

# Teoría de Números 4

## Ejercicios

### Problema 1

Sean  $a, n$  enteros mayores que 1. Pq si  $a^n - 1$  es primo  $\Rightarrow a = 2$  y  $n$  es primo

### Solución

Sea la descomposicion  $a^n - 1 = (a - 1)(a^{n-1} - 1 + a^{n-2} + \dots + a + 1)$  por tanto  $a - 1$  es 1  $\Rightarrow a = 2$ .

Supongamos que  $n$  no es primo  $\Rightarrow n = pq$  con  $p, q > 1$ , entonces  $a^n - 1 = (a^p - 1)(a^{p(q-1)} + a^{p(q-2)} + \dots + a^p + 1)$ , con lo cual  $(a^p - 1) = 1 \Rightarrow p - 1 = 0 \Rightarrow p = 1$ .

Análogamente se hace el análisis con  $q$  suponiendo que sea compuesto, llegando a la conclusión que es primo, por lo cual  $n$  debe ser primo.

### Problema 2

Sean  $a, n$  enteros mayores que 1. Prueba que si  $a^n + 1$  es primo  $\Rightarrow a$  es par y  $n$  es una potencia de 2.

### Solución

Que  $a$  sea par es *straightforward* (impar + par es impar).

Sea  $n = 2^p q$  con  $q$  impar, entonces  $a^n + 1 = (a^{2^p} + 1)(a^{2^p(q-1)} - a^{2^p(q-2)} + \dots - a^{2^p} + 1)$ , con lo cual es facil notar que para que  $a^n + 1$  sea primo  $a^{2^p} + 1$  debe ser igual a 1, lo cual es imposible, por tanto  $q = 1$ .

## Problema 3

Pq existe un bloque de 2022 enteros consecutivos donde hay exactamente 15 primos.

## Solución

Construyamos el conjunto  $A(n) = \{1 + n, 2 + n, \dots, 2022 + n\}$  en el cual, para un valor de  $n$  tenemos 2022 números consecutivos. Nótese que para  $A(1)$  tenemos más de 25 primos en el conjunto.

Probemos que existe un  $n$  tal que en el conjunto no hay primos. Sea  $p$  un entero, nótese que al sumarle a  $p! + 1$  una cantidad  $k$  con  $0 < k < p + 1$  podremos sacar factor común  $k$  porque  $p!$  contiene como factor todos los números hasta  $p$ , entonces habremos encontrado un bloque de  $p - 1$  números consecutivos compuestos.

Siguiendo esta lógica podemos construir un bloque de 2022 números compuestos consecutivos simplemente teniendo como primer número  $2023! + 1$ , o sea  $A(2023! + 1)$

Véase que cada vez que en  $A$  incrementamos  $n$ , como lo que estamos haciendo es eliminando el primer elemento y adicionando uno al final (en caso que lo tengamos en orden creciente) lo que está ocurriendo es que la cantidad de primos en el conjunto se mantiene constante, disminuye en 1 o aumenta en 1.

Demostremos que dado un conjunto de  $m$  números  $Q = \{q_1, q_2, \dots, q_m\}$ , si la diferencia modular entre cada término consecutivo es a lo sumo 1, entonces  $Q$  contiene a todos los elementos entre  $q_1$  y  $q_m$ . Procedamos por inducción:

- Caso base: para  $m = 2, m = 3$  se cumple
- Hipótesis: Supongamos que para  $m = k$  se cumple
- Para  $m = k + 1$  ocurre que el conjunto podemos dividirlo en  $\{q_1, q_2, \dots, q_k\}$  y  $\{q_{k+1}\}$ , en el primer grupo por hipótesis de inducción al conjunto pertenecen todos los números entre  $q_1$  y  $q_k$ , y como la diferencia modular entre  $q_k$  y  $q_{k+1}$  es a lo sumo 1 eso significa que entre  $q_k$  y  $q_{k+1}$  no existen elementos  $\Rightarrow$  en el conjunto  $Q$  estarían todos los elementos entre  $q_1$  y  $q_{k+1}$ , por tanto se cumple lo que queríamos demostrar.

Luego, inicialmente tenemos más de 25 primos, en cada incremento la cantidad varía en 1 o no y existe un  $n$  para el cual hay cero primos, eso significa que la primalidad para algún valor de  $n$  va a tomar el valor 15.

## Problema 4

Sean  $a, n, m$  enteros positivos y  $a > 1$ . Prueba que  $\text{mcd}(a^n - 1, a^m - 1) = a^{\text{mcd}(n,m)} - 1$

### Solución (Marlon)

Sea  $d = \text{mcd}(a^n - 1, a^m - 1)$ , entonces  $d \div (a^n - 1 - (a^m - 1)) \Rightarrow d \div (a^n - a^m)$ . Supongamos sin pérdida de generalidad que  $n > m, n = mq_1 + r_1$ , entonces  $d \div a^m(a^{m(q_1-1)+r_1} - 1)$ , como  $d \div a^m - 1$  y  $\text{mcd}(a^m - 1, a^m) = 1 \Rightarrow d \div a^{m(q_1-1)+r_1} - 1$ .

Repitiendo este proceso continuando con  $a^{m(q_1-1)+r_1} - 1$  y  $a^m - 1$  resulta que  $d \div a^{r_1} - 1$ , y si lo volvemos a aplicar con  $a^m - 1$  y  $a^{r_1} - 1$  obtendremos un  $r_2, r_3$  y así sucesivamente hasta que por el método de la división de Euclides resulta que  $d \div a^{\text{mcd}(n,m)} - 1$  que es lo que queríamos probar.

## Problema 5

Sean  $n$  entero mayor que 4. Prueba que  $n \div (n-1)! \Leftrightarrow n$  es compuesto.

### Solución

La demostración  $n \mid (n-1)! \Rightarrow n$  es compuesto es *straightforward*, ya que si  $n$  fuera primo  $\Rightarrow n$  es coprimo con todo número menor que él, y por tanto no divide a  $(n-1)!$ .

Demostremos que si  $n$  es compuesto  $\Rightarrow n \div (n-1)!$ . Sea  $n = ab$  con  $a, b > 1$  y  $n > a, b$  entonces:

- Si  $a = b \Rightarrow a, b$  pertenecen a  $\{2, \dots, n-1\}$  y por tanto  $n \div (n-1)!$
- Si  $a \neq b$  entonces probemos que  $n = a^2 > 2a$ , esto ocurre si  $a > 2$ , entonces para todo  $n > 4$  se cumple, que es lo que queríamos probar

## Problema 6

Se define la secuencia  $p_1, p_2, \dots, p_n$  para todo  $n > 1$  de la siguiente forma,  $p_1 = 2$  y  $p_n$  es el mayor primo que divide a  $p_1 p_2 \cdots p_{n-1} + 1$ . Prueba que 5 no está en la secuencia.

## Solución

Sea  $S = \{p_1, p_2, \dots, p_n\}$  la secuencia de los  $p_i$  que cumplen la condición y  $A(i) = p_1 p_2 \cdots p_i + 1$ , entonces:

- $A(1) = 2$  de donde  $p_1 = 2$
- $A(2) = 3$  de donde  $p_2 = 3$
- $A(3) = 7$  de donde  $p_3 = 7$
- ...

Nótese que si existe  $k$  tal que 5 cumple la condición en  $A(k)$  entonces  $A(k) = 5t$  siendo  $t$  un número compuesto por primos menores que 5 (o sea, 2 y 3), pero como  $p_1 = 2$  y  $p_2 = 3$  entonces  $A(k)$  es coprimo con 2 y 3, lo cual indica que  $t$  o es una potencia de 5 o es divisible entre un primo mayor que 5, lo cual no puede ser.

### Análisis de Abel

Analicemos el caso en que  $A(k)$  es una potencia de 5, en ese caso existe  $q$  tal que:

$$A(k) = p_1 p_2 \cdots p_k + 1 = 5^q$$

Lo cual es equivalente a:

$$p_1 p_2 \cdots p_k = 5^q - 1$$

Descomponiendo el miembro derecho resulta en:

$$p_1 p_2 \cdots p_k = (5 - 1)(5^{q-1} + 5^{q-2} + \cdots + 5 + 1)$$

Por lo que  $p_1 p_2 \cdots p_k$  sería múltiplo de 4, lo cual genera una contradicción porque solo tiene un factor 2, ya que los resultados de  $p_1 p_2 \cdots p_k + 1$  para  $k > 0$  son primos relativos con 2, lo que implica que no será divisible por 2.