

# Mathematical Induction

José Espinosa

<http://www.math.cl/induction.html>

Last modified on: 26th June 2011

## 1 Mathematical Induction Problems.

1. Let:

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

Prove by induction that  $F(n)$  is divisible by  $p^3$ , for all integers  $n \geq 0$ , where  $p$  is a prime number  $> 2$ .

2. The Fibonacci sequence is defined by  $F(1) = 1$ ,  $F(2) = 1$  and  $F(n) = F(n-1) + F(n-2)$  for  $n \geq 3$ . Use mathematical induction to prove the following:  $1 + 2^{2n} + 3^{2n} + 2((-1)^{F(n)} + 1)$  is divisible by 7 for all positive integers  $n$ .

3. Let  $F(n)$  be the  $n^{\text{th}}$  Fibonacci number. Prove the following in more ways than one:

$2(2^{2n} + 5^{2n} + 6^{2n}) + 3(-1)^{n+1}((-1)^{F(n)} + 1)$  is divisible by 13 for all positive integers  $n$ .

4. Suppose that:  $\sum_{i=1}^m a_i$  and that:  $\sum_{i=1}^m a_i^{jbc}$  are divisible by  $(bc)^2$  for all odd numbers  $j$ . ( $b$  and  $c$  are both odd primes,  $b < c$  and  $(c-1)$  is not divisible by  $b$ , the  $a_i$ 's are relatively prime with respect to  $b$  and  $c$ ).

Let:

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

Prove by induction that:  $F(n)$  is divisible by  $(bc)^2$ , for all integers  $n \geq 0$ .

5. Let  $a, b, c$  be three positive integers where  $c = a + b$ . Let  $d$  be an odd factor of  $a^2 + b^2 + c^2$  ( $d$  is not divisible by 3 for part (c)). Prove by induction that for all integers  $n > 0$ :

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

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

6. A sequence is given by  $F(1) = 1$ ,  $F(2) = 6$  and  $F(n) = F(n-1) + F(n-2)$ , for  $n \geq 3$ . Prove that for all integers  $n > 1$ :

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

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

7. Let  $2p + 1$  be a prime number where  $p$  is an odd number  $> 1$ . Prove by math induction that for all integers  $n > 0$ :

$$\sum_{k=1}^p k^{2^n}$$

is divisible by  $(2p + 1)$ . Prove it in more ways than one.

8. Let  $4p + 1$  be a prime number where  $p$  is an odd number  $> 1$ . Prove by induction that for all integers  $n > 0$ :

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

is divisible by  $(4p + 1)$ . The  $a_i$ 's are all different, belong to the set of the first  $2p$  positive integers and they have the property:  $a_k^{2p} - 1$  is divisible by  $(4p + 1)$ . The other members of the set have the property:  $b_k^{2p} + 1$  is divisible by  $(4p + 1)$ .

9. Prove that for all integers  $n \geq 1$ :  $2^{2n-1} + 4^{2n-1} + 9^{2n-1}$  is not a perfect square.  
 10. Prove that for every positive integer  $n$ :  $8^{2^n} - 5^{2^n}$  is not a perfect square. Prove it in two forms.  
 11. Let  $F(n) = 13^{6n+1} + 30^{6n+1} + 100^{6n+1} + 200^{6n+1}$  y let:

$$G(n) = 2F(n) + 2n(n-2)F(1) - n(n-1)F(2)$$

Prove by induction that for all integers  $n \geq 0$ :  $G(n)$  is divisible by  $7^3$ .

12. Let  $f(a)$  be a function from positive integers to positive integers. If  $(f(a+b) - kf(a))$  is divisible by  $p$  for all positive integers  $a$ , then prove that there exists  $b_0$  such that  $(f(a+b_0) - f(a))$  is divisible by  $p$ .  
 13. Prove the following in more ways than one :

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

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

14. Prove by induction that for all integers  $n \geq 0$ :  $(2(3^{4n+3} + 4^{4n+3}) - 25n^2 + 65n + 68)$  is divisible by 125.  
 15. Prove by induction that for each positive integer  $n$ :  $2^{2^n} + 3^{2^n} + 5^{2^n}$  is divisible by 19.  
 16. Let  $f(n) = (a-1)f(n-1) + af(n-2)$  and let:  $g(n) = f(n+2) + af(n+1) + (a-1)f(n)$ . Prove by induction that for all integers  $n > 0$ :

$$g(n) = (f(1) + f(2))(2a-1)a(n-1)$$

17. Let  $f(n) = 3(f(n-1) + f(n-2)) + 1$ ,  $f(1) = f(2) = 1$   
 Prove by induction that for all integers  $n > 0$ :

$$(f(3n) + f(3n+1))$$

is divisible by 32.

18. Let  $p$  be a prime number greater than 5. Let  $F(n) = 2^{1+(p-1)n} - 3^{1+(p-1)n} - 5^{1+(p-1)n} + 6^{1+(p-1)n}$  and let:

$$G(n) = 100F(n) - nF(100)$$

Prove by induction that for all integers  $n \geq 0$  :  $G(n)$  is divisible by  $p^2$ .

19. Let  $p$  be a positive integer. Let  $F(n)$  be a function from integers to integers.

If  $F(n)$  satisfies the following:

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

Then for all integers  $n \geq 0$ :

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

20. Let  $a(n) = a(n-1) + 2a(n-2) + 1$ ,  $a(1) = a(2) = 1$ . Prove by induction that for all integers  $n > 0$ :

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

21. Consider the first  $n^2$  Fibonacci numbers arranged in an anti-clockwise spiral as it is shown next for  $n = 3$  and  $n = 4$ .

$$\begin{array}{ccc} 5 & \mathbf{3} & 2 \\ \mathbf{8} & 1 & \mathbf{1} \\ 13 & \mathbf{21} & 34 \end{array}$$

$$\begin{array}{cccc} 987 & \mathbf{610} & 377 & 233 \\ \mathbf{5} & 3 & 2 & 144 \\ 8 & 1 & 1 & \mathbf{89} \\ 13 & 21 & \mathbf{34} & 55 \end{array}$$

Note that for  $n = 3$  have that  $(21 + 1) = 2(8 + 3)$  and for  $n = 4$  have that  $(610 + 5) = 5(89 + 34)$ . Guess and prove this result for all integers  $n > 2$  (not necessarily by induction).

22. What would happen if in Problem 21, we change the Fibonacci numbers by the Lucas numbers, by the even Fibonacci numbers, etc.?

23. Let  $p$  be a prime number greater than 3 such that divides  $a^2 + ab + b^2$  ( $a$  relatively prime to  $b$ ). Show in more ways than one that for all integers  $n \geq 0$ :

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

is divisible by  $p^2$ .

24. Let  $(6p+5)$  be a prime number where  $p$  is an integer non-negative. Prove by math induction that for all integers  $n \geq 0$ :

$$\sum_{k=1}^{3p+2} k^{2(3^n)}$$

is divisible by  $(6p+5)$ .

25. Let  $F(n)$  be the  $n^{\text{th}}$  Fibonacci number. Prove in several ways that:

$$F(n)^2 + F(n+1)^2 + F(n+2)^2 + F(n+3)^2 = 3F(2n+3)$$

26. Let  $F(n)$  be the  $n^{\text{th}}$  Fibonacci number. Prove that for every integer non-negative  $n$ :

$$F(5n+3) + F(5n+4)^2$$

is divisible by 11.

27. Let  $d$  be a fixed positive integer and let  $p$  be an odd prime number. Let  $F(n)$  be a function from integers to integers which satisfies the following congruence:

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

If  $F(a_0), F(a_1), \dots, F(a_{d-1})$  are divisible by  $p^d$  where  $(a_i - a_j)$  is not divisible by  $p$  for  $i \neq j$ , then prove that for all integers  $n \geq 0$ :  $F(n)$  is divisible by  $p^d$ .

28. Let  $F(n)$  be the  $n^{\text{th}}$  Fibonacci number. Let  $G_n(a) = 89a^n - F(n)a^{11} - F(n-11)$ .  
 Prove that for every integer non-negative  $n$ :  $G_n(a)$  is divisible by the polynomial  $a^2 - a - 1$ .
29. Let  $4m + 1$  be a prime number. Prove that for all integers non-negative  $n$ :

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

is divisible by  $4m + 1$ .

30. Let:

$$F(n) = \sum_{i=1}^{p-1} i^{n(p-1)+1} - \frac{p(p-1)(n(p-1)+1)}{2}$$

And let  $G(n) = 500500F(n) - \frac{n(n-1)}{2}F(1001)$ . Prove by induction that  $G(n)$  is divisible by  $p^3$ , for all integers  $n \geq 0$  where  $p$  is a prime number  $> 13$ .

31. Let  $p$  be an odd prime and let  $d$  be a divisor of  $p-1$ , it is known that the congruence  $a^d \equiv 1 \pmod{p}$  has exactly  $d$  distinct solutions. Let  $a_1, a_2, \dots, a_d$  be those solutions. Prove that:

$$\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$$

, where  $c_n = 1$  if  $n$  is divisible by  $d$  and 0 otherwise.

32. Prove or disprove the following property: given the statement of Problem 23 and let  $f(n)$  be:

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

Then:  $12f(n) \equiv (n-3)(n-4)f(0) \pmod{p^3}$  for all integers  $n \geq 0$ .

33. Let  $p > 3$  be a prime dividing  $x^2 + x + 1$  ( $1, x$  relatively prime). Let  $f(n)$  be

$$(1+x)^{(p-1)n+1} - x^{(p-1)n+1} - 1$$

Then:  $6f(n) \equiv -n(n-1)(x^2 + x + 1)^2 \pmod{p^3}$  for all  $n \geq 0$ .

## 2 Hints and Solutions.

### Hint Problem 1:

Use the following variant of the method of mathematical induction:

1. The statement is true for  $n = 0$ ,  $n = 1$  and  $n = 2$ .
2. If the statement is true for  $n = k$ ,  $n = k + 1$  and  $n = k + 2$ , then the statement is true for  $n = k + 3$ .

Prove the following relation:

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

Use Fermat's little theorem and the following result: If  $g(k) = ak^2 + bk + c$ , is simple to verify that  $g(k+3) = 3g(k+2) - 3g(k+1) + g(k)$ .

If you do not want to use the induction form indicated previously to note that:

$$F(k+3) - 3F(k+2) + 3F(k+1) - F(k) = (F(k+3) - 2F(k+2) + F(k+1)) - (F(k+2) - 2F(k+1) + F(k))$$

If we proved that  $(F(2) - 2F(1) + F(0))$  is divisible by  $p^3$ , we might prove that  $(F(k+2) - 2F(k+1) + F(k))$  is divisible by  $p^3$  for all  $k \geq 0$ . Similarly, if  $(F(k+2) - 2F(k+1) + F(k))$  is divisible by  $p^3$ , we can do the following:  $(F(k+2) - 2F(k+1) + F(k)) = (F(k+2) - F(k+1)) - (F(k+1) - F(k))$ . If  $p^3$  divides  $(F(1) - F(0))$ , then we can prove that  $(F(k+1) - F(k))$  is divisible by  $p^3$  for all  $k \geq 0$ . If we proved that  $(F(k+1) - F(k))$  is divisible by  $p^3$ , then it remains to show that  $F(0)$  is divisible by  $p^3$ , to prove that  $F(k)$  is divisible by  $p^3$  for all  $k \geq 0$ .

Summarizing, if we do the above, we can prove that  $F(n)$  is divisible by  $p^3$  for all integer  $n \geq 0$ . Note that if we proved that  $F(0)$ ,  $F(1)$  and  $F(2)$  are divisible by  $p^3$ , we proved that  $(F(2) - 2F(1) + F(0))$  and  $(F(1) - F(0))$  are divisible by  $p^3$ . Therefore both methods are enough similar.

### Hint Problem 2:

Let  $G(n) = 1 + 2^{2n} + 3^{2n} + 2((-1)^{F(n)} + 1)$ . Prove that  $(G(n+3) - G(n))$  is divisible by 7. Divide the original problem into three problems:  $n$  of the form  $3m$ ,  $n$  of the form  $3m - 1$  and  $n$  of the form  $3m - 2$ . Then apply induction on  $m$  for each one of the problems.

Another form to solve the problem is proving that  $(G(n) + G(n+1) + G(n+2))$  is divisible by 7 (using the principle of weak induction) and later to use the following form of induction:

1. The property is true for  $n = 1$  and  $n = 2$ .
2. If the property is true for  $n = k$  and  $n = k + 1$  implies that the property is true for  $n = k + 2$ .

### Hint Problem 3:

See hint for Problem 2. Let  $G(n) = 2(2^{2n} + 5^{2n} + 6^{2n}) + 3(-1)^{n+1}((-1)^{F(n)} + 1)$

For the second proof asked for, prove that:  $(G(n) - G(n+1) + G(n+2))$  is divisible by 13 or that  $(G(n)^2 + G(n+1)^2 + G(n+2)^2)$  is divisible by 13.

Note that if  $G(n)^2$  is divisible by 13,  $G(n)$  as well.

### Solution Problem 4:

We will use the following induction form:

1. The property is true for  $n = 0$  and  $n = 1$ .
2. Assume that the property is true for  $n = k$  and  $n = k + 1$ , then show that it is true for  $n = k + 2$ .

It follows straight from the statement that the property is true for  $n = 0$ . (Later we will prove that the property is true for  $n = 1$ .)

From Fermat's little theorem we can to conclude that:

$$\begin{aligned}
(a_i^{(b-1)(c-1)} - 1)^2 &= a_i^{2(b-1)(c-1)} - 2a_i^{(b-1)(c-1)} + 1 \equiv 0 \pmod{b^2c^2} \\
(a_i^{2(b-1)(c-1)} - 2a_i^{(b-1)(c-1)} + 1)a_i^{1+k(b-1)(c-1)} &\equiv 0 \pmod{b^2c^2} \\
(a_i^{1+(k+2)(b-1)(c-1)} - 2a_i^{1+(k+1)(b-1)(c-1)} + a_i^{1+k(b-1)(c-1)}) &\equiv 0 \pmod{b^2c^2} \\
\left(\sum_{i=1}^m (a_i^{1+(k+2)(b-1)(c-1)} - 2\sum_{i=1}^m a_i^{1+(k+1)(b-1)(c-1)} + \sum_{i=1}^m a_i^{1+k(b-1)(c-1)})\right) &\equiv 0 \pmod{b^2c^2}
\end{aligned}$$

Therefore:

$$(F(k+2) - 2F(k+1) + F(k)) \equiv 0 \pmod{b^2c^2} \quad (1)$$

We will prove that:

$$F(n) \equiv n \cdot F(1) \pmod{b^2c^2} \quad (2)$$

We will use the induction form indicated previously. For  $n = 0$  we must prove that  $F(0) \equiv 0 \cdot F(1) \pmod{b^2c^2}$ , which is true according to the statement. For  $n = 1$  we must prove that  $F(1) \equiv 1 \cdot F(1) \pmod{b^2c^2}$ , which is equivalent to prove that  $0 \equiv 0 \pmod{b^2c^2}$ , which is clearly fulfilled by positive integers  $b$  and  $c$ .

Suppose that the property is true for  $n = k$  and  $n = k + 1$ . We will prove that the property also is true for  $n = k + 2$ .

In effect, from the relation (1) and applying the inductive hypothesis we conclude that:

$$\begin{aligned}
F(k+2) - 2(k+1)F(1) + kF(1) &\equiv 0 \pmod{b^2c^2} \\
F(k+2) &\equiv (k+2)F(1) \pmod{b^2c^2}
\end{aligned}$$

Now we will prove that there exists  $k$  so that  $F(k)$  is divisible by  $(bc)^2$  and  $k$  is not divisible by  $(bc)$ (If we proved the above statement we can prove easily that  $F(1)$  is divisible by  $(bc)^2$ ).

We will prove that there exists  $k$  distinct from 0 so that  $(1 + (b-1)(c-1)k)$  is divisible by  $bc$  and that  $k$  is not divisible by  $bc$ .

If we prove the first one, we can to prove that, using the second assumption given in the statement that, for that  $k$ ,  $F(k)$  is divisible by  $(bc)^2$ ; and if we proved that  $k$  is not divisible by  $bc$ , we can to use the result (1) to prove that  $F(1)$  is divisible by  $(bc)^2$ .

We will prove that there exists  $k_b$  in such a way that  $(1 + (b-1)(c-1)k_b)$  is divisible by  $b$  and that there exists  $k_c$  in such a way that  $(1 + (b-1)(c-1)k_c)$  is divisible by  $c$ .

In effect, multiplying  $(b-1)(c-1)$  by  $k = 1, 2, \dots, (b-1)$ ; the remainders of the division by  $b$  are all different.

Suppose that for  $k = r$  and  $k = s$  the remainders are equal, with  $r$  and  $s$  positive integers  $\leq b-1$  and  $r$  distinct from  $s$ . Therefore  $(r-s)(b-1)(c-1)$  is divisible by  $b$ , but  $r-s$ ,  $b-1$  and  $c-1$  are not divisible by  $b$  ( $r$  and  $s$  are both  $< b$ , hence their difference is  $< b$  and either 0, because  $r$  is different from  $s$ ;  $b-1$  is not divisible by  $b$ , since 1 is not divisible by  $b$ ; and  $c-1$  is not divisible by  $b$  under the statement of the problem).

In conclusion, there exists a contradiction and therefore if the remainders are equal, then  $r = s$  and there exists a  $k < b$  so that the remainder is equal to  $(b-1)$ . Therefore for that  $k$ ,  $(1 + (b-1)(c-1)k)$  is divisible by  $b$ .

For  $c$  is a similar proof.

Now we need to find a  $k$  so that  $(1 + (b-1)(c-1)k)$  is divisible by  $bc$ .

$$\begin{aligned}
1 + (b-1)(c-1)(k_b + l_b b) &= 1 + (b-1)(c-1)(k_c + l_c c) \\
(k_b + l_b b) &= (k_c + l_c c) \\
l_b b &= (k_c - k_b) + l_c c
\end{aligned}$$

Note that there exists a positive integer  $l_c$  such that if the remainder of the division of  $(k_c - k_b)$  by  $b$  is added the remainder of the division of  $l_c c$  by  $b$  the result is  $b$  or 0 and so there exists a integer  $l_b$  satisfying

the above conditions. The proof is similar to that for  $c$  (dividing  $l_c c$  by  $b$  for  $l_c = 1, 2, \dots, b$ , we obtain  $b$  different remainders which are  $0, 1, 2, \dots, b-1$  in some order.)

Therefore we proved that there exists  $k$  so that  $(1 + (b-1)(c-1)k)$  is divisible by  $bc$ .

The  $k$  found is not divisible by  $bc$ , since of being divisible by  $bc$  it would imply that 1 is divisible by  $ab$ , which is a contradiction.

We proved that  $F(0)$  is divisible by  $b^2c^2$  and with the above result we proved that  $F(1)$  is divisible by  $b^2c^2$ .

Suppose that  $F(k)$  and  $F(k+1)$  are both divisible by  $b^2c^2$ , from result (1) we conclude that  $F(k+2)$  is also divisible by  $b^2c^2$ .

Therefore:  $F(n)$  is divisible by  $b^2c^2$ , for all non-negative integers  $n$ .

### Solution Problem 5:

#### Part a

Let us begin by proving that  $d^2$  is a divisor of  $(a^2b^2 + a^2c^2 + b^2c^2)$ . It is known that  $(a^2 + b^2 + c^2)$  is divisible by  $d$ , which implies that  $(a^2 + b^2 + c^2)^2$  is divisible by  $d^2$ . But  $(a^2 + b^2 + c^2)^2$  is equal to  $(a^4 + b^4 + c^4 + 2(a^2b^2 + a^2c^2 + b^2c^2))$ . Hence :  
 $(a^4 + b^4 + c^4 + 2(a^2b^2 + a^2c^2 + b^2c^2))$  is divisible by  $d^2$ .

On the other hand:

$$\begin{aligned} a + b &= c \\ (a + b)^2 &= c^2 \\ a^2 + 2ab + b^2 &= c^2 \\ a^2 + b^2 - c^2 &= -2ab \\ (a^4 + b^4 + c^4 + 2(a^2b^2 - a^2c^2 - b^2c^2)) &= 4a^2b^2 \\ (a^4 + b^4 + c^4 - 2(a^2b^2 + a^2c^2 + b^2c^2)) &= 0 \end{aligned}$$

From above results we have that  $4(a^2b^2 + a^2c^2 + b^2c^2)$  is divisible by  $d^2$ , but as  $d$  is an odd integer is deduced that  $(a^2b^2 + a^2c^2 + b^2c^2)$  is divisible by  $d^2$ .

Now we return to the main problem.

For  $n = 1$  we have that:  $a^{6-4} + b^{6-4} + c^{6-4} = a^2 + b^2 + c^2$

Which is divisible by  $d$  according to the statement of the problem.

Let  $t(n) = a^{2n} + b^{2n} + c^{2n}$ . Note that  $a^2, b^2$  and  $c^2$  are the roots of the polynomial

$$P(x) = x^3 - (a^2 + b^2 + c^2)x^2 + (a^2b^2 + a^2c^2 + b^2c^2)x - a^2b^2c^2$$

hence  $t(n)$  satisfies the recurrence relation:

$$t(n) = (a^2 + b^2 + c^2)t(n-1) - (a^2b^2 + a^2c^2 + b^2c^2)t(n-2) + a^2b^2c^2t(n-3)$$

so

$$t(3k-2) = (a^{6k-4} + b^{6k-4} + c^{6k-4})$$

and hence

$$t(3k+1) = (a^2 + b^2 + c^2)t(3k) - (a^2b^2 + a^2c^2 + b^2c^2)t(3k-1) + a^2b^2c^2t(3k-2)$$

Suppose that the statement is true for  $k$ . We will prove that the property is true for  $k+1$ .

We know that  $(a^2 + b^2 + c^2)$  and  $(a^2b^2 + a^2c^2 + b^2c^2)$  are divisible by  $d$ . Hence if  $(a^{6k-4} + b^{6k-4} + c^{6k-4})$  is divisible by  $d$ ,  $(a^{6(k+1)-4} + b^{6(k+1)-4} + c^{6(k+1)-4})$  is divisible by  $d$  as well.

**Part b**

For  $n = 1$  we have that:  $a^{6-2} + b^{6-2} + c^{6-2} = a^4 + b^4 + c^4$

From the results proved above we have that  $2(a^4 + b^4 + c^4)$  is divisible by  $d^2$ , which implies that  $(a^4 + b^4 + c^4)$  is divisible by  $d^2$ , since  $d$  is odd. Therefore the statement holds for  $n = 1$ .

Suppose that the statement is true for  $n = k$ . We will prove that the statement is true for  $n = k + 1$ .

Note that:

$$t(3k - 1) = (a^{6k-2} + b^{6k-2} + c^{6k-2})$$

and hence

$$t(3k + 2) = (a^2 + b^2 + c^2)t(3k + 1) - (a^2b^2 + a^2c^2 + b^2c^2)t(3k) + a^2b^2c^2t(3k - 1)$$

We know that  $(a^2 + b^2 + c^2)$  and  $(a^{6k-4} + b^{6k-4} + c^{6k-4})$  are divisible by  $p$ .

Therefore  $(a^2 + b^2 + c^2)(a^{6k-4} + b^{6k-4} + c^{6k-4})$  is divisible by  $p^2$ . On the other hand  $a^2b^2 + a^2c^2 + b^2c^2$  is divisible by  $d^2$ .

Hence if  $(a^{6k-2} + b^{6k-2} + c^{6k-2})$  is divisible by  $d^2$ ,  $(a^{6(k+1)-2} + b^{6(k+1)-2} + c^{6(k+1)-2})$  as well.

**Part c**

For  $n = 1$  we must prove that:

$a^2 + b^2 + c^2$  is divisible by  $d$ , which is true according to the statement.

$$(a^{2^n} + b^{2^n} + c^{2^n})^2 = a^{2^{n+1}} + b^{2^{n+1}} + c^{2^{n+1}} + 2((ab)^{2^n} + (ac)^{2^n} + (bc)^{2^n})$$

$$a + b = c$$

$$a^2 + 2ab + b^2 = c^2$$

On the other hand  $a^2 + b^2 + c^2$  is divisible by  $p$ .

From above results, we have that  $2ab \equiv 2c^2 \pmod{p}$ .

Thus,  $ab \equiv c^2 \pmod{d}$ , since  $p$  is odd. Similarly, it is easy to verify that  $ac \equiv -b^2 \pmod{d}$  and that  $bc \equiv -a^2 \pmod{d}$ .

Using the above results we have:

$$(a^{2^k} + b^{2^k} + c^{2^k})^2 \equiv a^{2^{k+1}} + b^{2^{k+1}} + c^{2^{k+1}} + 2((c^2)^{2^k} + (b^2)^{2^k} + (a^2)^{2^k}) \pmod{d}$$

$$(a^{2^k} + b^{2^k} + c^{2^k})^2 \equiv a^{2^{k+1}} + b^{2^{k+1}} + c^{2^{k+1}} + 2(a^{2^{k+1}} + b^{2^{k+1}} + c^{2^{k+1}}) \pmod{d}$$

$$(a^{2^k} + b^{2^k} + c^{2^k})^2 \equiv 3(a^{2^{k+1}} + b^{2^{k+1}} + c^{2^{k+1}}) \pmod{d}$$

It means that if the property is true for  $n = k$ , then for  $n = k + 1$  is true as well, since  $d$  is not divisible by 3.

For an alternative proof, note that if  $a$  and  $d$  have common prime factors, then  $b$  and  $a + b$  also have those common factors. Hence, factoring out the common factors, we get a similar expression with  $a_1$  and  $b_1$  relatively prime to  $d_1$ , where  $d_1$  is equal to  $d$  divided by the mentioned factors. So the integer  $a_1$  has an inverse modulo  $d_1$ . Let it be  $a_1^{-1}$ . Hence the original statement is equivalent to prove that:  $1 + (a_1^{-1}b_1)^{2^n} + (1 + a_1^{-1}b_1)^{2^n}$  is divisible by  $d_1$ . Moreover, it is easy to see that the following congruences hold:

$$(1 + a_1^{-1}b_1)^2 \equiv a_1^{-1}b_1 \pmod{d_1}$$

$$(a_1^{-1}b_1)^2 \equiv -(1 + a_1^{-1}b_1) \pmod{d_1}$$

Use these results to give an inductive proof.

**Part d**

For  $n = 1$  the property is true (see part (b)).

Suppose that the statement is true, for some integer  $k$ , this implies that:

$$\begin{aligned}
a^{4^k} + b^{4^k} &\equiv -c^{4^k} \pmod{d^2} \\
(a^{4^k} + b^{4^k})^2 &\equiv (c^{4^k})^2 \pmod{d^2} \\
(a^{4^k})^2 + 2a^{4^k}b^{4^k} + (b^{4^k})^2 &\equiv (c^{4^k})^2 \pmod{d^2} \\
(a^{4^k})^2 + (b^{4^k})^2 - (c^{4^k})^2 &\equiv -2a^{4^k}b^{4^k} \pmod{d^2} \\
a^{4^{k+1}} + b^{4^{k+1}} + c^{4^{k+1}} + 2((a^{4^k})^2(b^{4^k})^2 - (a^{4^k})^2(c^{4^k})^2 - (b^{4^k})^2(c^{4^k})^2) &\equiv 4(a^{4^k})^2(b^{4^k})^2 \pmod{d^2} \\
a^{4^{k+1}} + b^{4^{k+1}} + c^{4^{k+1}} - 2((a^{4^k})^2(b^{4^k})^2 + (a^{4^k})^2(c^{4^k})^2 + (b^{4^k})^2(c^{4^k})^2) &\equiv 0 \pmod{d^2} \tag{3a}
\end{aligned}$$

On the other hand,  $(a^{4^k})^2 + (b^{4^k})^2 + (c^{4^k})^2$  is divisible by  $d$  as a corollary of the property proved in part (c). Hence

$$((a^{4^k})^2 + (b^{4^k})^2 + (c^{4^k})^2)^2 = a^{4^{k+1}} + b^{4^{k+1}} + c^{4^{k+1}} + 2((a^{4^k})^2(b^{4^k})^2 + (a^{4^k})^2(c^{4^k})^2 + (b^{4^k})^2(c^{4^k})^2) \tag{4}$$

Combining (3a) and (4) we have that  $a^{4^{k+1}} + b^{4^{k+1}} + c^{4^{k+1}}$  is divisible by  $d^2$  and the result follows by induction.

The condition  $d$  not divisible by 3, is not necessary since the statements are also true for  $d$  divisible by 3. The reason to include the just mentioned condition is only for simplifying the inductive proof of part (c).

The property found by Naoki Sato in solving Problem 32 can be used to give an alternative solution for parts (a) and (b). Note also that the expressions indicated in parts (a) and (b) satisfy the conditions given in Problem 27. Hence, we can prove part (a), then part (d) and using result from Problem 27, prove part (b).

**Solution Problem 6:****Part a**

Proposed.

**Part b**

For  $n = 2$  we must prove that:

$$\begin{aligned}
F(2)^2 + F(2+1)^2 &= F(2 \cdot 2 + 4) - F(2 \cdot 2 - 3) \\
F(2)^2 + F(3)^2 &= F(8) - F(1)
\end{aligned}$$

Which is equivalent to prove that:

$6^2 + 7^2 = 86 - 1$ , i.e.  $36 + 49 = 85$ , which is clearly true.

Note that:

$$\sum_{i=1}^k F(i)^2 = F(k)F(k+1) - 5 \tag{5a}$$

$$\sum_{i=1}^{k+1} F(i)^2 = F(k+1)F(k+2) - 5 \tag{5b}$$

Adding (5a) and (5b) we have:

$$\begin{aligned}
F(1)^2 + \sum_{i=1}^k (F(i)^2 + F(i+1)^2) &= F(k+1)(F(k) + F(k+2)) - 10 \\
&= (F(k+2) - F(k))(F(k) + F(k+2)) - 10 \\
&= F(k+2)^2 - F(k)^2 - 10
\end{aligned}$$

On the other hand:

$$\begin{aligned}
F(k+1)^2 + F(k+2)^2 &= (F(k)^2 + F(k+1)^2) + (F(k+2)^2 - F(k)^2) \\
&= \sum_{i=1}^k (F(i)^2 + F(i+1)^2) + (F(k)^2 + F(k+1)^2) + 1^2 + 10 \\
&= F(1)^2 + F(2)^2 + \sum_{i=2}^k (F(i)^2 + F(i+1)^2) + 2(F(k)^2 + F(k+1)^2) + 1^2 + 10
\end{aligned}$$

Using the inductive hypothesis corresponding to the strong induction principle and replacing the values for  $F(1)$  and  $F(2)$  we have:

$$\begin{aligned}
F(k+1)^2 + F(k+2)^2 &= 1 + 36 + \sum_{i=2}^k (F(2i+4) - F(2i-3)) + (F(2k+4) - F(2k-3)) + 11 \\
&= \sum_{i=2}^k (F(2i+5) - F(2i+3)) - F(1) + \sum_{i=3}^k (F(2i-2) - F(2i-4)) \\
&\quad + (F(2k+4) - F(2k-3)) + 48 \\
&= (F(2k+1) - F(7)) - (F(2k) - F(2)) + (F(2k+4) + F(2k-3)) + 48 - F(1) \\
&= (F(2k+5) - 53) - (F(2k-2) - 6) + F(2k+4) - F(2k-3) + 48 - 1 \\
&= F(2k+5) - (2k-2) + F(2k+4) - F(2k-3) \\
&= (F(2k+4) + F(2k+5)) - (F(2k-3) + F(2k-2)) \\
&= F(2k+6) - F(2k-1) \\
&= F(2(k+1) + 4) - F(2(k+1) - 3)
\end{aligned}$$

Thus, by mathematical induction, the property is true for all integer  $n$  greater than 1.

**Solution Problem 7:** Let:

$$F(n) = \sum_{k=1}^n k^{2^n}$$

For  $n = 1$  we have:  $F(1) = \frac{p(p+1)(2p+1)}{6}$ , which is divisible by  $2p+1$ , since 6 cannot divide  $2p+1$  (prime greater than 3).

Suppose that the property is true for  $n = k$ . We will prove that is true for  $n = k+1$  as well.

**Proof 1**

Let  $r_i$  be the remainder of the division of  $i^2$  by  $2p+1$ . Let  $R_i$  be equal to  $r_i$ , if  $r_i$  is smaller or equal to  $p$ ; and  $R_i$  equal to  $2p+1 - r_i$  if  $r_i$  is greater than  $p$ .

Therefore  $i^2 \equiv \pm R_i \pmod{(2p+1)}$ . Using the binomial theorem we have:

$$\sum_{i=1}^p i^{2^{k+1}} = \sum_{i=1}^p i^{2(2)^k} \equiv \sum_{i=1}^p R_i^{2^k} \pmod{2p+1}$$

Now we need to prove that the  $R_i$ 's are all different.

Let  $a, b$  be positive integers smaller than or equal to  $p$ .

$$a^2 \equiv \pm R_a \pmod{(2p+1)}$$

$$b^2 \equiv \pm R_b \pmod{(2p+1)}$$

We suppose that  $R_a = R_b = R$  with  $a$  distinct from  $b$ :

Case 1: Suppose same sign in front of  $R$ . Suppose a plus sign. In the case of a minus sign the proof is similar.

$$a^2 \equiv R \pmod{(2p+1)} \quad (6a)$$

$$b^2 \equiv R \pmod{(2p+1)} \quad (6b)$$

Subtracting (6b) from (6a), we have:

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

The above result implies that  $2p+1$  divides  $a-b$  or  $a+b$ , since  $2p+1$  is prime. But neither  $a-b$  nor  $a+b$  are divisible by  $2p+1$ ,  $a$  and  $b$  are smaller or equal to  $p$  and therefore the absolute value of their difference is minor than  $2p+1$  and cannot either be zero, since  $a$  is different from  $b$ .

On the other hand,  $a+b$  also is smaller than  $2p+1$ , because the maximum value of  $a+b$  is obtained when one of the values is  $p$  and the other  $p-1$ , i.e. when their sum is  $2p-1$ .

Thus, if there exist such  $a$  and  $b$ , the  $R$ 's cannot have the same sign in front of them.

Case 2: Suppose opposite sign. Without loss of generality, we assume that the minus sign is associated to the remainder of  $b^2$ . The opposite case is similar.

$$a^2 \equiv R \pmod{(2p+1)} \quad (7a)$$

$$b^2 \equiv -R \pmod{(2p+1)} \quad (7b)$$

Recalling that  $p$  is odd and raising both sides of the congruences (7a) and (7b) to the power  $p$  we get:

$$\begin{aligned} a^{2p} &\equiv R^p \pmod{(2p+1)} \\ b^{2p} &\equiv -R^p \pmod{(2p+1)} \\ a^{2p} - 1 &\equiv R^p - 1 \pmod{(2p+1)} \\ b^{2p} - 1 &\equiv -R^p - 1 \pmod{(2p+1)} \end{aligned}$$

The previous results imply that  $R^p - 1$  and  $-R^p - 1$  are divisible by  $2p+1$  (using Fermat's little theorem) and therefore their sum as well, but their sum is  $-2$ , i.e. if we suppose that  $R_a = R_b = R$ , with  $a$  distinct from  $b$ , it implies that  $-2$  is divisible by  $2p+1$ , which is a contradiction. Therefore if  $a$  is different from  $b$ , it implies that  $R_a$  is different from  $R_b$ .

Since the  $R_i$ 's are all different and moreover from the definition of  $R_i$ , we deduce that:

$$\sum_{i=1}^p R_i^{2^k} = \sum_{i=1}^p i^{2^k} \quad (8)$$

So  $F(k+1) \equiv F(k) \pmod{(2p+1)}$ . Hence if  $F(k)$  is divisible by  $2p+1$ ,  $F(k+1)$  as well.

## Proof 2

$$(F(k))^2 = F(k+1) + 2 \sum_{i=1}^{p-1} \sum_{j=i+1}^p (ij)^{2^k} \quad (9)$$

Let  $r_{ij}$  be the remainder when  $ij$  is divided by  $2p+1$ .

Let  $R_{ij}$  be equal to  $r_{ij}$ , if  $r_{ij}$  is smaller than or equal to  $p$  and  $R_{ij}$  equal to  $2p+1 - r_{ij}$  if  $r_{ij}$  is greater than  $p$ .

Therefore  $(ij) \equiv \pm R_{ij} \pmod{(2p+1)}$ .

$$(F(k))^2 \equiv F(k+1) + 2 \sum_{i=1}^{p-1} \sum_{j=i+1}^p (R_{ij})^{2^k} \pmod{(2p+1)} \quad (10a)$$

$$(F(k))^2 \equiv F(k+1) + 2 \sum_{r=1}^p c_r \cdot r^{2^k} \pmod{(2p+1)} \quad (10b)$$

Where  $c_r$  is the number of times the integer  $r$  appears in the double summation shown in (10a).

$$\sum_{r=1}^p c_r = \frac{p(p-1)}{2} \quad (11)$$

Several forms exist to prove the previous statement, but I think that the easiest is the following: The expansion of  $(F(k))^2$  in the equality (10a) has  $p^2$  terms. The right hand side of the equality has  $p$  terms (corresponding to  $F(k)$ ) more twice the number of terms looked for. Solving this equation yields the result sought.

We are going to prove that  $c_r \leq \frac{p-1}{2}$ , which is equivalent to prove that given the first  $p$  positive integers, we can form at the most  $\frac{p-1}{2}$  pairs of numbers  $d$  and  $e$  such that  $d \cdot e \equiv \pm r \pmod{2p+1}$ .

We know that  $p$  is odd, therefore  $p-1$  is even. Hence with the first  $p$  positive integers we can form at most  $\frac{p-1}{2}$  pairs without repeating numbers. In order to be able to form more pairs we must occupy the number not used and use again a number already used. But do the latter or to form a pair with another combination with two numbers previously occupied would imply the following:

$$d \cdot e \equiv \pm r \pmod{2p+1} \quad (12)$$

$$d \cdot f \equiv \pm r \pmod{2p+1} \quad (13)$$

with  $f$  different from  $e$

We have two cases: either same sign in front of  $r$ , or opposite sign.

If they have the same sign, we can subtract (12) from (13) getting:

$$d(f-e) \equiv 0 \pmod{2p+1}$$

If they have opposite sign, we can add (12) to (13) getting:

$$d(f+e) \equiv 0 \pmod{2p+1}$$

The above results imply that  $2p+1$  divides  $d$ ,  $f-e$  or  $f+e$ , since  $2p+1$  is prime. But  $d$  is not divisible by  $2p+1$ , since it is a positive integer smaller than  $2p+1$  and neither  $f-e$  nor  $f+e$  can be divisible by  $2p+1$ ,  $f$  and  $e$  are smaller than or equal to  $p$  and therefore the absolute value of their difference is minor than  $2p+1$  and cannot either be zero, since  $f$  is distinct from  $e$ .

On the other hand,  $f+e$  also it is smaller than  $2p+1$ , because the maximum value of  $f+e$  is obtained when one of the values is  $p$  and the other  $p-1$ , i.e. when their sum is  $2p-1$ .

Hence, to assume that we can form more than  $\frac{p-1}{2}$  pairs lead to a contradiction. So we can form at most  $\frac{p-1}{2}$  pairs.

Hence we can deduce that  $c_i \leq \frac{p-1}{2}$  for  $i = 1, \dots, p$ , but each  $c_r$  satisfies the equality (11). So the only possible value for  $c_r$  for  $r = 1, \dots, p$  is  $\frac{p-1}{2}$ , since otherwise the equality not holds.

From the previous result we conclude that:

$$\begin{aligned} (F(k))^2 &\equiv (F(k+1) + (p-1)F(k)) \pmod{2p+1} \\ F(k+1) &\equiv -F(k)(F(k) - p + 1) \pmod{2p+1} \end{aligned}$$

Therefore if  $F(k)$  is divisible by  $2p+1$ ,  $F(k+1)$  as well.

### Proof 3

Let  $a$  be a positive integer smaller than or equal to  $p$ , and greater than 1, prove that:  $(a^{2^k} - 1) \sum_{i=1}^p i^{2^n}$  is divisible by  $2p+1$ . Then prove that  $(a^{2^k} - 1)$  can be factored as the product of sum of squares by  $(a-1)(a+1)$ .

Then prove that  $2p+1$  cannot divide the sum of two squares (See Proof 1) and deduce it asked for.

**Hints in order to prove a more general property:**

Now we will give hints to prove that  $\sum_{i=1}^p i^{2n}$  is divisible by  $2p+1$ , except for  $n$  multiple of  $p$ . Note that the property just proved is a special case of this more general property.

We will consider the first  $p$  cases, since:

$$\sum_{i=1}^p i^{2(n+p)} \equiv \sum_{i=1}^p i^{2n} \pmod{(2p+1)}$$

The above expression is a direct result from Fermat's little theorem.

On the other hand, using the just mentioned theorem, it is easy to prove that for  $n$  multiple of  $p$ :  $\sum_{i=1}^p i^{2n}$  is of the form  $(2p+1)m+p$  and therefore is not divisible by  $2p+1$ .

Prove that:

$$\left(\sum_{i=1}^p i^{2n}\right)\left(\sum_{i=1}^p i^{2n} - p\right) \equiv 0 \pmod{(2p+1)} \quad (14)$$

Then, to prove that:

$$\left(\sum_{i=1}^p i^2 + \sum_{i=1}^p i^4 + \dots + \sum_{i=1}^p i^{2(p-1)}\right) \equiv 0 \pmod{(2p+1)} \quad (15)$$

Use the following trick: Rearrange the terms forming geometric progressions.

From (14), we deduced that  $\sum_{i=1}^p i^{2n}$  is divisible by  $2p+1$  or  $(\sum_{i=1}^p i^{2n}) - p$  is divisible by  $2p+1$ .

Therefore:

$$\sum_{i=1}^p i^{2n} \equiv c_n p \pmod{2p+1} \quad (\text{Where } c_n \text{ is 0 or 1.})$$

Replacing the above congruence in the result (15), we have that:  $(c_1 + c_2 + \dots + c_{p-1})p$  is divisible by  $2p+1$ .

Hence:  $(c_1 + c_2 + \dots + c_{p-1})$  is divisible by  $2p+1$ , since  $2p+1$  is prime.

The expression  $(c_1 + c_2 + \dots + c_{p-1})$  ranges from 0 to  $p-1$ , and thus the only possible value for this sum is 0, since otherwise  $(c_1 + c_2 + \dots + c_{p-1})$  is not divisible by  $2p+1$ .

Therefore  $\sum_{i=1}^p i^{2n}$  is divisible by  $2p+1$  for  $n = 1, 2, \dots, p-1$ .

### Hint Problem 8:

For  $n = 1$  we must to prove that  $4p+1$  divides  $\sum_{i=1}^p a_i^2$

### Proof 1

Let  $b$  be a positive integer so that  $b$  is smaller than or equal to  $2p$  and has the property:  $b^{2p} + 1$  is divisible by  $4p+1$ .

$$b^2 \sum_{i=1}^p a_i^2 = \sum_{i=1}^p (b \cdot a_i)^2$$

Let  $b_i$  be the remainder of the division of  $(b \cdot a_i)$  by  $4p+1$ . Let  $B_i$  be equal to  $b_i$ , if  $b_i$  is smaller or equal to  $2p$ ; and  $B_i$  equal to  $(4p+1) - b_i$ , if  $b_i$  is greater than  $2p$ . Therefore  $(b \cdot a_i) \equiv \pm B_i \pmod{4p+1}$ .

Subsequently, to prove that the  $B_i$ 's are all different, they are elements of the set formed by the first  $2p$  positive integers and that they have the property:  $B_i^{2p} + 1$  is divisible by  $4p+1$ .

So:

$$b^2 \sum_{i=1}^p a_i^2 \equiv \sum_{i=1}^p B_i^2 \pmod{(4p+1)}$$

and hence

$$(b^2 \sum_{i=1}^p a_i^2 + \sum_{i=1}^p a_i^2) \equiv (\sum_{i=1}^p B_i^2 + \sum_{i=1}^p a_i^2) \pmod{(4p+1)}$$

Note that  $(\sum_{i=1}^p B_i^2 + \sum_{i=1}^p a_i^2)$  is the summation of the first  $2p$  positive integers, i.e.  $\frac{(2p(2p+1)(4p+1))}{6}$ , which is divisible by  $(4p+1)$ , since  $4p+1$  is not divisible by 6 ( $4p+1$  is a prime number greater than 3).

Therefore:

$$(b^2 + 1) \sum_{i=1}^p a_i^2 \equiv 0 \pmod{4p+1}$$

We can select  $b_r$  and  $b_s$  ( $b_r$  distinct from  $b_s$ ) so that at the most one of them has the property:  $(b^2 + 1)$  is divisible by  $(4p+1)$ . Prove it and complete the proof.

**Proof 2**

To parallel proof 1, but choosing an  $a$  so that  $a^{2p} - 1$  is divisible by  $(4p+1)$  ( $a$  distinct from 1).

For the rest of the proof, see solution to Problem 7.

**Hint Problem 9:**

Consider the quadratic residues of 13. Moreover, it is easy to prove that  $4^{2n-1} + 9^{2n-1}$  is divisible by 13.

**Hint Problem 10:**

Prove that  $8^{2^n} - 5^{2^n}$  is divisible by 13 and is not divisible by  $13^2$ . Let  $F(n)$  be  $8^{2^n} - 5^{2^n}$ . Note that:

$$F(k+1) = F(k)(F(k) + 2 \cdot 5^{2^k})$$

**Hint Problem 11:**

See hint to Problem 1.

**Hint Problem 12:**

Guess and prove that for every positive integer  $n$ :

$$f(a + n \cdot b) \equiv k^n f(a) \pmod{p}.$$

Then to use Euler's theorem.

**Hint Problem 13:**

Let:

$$f(n) = 1 + 2^{4n+2} + 3^{4n+2} + 4^{4n+2} + 5^{4n+2} + 6^{4n+2}$$

Note that:

$$\begin{aligned} f(k) &= (1 + 5^{2(2k+1)}) + (2^{2(2k+1)} + 3^{2(2k+1)}) + (4^{2(2k+1)} + 6^{2(2k+1)}) \\ &= (1 + 5^{2(2k+1)}) + (2^{2(2k+1)} + 3^{2(2k+1)}) + 2^{2(2k+1)}(2^{2(2k+1)} + 3^{2(2k+1)}) \\ &= (1 + 5^{2(2k+1)}) + (1 + 2^{2(2k+1)})(2^{2(2k+1)} + 3^{2(2k+1)}) \end{aligned}$$

Then to prove that  $(1 + 5^{2(2n+1)})$  and  $(2^{2(2n+1)} + 3^{2(2n+1)})$  are divisible by 13.

Another solution is to divide the original problem into three problems:  $n$  of the form  $3m$ ,  $n$  of the form  $3m-1$  and  $n$  of the form  $3m-2$ .

**Hint Problem 14:**

Let  $f(n) = (2(3^{4n+3} + 4^{4n+3}) - 25n^2 + 65n + 68)$ .

Consider  $f(n+1) - 34f(n)$ . For another solution to use hint to Problem 1.

**Hint Problem 15:**

Let:

$$F(n) = (2^{2^n} + 3^{2^n} + 5^{2^n})$$

Note that

$$\begin{aligned} F(k+2) &= (2^{2^{k+2}} + 3^{2^{k+2}} + 5^{2^{k+2}}) \\ &= ((2^4)^{2^k} + (3^4)^{2^k} + (5^4)^{2^k}) \\ &= (16^{2^k} + 81^{2^k} + 625^{2^k}) \\ &= ((19-3)^{2^k} + (19 \cdot 4 + 5)^{2^k} + (19 \cdot 33 - 2)^{2^k}) \end{aligned}$$

Using binomial theorem, we have that:  $F(n+2) \equiv F(n) \pmod{19}$

In order to complete the proof to divide the original problem into two problems: odd  $n$  and even  $n$ . Also we can prove that  $(F(n) + F(n+1))$  is divisible by 19 and then to deduce that  $F(n)$  is divisible by 19. See hint to Problem 2.

**Solution Problem 16:**

For  $n = 1$  we must prove that:  $g(1) = (f(1) + f(2))(2a - 1) \cdot a^0$

In effect:

$$\begin{aligned} g(1) &= f(3) + af(2) + (a-1)f(1) \\ &= (a-1)f(2) + af(1) + af(2) + (a-1)f(1) \\ &= (2a-1)(f(1) + f(2)) = (2a-1)(f(1) + f(2)) \cdot a^0 \end{aligned}$$

**Proof 1**

$$\begin{aligned} g(k+1) &= f(k+3) + af(k+2) + (a-1)f(k+1) \\ a \cdot g(k) &= af(k+2) + a^2f(k+1) + a(a-1)f(k) \end{aligned}$$

Hence:

$$\begin{aligned} g(k+1) - a \cdot g(k) &= \\ &= f(k+3) + af(k+2) + (a-1)f(k+1) - af(k+2) - a^2f(k+1) - a(a-1)f(k) \\ &= f(k+3) - (a^2 - a + 1)f(k+1) - a(a-1)f(k) \end{aligned}$$

But

$$\begin{aligned} f(k+3) &= (a-1)f(k+2) + af(k+1) \\ &= (a-1)((a-1)f(k+1) + af(k)) + af(k+1) \\ &= ((a-1)^2 + a)f(k+1) + a(a-1)f(k) \\ &= (a^2 - a + 1)f(k+1) + a(a-1)f(k) \end{aligned}$$

Therefore:  $f(k+3) - (a^2 - a + 1)f(k+1) - a(a-1)f(k) = 0$ , and therefore  $g(n+1) - a \cdot g(n) = 0$  which is equivalent to  $g(n+1) = a \cdot g(n)$

Applying the inductive hypothesis we have:

$$\begin{aligned} g(k+1) &= a \cdot (f(1) + f(2)) \cdot (2a-1) \cdot a^{(k-1)} \\ &= (f(1) + f(2)) \cdot (2a-1) \cdot a^{((k+1)-1)} \end{aligned}$$

### Proof 2

$$\begin{aligned} g(k) &= f(k+2) + af(k+1) + (a-1)f(k) \\ &= (a-1)f(k+1) + af(k) + af(k+1) + (a-1)f(k) \\ &= (2a-1)(f(k) + f(k+1)) \end{aligned}$$

Therefore, we can prove that

$$(f(k) + f(k+1)) = (f(1) + f(2))a^{(k-1)} \quad (16)$$

For  $n=1$  is clear that  $(f(1) + f(2)) = (f(1) + f(2))a^{(1-1)}$

We know that  $f(k+2) = (a-1)f(k+1) + af(k)$ . Adding  $f(k+1)$  to both sides of the equation (16), we have that:

$$f(k+2) + f(k+1) = a(f(k+1) + f(k))$$

Applying the inductive hypothesis we have that:

$$\begin{aligned} f(k+2) + f(k+1) &= a(f(1) + f(2)) \cdot a^{(k-1)} \\ f((k+1)+1) + f(k+1) &= (f(1) + f(2)) \cdot a^{((k+1)-1)} \end{aligned}$$

### Solution Problem 17:

For  $n=1$  we have:  $f(3 \cdot 1) + f(3 \cdot 1 + 1) = f(3) + f(4)$

$$f(3) = 3(1+1) + 1 = 7$$

$$f(4) = 3(7+1) + 1 = 25$$

Hence:  $f(3) + f(4) = 7 + 25 = 32$ , which is divisible by 32.

$$\begin{aligned} f(3(k+1)) + f(3(k+1)+1) &= f(3k+3) + f(3k+4) \\ &= f(3k+3) + 3(f(3k+3) + f(3k+2)) + 1 \\ &= 4f(3k+3) + 3f(3k+2) + 1 \\ &= 4(3(f(3k+2) + f(3k+1)) + 1) + 3f(3k+2) + 1 \\ &= 15f(3k+2) + 12f(3k+1) + 5 \\ &= 15(3(f(3k+1) + f(3k)) + 1) + 12f(3k+1) + 5 \\ &= 12f(3k+1) + 20 + 45(f(3k+1) + f(3k)) \\ &= 4(3f(3k+1) + 5) + 45(f(3k+1) + f(3k)) \end{aligned}$$

If we prove that  $3f(3k+1) + 5$  is divisible by 8, we can complete the proof.

For  $k=1$ , we must prove that:  $3f(3 \cdot 1 + 1) + 5$  is divisible by 8.  $3f(4) + 5 = 3 \cdot 25 + 5 = 80$ , which is

clearly divisible by 8.

$$\begin{aligned}
3f(3(k+1)+1)+5 &= 3f(3k+4)+5 \\
&= 3(3(f(3k+3)+f(3k+2))+1)+5 \\
&= 3(3(3(f(3k+2)+f(3k+1))+1+f(3k+2))+1)+5 \\
&= 3(12f(3k+2)+9f(3k+1)+4)+5 \\
&= 36f(3k+2)+27f(3k+1)+17 \\
&= 36f(3k+2)+9(3f(3k+1)+5)-28 \\
&= 4(9f(3k+2)-7)+9(3f(3k+1)+5)
\end{aligned}$$

We would need to prove that  $(9f(3k+2)-7)$  is divisible by 2, or that  $(f(3k+2)-1)$  is divisible by 2.

We will prove that  $(f(3k+2)-1)$  is divisible by 2.

For  $k=1$ , we must prove that:  $f(3 \cdot 1 + 2) - 1$  is divisible by 2.  $f(5) - 1 = 97 - 1 = 96$ , which clearly is divisible by 2.

$$\begin{aligned}
f(3(k+1)+2)-1 &= f(3k+5)-1 \\
&= 3(f(3k+4)+f(3k+3))+1-1 \\
&= 3(3(f(3k+3)+f(3k+2))+1+f(3k+3)) \\
&= 12f(3k+3)+9f(3k+2)+3 \\
&= 12(f(3k+3)+1)+9(f(3k+2)-1)
\end{aligned}$$

So if  $f(3k+2)-1$  is divisible by 2,  $f(3(k+1)+2)-1$  as well.

Therefore  $(9f(3k+2)-7)$  is divisible by 2, with which we can complete the proof of that  $3f(3k+1)+5$  is divisible by 8 and hence to finish proving that for all positive integers  $n$ :  $(f(3n)+f(3n+1))$  is divisible by 32.

**Hint Problem 18:**

Prove that  $f(n) \equiv n \cdot f(1) \pmod{p^2}$ , using hint to Problem 20 (but base cases are 0 and 1). Then to prove that  $f(100)$  is divisible by  $p^2$  and that  $f(1)$  is divisible by  $p^2$ .

**Hint Problem 19:**

See hint to Problem 1.

**Hint Problem 20:**

Use the following form of induction:

1. The property is true for  $n=1$  and  $n=2$ .
2. Show that for all integers  $k \geq 1$ , if the property is true for  $n=k$  and  $n=k+1$ , then it is true for  $n=k+2$ .

**Hint Problem 21:**

Note that we must determine  $S_1(n)$ ,  $S_2(n)$ ,  $S_3(n)$ ,  $S_4(n)$  and  $S_5(n)$  such that:

$$F(S_1(n)) + F(S_1(n)) = F(S_3(n))(F(S_4(n)) + F(S_5(n)))$$

Consider a few values of  $n$  and take the successive differences for each  $S_i(n)$ . Use Binet's formula.

**Hint Problem 22:** See hint to Problem 21.

**Hint Problem 23:**

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

Prove that  $f(n) \equiv ((1-n)f(0) + nf(1)) \pmod{p^2}$  for  $n \geq 0$ . Use the following form of induction:

1. The property is true for  $n = 0$  and  $n = 1$ .

2. If the property is true for  $n = k$  and  $n = k + 1$ , then the property is true for  $n = k + 2$ .

Let  $g(k) = a^{(6k-2)} + b^{(6k-2)} + (a+b)^{(6k-2)}$ . From Problem 5(b), we know that  $g(k)$  is divisible by  $p^2$  for every positive integer  $k$ . In particular for  $k = 1$  and  $k = p$ , but notice that  $g(1) = f(0)$  and  $g(p) = f(6)$ . Hence  $f(0)$  and  $f(6)$  are both divisible by  $p^2$ . So  $f(6) \equiv 6f(1) \pmod{p^2}$ , then  $f(1)$  is divisible by  $p^2$  ( $p$  is relatively prime to 6) and therefore  $f(n) \equiv 0 \pmod{p^2}$  for each integer  $n \geq 0$ .

**Hint Problem 24:**

See hint to Problem 7 and use the following result:  $a^2 - ab + b^2$  and  $a^2 + ab + b^2$  are divisible only by primes of the form  $6k + 1$  or by 3 ( $a$  relatively prime to  $b$ ).

**Hint Problem 25:**

Show that:  $\sum_{i=1}^n F(i)^2 = F(n)F(n+1)$  and see solution to Problem 6. For another solution to use Binet's formula.

**Hint Problem 26:**

Consider separately the cases when  $n$  is even and when  $n$  is odd, and use the following:

$$\begin{aligned} F(n+10) &= 55F(n+1) + 34F(n) \\ F(n+10) &= 11(5F(n+1) + 3F(n)) + F(n) \end{aligned}$$

**Hint Problem 27:**

Let:

$$F_i(n) = (n-0) \dots (n-(i-1))(n-(i+1)) \dots (n-(d-1))$$

Prove that:

$$F(n) \equiv \frac{F_0(n)F(0)}{F_0(0)} + \frac{F_1(n)F(1)}{F_1(1)} + \dots + \frac{F_{d-1}(n)F(d-1)}{F_{d-1}(d-1)} \pmod{p^d}$$

(Note that for  $d = 2$ ,  $F(n) \equiv ((1-n)F(0) + nF(1)) \pmod{p^2}$  and for  $d = 3$ ,  $F(n) \equiv (\frac{(n-1)(n-2)}{2}F(0) - n(n-2)F(1) + \frac{n(n-1)}{2}F(2)) \pmod{p^3}$ )

Use the form of induction that is indicated next:

1. The property holds for all  $n = 0, 1, \dots, d-1$

2. If the property holds for  $n = k, n = k + 1, \dots, n = k + d - 1$ , then the property holds for  $n = k + d$ .

It is easy to see that for  $n = 0$   $F(0) \equiv F(0) \pmod{p^d}$ , for  $n = 1$   $F(1) \equiv F(1) \pmod{p^d}, \dots$ , for  $n = i$   $F(i) \equiv F(i) \pmod{p^d}, \dots$ , and for  $n = d-1$ :  $F(d-1) \equiv F(d-1) \pmod{p^d}$ . Hence the property is true for  $n = 0, n = 1, n = 2, \dots, n = d-1$ .

For the inductive step note that:

$$g(k) = \frac{F_0(k)F(0)}{F_0(0)} + \frac{F_1(k)F(1)}{F_1(1)} + \dots + \frac{F_{d-1}(k)F(d-1)}{F_{d-1}(d-1)}$$

Is a polynomial in the indeterminate  $k$  of degree at most  $d-1$ . Therefore from calculus of finite differences we have:

$$\sum_{i=0}^d \binom{d}{i} (-1)^{d-i} g(k+i) = 0$$

Complete this part of the proof using the fact that:

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

If  $F(a_0), F(a_1), \dots, F(a_{d-1})$  are divisible by  $p^d$ , we have the following system:

$$\begin{aligned} \frac{F_0(a_0)F(0)}{F_0(0)} + \frac{F_1(a_0)F(1)}{F_1(1)} + \dots + \frac{F_{d-1}(a_0)F(d-1)}{F_{d-1}(d-1)} &= c_0 p^d \\ \frac{F_0(a_1)F(0)}{F_0(0)} + \frac{F_1(a_1)F(1)}{F_1(1)} + \dots + \frac{F_{d-1}(a_1)F(d-1)}{F_{d-1}(d-1)} &= c_1 p^d \\ &\vdots \\ \frac{F_0(a_{d-1})F(0)}{F_0(0)} + \frac{F_1(a_{d-1})F(1)}{F_1(1)} + \dots + \frac{F_{d-1}(a_{d-1})F(d-1)}{F_{d-1}(d-1)} &= c_{d-1} p^d \end{aligned}$$

By Cramer's rule  $F(i) = \frac{\det(A_i)}{\det(A)}$ ,  $p^d$  is factor of  $\det(A_i)$  (also it may be proved that  $\frac{F_i(n)}{F_i(i)}$  is an integer for  $i = 0, \dots, (d-1)$  using the same form of induction indicated above). On the other hand it can be proved that  $\det(A)$  has the factors  $(a_i - a_j)$  with  $i$  different from  $j$ . The remaining factor of  $\det(A)$  is a constant that can be calculated evaluating  $a_0 = 0, \dots, a_{d-1} = d-1$  (the constant is a unit fraction). We know that  $F(i)$  is integer, hence:

If  $F(a_0), F(a_1), \dots, F(a_{d-1})$  are divisible by  $p^d$  where  $(a_i - a_j)$  is not divisible by  $p$  for  $i$  different from  $j$ , then  $F(i)$  is divisible by  $p^d$  for  $i = 0, \dots, (d-1)$ . So  $F(n) \equiv 0 \pmod{p^d}$ .

**Hint Problem 28:**

Note that  $G_{n+2}(a) \equiv (G_{n+1}(a) + G_n(a)) \pmod{a^2 - a - 1}$  (Congruence modulo a polynomial)

Prove that:  $G_n(a) \equiv (F(n-1)G_0(a) + F(n)G_1(a)) \pmod{a^2 - a - 1}$

Use the following form of induction:

1. The property is true for  $n = 0$  and  $n = 1$ .
2. Show that for all integer  $k \geq 0$ , if the property is true for  $n = k$  and  $n = k + 1$ , then the property is true for  $n = k + 2$ .

Then show that  $G_0(a) = G_{11}(a) = 0$  (zero polynomial), hence the polynomial  $G_1(a)$  has the factor  $a^2 - a - 1$ , and so:  $G_n(a)$  is divisible by  $a^2 - a - 1$  for every integer non-negative  $n$ . Also it is possible to determine, directly, that:

$$G_1(a) = -(a^2 - a - 1)(a^9 + a^8 + 2a^7 + 3a^6 + 5a^5 + 8a^4 + 13a^3 + 21a^2 + 34a + 55)$$

**Hint Problem 29:**

From Wilson's theorem, it follows that there exists an integer  $a$  so that  $a^2 \equiv -1 \pmod{4k+1}$ . Prove that the integers from 1 to  $2k$  can be arranged into  $k$  pairs such that the sum of the squares of each pair is divisible by  $(4k+1)$ . The result follows from the well-known property:  $x^{2n+1} + y^{2n+1}$  is divisible by  $(x+y)$ .

**Hint Problem 30:**

Prove that  $G(n) \equiv (n(n-1)/2)G(2) \pmod{p^3}$ , then  $G(1001) \equiv 500500 \cdot G(2) \pmod{p^3}$  and conclude.

**Solution Problem 31:**

We can to prove that:

$$\left(\sum_{i=1}^d a_i^n\right) \left(\left(\sum_{i=1}^d a_i^n\right) - d\right) \equiv 0 \pmod{p}$$

Let  $1 \leq i \leq d$ , it is easy prove that the remainders modulo  $p$  of the numbers  $a_1 \cdot a_i, a_2 \cdot a_i, a_3 \cdot a_i, \dots, a_d \cdot a_i$  are all different and they satisfy  $r^d - 1 \equiv 0 \pmod{p}$ . Hence are just  $a_1, a_2, a_3, \dots, a_d$  in some order.

The result follows summing and using binomial theorem. Therefore:  $\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$  where  $c_n$  is 0 or 1.

On the other hand:

$$\left(\sum_{i=1}^d a_i^1 + \sum_{i=1}^d a_i^2 + \dots + \sum_{i=1}^d a_i^{d-1}\right) \equiv 0 \pmod{p}$$

We can rearrange the terms forming geometric progressions (we may assume that  $a_1 = 1$ , since  $1^d \equiv 1 \pmod{p}$ ) and then to use the fact that  $a_i^d \equiv 1 \pmod{p}$ . Hence we have that:  $(c_1 + c_2 + \dots + c_{d-1})d$  is divisible by  $p$ ,  $d$  is relatively prime to  $p$  so the only possible value of  $(c_1 + c_2 + \dots + c_{d-1})$  is zero, since otherwise the expression is not divisible by  $p$ . Therefore we may deduce that  $c_1 = c_2 = \dots = c_{d-1} = 0$  and  $\sum_{i=1}^d a_i^n$  is divisible by  $p$  for  $n = 1, 2, \dots, d-1$ .

$$\sum_{i=1}^d a_i^{n+d} \equiv \sum_{i=1}^d a_i^n \pmod{p}$$

On the other hand, it is easy to prove that for  $n$  multiple of  $d$ :  $\sum_{k=1}^d k^n$  is of the form  $p \cdot m + d$ . Hence  $\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$ , where  $c_n = 1$  if  $n$  is divisible by  $d$  and 0 otherwise.

**Hint Problem 32:**

See Naoki Sato's solution to Problem 32.

For another proof use the following results:

Let  $t(k)$  denote  $a^{6k+4} + b^{6k+4} + c^{6k+4}$ , then  $t(k) = a^4(a^6)^k + b^4(b^6)^k + c^4(c^6)^k$ . Note that  $a^6$ ,  $b^6$  and  $c^6$  are the roots of the polynomial

$$P(x) = x^3 - (a^6 + b^6 + c^6)x^2 + (a^6b^6 + a^6c^6 + b^6c^6)x - a^6b^6c^6$$

hence  $t(k)$  satisfies the recurrence relation:

$$t(k) = (a^6 + b^6 + c^6)t(k-1) - (a^6b^6 + a^6c^6 + b^6c^6)t(k-2) + a^6b^6c^6t(k-3)$$

Given the statement of the problem, the multiplicative inverse of  $a$  modulo  $p^3$  exists. Putting  $x = a^{-1}b$  and gives that  $c = a + b$ , we have:

$$g_{k+3}(x) = (1 + x^6 + (x+1)^6)g_{k+2}(x) - (x^6 + (x+1)^6 + x^6(x+1)^6)g_{k+1}(x) + x^6(x+1)^6g_k(x)$$

Then, using the above relation, prove the Naoki Sato's formula for  $g_k(x)$ , i.e. show that for all integer  $k \geq 0$ ,

$$g_k(x) = Q_k(x)(x^2 + x + 1)^3 + (2k+1)(3k+2)(x^2 + x + 1)^2$$

where  $Q_k(x)$  is a polynomial with integer coefficients. Note that  $x^2 + x + 1$  is factor of both  $x^6 - 1$  and  $(x+1)^6 - 1$ .

To ease the proofs of the base cases, we can obtain another recurrence relation in order to prove the case bases recursively.

Returning to the original problem, we can prove that the property is true for  $n = 0$ ,  $n = 6$  and  $n = 12$ . Hence using the result from Problem 27, the property is true for all  $n \geq 0$ .

**Hint Problem 33:**

Let  $g_k(x)$  be  $(x+1)^{6k+1} - x^{6k+1} - 1$ , then

$$g_k(x) = Q_k(x)(x^2 + x + 1)^3 - k(6k+1)(x^2 + x + 1)^2$$

where  $Q_k(x)$  is a polynomial with integer coefficients.