

Inducción Matemática

José Espinosa
<http://www.math.cl>

Última modificación: 08 de Junio de 2011

1. Problemas de Inducción Matemática.

1. Sea:

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

Mostrar por inducción que $F(n)$ es divisible por p^3 , para todo entero $n \geq 0$ (p es un número primo mayor que 2).

2. La sucesión de Fibonacci está definida por $F(1) = 1$, $F(2) = 1$ y $F(n) = F(n-1) + F(n-2)$, para $n \geq 3$. Usar inducción matemática para probar que:

$1 + 2^{2n} + 3^{2n} + 2((-1)^{F(n)} + 1)$ es divisible por 7 para todo entero positivo n .

3. Sea $F(n)$ el n -ésimo número de Fibonacci. Probar de dos maneras que: $2(2^{2n} + 5^{2n} + 6^{2n}) + 3(-1)^{n+1}((-1)^{F(n)} + 1)$ es divisible por 13 para todo entero positivo n .

4. Supongamos que: $\sum_{i=1}^m a_i$ sea divisible por b^2c^2 y que; $\sum_{i=1}^m a_i^{jbc}$ sea divisible por b^2c^2 , para todo número positivo impar j . (b y c son números primos impares, $b < c$ y $(c-1)$ no es divisible por b , los a_i son primos relativos con respecto a b y c). Sea:

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

Mostrar por inducción que: $F(n)$ es divisible por b^2c^2 , para todo entero no negativo n .

5. Sean a, b, c tres números enteros positivos tales que $c = a + b$. Sea d un factor impar de $a^2 + b^2 + c^2$ (para la parte (c), d no divisible por 3). Mostrar por inducción que para todo entero positivo n :

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

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

c) $(a^{2n} + b^{2n} + c^{2n})$ es divisible por d .

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

Observación: Notar que las propiedades (c) y (d) son casos particulares de a) y b), pero se pueden demostrar de manera independiente. Para la parte (c) se agrega la condición de que p no es divisible por 3 para no tener que hacer demostraciones adicionales.

6. Una secuencia está dada por $F(1) = 1$, $F(2) = 6$ y $F(n) = F(n-1) + F(n-2)$, para $n \geq 3$. Mostrar que para todo entero $n > 1$:

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. Sea $(2p+1)$ un número primo con p impar mayor que 1. Demostrar por inducción que para todo entero positivo n :

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

es divisible por $(2p+1)$. Probarlo de tres formas. Si cambiamos el exponente 2^n por $2n$ la propiedad se mantiene excepto para n múltiplo de p . Demostrarlo. No considerar lo anterior en las tres formas solicitadas.

8. Sea $(4p+1)$ un número primo con p impar mayor que 1. Demostrar por inducción que para todo entero positivo n :

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

es divisible por $(4p+1)$. Los a_k son todos distintos, pertenecen al conjunto formado por los primeros $2p$ enteros positivos y tienen la siguiente propiedad: $a_k^{2p} - 1$ es divisible por $(4p+1)$. Los otros números pertenecientes al mencionado conjunto tienen la propiedad: $b_k^{2p} + 1$ es divisible por $(4p+1)$.

9. Demostrar que para todo entero positivo n :

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

nunca es un cuadrado perfecto.

10. Demostrar que para todo entero positivo n :

$$8^{2^n} - 5^{2^n}$$

nunca es un cuadrado perfecto. Demostrarlo de dos maneras.

11. Sea $F(n) = 13^{6n+1} + 30^{6n+1} + 100^{6n+1} + 200^{6n+1}$ y sea:

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

Probar que para todo entero no negativo n : $G(n)$ es divisible por 7^3 .

12. Sea $f(a)$ una función de enteros positivos sobre enteros positivos. Si $(f(a+b) - kf(a))$ es divisible por p para todo entero positivo a , demostrar que existe b tal que $(f(a+b_0b) - f(a))$ es divisible por p .

13. Demostrar de dos formas que para todo entero no negativo n :

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

es divisible por 13.

14. Demostrar que para todo entero no negativo n :

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

es divisible por 125. Este problema puede ser resuelto usando lo señalado en la indicación del Problema 1, pero existe al menos una forma adicional para solucionarlo.

15. Demostrar que para todo entero positivo n :

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

es divisible por 19.

Existe a lo menos una forma adicional a las usadas en el Problema 5 para resolver este problema.

16. Sea $f(n) = (a - 1)f(n - 1) + af(n - 2)$ y sea $g(n) = f(n + 2) + af(n + 1) + (a - 1)f(n)$. Demostrar que para todo entero positivo n :

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

No es necesario determinar la fórmula cerrada de $f(n)$.

17. Sea $f(1) = f(2) = 1$ y $f(n) = 3(f(n - 1) + f(n - 2)) + 1$ para $n \geq 3$. Demostrar que para todo entero positivo n :

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

es divisible por 32.

18. Sea p un número primo mayor que 5. Sea $F(n) = 2^{1+(p-1)n} - 3^{1+(p-1)n} - 5^{1+(p-1)n} + 6^{1+(p-1)n}$ y sea:

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

Demostrar que para todo entero n no negativo: $G(n)$ es divisible por p^2 .

19. Sea p un entero positivo. Sea $F(n)$ una función de enteros sobre enteros. Si $F(n)$ satisface la siguiente congruencia:

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

Entonces para todo entero no negativo n :

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

20. Sea $a(1) = a(2) = 1$ y $a(n) = a(n - 1) + 2a(n - 2) + 1$ para $n \geq 3$. Probar por inducción que para todo entero $n > 0$:

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

21. Consideremos los primeros n^2 números de Fibonacci ordenados en espiral como se muestra a continuación para $n = 3$ y $n = 4$.

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

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

Notar que para $n = 3$ tenemos que $(21 + 1) = 2(8 + 3)$ y para $n = 4$ tenemos $(610 + 5) = 5(89 + 34)$. Conjeturar y probar este resultado para todo entero $n > 2$ (no necesariamente por inducción).

22. ¿Qué sucedería si en el Problema 21 cambiamos los números de Fibonacci por los números de Lucas, por números de Fibonacci pares, etc.?

23. Sea p un número primo mayor que 3 tal que divide a $a^2 + ab + b^2$ (a y b son primos relativos). Demostrar en más de una forma que para todos los enteros $n \geq 0$:

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

es divisible por p^2 .

24. Sea $(6m + 5)$ un número primo con m entero no negativo. Probar por inducción que para todo entero $n \geq 0$:

$$\sum_{i=1}^{3m+2} i^{2(3^n)}$$

es divisible por $(6m + 5)$.

25. Sea $F(n)$ el enésimo número de Fibonacci. Probar de varias formas que:

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

26. Sea $F(n)$ el enésimo número de Fibonacci. Probar que para cada entero no negativo n :

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

es divisible por 11.

27. Sea d un entero positivo fijo y sea p un número primo impar. Sea $F(n)$ una función de enteros a enteros que satisface la siguiente congruencia:

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

Si $F(a_0), F(a_1), \dots, F(a_{d-1})$ son divisibles por p , con $(a_i - a_j)$ no divisible por p para i distinto de j , entonces probar que para todo entero $n \geq 0$: $F(n)$ es divisible por p^d .

28. Sea $F(n)$ el enésimo número de Fibonacci. Sea $G_n(a) = 89a^n - F(n)a^{11} - F(n-11)$. Probar que para cada entero no negativo n : $G_n(a)$ es divisible por el polinomio $a^2 - a - 1$.

29. Sea $4k + 1$ un número primo. Demostrar que para todo entero n no negativo:

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

es divisible por $4k + 1$.

30. Sea:

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

y sea $G(n) = 500500F(n) - \frac{n(n-1)}{2}F(1001)$. Demostrar por inducción que $G(n)$ es divisible por p^3 , para todo entero $n \geq 0$ (p es un número primo mayor que 13).

31. Sea p un número primo impar y sea d un divisor de $p-1$, se sabe que la congruencia $a^d \equiv 1 \pmod{p}$ tiene exactamente d soluciones distintas. Sean a_1, a_2, \dots, a_d aquellas soluciones. Probar que:

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

donde $c_n = 1$ si n es divisible por d y 0 en caso contrario.

32. Probar o refutar la siguiente propiedad: dado el enunciado del Problema 23 y sea

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

Entonces: $12f(n) \equiv (n-3)(n-4)f(0) \pmod{p^3}$ para todos los enteros $n \geq 0$.

33. Sea $p > 3$ un número primo que divide $x^2 + x + 1$ ($1, x$ primos relativos). Sea

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

Entonces: $6f(n) \equiv -n(n-1)(x^2 + x + 1)^2 \pmod{p^3}$ para todo entero $n \geq 0$.

2. Indicaciones y Soluciones.

Indicación Problema 1:

Utilizar la forma de inducción que se indica a continuación:

1. La propiedad es verdadera para $n = 0$, $n = 1$ y $n = 2$.
2. Si la propiedad es verdadera para $n = k$, $n = k + 1$ y $n = k + 2$, implica que la propiedad es verdadera para $n = k + 3$.

Demostrar la siguiente relación:

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

(Usar el Teorema de Fermat $a^{p-1} \equiv 1 \pmod{p}$ con p número primo y a primo relativo con p) y el siguiente resultado: Si $g(n) = an^2 + bn + c$, es sencillo comprobar que $g(n+3) = 3g(n+2) - 3g(n+1) + g(n)$. Recordemos que la notación $a \equiv b \pmod{m}$ significa que $(a-b)$ es divisible por m .

Si no quieren usar la forma de inducción señalada anteriormente notar que:

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

Podemos demostrar que $(F(n+2) - 2F(n+1) + F(n))$ es divisible por p^3 , nos faltaría probar que $(F(2) - 2F(1) + F(0))$ es divisible por p^3 . Si probamos que $(F(n+2) - 2F(n+1) + F(n))$ es divisible por p^3 , podemos hacer lo siguiente:

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

Podemos demostrar que $(F(n+1) - F(n))$ es divisible por p^3 para todo entero no negativo n , nos faltaría demostrar que $(F(1) - F(0))$ es divisible por p^3 . Si probamos que $(F(n+1) - F(n))$ es divisible por p^3 , nos restaría demostrar que $F(0)$ es divisible por p^3 , para probar que $F(n)$ es divisible por p^3 .

Resumiendo, si hacemos lo anterior y demostramos que: $(F(2) - 2F(1) + F(0))$, $(F(1) - F(0))$ y $F(0)$ son divisibles por p^3 , podemos probar que $F(n)$ es divisible por p^3 , para todo entero no negativo n , pero si probamos que $F(0)$, $F(1)$ y $F(2)$ son divisibles por p^3 , demostramos que $(F(2) - 2F(1) + F(0))$, $(F(1) - F(0))$ y $F(0)$ son divisibles por p^3 .

Por lo tanto los dos enfoques son bastante parecidos.

Indicación Problema 2:

Sea $G(n) = 1 + 2^{2n} + 3^{2n} + 2((-1)^{F(n)} + 1)$. Probar que $(G(n+3) - G(n))$ es divisible por 7. Dividan el problema original en tres problemas: n de la forma $3m$, n de la forma $3m-1$ y n de la forma $3m-2$. Luego apliquen inducción sobre m para cada uno de los problemas.

Otra forma de resolver el problema es demostrando que $(G(n) + G(n+1) + G(n+2))$ es divisible por 7 (usando el principio de inducción débil) y posteriormente utilizar la siguiente forma de inducción:

1. La propiedad es verdadera para $n = 1$ y $n = 2$.
2. Si la propiedad es verdadera para $n = k$ y $n = k + 1$, implica que la propiedad es verdadera para $n = k + 2$.

Indicación Problema 3:

Ver indicación para el Problema 2.

Sea $F(n) = 2(2^{2n} + 5^{2n} + 6^{2n}) + 3(-1)^{n+1}((-1)^{F(n)} + 1)$.

Para la segunda demostración solicitada prueben que: $(G(n) - G(n+1) + G(n+2))$ es divisible por 13 o que $(G(n)^2 + G(n+1)^2 + G(n+2)^2)$ es divisible por 13. Notar que si $G(n)^2$ es divisible por 13, $G(n)$ también lo es.

Solución Problema 4:

Utilizaremos la siguiente forma de inducción:

1. La propiedad es verdadera para $n = 0$ y $n = 1$.
2. Si la propiedad es verdadera para $n = k$ y $n = k + 1$, entonces la propiedad es verdadera para $n = k + 2$.

Del enunciado se deduce directamente que la propiedad es verdadera para $n = 0$. (Dejaremos pendiente la demostración de que la propiedad es verdadera para $n = 1$.)

Del teorema de Euler (en realidad es suficiente con el teorema de Fermat) se deduce que:

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

Por lo tanto:

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

Probaremos que:

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

Usaremos la forma de inducción indicada anteriormente.

Para $n = 0$ debemos probar que $F(0) \equiv 0F(1) \pmod{b^2c^2}$, lo cual es cierto de acuerdo al enunciado.

Para $n = 1$ debemos probar que $F(1) \equiv 1F(1) \pmod{b^2c^2}$, lo cual es equivalente a demostrar que $0 \equiv 0 \pmod{b^2c^2}$, lo que claramente se cumple para enteros positivos b y c .

Supongamos que la propiedad se cumple para $n = k$ y para $n = k + 1$. Probaremos que la propiedad también se cumple para $n = k + 2$.

En efecto, de la relación (1) y aplicando la hipótesis inductiva se deduce que:

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

Ahora probaremos que existe k tal que $F(k)$ es divisible por b^2c^2 y k no es divisible por (bc) (si demostramos lo anterior podemos probar fácilmente que $F(1)$ es divisible por b^2c^2).

Vamos a probar que existe k distinto de 0 tal que $(1 + (b-1)(c-1)k)$ es divisible por bc y que k no es divisible por bc . Si probamos lo primero podemos demostrar, utilizando la segunda propiedad dada en el enunciado, que para ese k , $F(k)$ es divisible por b^2c^2 y si probamos que k no es divisible por bc , podemos usar el resultado (1) para demostrar que $F(1)$ es divisible por b^2c^2 .

Demostraremos que existe k_b tal que $(1 + (b-1)(c-1)k_b)$ es divisible por b y que existe k_c tal que $(1 + (b-1)(c-1)k_c)$ es divisible por c .

En efecto, al multiplicar $(b-1)(c-1)$ por $n = 1, 2, \dots, (b-1)$, los restos de la división por b son todos distintos.

Supongamos que para $k = r$ y $k = s$ los restos son iguales, con r y s enteros positivos menores o iguales a $(b-1)$ y r distinto de s . Por lo tanto $(r-s)(b-1)(c-1)$ es divisible por b , pero $(r-s)$, $(b-1)$ y $(c-1)$ no son divisibles por b (r y s son menores que b , por lo tanto su diferencia es aún menor y no puede ser 0, porque r es distinto de s ; $(b-1)$ no es divisible por b , ya que 1 no es divisible por b ; y $(c-1)$ no es divisible por b de acuerdo al enunciado). Como conclusión existe una contradicción y por ende si los restos son iguales se debe cumplir que $r = s$ y existe un k menor que b tal que el resto es igual a $(b-1)$. Por lo tanto para ese k , $(1 + (b-1)(c-1)k)$ es divisible por b .

Para c es una demostración similar.

Ahora necesitamos encontrar un k tal que $(1 + (b - 1)(c - 1)k)$ sea divisible por bc .

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

Notar que existe un l_c tal que si al resto de la división de $l_c c$ por b le sumamos el resto de la división de $(k_c - k_b)$ por b el resultado es b o cero. La demostración es similar a la hecha anteriormente (al dividir $l_c c$ por b para $l_c = 1, 2, \dots, b - 1$ se obtienen $b - 1$ restos distintos los cuales son $1, 2, \dots, b - 1$.)

Por lo tanto probamos que existe k tal que $(1 + (b - 1)(c - 1)k)$ es divisible por bc ,

El k encontrado no es divisible por bc , ya que de ser divisible por bc implicaría que 1 es divisible por bc , lo cual es una contradicción.

Probamos que $F(0)$ es divisible por $b^2 c^2$ y con lo anterior probamos que $F(1)$ es divisible por $b^2 c^2$.

Supongamos que $F(k)$ y $F(k + 1)$ sean divisibles por $b^2 c^2$, del resultado (1) se deduce que $F(k + 2)$ también es divisible por $b^2 c^2$.

Por lo tanto: $F(n)$ es divisible por $b^2 c^2$, para todo entero no negativo n .

Comentario: La demostración se puede simplificar bastante usando el hecho que bc y $(b - 1)(c - 1)$ son primos relativos y por lo tanto existen enteros x e y tales que $bcx + (b - 1)(c - 1)y = 1$.

Solución Problema 5:

Parte a

Probaremos, previamente, que $(a^2 b^2 + a^2 c^2 + b^2 c^2)$ es divisible por d^2 . Se sabe que $(a^2 + b^2 + c^2)$ es divisible por d , lo que implica que $(a^2 + b^2 + c^2)^2$ es divisible por d^2 . Pero $(a^2 + b^2 + c^2)^2$ es igual a $(a^4 + b^4 + c^4 + 2(a^2 b^2 + a^2 c^2 + b^2 c^2))$.

Por lo tanto :

$(a^4 + b^4 + c^4 + 2(a^2 b^2 + a^2 c^2 + b^2 c^2))$ es divisible por d^2 . Por otro lado:

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

De lo anterior, tenemos que $4(a^2 b^2 + a^2 c^2 + b^2 c^2)$ es divisible por d^2 , pero como d es un número impar se deduce que $(a^2 b^2 + a^2 c^2 + b^2 c^2)$ es divisible por d^2 .

Ahora volvamos al problema original.

Para $n = 1$ tenemos que:

$$a^{6-4} + b^{6-4} + c^{6-4} = a^2 + b^2 + c^2$$

Lo cual es divisible por d de acuerdo al enunciado.

Sea $t(n) = a^{2n} + b^{2n} + c^{2n}$. Notar que a^2 , b^2 y c^2 son las raíces del polinomio

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

por lo tanto $t(n)$ satisface la relación de recurrencia:

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

así

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

y por ende

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

Sabemos que $(a^2 + b^2 + c^2)$ y $(a^2b^2 + a^2c^2 + b^2c^2)$ son divisibles por d . Por lo tanto si $(a^{6k-4} + b^{6k-4} + c^{6k-4})$ es divisible por d , $(a^{6(k+1)-4} + b^{6(k+1)-4} + c^{6(k+1)-4})$ también lo es.

Parte b

Para $n = 1$ tenemos que:

$$a^{6-2} + b^{6-2} + c^{6-2} = a^4 + b^4 + c^4$$

De los resultados probados anteriormente tenemos que $2(a^4 + b^4 + c^4)$ es divisible por d^2 , lo que implica que $(a^4 + b^4 + c^4)$ es divisible por d^2 , ya que d es impar. Por lo tanto la propiedad es verdadera para $n = 1$.

Supongamos que la proposición es verdadera para $n = k$. Por demostrar que la propiedad es verdadera para $n = k + 1$.

Notemos que:

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

y por lo tanto

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

Sabemos que $(a^2 + b^2 + c^2)$ y $(a^{6n-4} + b^{6n-4} + c^{6n-4})$ son divisibles por d .

Por lo tanto $(a^2 + b^2 + c^2)(a^{6k-4} + b^{6k-4} + c^{6k-4})$ es divisible por d^2 . Por otro lado $a^2b^2 + a^2c^2 + b^2c^2$ es divisible por d^2 .

Por consiguiente si $(a^{6k-2} + b^{6k-2} + c^{6k-2})$ es divisible por d^2 , $(a^{6(k+1)-2} + b^{6(k+1)-2} + c^{6(k+1)-2})$ también.

Parte c

Para $n = 1$ debemos probar que:

$a^2 + b^2 + c^2$ es divisible por d , lo cual es verdadero de acuerdo al enunciado.

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

$$a + b = c$$

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

Por otra parte $a^2 + b^2 + c^2$ es divisible por d .

De lo anterior tenemos que $2ab \equiv 2c^2 \pmod{d}$.

Así, $ab \equiv c^2 \pmod{d}$, ya que d es impar. Similarmente, es fácil verificar que $ac \equiv -b^2 \pmod{d}$ y que $bc \equiv -a^2 \pmod{d}$.

Usando los resultados anteriores tenemos que:

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

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

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

Por lo tanto si la propiedad es verdadera para $n = k$, entonces para $n = k + 1$ también es verdadera, ya que d no es divisible por 3.

Para una demostración alternativa, notar que si a y d tienen factores primos en común, entonces $a + b$ y b tienen esos mismos factores comunes. Por lo tanto podemos factorizar los factores comunes primos obteniendo una expresión similar a la del enunciado, con a_1 y b_1 primos relativos entre sí y con respecto a d_1 , donde d_1 es d dividido por los mencionados factores comunes. Así, el entero a_1 tiene inverso modulo d_1 . Sea éste igual a a_1^{-1} . Por lo tanto el enunciado original es equivalente a probar que: $1 + (a_1^{-1}b_1)^{2^n} + (1 + a_1^{-1}b_1)^{2^n}$ es divisible por d_1 . Además, es fácil ver que se cumplen las siguientes congruencias:

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

Usar estos resultados para dar una demostración por inducción.

Parte d

Para $n = 1$ la propiedad es verdadera (ver parte (b)).

Supongamos que la propiedad es verdadera, para algún entero positivo k , esto implica que:

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

Por otra parte, $(a^{4^k})^2 + (b^{4^k})^2 + (c^{4^k})^2$ es divisible por d como corolario de la propiedad probada en parte (c). Por lo tanto

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

Combinando (3a) y (4), tenemos que $a^{4^{k+1}} + b^{4^{k+1}} + c^{4^{k+1}}$ es divisible por d^2 y el resultado sigue por inducción.

Comentarios: La propiedad encontrada por Naoki Sato al resolver el Problema 32, puede ser usada para dar una solución alternativa para partes (a) y (b). Notar también que la expresiones indicadas en las partes (a) y (b), satisfacen las condiciones dadas en el Problema 27. Por lo tanto, podemos probar parte (a), luego parte (d) y usando el resultado de el Problema 27, probar parte (b).

Solución Problema 6:

Parte a

Propuesto.

Parte b

Para $n = 2$ debemos probar que:

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

Lo cual es equivalente a demostrar que:
 $6^2 + 7^2 = 86 - 1$, es decir $36 + 49 = 85$, lo cual claramente es cierto.

Notemos que:

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

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

Sumando (5a) y (5b), tenemos que:

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

Por otra parte:

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

Usando la hipótesis inductiva correspondiente al principio de inducción fuerte y reemplazando los valores de $F(1)$ y $F(2)$ tenemos que:

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

Así, por el principio de inducción matemática, la propiedad es verdadera para todo entero n mayor que 1.

Solución Problema 7:

Sea:

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

Para $n = 1$ tenemos que:

$F(1) = \frac{p(p+1)(2p+1)}{6}$, lo cual es divisible por $(2p+1)$, ya que 6 no puede dividir a $2p+1$ (primo mayor que 3).

Supongamos que la propiedad es verdadera para $n = k$. Por demostrar que es verdadera para $n = k + 1$.

Demostración 1

Sea r_i el resto de la división de i^2 dividido por $(2p+1)$ y sea R_i igual a r_i , si r_i es menor o igual a p ; y R_i igual a $(2p+1 - r_i)$, si r_i es mayor que p .

Por lo tanto $i^2 \equiv \pm R_i \pmod{(2p+1)}$. Usando el teorema del binomio tenemos que:

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

Ahora necesitamos probar que los R_i son todos distintos.

Sean a y b enteros positivos menores o iguales a p .

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

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

Supongamos que $R_a = R_b = R$ con a distinto de b :

Caso 1: Supongamos igual signo. Vamos a suponer signo positivo. Para el caso de signo negativo la demostración es similar.

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

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

Restando (6a) menos (6b) tenemos que:

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

$$(a-b)(a+b) \equiv 0 \pmod{(2p+1)}$$

Lo anterior implica que $2p+1$ divide a $(a-b)$ o $(a+b)$, ya que $2p+1$ es primo. Pero tanto $(a-b)$ como $(a+b)$ no pueden ser divisibles por $2p+1$, a y b son menores o iguales a p y por lo tanto el valor absoluto de su diferencia es menor que $2p+1$ y tampoco puede ser cero, ya que a es distinto de b .

Por otro lado $(a+b)$ también es menor que $2p+1$, pues en el mayor valor de $(a+b)$ se obtiene cuando uno de los valores es p y el otro $p-1$, es decir cuando su suma es $2p-1$.

Por lo tanto, de existir a y b , no pueden tener el mismo signo.

Caso 2: distinto signo. Vamos a suponer que el signo negativo corresponde a b . El caso contrario es similar.

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

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

Recordando que p es impar y elevando (7a) y (7b) a p obtenemos:

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

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

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

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

Lo anterior implica que $R^p - 1$ y $-R^p - 1$ son divisibles por $2p+1$ (usando teorema de Fermat) y por lo tanto su suma también lo es, pero su suma es -2 , es decir si suponemos que $R_a = R_b = R$ con a distinto de

b implica que -2 es divisible por $2p + 1$, lo cual es una contradicción. Por lo tanto si a distinto de b implica que R_a es distinto de R_b .

Acabamos de probar que los R_i son todos distintos y además de la definición de R_i se deduce que:

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

Por lo tanto $F(k+1) \equiv F(k) \pmod{2p+1}$. Por ende si $F(k)$ es divisible por $2p+1$, $F(k+1)$ también.

Demostración 2

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

Sea r_{ij} el resto de la división de (ij) dividido por $(2p+1)$ y sea R_{ij} igual a r_{ij} , si r_{ij} es menor o igual a p ; y R_{ij} igual a $(2p+1 - r_{ij})$, si r_{ij} es mayor que p .

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

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

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

Donde c_r es el número de veces que el entero r aparece en la doble sumatoria mostrada en (10a).

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

Existen varias formas de probar lo anterior pero creo que la más fácil es la siguiente: El lado izquierdo de la igualdad (10a) tiene p^2 términos correspondientes a $(F(k))^2$. El lado derecho tiene p términos correspondientes a $F(k)$, más dos veces el número de términos que deseamos determinar. Por lo tanto despejando la incógnita obtenemos el resultado buscado.

Vamos a demostrar que $c_r \leq \frac{(p-1)}{2}$, lo que equivale a probar que dados los primeros p enteros positivos podemos formar como máximo $\frac{(p-1)}{2}$ parejas de números d y e tales que $d \cdot e \equiv \pm r \pmod{2p+1}$.

Sabemos que p es impar por ende $(p-1)$ es par. Por lo tanto podemos formar $\frac{(p-1)}{2}$ parejas sin repetir números. Para poder formar más parejas debemos ocupar el número que nos sobró y volver a ocupar otro número o bien hacer otra combinación con dos números ya utilizados. Pero hacer lo anterior implicaría lo siguiente:

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

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

Con f diferente de e

Tenemos dos casos: igual signo o distinto signo. Si tienen igual signo podemos restar (13) menos (12).

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

Si tienen igual distinto signo podemos sumar (13) más (12).

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

Lo anterior implica que $2p+1$ divide a d , $(f - e)$ o $(f + e)$, ya que $2p+1$ es primo. Pero d no es divisible por $2p+1$, ya que es un entero positivo menor que $2p+1$ y tanto $(f - e)$ como $(f + e)$ no pueden ser divisibles

por $2p + 1$, f y e son menores o iguales a p y por lo tanto el valor absoluto de su diferencia es menor que $2p + 1$ y tampoco puede ser cero, ya que f es distinto de e .

Por otro lado $(f + e)$ también es menor que $2p + 1$, pues el mayor valor de $(f + e)$ se obtiene cuando uno de los valores es p y el otro $p - 1$, es decir cuando su suma es $2p - 1$. Suponer que podemos formar más de $\frac{(p-1)}{2}$ parejas nos lleva a una contradicción. Por ende podemos formar como máximo $\frac{(p-1)}{2}$ parejas.

Por lo tanto $c_r \leq \frac{(p-1)}{2}$, para $r = 1, \dots, p$. Pero los c_r satisfacen la igualdad (11). Por ende el único valor posible para c_r , para $r = 1, \dots, p$ es $\frac{(p-1)}{2}$, ya que de otro modo no se cumpliría la igualdad.

De lo anterior deducimos que:

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

Por lo tanto si $F(k)$ es divisible por $2p + 1$, $F(k + 1)$ también.

Demostración 3

Sea a un entero positivo menor o igual a p y mayor que 1, demostrar que: $(a^{2^n} - 1) \sum_{k=1}^p k^{2^n}$ es divisible por $2p + 1$. Luego pruebe que $(a^{2^n} - 1)$ puede ser expresado como el producto de sumas de cuadrados por $(a - 1)(a + 1)$.

Posteriormente demuestre que $2p + 1$ no puede dividir la suma de dos cuadrados (Ver Demostración 1) y deduzca lo solicitado.

Indicaciones para probar una propiedad más general

Ahora daremos indicaciones para probar que $\sum_{k=1}^p k^{2^n}$ es divisible por $2p + 1$, excepto para n múltiplo de p . De hecho la propiedad que acabamos de demostrar es un caso particular de esta propiedad más general. Nos concentraremos en los primeros p casos, ya que:

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

Lo anterior es un resultado directo del teorema de Fermat. Por otro lado, usando el mismo teorema anterior, es fácil probar que para n múltiplo de p , $(\sum_{k=1}^p k^{2^n})$ es de la forma $(2p + 1)m + p$ y por ende no divisible por $2p + 1$. Probar que :

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

Es divisible por $2p + 1$.

Luego demuestre que:

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

Es divisible por $2p + 1$. Reordene los términos formando progresiones geométricas. De (14) se deduce que $\sum_{k=1}^p k^{2^n}$ es divisible por $2p + 1$ o $\sum_{k=1}^p k^{2^n} - p$ es divisible por $2p + 1$.

Por lo tanto:

$$\sum_{i=1}^p i^{2n} \equiv c_n p \pmod{2p+1} \quad (\text{Donde } c_n \text{ es } 0 \text{ o } 1.)$$

Reemplazando lo anterior en el resultado (15), tenemos que: $(c_1 + c_2 + \dots + c_{p-1})p$ es divisible por $2p + 1$.

Por lo tanto: $(c_1 + c_2 + \dots + c_{p-1})$ es divisible por $2p + 1$, ya que $2p + 1$ es primo.

Lo anterior es como mínimo 0 y como máximo $(p - 1)$, y por ende el único valor posible es cero, ya que de otro modo $(c_1 + c_2 + \dots + c_{p-1})$ no podría ser divisible por $2p + 1$.

Por lo tanto $\sum_{k=1}^p k^{2n}$ es divisible por $2p+1$ para $n = 1, 2, \dots, p-1$.

Comentario: Para otra demostración del resultado que acabamos de probar, se puede hacer uso de la siguiente propiedad: el número de enteros entre 1 y $p-1$ que tienen orden d es $\phi(d)$.

Indicación Problema 8:

Para $n = 1$ debemos probar que $4p+1$ divide a $\sum_{k=1}^p a_k^2$

Demostración 1

Sea b un entero positivo menor o igual a $2p$ que tenga la propiedad: $b^{2p} + 1$ es divisible por $(4p+1)$.

$$b^2 \sum_{k=1}^p a_k^2 = \sum_{k=1}^p (b \cdot a_k)^2$$

Sea b_k el resto de la división de $(b \cdot a_k)$ dividido por $(4p+1)$.

Sea B_i igual a b_i , si b_i es menor o igual a $2p$; y B_i igual a $(4p+1 - b_i)$, si b_i es mayor que $2p$. Por lo tanto $(b \cdot a_i) \equiv \pm B_i \pmod{(4p+1)}$. Luego probar que los B_i son todos diferentes, pertenecen al conjunto de los primeros $2p$ enteros positivos y que tienen la propiedad: $B_i^{2p} + 1$ es divisible por $(4p+1)$.

Así :

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

y por lo tanto

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

Notar que $(\sum_{i=1}^p B_i^2 + \sum_{i=1}^p a_i^2)$ es la sumatoria de los primeros $2p$ enteros positivos, es decir $\frac{(2p(2p+1)(4p+1))}{6}$, lo cual es divisible por $(4p+1)$, ya que 6 no puede dividir a $4p+1$ (número primo mayor que 3).

Por consiguiente:

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

Pueden seleccionar b_r y b_s (b_r distinto de b_s) de modo que a lo más uno de ellos tiene la propiedad: $(b^2 + 1)$ es divisible por $(4p+1)$. Probarlo y completar la prueba.

Demostración 2

Hacer algo similar a la Demostración 1, pero con a tal que: $a^{2p} - 1$ es divisible por $(4p+1)$ (a distinto de 1).

Para el resto de la solución ver solución de Problema 7.

Indicación Problema 9:

Considerar los residuos cuadráticos de 13, es decir, los números a para los cuales existe x tal que $x^2 \equiv a \pmod{13}$. Además es fácil demostrar que $4^{2n-1} + 9^{2n-1}$ es divisible por 13.

Indicación Problema 10:

Probar que $8^{2^n} - 5^{2^n}$ es divisible por 13 y no es divisible por 13^2 . Sea $F(n) = 8^{2^n} - 5^{2^n}$. Notar que:

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

Indicación Problema 11:

Ver indicación problema 1.

Indicación Problema 12:

Conjeturar y probar que para cada entero positivo n :

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

Luego usar el teorema de Euler.

Indicación Problema 13:

Sea:

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

Notar que

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

Luego demostrar que $(1 + 5^{2(2n+1)})$ y $(2^{2(2n+1)} + 3^{2(2n+1)})$ son divisibles por 13.

Otra solución es dividir el problema original en tres problemas: n de la forma $3m$, n de la forma $3m - 1$ y n de la forma $3m - 2$.

Indicación Problema 14:

Sea $f(n) = (2(3^{4n+3} + 4^{4n+3}) - 25n^2 + 65n + 68)$. Considerar $f(n + 1) - 34f(n)$. Otra solución es usar indicación de Problema 1.

Indicación Problema 15:

Sea:

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

Notemos que

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

Usando el teorema del binomio, tenemos que: $F(k + 2) \equiv F(k) \pmod{19}$

Para completar la demostración dividir el problema original en dos problemas: k impar y k par. También podemos demostrar que $(F(k) + F(k + 1))$ es divisible por 19 y posteriormente deducir que $F(k)$ es divisible por 19. Ver indicación Problema 2.

Solución Problema 16:

Para $n = 1$ debemos probar que: $g(1) = (f(1) + f(2))(2a - 1) \cdot a^0$

En efecto:

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

Demostración 1

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

Por consiguiente:

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

Pero

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

Por lo tanto: $f(k+3) - (a^2 - a + 1)f(k+1) - a(a-1)f(k) = 0$, y por ende $g(n+1) - a \cdot g(n) = 0$, lo cual es equivalente a $g(n+1) = a \cdot g(n)$.

Aplicando la hipótesis inductiva tenemos que:

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

Demostración 2

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

Por lo tanto podemos probar que

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

Para $n = 1$ es claro que $(f(1) + f(2)) = (f(1) + f(2))a^{(1-1)}$

Sabemos que $f(k+2) = (a-1)f(k+1) + af(k)$. Sumando $f(k+1)$ a ambos lados de la igualdad (16), tenemos que:

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

Finalmente usando la hipótesis inductiva:

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

Solución Problema 17:

Para $n = 1$ tenemos que: $f(3 \cdot 1) + f(3 \cdot 1 + 1) = f(3) + f(4)$

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

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

Por lo tanto:

$$f(3) + f(4) = 7 + 25 = 32, \text{ lo cual es divisible por } 32.$$

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

Si probamos que $3f(3n+1) + 5$ es divisible por 8 para todo entero positivo n , podemos completar la demostración.

Para $n = 1$, debemos probar que: $3f(3 \cdot 1 + 1) + 5$ es divisible por 8. $3f(4) + 5 = 3 \cdot 25 + 5 = 80$, lo cual es divisible por 8.

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

Nos faltaría probar que $(9f(3n+2) - 7)$ es divisible por 2, o que $(f(3n+2) - 1)$ es divisible por 2 para todo entero positivo n .

Probaremos que $(f(3n+2) - 1)$ es divisible por 2.

Para $n = 1$, debemos probar que: $f(3 \cdot 1 + 2) - 1$ es divisible por 2. $f(5) - 1 = 97 - 1 = 96$, lo cual es divisible por 2.

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

Por lo tanto si $f(3k+2) - 1$ es divisible por 2, $f(3(k+1) + 2) - 1$ también lo es.

Por consiguiente $(9f(3k+2) - 7)$ es divisible por 2, con lo cual podemos completar la demostración de que $3f(3n+1) + 5$ es divisible por 8 y por ende terminar de demostrar que para todo entero positivo n : $(f(3n) + f(3n+1))$ es divisible por 32.

Indicación Problema 18:

Probar que $f(n) \equiv n \cdot f(1) \pmod{p^2}$, usando la indicación del Problema 20, pero los casos bases son $n = 0$ y $n = 1$. A continuación probar que $f(100)$ es divisible por p^2 y por lo tanto $f(1)$ es divisible por p^2 ,

ya que 100 no es divisible por p de acuerdo al enunciado.

Indicación Problema 19:

Ver indicación Problema 1.

Indicación Problema 20:

Usar la siguiente forma de inducción:

1. La propiedad es verdadera para $n = 1$ y $n = 2$.
2. Si la propiedad es verdadera para $n = k$ y $n = k + 1$, entonces la propiedad es verdadera para $n = k + 2$.

Indicación Problema 21:

Notar que debemos determinar $S_1(n)$, $S_2(n)$, $S_3(n)$, $S_4(n)$ y $S_5(n)$ tal que:

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

Considerar unos pocos valores de n y tomar las sucesivas diferencias de $S_i(n)$. Usar la fórmula de Binet.

Indicación Problema 22:

Ver indicación del problema 21.

Indicación Problema 23:

Demostración 1

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

Probar que $f(n) \equiv ((1-n)f(0) + nf(1)) \pmod{p^2}$ para $n \geq 0$. Usar la siguiente forma de inducción:

1. La propiedad es verdadera para $n = 0$ y $n = 1$.
2. Si la propiedad es verdadera para $n = k$ y $n = k + 1$, entonces la propiedad es verdadera para $n = k + 2$.

Sea $g(k) = a^{(6k-2)} + b^{(6k-2)} + (a+b)^{(6k-2)}$. Del problema 5(b), sabemos que $g(k)$ es divisible por p^2 para cada entero positivo k . En particular para $k = 1$ y $k = p$, pero notar que $g(1) = f(0)$ y $g(p) = f(6)$. Por lo tanto $f(0)$ y $f(6)$ son divisibles por p^2 . Así $f(6) \equiv 6f(1) \pmod{p^2}$, luego $f(1)$ es divisible por p^2 (p es primo relativo con 6) y por consiguiente $f(n) \equiv 0 \pmod{p^2}$ para cada entero $n \geq 0$.

Demostración 2

Notar que

$$a^2 + ab + b^2 \equiv 0 \pmod{p}$$

Es fácil probar que a y b no son divisibles por p . Por lo tanto tienen inverso módulo p .

$$(ab^{-1})^2 + ab^{-1} + 1 \equiv 0 \pmod{p} \tag{17a}$$

$$(ab^{-1} - 1)((ab^{-1})^2 + ab^{-1} + 1) \equiv 0 \pmod{p} \tag{17b}$$

$$(ab^{-1})^3 \equiv 1 \pmod{p} \tag{17c}$$

Si $ab^{-1} - 1 \equiv 0 \pmod{p}$ implicaría que $a \equiv b \pmod{p}$, pero entonces $3a^2 \equiv 0 \pmod{p}$ (reemplazando en (17a)), lo cual es una contradicción, ya que 3 y a no son divisibles por p . Por consiguiente el elemento ab^{-1} es distinto de 1 y de acuerdo a (17c) tiene orden 3. Por lo tanto por el teorema de Lagrange, 3 divide a $p - 1$. Además es claro que $p - 1$ es par. En conclusión $4 + (p - 1)n$ es siempre de la forma $6k - 2$ y usando el problema 5 (b) se obtiene el resultado solicitado.

Demostración 3

Notar que

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

Por lo tanto -3 es un residuo cuadrático módulo p . Usando el símbolo de Legendre

$$\left(\frac{-3}{p}\right) = 1$$

Por otra parte:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right)$$

Es bien conocido que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Además por la Ley de la Reciprocidad Cuadrática:

$$\left(\frac{3}{p}\right) \left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2} \frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$$

Utilizando los resultados anteriores, se deduce que:

$$\left(\frac{p}{3}\right) = 1$$

Por lo tanto, $p - 1$ es divisible por 3 y como p es impar, se tiene que p es de la forma $6k + 1$. El resto de la demostración es igual a la anterior.

Indicación Problema 24:

Ver indicación del Problema 7 y usar el siguiente resultado: $a^2 - ab + b^2$ y $a^2 + ab + b^2$ son divisibles únicamente por primos de la forma $6k + 1$ o por 3 (con a y b primos relativos)(Ver Problema 23).

Notar que este problema también puede ser resuelto usando la propiedad probada al final de la solución del Problema 7.

Indicación Problema 25:

Mostrar que: $\sum_{i=1}^n F(i)^2 = F(n)F(n+1)$ y ver solución del Problema 6. Otra solución es usar la fórmula de Binet.

Indicación Problema 26:

Considerar separadamente los casos n par y n impar, y usar lo siguiente:

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

Indicación Problema 27:

Sea:

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

Probar que:

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

(Notar que para $d = 2$, $F(n) \equiv ((1-n)F(0) + nF(1)) \pmod{p^2}$ y para $d = 3$
 $F(n) \equiv (\frac{(n-1)(n-2)}{2}F(0) - n(n-2)F(1) + \frac{n(n-1)}{2}F(2)) \pmod{p^3}$)

Usar la forma de inducción que es indicada a continuación:

1. La propiedad es verdadera para $n = 0, n = 1, n = 2, \dots, n = d - 1$
2. Si la propiedad es verdadera para $n = k, n = k + 1, n = k + 2, \dots, n = k + d - 1$, entonces la propiedad es verdadera para $n = k + d$.

Es fácil ver que para $n = 0$, $F(0) \equiv F(0) \pmod{p^d}$, para $n = 1$, $F(1) \equiv F(1) \pmod{p^d}, \dots$, para $n = i$, $F(i) \equiv F(i) \pmod{p^d}, \dots$, y para $n = d - 1$, $F(d - 1) \equiv F(d - 1) \pmod{p^d}$. Por lo tanto la propiedad es verdadera para $n = 0, n = 1, n = 2, \dots, n = d - 1$.

Para el paso inductivo notar que:

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

Es un polinomio en k de grado a lo más $d - 1$. Por lo tanto del cálculo de diferencias finitas tenemos que:

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

Completar esta parte de la demostración usando el hecho que:

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

Si $F(a_0), F(a_1), \dots, F(a_{d-1})$ son divisibles por p^d , tenemos el siguiente sistema:

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

Por Regla de Cramer, $F(i) = \frac{\det(A_i)}{\det(A)}$, p^d es factor de $\det(A_i)$ (también puede ser probado que $\frac{F_i(n)}{F_i(i)}$ es un entero para $i = 0, \dots, d - 1$ usando la misma forma de inducción indicada anteriormente). Por otra parte se puede probar que $\det(A)$ tiene los factores $(a_i - a_j)$ con i distinto de j . El factor restante de $\det(A)$ es una constante que puede ser calculada evaluando $a_0 = 0, \dots, a_{d-1} = d - 1$ (la constante es una fracción unitaria). Sabemos que $F(i)$ es entero, por lo tanto:

Si $F(a_0), F(a_1), \dots, F(a_{d-1})$ son divisibles por p^d donde $(a_i - a_j)$ no es divisible por p para i distinto de j , entonces $F(i)$ es divisible por p^d para $i = 0, \dots, d - 1$. Así $F(n) \equiv 0 \pmod{p^d}$.

Indicación Problema 28:

Notar que $G_{n+2}(a) \equiv (G_{n+1}(a) + G_n(a)) \pmod{a^2 - a - 1}$ (Congruencia modulo un polinomio)

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

Usar la siguiente forma de inducción:

1. La propiedad es verdadera para $n = 0$ y $n = 1$.
2. Si la propiedad es verdadera para $n = k$ y $n = k + 1$, entonces la propiedad es verdadera para $n = k + 2$.

Luego probar que $G_0(a) = G_{11}(a) = 0$ (polinomio cero), por ende el polinomio $G_1(a)$ tiene el factor $a^2 - a - 1$ y por lo tanto: $G_n(a)$ es divisible por $a^2 - a - 1$ para cada entero no negativo n . También es posible determinar, directamente, que:

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

Indicación Problema 29:

Del teorema de Wilson se deduce que existe un entero a tal que $a^2 \equiv -1 \pmod{4k+1}$. Demostrar que los enteros de 1 a $2k$ pueden ser ordenados en k pares tales que la suma de los cuadrados de cada par es divisible por $(4k+1)$. El resultado es deducido, inmediatamente, de la bien conocida propiedad: $x^{2n+1} + y^{2n+1}$ es divisible por $(x+y)$. Notar que este problema también puede ser resuelto usando la propiedad probada al final de la solución del Problema 7.

Indicación Problema 30:

Probar que $G(n) \equiv (n(n-1)/2)G(2) \pmod{p^3}$, luego $G(1001) \equiv 500500 * G(2) \pmod{p^3}$ y concluir.

Solución Problema 31:

Podemos probar que:

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

Sea $1 \leq i \leq d$, es fácil probar que los residuos modulo p de los números $a_1 \cdot a_i, a_2 \cdot a_i, a_3 \cdot a_i, \dots, a_d \cdot a_i$ son todos diferentes y satisfacen: $r^d - 1 \equiv 0 \pmod{p}$. Por consiguiente, son sólo $a_1, a_2, a_3, \dots, a_d$ en algún orden. El resultado sigue sumando y usando el teorema del binomio. Por lo tanto: $\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$, donde c_n es 0 o 1.

Por otro lado:

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

Podemos reordenar los términos formando progresiones geométricas (podemos asumir que $a_1 = 1$, dado que $1^d \equiv 1 \pmod{p}$) y luego usar el hecho que $a_i^d \equiv 1 \pmod{p}$. Por lo tanto tenemos que: $(c_1 + c_2 + \dots + c_{d-1})d$ es divisible por p , d es primo relativo con p , así único posible valor de $(c_1 + c_2 + \dots + c_{d-1})$ es cero, ya que de otro modo la expresión no sería divisible por p . Por ende, podemos deducir que $c_1 = c_2 = \dots = c_{d-1} = 0$ y $\sum_{i=1}^d a_i^n$ es divisible por p para $n = 1, 2, \dots, d-1$.

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

Por otra parte, es fácil probar que para n múltiplo de d : $\sum_{k=1}^d k^n$ es de la forma $p \cdot m + d$. Por lo tanto, $\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$, donde $c_n = 1$, si n es divisible por d y 0 en caso contrario.

Indicación Problema 32:

Ver la solución de Naoki Sato para el Problema 32.

Para otra demostración, usar los siguientes resultados:

Sea $t(k)$ igual a $a^{6k+4} + b^{6k+4} + c^{6k+4}$, entonces $t(k) = a^4(a^6)^k + b^4(b^6)^k + c^4(c^6)^k$. Notar que a^6, b^6 y c^6 son las raíces del polinomio

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

por lo tanto $t(k)$ satisface la relación de recurrencia:

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

Dado el enunciado del problema, el inverso multiplicativo de a modulo p^3 existe. Poniendo $x = a^{-1}b$ y dado que $c = a + b$, tenemos:

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

Entonces, usando la anterior relación, probar la formula de Naoki Sato para $g_k(x)$, es decir, mostrar que para todos los enteros $k \geq 0$,

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

donde $Q_k(x)$ es un polinomio con coeficientes enteros. Notar que $x^2 + x + 1$ es factor de $x^6 - 1$ y de $(x+1)^6 - 1$.

Para facilitar las demostraciones para los casos bases, podemos obtener otra relación de recurrencia para probar los casos bases recursivamente.

Volviendo al problema original, podemos probar que la propiedad es verdadera para $n = 0$, $n = 6$ y $n = 12$. Por lo tanto, usando el resultado del Problema 27, la propiedad es verdadera para todo entero $n \geq 0$.

Indicación Problema 33:

Sea $g_k(x) = (1+x)^{6k+1} - x^{6k+1} - 1$, entonces

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

donde $Q_k(x)$ es un polinomio con coeficientes enteros.