

Curso de Iniciación Científica para Jóvenes Talentos
Nivel Pre-Avanzado
Teoría de números

1. Aritmética Modular

1.1. Congruencias

Prueba 1.1. *Escoja 3 y -21 , por ejemplo.*

Prueba 1.2. 1. $(1 \equiv 4 \pmod{3}) \wedge (4 \equiv 2 \pmod{2})$ no implica $1 \equiv 2 \pmod{2}$.

2. $2 \cdot 12 \equiv 2 \cdot 3 \pmod{6}$ no implica $12 \equiv 3 \pmod{6}$.

3. $1^2 \equiv 2^2 \pmod{3}$.

Prueba 1.3. 1. $2^7 \equiv 5 \pmod{41} \implies (2^7)^3 \equiv 5^3 \equiv 125 \equiv 2 \pmod{41} \implies 2^{21} \cdot 21 \equiv 2 \cdot 21 \equiv 1 \pmod{41} \implies 2^{20} \cdot 2 \cdot 21 \equiv 2^{20} \equiv 1 \pmod{41} \square$

2. $20^3 \equiv 8000 \equiv 9 \pmod{61} \implies 20^6 \equiv 9^2 \equiv 20 \pmod{61} \implies 20^{15} \equiv (20^6)^2 \cdot 20^3 \equiv 20^2 \cdot 9 \equiv 34 \cdot 9 \equiv 306 \equiv 1 \pmod{61} \square$

3. $2^6 \equiv -1 \pmod{13} \implies 2^{12} \equiv 1 \pmod{13} \implies 2^{60} \equiv 1 \pmod{13} \implies 2^{70} \equiv 2^{10} \equiv -2^4 \equiv -16 \equiv -3 \pmod{13}$. Del mismo modo, tenemos que $3^3 \equiv 1 \pmod{13} \implies 3^{69} \equiv 1 \pmod{13} \implies 3^{70} \equiv 3 \pmod{13} \implies 2^{70} + 3^{70} \equiv 0 \pmod{13} \square$

Prueba 1.4. Note que $12|k!$, $\forall k \geq 4$. Luego $\sum_{i=1}^{99} i! \equiv 1! + 2! + 3! \pmod{12} \equiv 1 + 2 + 6 \equiv 9$.

Prueba 1.5. Sea $k = \overline{a_1 a_2 \dots a_n}$ un número cualquiera. Entonces $k = \sum_{i=1}^n 10^{i-1} \cdot a_i$. Note que $10^{2j} \equiv 1 \pmod{11}$ y $10^{2j+1} \equiv -1 \pmod{11}$, luego $k \equiv \sum_{i=1}^n (-1)^{i-1} \cdot a_i \pmod{11}$. Lo cual representa la suma de las cifras en posiciones pares menos la suma de los números en posiciones impares.

Prueba 1.6. $a^2 \equiv 1 \pmod{24} \iff (a-1)(a+1) \equiv 0 \pmod{24}$. Pero como a es impar, tanto $a+1$ como $a-1$ son pares y uno de ellos es múltiplo de 4. Finalmente, como a no es múltiplo de 3, uno de los números $(a+1)$ o $(a-1)$ es múltiplo de 3. Eso implica que $(a+1)(a-1) \equiv 0 \pmod{24}$.

Prueba 1.7. Simplemente note que $a \equiv b \pmod{m} \implies a^k \equiv b^k \pmod{m}$ (Caso conocido de factorización)

Prueba 1.8. Análogo al ejercicio anterior.

Prueba 1.9. Haciendo cuentas se puede llegar a que $2^{24} \equiv -1 \pmod{97}$. Lo cual implica que $2^{48} \equiv 1 \pmod{97}$. Vea que $2^4 \equiv 16 \pmod{48}$, $2^5 \equiv 32 \pmod{48}$, $2^6 \equiv 16 \pmod{48}$, y el ciclo se repite. Luego, como 2011 es impar, $2^{2011} \equiv 32 \pmod{48}$. Eso significa que $2^{2011} = 48k + 32 \implies 2^{2^{2011}} \equiv 2^{48k+32} \pmod{97} \equiv 2^{32} \equiv 2^{24} \cdot 2^8 \equiv -256 \equiv 35 \pmod{97} \square$

Prueba 1.10. Note que si $k = 3q$, la cifra de las decenas de k solo dependerá de la cifra de las decenas de q y las cifras de las unidades de q . Procedemos por inducción. Los casos bases son satisfechos. Observe que si 3^k tiene como dígito de las decenas a y como dígito de las unidades b entonces a es par por hipótesis de inducción. 3^{k+1} tiene como dígito de las decenas al dígito de las unidades de $3 \cdot a$ mas el dígito de las decenas de $3 \cdot b$. Note que estos dos dígitos mencionados anteriormente son siempre pares, puesto que $b \in \{1, 3, 7, 9\} \implies 3b \in \{3, 9, 21, 27\}$ y a es par. Eso concluye la inducción

1.2. Clases de residuos

Prueba 1.11. Observe los siguientes conjuntos: $\{0\}, \{1, -1\}, \{2, -2\}, \{3, -3\}, \{4, -4\}, \{5, -5\}$. Son seis conjuntos, y representan todos los residuos módulo 11, agrupados. Luego, como hay 7 números, algunos de los números (o sus recíprocos aditivos [el recíproco aditivo de a es $-a$]) caeran en el mismo conjunto, por palomar. Esto implica que hay dos cuya suma o diferencia es múltiplo de 11

Prueba 1.12. Aplique módulo 4 a la ecuación, lo cual implica que $1+2 \equiv 1 \pmod{4}$. Contradicción.

Prueba 1.13. Note que $n^3 - 1 = (n-1)(n^2+n+1)$. Por el algoritmo de euclides, $(n+1, n^2+n+1) = 1$. Luego, si $n+1 | n^3 - 1 \implies n+1 | n-1$. Lo cual es una contradicción, a menos que $n = 1$.

Prueba 1.14. Veamos que $n = 1, 2$ satisfacen, luego podemos suponer que $n > 2$. Observe que $2n-1 | n^3+1 \iff (2n-1, n^3+1) = 2n-1, (\bullet, \bullet)$ denotando el máximo común divisor. Además, observe que $(a, bc) = (a, b) \cdot (a, c)$, para cualesquiera enteros positivos a, b, c . Vea que $(2n-1, n^3+1) = (2n-1, n+1) \cdot (2n-1, n^2+n-1) \leq 3 \cdot (2n-1, n^2-3n+2) = 3 \cdot (2n-1, n-1) \cdot (2n-1, n-2) = 3$. Donde usamos el algoritmo de euclides $(a, b) = (a, a-b)$. Luego $n > 2 \implies 2n-1 > 3$ y por lo tanto $(2n-1, n^3+1) \neq 2n-1$.

1.3. División Modular

Prueba 1.15. Procedemos por absurdo. Sea a un divisor de cero invertible en \mathbb{Z}_n . Luego existen b y c tal que $(a \cdot b \equiv 1) \wedge (a \cdot c \equiv 0)$. Tenemos que $n | a \cdot c \implies n = (n, a \cdot c) = (n, a) \cdot (n, c) = (n, c)$. Note que $(n, a) = 1$ por el teorema 1.1 de la sección 1.3. Es decir $n | c$. Pero eso es una contradicción, por la definición de divisor del cero.

Prueba 1.16. (\Leftarrow) Es claro debido a la proposición 1.5 de la sección 1.1. (\Rightarrow) Multiplique ambos lados de la ecuación por $\frac{1}{a}$. (existe debido al teorema 1.1).

Prueba 1.17. Sea $q = (n, a) > 1$. Entonces $k = \frac{n}{q}$ es un entero con $k \not\equiv 0 \pmod{n}$ debido a que $0 < k < n$. Pero $a \cdot k \equiv 0 \pmod{n}$. Claramente, a es divisor del cero.

Prueba 1.18. Escoja el k del ejercicio anterior, y $l = 0$.

Prueba 1.19. Defina $c = \frac{1}{a} \cdot \frac{1}{b}$ el candidato a inverso de $a \times b$. En efecto, $a \times b \times c \equiv a \cdot \frac{1}{a} \cdot b \cdot \frac{1}{b} \equiv 1 \pmod{n} \implies a \times b \in (\mathbb{Z}_n)^*$

Prueba 1.20.

$$7x \equiv 3 \pmod{15} \quad (1)$$

$$13 \cdot 7x \equiv 3 \cdot 13 \pmod{15} \quad (2)$$

$$x \equiv 9 \pmod{15} \quad (3)$$

Para la segunda parte:

$$3x \equiv 7 \pmod{15} \quad (4)$$

$$5 \cdot 3x \equiv 5 \cdot 7 \pmod{15} \quad (5)$$

$$0 \equiv 6 \pmod{15} \quad (6)$$

Prueba 1.21. Si a es su propio inverso, tenemos que $a^2 \equiv 1 \pmod{p}$. Luego $(a-1)(a+1) \equiv 0 \pmod{p}$. Como todos los residuos diferentes de cero son coprimos con p , sigue que $a \equiv \pm 1 \pmod{p}$.

2. Funcion Phi de Euler

Prueba 2.1. 1. $\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$

2. Vea el siguiente item

3. $\varphi(p^k) = p^k - p^{k-1}$

Prueba 2.2. $\varphi(pq) = (p-1)(q-1)$

Prueba 2.3. Ejercicio para el lector

Prueba 2.4. Vea que $\varphi(n) = \prod_{i=1}^r p_i^{e_i-1}(p_i-1)$. Si hay algún p_i que es impar, p_i-1 es par, y caso contrario si $p_1 = 2, r = 1$ entonces $\varphi(n) = 2^{e_1-1}$. Como $n \geq 3 \implies e_i \geq 2 \implies 2|\varphi(n)$

Prueba 2.5. Note que $(k, n) = (n-k, n)$, debido al algoritmo de Euler. Sea S_n la suma que queremos encontrar. Tenemos por lo tanto que

$$2S_n = 2 \sum_{\substack{(n,k)=1 \\ 1 \leq k \leq n}} k = \sum_{\substack{(n,k)=1 \\ 1 \leq k \leq n}} k + \sum_{\substack{(n,k)=1 \\ 1 \leq k \leq n}} n-k = \sum_{\substack{(n,k)=1 \\ 1 \leq k \leq n}} n = n \cdot \varphi(n) \quad (7)$$

Concluyendo que $S_n = \frac{n \cdot \varphi(n)}{2}$

Prueba 2.6. Sea $\varphi(a) = \prod_{i=1}^r p_i^{e_i-1}(p_i-1), \varphi(b) = \prod_{j=1}^k p_j^{v_j-1}(p_j-1)$. Como $a|b \implies (r \leq k) \wedge (e_i \leq v_i, \forall i \leq r)$. Por lo tanto, $\varphi(a)|\varphi(b)$.

Prueba 2.7. Veamos que si $\varphi(n) = 4$, entonces ningún primo mayor a 5 puede dividir a n . Si $5|n$, entonces $n = 5$. Luego, solo 2 y 3 dividen a $n = 2^a 3^b$. Luego $\varphi(n) = 2^a \cdot 3^{b-1}$. Vemos que $b = 1$, luego $n = 4 \cdot 3 = 12$. Si $b = 0$, entonces $a = 3 \implies n = 8$. Las soluciones son entonces $n = 8, 12$. (Falta revisar)

Prueba 2.8. (Solución 1 - Elvis) Aplicaremos Inducción sobre n . Se pueden checar valores chicos, para corroborar el caso base. Por ejemplo, $n = 1, 2, 3, 4, 5$. Supongamos que la fórmula se cumple para n , y sea q un primo cualquiera. Queremos probar que la fórmula es satisfecha para nq .

Sea v la máxima potencia de q que divide a n . Luego,

$$\begin{aligned} \sum_{d|nq} \varphi(d) &= \\ &= \sum_{\substack{d|nq \\ q^{v+1} \nmid d}} \varphi(d) + \sum_{\substack{d|nq \\ q^{v+1} | d}} \varphi(d) \\ &= \sum_{d|n} \varphi(d) + \sum_{d|\frac{nq}{q^{v+1}}} \varphi(q^{v+1})\varphi(d) \\ &= n + \varphi(q^{v+1}) \left(\sum_{i|\frac{n}{q^v}} \varphi(i) \right) \\ &= n + q^v(q-1) \frac{n}{q^v} \\ &= n + (q-1)n = nq \end{aligned}$$

La primera igualdad sigue de dividir los divisores de nq en aquellos que dividen a n pero no a nq y aquellos que dividen a n y nq . Seguidamente, se utilizó la hipótesis inductiva 2 veces.

3. EL teorema de Euler

Prueba 3.1. Suponga que el conjunto no es un sistema completo de residuos módulo n . Entonces existen i, j tal que $i \neq j, a \cdot r_i + b \equiv a \cdot r_j + b \pmod{n} \implies a \cdot r_i \equiv a \cdot r_j \pmod{n} \implies r_i \equiv r_j$, que es una contradicción

Prueba 3.2. Copie la prueba del ejercicio anterior y use el ejercicio 1.19 de la sección 1.3

Prueba 3.3. $a \cdot b^p - b \cdot a^p = ab(b^{p-1} - a^{p-1}) \equiv 0$ debido a que si uno de los dos números a o b son múltiplos de p , el resultado final lo será. Caso contrario, el teorema de Fermat garantiza que $a^{p-1} \equiv b^{p-1}$.

Prueba 3.4. $p^8 \equiv 1 \pmod{240} \iff (p-1)(p+1)(p^2+1)(p^4+1) \equiv 0 \pmod{240}$. Veamos que todos los factores de la parte izquierda de la equivalencia son pares, luego $2^4 | p^8 - 1$. Además, $(p+1)$ o $(p-1)$ son múltiplos de 3, luego $3 | p^8 - 1$. Falta probar que $5 | p^8 - 1$. Suponamos que $p \not\equiv \pm 1 \pmod{5}$. Entonces $p \equiv 2$ o $3 \pmod{5}$. En cualquier caso, $p^2 + 1 \equiv 0 \pmod{5}$. Por lo que el resultado sigue.

Prueba 3.5. Tome $m = \varphi(b) - 1, n = \varphi(a) - 1$. Entonces $a^m + b^n \equiv b^n \equiv 1 \pmod{a}$. Del mismo modo, $a^m + b^n \equiv 1 \pmod{b}$. Es decir, $(a | a^m + b^n - 1) \wedge (b | a^m + b^n - 1) \implies ab | a^m + b^n - 1 \implies a^m + b^n \equiv 1 \pmod{ab}$.

Prueba 3.6. Supongamos que p no es primo. Es decir, $p = a \cdot b$ con $1 < a, b < p$. Luego, $ab | (p-1)! \implies p | (p-1)! \implies (p-1)! \equiv 0 \pmod{p}$. Contradicción.

Prueba 3.7. Supongamos que si. Primero observemos que podemos suponer que $a_p \equiv b_p \equiv 0 \pmod{p}$ (Ya que solo debe haber un cero módulo p). Entonces $1 = (-1)^2 = (p-1)! \cdot (p-1)! = (\prod_{i=1}^{p-1} a_i) \cdot (\prod_{i=1}^{p-1} b_i) = \prod_{i=1}^{p-1} a_i b_i \equiv (p-1)! \equiv -1 \pmod{p}$. Contradicción.

Prueba 3.8. Veamos que con 4 2's y 1484 1's se puede lograr el cometido en (a). Para (b), note que $x^7 \equiv x \pmod{7}$. Luego, $1998 \equiv \sum_x x^7 \equiv \sum_x x \equiv 1492 \pmod{7}$, pero $1998 \not\equiv 1492 \pmod{7}$.

Prueba 3.9. Supongamos que n satisface la propiedad del ejercicio. Entonces el sistema

$$a^{25} \equiv a \pmod{n} \quad (8)$$

es equivalente a (ejercicio 4.2).

$$a^{25} \equiv a \pmod{p_1^{e_1}} \quad (9)$$

$$a^{25} \equiv a \pmod{p_2^{e_2}} \quad (10)$$

$$\vdots \quad (11)$$

$$a^{25} \equiv a \pmod{p_r^{e_r}} \quad (12)$$

$$(13)$$

Donde $n = \prod_{i=1}^r p_i^{e_i}$.

Observemos que si $e_i \geq 2$ para algún i , entonces escogemos $a = p_i^{e_i-1}$, donde $a^{25} = p_1^{25e_i-25} \equiv 0 \not\equiv p_i^{e_i-1} \pmod{p_i^{e_i}}$. Por lo tanto podemos suponer que $e_i = 1, \forall i$. Es decir, podemos suponer que n es primo. Primero notemos que si $\varphi(n) | 24$, entonces el resultado sigue del pequeño teorema de Fermat. Esto es verdad para $p = 2, 3, 5, 7, 13$. En otros casos, veamos que $2^{24} \equiv 1 \pmod{p}$ implica que $p | 2^{24} - 1$. Pero como $2^{24} - 1 = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$, obtenemos que los únicos valores de p posibles ahora son 17 y 241. Se puede verificar que $3^{25} \not\equiv 3 \pmod{17, 241}$. Por lo tanto n es de la forma $n = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4} \cdot 13^{b_5}$, donde $b_i \in \{0, 1\}$ y $\sum b_i \geq 1$ (Hay 31 enteros positivos con esta propiedad).

Prueba 3.10. a. Observe que $2 \equiv 2 \pmod{7}, 2^2 \equiv 4 \pmod{7}, 2^3 \equiv 1 \pmod{7}$, y el ciclo se repite. Luego, solo para $n \equiv 1 \pmod{3}$ se tiene que $2^n \equiv 1 \pmod{7}$.

b. $2^1 + 1 \equiv 3 \pmod{7}, 2^2 + 1 \equiv 5 \pmod{7}, 2^3 + 1 \equiv 2 \pmod{7}, 2^4 + 1 \equiv 3 \pmod{7}$. El ciclo se repite debido a que $2^k \equiv 2^{k+3} \pmod{7}$. Como en el primer ciclo no hubo ningún cero, tenemos que la ecuación $2^n + 1 \equiv 0 \pmod{7}$ no tiene soluciones.

Prueba 3.11. Observe que $\forall k \geq 0, m$ y $m \cdot 10^k$ tienen la misma suma de sus dígitos. Por lo tanto, podemos asumir que $(s, 10) = 1$. Por el teorema de Euler, obtenemos que $10^{\varphi(s) \cdot k} \equiv 1 \pmod{s}, \forall k \geq 1$. Si definimos $n = \sum_{i=1}^s 10^{\varphi(s) \cdot i}$, vemos que n satisface las propiedades del problema.

Prueba 3.12. Repita la prueba del ejercicio 4.2. Entonces, vea que el sistema es equivalente a $(p-1)! \equiv (p-1) \pmod{p}, (p-1)! \equiv p-1 \pmod{(p-1)}$. Lo cual es trivialmente verdadero.

Prueba 3.13. Probaremos que siempre existe un k para el cual a_k no es coprimo con p , sea cual sea p primo. Para eso, veamos que $2|a_1, 3|a_2$, por lo que podemos asumir que $(p, 6) = 1$. Por lo que

$$a_{p-2} \equiv 2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 0 \iff \quad (14)$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \iff \quad (15)$$

$$6 \cdot \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1\right) \equiv 6 \cdot 0 \iff \quad (16)$$

$$3 + 2 + 1 - 6 \equiv 0 \quad (17)$$

Lo cual es verdad. En la segunda línea se usó el pequeño teorema de Fermat: $a^{\varphi(p)-1} \equiv \frac{1}{a} \pmod{p}$.

Prueba 3.14. Procederemos por inducción. Suponga que hemos escogido los primeros n elementos ($e_i = 2^{v_i} - 3$) de la lista. Defina $e_{n+1} = 2^{\prod_{k=1}^n e_k} - 3$. Vea que $e_{n+1} \equiv 1 - 3 \equiv -2 \pmod{e_i}$, $\forall i$, por el teorema de Euler. Por lo tanto $(e_{n+1}, e_i) = (e_i - 2, e_i) = 1$, debido a que e_i es impar para todo i . Esto concluye la prueba.

Prueba 3.15. Notación: Denotamos $S(n)$ al conjunto de números primos que dividen a n , y sea $b_i = a^{i+1}a^i - 1$. Observemos que $(b_i, a) = 1$, $\forall i \in \mathbb{N}$. Procederemos por inducción para demostrar la existencia del subconjunto. Escogemos el primer elemento, b_i , al azar. Supongamos que tenemos $\{b_{v_1}, b_{i_2} \dots b_{i_k}\}$ elementos en el subconjunto y queremos agregar uno mas. Para lo cual, tomamos $i_{k+1} = \prod_{p \in S(\prod_{j=1}^k b_{i_j})} \varphi(p)$, sigue que $b_{i_{k+1}} \equiv a \not\equiv 0 \pmod{p}$, $\forall p \in S(\prod_{j=1}^k b_{i_j})$. ($a \not\equiv 0 \pmod{p}$) debido a que $(b_i, a) = 1$). Eso completa la hipótesis inductiva. Vemos que en efecto $(b_a, b_c) = 1$, $\forall a, c$.

4. Congruencias Lineales

Prueba 4.1.

$$4x + 20 \equiv 27x - 1 \pmod{15} \quad (18)$$

$$21 \equiv 23x \pmod{15} \quad (19)$$

$$21 \cdot 2 \equiv 46x \pmod{15} \quad (20)$$

$$2 \equiv x \pmod{15} \quad (21)$$

Prueba 4.2. $a \equiv b \pmod{n} \iff n|a-b \iff p_i^{e_i}|a-b, \forall i \iff a \equiv b \pmod{p_i^{e_i}}$

Prueba 4.3. Analicemos la tercera ecuación. $4x \equiv 20 \pmod{12}$ es equivalente a $(4x \equiv 20 \pmod{4}) \wedge (4x \equiv 20 \pmod{3})$ que a su vez es equivalente a $x \equiv 2 \pmod{3}$. Entonces la cuarta ecuación puede ser ignorada, ya que es equivalente a la tercera ecuación. La segunda ecuación es $2x \equiv 8 \pmod{4} \implies x \equiv 0 \pmod{2}$. La primera ecuación dice $x \equiv 0 \pmod{5}$. Juntando todo da $x \equiv 20 \pmod{30}$.

Prueba 4.4. Tome $s = 1848$. Vea que 2011 es primo. Luego $2^{2000} \equiv \frac{1}{2^{10}} \cdot 2^{2010} \equiv \frac{1}{2^{10}} \cdot 2^{\varphi(2011)} \equiv \frac{1}{2^{10}} \equiv \frac{1}{1024} \equiv 1848 \pmod{2011}$.

Prueba 4.5. Un número es autoreplicante si $n^2 \equiv n \pmod{10000} \implies n(n-1) \equiv 0 \pmod{10000}$. Como n y $n-1$ son coprimos, tenemos que $n = 0, 1 \pmod{10000}$. Es decir, $n = 10000 \cdot k + p, p \in \{0, 1\}$. Observe que ningún número de esta forma está entre 1000 y 9999.

Prueba 4.6. Sea $\{p_i\}_{i \in \mathbb{N}}$ una enumeración de los primos. Considere el sistema de ecuaciones

$$x \equiv -1r \pmod{p_1^k} \quad (22)$$

$$x \equiv -2r \pmod{p_2^k} \quad (23)$$

$$\vdots \quad \vdots \quad (24)$$

$$x \equiv -nr \pmod{p_n^k} \quad (25)$$

Debido a que todos los módulos son coprimos, podemos aplicar el TCR. Entonces existe x una solución al sistema de congruencias. Luego, tenemos una progresión aritmética $x+r, x+2r, \dots, x+rn$ tal que $p_i^k | x+ir, \forall i$.

Prueba 4.7. Observe el siguiente sistema de ecuaciones

$$x \equiv -1 \pmod{2} \quad (26)$$

$$x \equiv -2 \pmod{3} \quad (27)$$

$$x \equiv -4 \pmod{7} \quad (28)$$

$$x \equiv -6 \pmod{5} \quad (29)$$

$$x \equiv -10 \pmod{11} \quad (30)$$

$$x \equiv -12 \pmod{13} \quad (31)$$

Es fácil ver que $x+1, x+2, x+3, \dots, x+21$ es el conjunto buscado. Por ejemplo, el conjunto 9440, 9441, \dots , 9460 cumple con las condiciones del problema.

Prueba 4.8. Sea $\{p_i\}_{i \in \mathbb{N}}$ una enumeración de los primos. Sea $q_i = \prod_{j=1}^n p_{(i-1) \cdot n + j}$. Considere el sistema de ecuaciones

$$x \equiv -1 \pmod{q_1} \quad (32)$$

$$x \equiv -2 \pmod{q_2} \quad (33)$$

$$\vdots \quad \vdots \quad (34)$$

$$x \equiv -k \pmod{q_n} \quad (35)$$

Debido a que todos los módulos son coprimos, podemos aplicar el TCR. Entonces existe x una solución al sistema de congruencias. Luego, tenemos una progresión aritmética de razón 1 tal que $q_i | x+i$. Es decir, $x+i$ tiene al menos n primos distintos en su descomposición

Prueba 4.9. Solución en proceso

Prueba 4.10. Observe primero que los residuos cuadráticos módulo 8 son 0, 1, 4. Como los cuadrados deben ser de números impares, vemos que la suma de cinco (o nueve) elementos consecutivos es congruente a 1 módulo 8. Sea $\{a_i\}_{i \leq 100}$ la secuencia. Entonces tome 9 elementos consecutivos, y tome un subconjunto de 5 elementos consecutivos de éste. Si substraemos el primer conjunto del segundo, tenemos que $a+b+c+d = p^2 - q^2 = (p-q)(p+q) \equiv 0 \pmod{8}$ debido a que tanto p como q son impares. Podemos tomar estos cuatro elementos a, b, c, d como siendo consecutivos

$$v_1, v_2, v_3, v_4, v_5, a, b, c, d, e \quad (36)$$

Por ejemplo, arriba $v_1+v_2+v_3+v_4+v_5$ es un cuadrado perfecto y también $v_1+v_2+v_3+v_4+v_5 + a+b+c+d$. Sigue que $a+b+c+d \equiv 0 \pmod{8}$. Sigue que $v_1 \equiv e \equiv 1 \pmod{8}$. Podemos trasladar este raciocinio hacia la derecha y concluir que $a \equiv 1 \pmod{8}$. Así, $a_i \equiv 1 \pmod{8}, \forall 1 \leq i \leq 90$. Pero entonces tenemos que $a+b+c+d \equiv 4 \pmod{8}$, lo cual es una contradicción a una afirmación hecha mas arriba.

Prueba 4.11. Sea $\{p_i\}_{i \in \mathbb{N}}$ una enumeración de los primos. Escriba $a_i = \prod_{j \geq 1} p_i^{e_{ij}}$. Escoja n números primos suficientemente grandes ($q_i, i \leq n$). Considere los siguientes sistemas de congruencias, para cada j :

$$v_j \equiv -e_{1j} \pmod{q_1} \quad (37)$$

$$v_j \equiv -e_{2j} \pmod{q_2} \quad (38)$$

$$\vdots \quad \vdots \quad (39)$$

$$v_j \equiv -e_{nj} \pmod{q_n} \quad (40)$$

Como los módulos son todos coprimos, podemos aplicar el TCR a cada sistema. Finalmente, definamos $b = \prod_{j \geq 1} p_j^{v_j}$. Tenemos que para j suficientemente grande, $v_j = 0$, debido a que $a_i < \infty, \forall i$. Tenemos entonces el conjunto $\{ba_1, ba_2, ba_3 \dots ba_n\} = \{\prod_{j \geq 1} p_j^{e_{1j}+v_j}, \prod_{j \geq 1} p_j^{e_{2j}+v_j}, \dots, \prod_{j \geq 1} p_j^{e_{nj}+v_j}\}$. Note que $v_j + e_{ij} \equiv 0 \pmod{q_i}$, entonces $\{ba_1, ba_2, ba_3 \dots ba_n\} = \{\prod_{j \geq 1} p_j^{k_{1j} \cdot q_1}, \prod_{j \geq 1} p_j^{k_{2j} \cdot q_2}, \dots, \prod_{j \geq 1} p_j^{k_{nj} \cdot q_n}\} = \{s_1^{q_1}, s_2^{q_2}, \dots, s_n^{q_n}\}$.

5. Residuos Cuadraticos y el simbolo de Legendre

Prueba 5.1. ■ $\left(\frac{44}{103}\right) = \left(\frac{11}{103}\right) \cdot \left(\frac{4}{103}\right) = \left(\frac{11}{103}\right) = \frac{(-1)^{\frac{11-1}{2} \cdot \frac{103-1}{2}}}{\left(\frac{103}{11}\right)} = \frac{-1}{\left(\frac{4}{11}\right)} = -\left(\frac{4}{11}\right) =$

-1

■ $\left(\frac{-60}{1019}\right) = \left(\frac{-90}{1019}\right) \cdot \left(\frac{2}{1019}\right) \cdot \left(\frac{3}{1019}\right) = 1 \cdot -1 \cdot -\left(\frac{1019}{3}\right) = -1.$

Recordando que $\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^{-1}$ y $\left(\frac{-120}{1019}\right) = \left(\frac{-40}{1019}\right) \cdot \left(\frac{2}{1019}\right)$

■ $\left(\frac{2010}{1019}\right) = \left(\frac{44}{103}\right) = \left(\frac{-28}{1019}\right) = \left(\frac{-1}{1019}\right) \cdot \left(\frac{7}{1019}\right) = -\left(\frac{7}{1019}\right) = \left(\frac{1019}{7}\right) = \left(\frac{4}{7}\right) = 1$

Prueba 5.2. Notemos que $\varphi(49) = 42$. Además, si x satisface la ecuación del problema, entonces $(x, 7) = 1$. Eso implica que podemos afirmar que el pequeño teorema de Fermat es satisfecho. Es decir, $x^{42} \equiv 1 \implies x^2 \equiv 1 \implies (x+1)(x-1) \equiv 0 \implies x \equiv \pm 1$, debido a que $(x+1, x-1) \leq 2$. Verificamos que esos dos casos son en realidad los únicos posibles.

Prueba 5.3. Observe que $\left(\frac{\frac{p-1}{4}}{p}\right) = \left(\frac{\frac{p-1}{4}}{p}\right) \cdot \left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{2n} = 1.$

Entonces $\exists a, a^2 = \left(\frac{\frac{p-1}{4}}{p}\right)$, por lo tanto $n^n = \left(\frac{p-1}{4}\right)^{\frac{p-1}{4}} = a^{2a^2}$

Prueba 5.4. Note que $\left(\frac{236}{257}\right) = \left(\frac{4}{257}\right) \cdot \left(\frac{59}{257}\right) = \left(\frac{59}{257}\right) = \left(\frac{257}{59}\right) = \left(\frac{21}{59}\right) = \left(\frac{3}{59}\right) \cdot \left(\frac{7}{59}\right) = \left(\frac{59}{3}\right) \cdot \left(\frac{59}{7}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{3}{7}\right) = \left(\frac{-3}{7}\right) = \left(\frac{4}{7}\right) = 1$

Prueba 5.5. Supongamos que tenemos una lista finita de primos de la forma $3k-1$, $\{p_i\}_{i \leq n}$. Definamos el número $n = (\prod_{i=1}^n p_i)^2 + 1$. Claramente $(n, p_i) = 1$, $\left(\frac{n}{3}\right) = -1$. Sigue que $\exists q|n$, primo tal que $\left(\frac{q}{3}\right) = 1$ (si no existiese tendríamos $\left(\frac{n}{3}\right) = 1$). Pero como q es coprimo con todos los números anteriores de la lista, tenemos que q no pertenece a la lista y $q \equiv -1 \pmod{3}$, lo cual es una contradicción.

Ahora supongamos que la lista está conformada únicamente por elementos de la forma $3k+1$. Defina $N = (2 \prod_{i=1}^n p_i)^2 + 3$. Tenemos que $N \equiv 1 \pmod{3}$. Supongamos que $q|N$, es decir, $-3 \equiv (2 \prod_{i=1}^n p_i)^2 \pmod{q}$. Es decir, $\left(\frac{-3}{q}\right) = 1$. Observe que $\left(\frac{-3}{q}\right) = (-1)^{q-1} \cdot \left(\frac{q}{3}\right) = q \pmod{3} \implies q = 3k+1$. Finalmente, vea que $(q, p_i) \leq (N, p_i) = (3, p_i) = 1$. Es decir, q es coprimo con todos los elementos anteriores de la lista. Concluimos que q no estaba en la lista desde un principio.

Prueba 5.6. Solucion pendiente

Prueba 5.7. Supongamos lo contrario, es decir existe un primo q tal que $q|2^n + 1$ y $q = 8k+7$. Notemos que $\left(\frac{2}{q}\right) = 1$ y $\left(\frac{-1}{q}\right) = -1$. Pero

$$(a^n)^2 \equiv (a^2)^n \equiv 2^n \equiv -1 \implies \left(\frac{-1}{q}\right) = 1 \quad (41)$$

Lo cual es una contradicción.

Prueba 5.8. Llame $c_n = a_n b_n$. Supongamos por contradicción que $2003|c_{n_0}$ (y que es el menor con esta propiedad). Observemos que $c_{n+1} = a_n b_n = (a_n b_n)^{2001} + a_n b_n + a_n^{2002} + b_n^{2002}$, entonces, para $k < n_0$ obtenemos que $c_{k+1} \equiv c_k^{2001} + c_k + 2 \pmod{2003}$, ($\varphi(2003) = 2002$). Ponemos $k = n_0 - 1$ en la ecuación anterior, nos da que $c_{n_0-1}^{2001} + c_{n_0-1} + 2 \equiv 0 \iff 1 + c_{n_0-1}^2 + 2c_{n_0-1} \equiv 0 \iff (c_{n_0-1} + 1)^2 \equiv$

0 $\iff c_{n_0-1} \equiv -1$. En particular, tenemos que para $n < n_0$, $c_n c_{n-1} \equiv (1 + c_{n-1})^2 \implies \left(\frac{c_n c_{n-1}}{2003}\right) = 1 \implies \left(\frac{c_n}{2003}\right) = \left(\frac{c_{n-1}}{2003}\right)$. Como $c_{n_0-1} = -1 \implies -1 = \left(\frac{c_{n_0-1}}{2003}\right) = \left(\frac{c_0}{2003}\right) = \left(\frac{4}{2003}\right) = 1$. Lo cual es una contradicción.