

    By induction, it is easy to prove that $f(n+mc) \equiv k^m f(n)$ for all $m \geq 0$, for all n. Take $m = p-1$; then by Fermat's Little Theorem, $k^{p-1} \equiv 1$ mod p, so $f(n+(p-1)c) \equiv f(n)$ for all n. Thus, we can take $b = p-1$.

13. For all $n \geq 0$,

$$\begin{aligned} &1 + 2^{4n+2} + 3^{4n+2} + 4^{4n+2} + 5^{4n+2} + 6^{4n+2} \\ &\equiv 1 + 4 \cdot 3^n + 9 \cdot 3^n + 3 \cdot 9^n + 12 \cdot 1^n + 10 \cdot 9^n \\ &\equiv 0 \pmod{13}. \end{aligned}$$

14. By the Binomial Theorem,

$$\begin{aligned} 3^{4n+3} &\equiv 27 \cdot 81^n \\ &\equiv 27 \cdot (1+80)^n \\ &\equiv 27 \cdot [1 + 80n + 6400(n)(n-1)/2] \\ &\equiv 27 + 10n + 25n^2 \pmod{125}. \end{aligned}$$

Similarly,

$$\begin{aligned} 4^{4n+3} &\equiv 64 \cdot 256^n \\ &\equiv 64 \cdot (1+5)^n \\ &\equiv 64 \cdot [1 + 5n + 25n(n-1)/2] \\ &\equiv 64 + 20n + 50n^2 \pmod{125}. \end{aligned}$$

Therefore,

$$\begin{aligned} &2(3^{4n+3} + 4^{4n+3}) - 25n^2 + 65n + 68 \\ &\equiv 2(27 + 10n + 25n^2 + 64 + 20n + 50n^2) - 25n^2 + 65n + 68 \\ &\equiv 0 \pmod{125}. \end{aligned}$$

15. Let $F(n) = 2^{2^n} + 3^{2^n} + 5^{2^n}$. Then $F(1) = 38 = 2 \cdot 19$ and $F(2) = 38 \cdot 19$. Also, for $n \geq 1$,

$$\begin{aligned} F(n+2) &= 2^{2^{n+2}} + 3^{2^{n+2}} + 5^{2^{n+2}} \\ &= 2^{4 \cdot 2^n} + 3^{4 \cdot 2^n} + 5^{4 \cdot 2^n} \\ &= 16^{2^n} + 81^{2^n} + 625^{2^n} \\ &\equiv 3^{2^n} + 5^{2^n} + 2^{2^n} \\ &\equiv F(n) \pmod{19}. \end{aligned}$$

Therefore, by induction, $F(n)$ is divisible by 19 for all $n \geq 1$.

Note that this problem is also a special case of Problem 5(c).

16. For all $n \geq 1$, $f(n+1) + f(n) = af(n) + af(n-1) = a[f(n) + f(n-1)]$. Therefore, $f(n+1) + f(n) = a^{n-1}[f(2) + f(1)]$, and

$$\begin{aligned} g(n) &= f(n+2) + af(n+1) + (a-1)f(n) \\ &= (2a-1)f(n+1) + (2a-1)f(n) \\ &= (2a-1)[f(n+1) + f(n)] \\ &= (2a-1)a^{n-1}[f(2) + f(1)]. \end{aligned}$$

17. Hint: Show that $f(n)$ has period 12 modulo 32.

18. Hint: See the solution to Problem 1.

19. Hint: Show that $f(n) \equiv an^2 + bn + c \pmod{p^3}$ for some constants a, b, and c. By substituting $n = 0$, 1, and 2, find a, b, and c in terms of $f(0)$, $f(1)$, and $f(2)$.

20. This is a straight-forward induction problem.

21. The problem boils down to showing that $F_{n^2-2n+2} + F_{n^2+2n} = F_{2n-1}(F_{n^2} + F_{n^2+2})$ for all $n \geq 1$.

    Let $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$. Then α and β are the roots of the equation $x^2 - x - 1 = 0$, and so $\alpha\beta = -1$, and $1/\alpha = \alpha - 1$ and $1/\beta = \beta - 1$.

    Binet's Formula states that

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

    for all n. Hence,

$$\begin{aligned}
&F_{2n-1}(F_{n^2} + F_{n^2+2}) \\
&= \left(\frac{\alpha^{2n-1} - \beta^{2n-1}}{\sqrt{5}}\right)\left(\frac{\alpha^{n^2} - \beta^{n^2} + \alpha^{n^2+2} - \beta^{n^2+2}}{\sqrt{5}}\right) \\
&= \frac{1}{5}(\alpha^{n^2+2n-1} - \alpha^{2n-1}\beta^{n^2} + \alpha^{n^2+2n+1} - \alpha^{2n-1}\beta^{n^2+2} \\
&\quad - \alpha^{n^2}\beta^{2n-1} + \beta^{n^2+2n-1} - \alpha^{n^2+2}\beta^{2n-1} + \beta^{n^2+2n+1}) \\
&= \frac{1}{5}(\alpha^{n^2+2n-1} + \beta^{n^2-2n+1} + \alpha^{n^2+2n+1} + \beta^{n^2-2n+3} \\
&\quad + \alpha^{n^2-2n+1} + \beta^{n^2+2n-1} + \alpha^{n^2-2n+3} + \beta^{n^2+2n+1}) \\
&= \frac{1}{5}\left[\left(\frac{1}{\alpha} + \alpha\right)(\alpha^{n^2-2n+2} + \alpha^{n^2+2n}) + \left(\frac{1}{\beta} + \beta\right)(\beta^{n^2-2n+2} + \beta^{n^2+2n})\right] \\
&= \frac{1}{5}\left[(2\alpha - 1)(\alpha^{n^2-2n+2} + \alpha^{n^2+2n}) + (2\beta - 1)(\beta^{n^2-2n+2} + \beta^{n^2+2n})\right] \\
&= \frac{\alpha^{n^2-2n+2} - \beta^{n^2-2n+2}}{\sqrt{5}} + \frac{\alpha^{n^2+2n} - \beta^{n^2+2n}}{\sqrt{5}} \\
&= F_{n^2-2n+2} + F_{n^2+2n}.
\end{aligned}$$

22. Hint: See the solution to Problem 21.

23. If p divided b, then p would also divide a, contradicting that a and b are relatively prime. Therefore, b^{-1} modulo p exists, and

$$\begin{aligned} a^2 + ab + b^2 &\equiv 0 \\ \Rightarrow\ (ab^{-1})^2 + ab^{-1} + 1 &\equiv 0 \\ \Rightarrow\ 4(ab^{-1})^2 + 4ab^{-1} + 4 &\equiv 0 \\ \Rightarrow\ (2ab^{-1} + 1)^2 &\equiv -3 \pmod{p}. \end{aligned}$$

Hence, -3 is a quadratic residue modulo p. By results in number theory, this implies that $p \equiv 1 \pmod 6$. Therefore, the result follows from Problem 5(b).

24. Let s denote the given sum, and let t denote

$$\begin{aligned} \sum_{i=1}^{p-1} i^{2\cdot 3^n} &= \sum_{i=1}^{3k+2} i^{2\cdot 3^n} + \sum_{i=3k+3}^{6k+4} i^{2\cdot 3^n} \\ &= \sum_{i=1}^{3k+2} i^{2\cdot 3^n} + \sum_{i=1}^{3k+2} (p-i)^{2\cdot 3^n} \\ &\equiv 2s \pmod{p}. \end{aligned}$$

Now, $p - 1 = 6k + 4 = 2(3k + 2)$, which cannot divide $2 \cdot 3^n$. Therefore, $t \equiv 0 \pmod p$, and so $s \equiv 0 \pmod p$.

25. Hint: See the solution to Problem 6(b). Alternatively, show that $F_n^2 + F_{n+1}^2 = F_{2n+1}$ for all n.

26. Hint: Show that F_n has period 10 modulo 11.

27. The given relation implies that F can be modelled by a polynomial of degree at most $k - 1$.

For $0 \le i \le k - 1$, let

$$F_i(n) = (n - a_0)(n - a_1)\cdots(n - a_{i-1})(n - a_{i+1})\cdots(n - a_{k-1}).$$

Then by the Lagrange Interpolation Formula,

$$F(n) \equiv \frac{F_0(n)}{F_0(a_0)}F(a_0) + \frac{F_1(n)}{F_1(a_1)}F(a_1) + \cdots + \frac{F_{k-1}(n)}{F_{k-1}(a_{k-1})}F(a_{k-1}) \pmod{p^k}.$$

Since $a_s - a_t$ is not divisible by p for all $s \neq t$, $F_i(a_i)^{-1}$ exists modulo p^k.

Finally, $F(a_i) \equiv 0 \pmod{p^k}$ for all i, so $F(n) \equiv 0 \pmod{p^k}$ for all n.

28. Let $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$, so that α and β are the roots of $x^2 - x - 1 = 0$. Then it suffices to show that $G_n(\alpha) = G_n(\beta) = 0$. Note that $\alpha\beta = -1$, so $\alpha^{11}\beta^{11} = -1$.

    By Binet's Formula,

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

for all $n \geq 0$. Hence,

$$\begin{aligned} G_n(\alpha) &= 89\alpha^n - \left(\frac{\alpha^n - \beta^n}{\sqrt{5}}\right)\alpha^{11} - \frac{\alpha^{n-11} - \beta^{n-11}}{\sqrt{5}} \\ &= 89\alpha^n - \frac{\alpha^{n+11} - \alpha^{11}\beta^n + \alpha^{n-11} - \beta^{n-11}}{\sqrt{5}} \\ &= 89\alpha^n - \frac{\alpha^{n+11} + \beta^{n-11} + \alpha^{n-11} - \beta^{n-11}}{\sqrt{5}} \\ &= \alpha^n\left(89 - \frac{\alpha^{11} + \alpha^{-11}}{\sqrt{5}}\right) \\ &= \alpha^n\left(89 - \frac{\alpha^{11} - \beta^{11}}{\sqrt{5}}\right) \\ &= \alpha^n(89 - F_{11}) \\ &= 0. \end{aligned}$$

That $G_n(\beta) = 0$ is similarly shown.

29. Let s denote the given sum, and let t denote

$$\begin{aligned} \sum_{i=1}^{p-1} i^{4n+2} &= \sum_{i=1}^{2k} i^{4n+2} + \sum_{i=2k+1}^{4k} i^{4n+2} \\ &= \sum_{i=1}^{2k} i^{4n+2} + \sum_{i=1}^{2k} (p-i)^{4n+2} \\ &\equiv 2s \pmod{p}. \end{aligned}$$

Since $p-1 = 4k$ cannot divide $4n+2$, $t \equiv 0 \pmod{p}$, so $s \equiv 0 \pmod{p}$.

30. By Problem 1,

$$F(n) \equiv \frac{n(n-1)}{2} \sum_{k=1}^{p-1} (k^{2p-1} - 3k^2) \equiv \frac{n(n-1)}{2} C \pmod{p^3},$$

where C is a constant independent of n.

Therefore,

$$\begin{aligned} G(n) &= 500500F(n) - n(n-1)/2 \cdot F(1001) \\ &\equiv 500500 \cdot n(n-1)/2 \cdot C - n(n-1)/2 \cdot 1001 \cdot 1000/2 \cdot C \\ &\equiv 0 \pmod{p^3}. \end{aligned}$$

31. (a) A result in number theory states that the congruence $a^n \equiv 1 \pmod{p}$ has $\gcd(n, p-1)$ solutions modulo p. Since $2m$ divides $p-1$, $\gcd(2m, p-1) = 2m$.

Now, if a satisfies $a^{2m} \equiv 1 \pmod{p}$, then $(p-a)^{2m} \equiv 1 \pmod{p}$. Therefore, half of the solutions, when reduced, are between 1 and $(p-1)/2$ inclusive.

(b) For $m+1 \le i \le 2m$, let $a_i = p - a_{2m+1-i}$, so by part (a), a_1, a_2, $\ldots$, a_{2m} are the $2m$ solutions to $a^{2m} \equiv 1 \pmod{p}$.

Let g be a primitive root of modulo p. Then another result in number theory states that a_1, a_2, $\ldots$, a_{2m} are, in some order, congruent to 1, $g^{2^{j-1}}$, $g^{2\cdot 2^{j-1}}$, $g^{3\cdot 2^{j-1}}$, $\ldots$, $g^{(2m-1)\cdot 2^{j-1}}$.

Let s denote the given sum, and let t denote the sum

$$\begin{aligned} \sum_{i=1}^{2m} a_i^{2n} &= \sum_{i=1}^{m} a_i^{2n} + \sum_{i=m+1}^{2m} a_i^{2n} \\ &= \sum_{i=1}^{m} a_i^{2n} + \sum_{i=1}^{m} (p-a_i)^{2n} \\ &\equiv 2s \pmod{p}. \end{aligned}$$

Also,

$$t \equiv \sum_{i=0}^{2m-1} g^{i\cdot 2^{j-1}\cdot 2n} \equiv \sum_{i=0}^{2m-1} g^{i\cdot 2^j n} \pmod{p}.$$

If n is divisible by m, then $n = md$ for some d, and

$$t \equiv \sum_{i=0}^{2m-1} g^{i\cdot 2^j md} \equiv \sum_{i=0}^{2m-1} g^{id(p-1)} \equiv \sum_{i=0}^{2m-1} 1 \equiv 2m \pmod{p},$$

so t is not divisible by p, and neither is s.

On the other hand, if n is not divisible by m, then

$$\begin{aligned}(1-g^{2^j n})t &\equiv 1 - g^{2m\cdot 2^j n} \\ &\equiv 1 - g^{2n(p-1)} \\ &\equiv 0 \pmod{p}.\end{aligned}$$

Since n is not divisible by m, $2^j n = n(p-1)/m$ is not divisible by $p-1$, so $1 - g^{2^j n}$ is not congruent to 0, so finally t is divisible by p, which implies that s is divisible by p.

32. We have that a and b are relatively prime to p, so by Fermat's little theorem, $a^{p-1} - 1 \equiv 0 \pmod{p}$. Cubing, we get

$$a^{3(p-1)} - 3a^{2(p-1)} + 3a^{p-1} - 1 \equiv 0 \pmod{p^3}.$$

Multiplying by $a^{(p-1)n+4}$, we get

$$\begin{aligned}&a^{(p-1)(n+3)+4} - 3a^{(p-1)(n+2)+4} \\ &\quad + 3a^{(p-1)(n+1)+4} - a^{(p-1)n+4} \equiv 0 \pmod{p^3}\end{aligned}$$

for all integers $n \geq 0$.

Similarly,

$$\begin{aligned}&b^{(p-1)(n+3)+4} - 3b^{(p-1)(n+2)+4} \\ &\quad + 3b^{(p-1)(n+1)+4} - b^{(p-1)n+4} \equiv 0 \pmod{p^3},\end{aligned}$$

and

$$\begin{aligned}&(a+b)^{(p-1)(n+3)+4} - 3(a+b)^{(p-1)(n+2)+4} \\ &\quad + 3(a+b)^{(p-1)(n+1)+4} - (a+b)^{(p-1)n+4} \equiv 0 \pmod{p^3}\end{aligned}$$

for all $n \geq 0$.

Adding, we get $f(n+3) - 3f(n+2) + 3f(n+1) - f(n) \equiv 0 \pmod{p^3}$ for all $n \geq 0$. Then by problem 19, there exist constants A, B, C, such that $f(n) \equiv An^2 + Bn + C \pmod{p^3}$ for all $n \geq 0$.

Now, we claim we can assume that $b = 1$. This is because if p divides $a^2 + ab + b^2$, then p also divides $1 + ab^{-1} + a^2b^{-2}$.

Let
$$g_n(x) = 1 + x^{6n+4} + (1+x)^{6n+4}.$$

We claim that $g_n(x) = Q_n(x)(1 + x + x^2)^3 + R_n(1 + x + x^2)^2$ for some polynomial $Q_n(x)$ with integer coefficients and integer R_n, for all $n \geq 0$. We prove this by induction.

For $n = 0$,
$$1 + x^4 + (1+x)^4 = 2(1 + x + x^2)^2,$$
so we can take $R_0 = 2$.

For $n = 1$,
$$\begin{aligned}&1 + x^{10} + (1+x)^{10} \\ &\quad = (-13 + 19x + 21x^2 + 4x^3 + 2x^4)(1 + x + x^2)^3 + 15(1 + x + x^2)^2,\end{aligned}$$
so we can take $R_1 = 15$.

For $n = 2$,
$$\begin{aligned}&1 + x^{16} + (1+x)^{16} \\ &\quad = (-38 + 50x + 78x^2 + 212x^3 + 554x^4 + 702x^5 \\ &\quad + 514x^6 + 252x^7 + 78x^8 + 10x^9 + 2x^{10})(1 + x + x^2)^3 \\ &\quad + 40(1 + x + x^2)^2,\end{aligned}$$
so we can take $R_2 = 40$.

Now, assume the claim is true for some $n = k$, $k + 1$, and $k + 2$, so
$$\begin{aligned}g_k(x) &= Q_k(x)(1 + x + x^2)^3 + R_k(1 + x + x^2)^2, \\ g_{k+1}(x) &= Q_{k+1}(x)(1 + x + x^2)^3 + R_{k+1}(1 + x + x^2)^2, \\ g_{k+2}(x) &= Q_{k+2}(x)(1 + x + x^2)^3 + R_{k+2}(1 + x + x^2)^2.\end{aligned}$$

We can calculate that

$$\begin{aligned}
&g_{k+3}(x) - 3g_{k+2}(x) + 3g_{k+1}(x) - g_k(x)\\
&\quad = x^{6(k+3)+4} - 3x^{6(k+2)+4} + 3x^{6(k+1)+4} - x^{6k+4}\\
&\quad + (1+x)^{6(k+3)+4} - 3(1+x)^{6(k+2)+4} + 3(1+x)^{6(k+1)+4} - (1+x)^{6k+4}\\
&\quad = x^{6k+4}(x^6-1)^3 + (1+x)^{6k+4}[(1+x)^6-1]^3.
\end{aligned}$$

Both $x^6 - 1$ and $(1+x)^6 - 1$ are divisible by $1 + x + x^2$, so the whole expression is divisible by $(1 + x + x^2)^3$ – say it is equal to $P_k(x)(1 + x + x^2)^3$. Then

$$\begin{aligned}
g_{k+3}(x) &= 3g_{k+2}(x) - 3g_{k+1}(x) + g_k(x) + P_k(x)(1+x+x^2)^3\\
&= [3Q_{k+2}(x) - 3Q_{k+1}(x) + Q_k(x) + P_k(x)](1+x+x^2)^3\\
&\quad + (3R_{k+2} - 3R_{k+1} + R_k)(1+x+x^2)^2,
\end{aligned}$$

which proves the claim for $n = k + 3$. Furthermore, we have that $R_{n+3} - 3R_{n+2} + 3R_{n+1} - R_n = 0$ for all $n \geq 0$, so R_n is quadratic in n. From $R_0 = 2$, $R_1 = 15$, and $R_2 = 40$, we have that $R_n = 6n^2+7n+2 = (2n + 1)(3n + 2)$.

By the solution to problem 23, $p \equiv 1 \pmod 6$. Let $p = 6t + 1$. Then

$$\begin{aligned}
f(n) &= 1 + a^{(p-1)n+4} + (1+a)^{(p-1)n+4}\\
&= 1 + a^{6tn+4} + (1+a)^{6tn+4}\\
&= g_{tn}(a)\\
&\equiv R_{tn}(1+a+a^2)^2\\
&\equiv (2tn+1)(3tn+2)(1+a+a^2)^2 \pmod{p^3}
\end{aligned}$$

for all $n \geq 0$.

Then

$$\begin{aligned}
f(3) &\equiv (6t+1)(9t+2)(1+a+a^2)^2\\
&\equiv p(9t+2)(1+a+a^2)^2\\
&\equiv 0 \pmod{p^3},
\end{aligned}$$

and

$$\begin{aligned}
f(4) &\equiv (8t+1)(12t+2)(1+a+a^2)^2\\
&\equiv (8t+1)(2p)(1+a+a^2)^2\\
&\equiv 0 \pmod{p^3}.
\end{aligned}$$

As stated above, there exist constants A, B, C, such that $f(n) \equiv An^2 + Bn + C \pmod{p^3}$ for all $n \geq 0$, so $f(n) \equiv A(n-3)(n-4) \pmod{p^3}$ for all $n \geq 0$. Taking $n = 0$ gives $f(0) \equiv 12A \pmod{p^3}$. We conclude that $12f(n) \equiv 12A(n-3)(n-4) \equiv (n-3)(n-4)f(0) \pmod{p^3}$ for all $n \geq 0$.