Preparación para el examen

Coda

José Cuevas Barrientos

28 de noviembre de 2025

Congruencias

Problema (teorema de Wilson)

Pruebe que $(p-1)! \equiv (-1)^p \pmod{p}$.

(Una) solución

Hay mil maneras de demostrarlo. Procederemos de manera no estándar.

(Una) solución

Hay mil maneras de demostrarlo. Procederemos de manera no estándar. Considere el polinomio mónico de grado $p-1$

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

cuyas raíces son los elementos de $\mathbb{F}_p^\times$ sin repetición.

(Una) solución

Hay mil maneras de demostrarlo. Procederemos de manera no estándar. Considere el polinomio mónico de grado $p-1$

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

cuyas raíces son los elementos de $\mathbb{F}_p^\times$ sin repetición. Por otro lado, el polinomio $g(x) := x^{p-1} - 1$ también es mónico del mismo grado y tiene raíz en cada elemento de $\mathbb{F}_p^\times$ por el pequeño teorema de Fermat.

(Una) solución

Hay mil maneras de demostrarlo. Procederemos de manera no estándar. Considere el polinomio mónico de grado $p-1$

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

cuyas raíces son los elementos de $\mathbb{F}_p^\times$ sin repetición. Por otro lado, el polinomio $g(x) := x^{p-1} - 1$ también es mónico del mismo grado y tiene raíz en cada elemento de $\mathbb{F}_p^\times$ por el pequeño teorema de Fermat. Por tanto, $f \equiv g \pmod{p}$ y, en particular, $a_0 = -1$; pero

$$a_0 = (-1)(-2)\cdots(-p+1) = (-1)^{p-1}(p-1)!$$

de lo que se sigue el enunciado.

Congruencias

Problema (teorema de Wolstenholme)

Sea $p \geq 5$ primo. Pruebe que

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}.$$

Solución

Igual que antes considere el polinomio

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

cuyas raíces son los elementos de $\mathbb{F}_p^{\times}$.

Solución

Igual que antes considere el polinomio

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

cuyas raíces son los elementos de $\mathbb{F}_p^\times$. Como $f(x) \equiv x^{p-1} - 1 \pmod{p}$, se sigue que

$$a_1 = (-1)^p (p-1)! \left(1 + \frac{1}{2} + \cdots + \frac{1}{p-1}\right) \equiv 0 \pmod{p}$$

y, además, cada $a_j \equiv 0 \pmod{p}$ cuando $j > 0$.

Solución

Igual que antes considere el polinomio

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

cuyas raíces son los elementos de $\mathbb{F}_p^\times$. Como $f(x) \equiv x^{p-1} - 1 \pmod{p}$, se sigue que

$$a_1 = (-1)^p (p-1)! \left(1 + \frac{1}{2} + \cdots + \frac{1}{p-1}\right) \equiv 0 \pmod{p}$$

y, además, cada $a_j \equiv 0 \pmod{p}$ cuando $j > 0$.
Mejor aún, el lector puede notar que $f(0) = f(p) = (p-1)! = a_0$ (¡recuerde que $p \neq 2$!), de modo que $f(p) - a_0 = 0$.

Solución

Igual que antes considere el polinomio

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

cuyas raíces son los elementos de $\mathbb{F}_p^\times$. Como $f(x) \equiv x^{p-1} - 1 \pmod{p}$, se sigue que

$$a_1 = (-1)^p (p-1)! \left(1 + \frac{1}{2} + \cdots + \frac{1}{p-1}\right) \equiv 0 \pmod{p}$$

y, además, cada $a_j \equiv 0 \pmod{p}$ cuando $j > 0$.
Mejor aún, el lector puede notar que $f(0) = f(p) = (p-1)! = a_0$ (¡recuerde que $p \neq 2$!), de modo que $f(p) - a_0 = 0$. Cancelando por p, obtenemos la igualdad

$$p^{p-2} + a_{p-2}p^{p-3} + \cdots + a_2 p + a_1 = 0.$$

Mirando congruencias módulo p^2 se sigue el enunciado.

Caracteres

Problema

Pruebe que si χ, ψ son caracteres *primitivos* módulo n, m resp., donde n y m son enteros coprimos. Entonces $\chi \cdot \psi$ es un caracter primitivo módulo nm.

Caracteres

Problema

Pruebe que si χ, ψ son caracteres *primitivos* módulo n, m resp., donde n y m son enteros coprimos. Entonces $\chi \cdot \psi$ es un caracter primitivo módulo nm.

Caracteres

Problema

Pruebe que si χ, ψ son caracteres *primitivos* módulo n, m resp., donde n y m son enteros coprimos. Entonces $\chi \cdot \psi$ es un caracter primitivo módulo nm.

(Recuerde que un caracter χ módulo n se dice ***primitivo*** si no existe un divisor $r \mid n$ con $|r| < |n|$, y un caracter θ módulo r tales que $\chi(a) = \theta(a)$ para todo $a \in \mathbb{Z}$.)

Solución

Claramente $\chi \cdot \psi$ es caracter módulo nm. Si no fuera primitivo, existe $r \mid nm$ y un caracter θ módulo r tal que $\chi(a)\psi(a) = \theta(a)$.

Solución

Claramente $\chi \cdot \psi$ es caracter módulo nm. Si no fuera primitivo, existe $r \mid nm$ y un caracter θ módulo r tal que $\chi(a)\psi(a) = \theta(a)$. Por coprimalidad, $r = n'm'$ de manera única con $n' \mid n$ y $m' \mid m$; y por teorema chino del resto, existen caracteres χ', ψ' módulo n', m' resp. tales que $\theta(a) = \chi'(a)\psi'(a)$.

Solución

Claramente $\chi \cdot \psi$ es caracter módulo nm. Si no fuera primitivo, existe $r \mid nm$ y un caracter θ módulo r tal que $\chi(a)\psi(a) = \theta(a)$. Por coprimalidad, $r = n'm'$ de manera única con $n' \mid n$ y $m' \mid m$; y por teorema chino del resto, existen caracteres χ', ψ' módulo n', m' resp. tales que $\theta(a) = \chi'(a)\psi'(a)$.
Dado una clase $[b]$ coprima a n, siempre podemos elegir un representante tal que $b \equiv 1 \pmod{m}$ (y, por ende, $\equiv 1 \pmod{m'}$) de modo que $\chi(b) = \theta(b) = \chi'(b)$, y análogamente se verifica que $\psi = \psi'$; esto contradice la primitividad de χ y ψ.

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\dfrac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\dfrac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$
2. $\left(\frac{d}{p}\right)_K = 0$ si $p \mid d$.

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\dfrac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$
2. $\left(\frac{d}{p}\right)_K = 0$ si $p \mid d$.
3. $\left(\dfrac{d}{2}\right)_K = \begin{cases} 1, & d \equiv 1 \pmod 8, \\ -1, & d \equiv 5 \pmod 8. \end{cases}$

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\dfrac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$
2. $\left(\frac{d}{p}\right)_K = 0$ si $p \mid d$.
3. $\left(\dfrac{d}{2}\right)_K = \begin{cases} 1, & d \equiv 1 \pmod 8, \\ -1, & d \equiv 5 \pmod 8. \end{cases}$
4. $\left(\frac{d}{p}\right)_K = \left(\frac{d}{p}\right)_L$ si $p > 2$ y $p \nmid d$.

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\dfrac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$
2. $\left(\frac{d}{p}\right)_K = 0$ si $p \mid d$.
3. $\left(\dfrac{d}{2}\right)_K = \begin{cases} 1, & d \equiv 1 \pmod 8, \\ -1, & d \equiv 5 \pmod 8. \end{cases}$
4. $\left(\frac{d}{p}\right)_K = \left(\frac{d}{p}\right)_L$ si $p > 2$ y $p \nmid d$.
5. $\left(\frac{d}{n}\right)_K$ es completamente multiplicativa en el parámetro n.

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\dfrac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$
2. $\left(\frac{d}{p}\right)_K = 0$ si $p \mid d$.
3. $\left(\dfrac{d}{2}\right)_K = \begin{cases} 1, & d \equiv 1 \pmod 8, \\ -1, & d \equiv 5 \pmod 8. \end{cases}$
4. $\left(\frac{d}{p}\right)_K = \left(\frac{d}{p}\right)_L$ si $p > 2$ y $p \nmid d$.
5. $\left(\frac{d}{n}\right)_K$ es completamente multiplicativa en el parámetro n.

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\frac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$
2. $\left(\frac{d}{p}\right)_K = 0$ si $p \mid d$.
3. $\left(\frac{d}{2}\right)_K = \begin{cases} 1, & d \equiv 1 \pmod 8, \\ -1, & d \equiv 5 \pmod 8. \end{cases}$
4. $\left(\frac{d}{p}\right)_K = \left(\frac{d}{p}\right)_L$ si $p > 2$ y $p \nmid d$.
5. $\left(\frac{d}{n}\right)_K$ es completamente multiplicativa en el parámetro n.

Pruebe que $\chi_d(n) := \left(\frac{d}{n}\right)_K$ es un caracter primitivo módulo $|d|$ cuando d satisface una de las dos:

(a) $d \equiv 1 \pmod 4$ y es libre de cuadrados.

Caracteres

Problema

Definimos el ***símbolo de Kronecker*** $\left(\frac{d}{n}\right)_K$ mediante las siguientes propiedades:

1. $\left(\frac{d}{-1}\right)_K = \begin{cases} 1, & d > 0, \\ -1, & d < 0. \end{cases}$
2. $\left(\frac{d}{p}\right)_K = 0$ si $p \mid d$.
3. $\left(\frac{d}{2}\right)_K = \begin{cases} 1, & d \equiv 1 \pmod 8, \\ -1, & d \equiv 5 \pmod 8. \end{cases}$
4. $\left(\frac{d}{p}\right)_K = \left(\frac{d}{p}\right)_L$ si $p > 2$ y $p \nmid d$.
5. $\left(\frac{d}{n}\right)_K$ es completamente multiplicativa en el parámetro n.

Pruebe que $\chi_d(n) := \left(\frac{d}{n}\right)_K$ es un caracter primitivo módulo $|d|$ cuando d satisface una de las dos:

(a) $d \equiv 1 \pmod 4$ y es libre de cuadrados.

(b) $4 \mid d$, $d/4 \not\equiv 1 \pmod 4$ y $d/4$ es libre de cuadrados.

Solución

Es inmediato que $\chi_4(n) := \left(\frac{-4}{n}\right)_K$ es un caracter primitivo módulo 4.

Solución

Es inmediato que $\chi_4(n) := \left(\frac{-4}{n}\right)_K$ es un caracter primitivo módulo 4. Así mismo, χ_8 y χ_{-8} son caracteres y son primitivos pues $\chi_8(q) = 1$ para un primo $q \equiv 1 \pmod 8$ y $\chi_8(q) = -1$ para $q \equiv 5 \pmod 8$. Similarmente, $\chi_{-8}(3) = 1 \neq -1 = \chi_{-8}(7)$.

Solución

Es inmediato que $\chi_4(n) := \left(\frac{-4}{n}\right)_K$ es un caracter primitivo módulo 4. Así mismo, χ_8 y χ_{-8} son caracteres y son primitivos pues $\chi_8(q) = 1$ para un primo $q \equiv 1 \pmod 8$ y $\chi_8(q) = -1$ para $q \equiv 5 \pmod 8$. Similarmente, $\chi_{-8}(3) = 1 \neq -1 = \chi_{-8}(7)$.

Si $d = p \equiv 1 \pmod 4$ es primo, entonces $\left(\frac{p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ pues la igualdad se da por reciprocidad cuadrática, y por propiedades 4 y 5, notando que $\left(\frac{p}{2}\right)_K = \left(\frac{2}{p}\right)_L$ para $p > 2$ primo, y que $\left(\frac{p}{-1}\right)_K = -1 = \left(\frac{-1}{p}\right)_L$.

Solución

Es inmediato que $\chi_4(n) := \left(\frac{-4}{n}\right)_K$ es un caracter primitivo módulo 4. Así mismo, χ_8 y χ_{-8} son caracteres y son primitivos pues $\chi_8(q) = 1$ para un primo $q \equiv 1 \pmod 8$ y $\chi_8(q) = -1$ para $q \equiv 5 \pmod 8$. Similarmente, $\chi_{-8}(3) = 1 \neq -1 = \chi_{-8}(7)$.

Si $d = p \equiv 1 \pmod 4$ es primo, entonces $\left(\frac{p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ pues la igualdad se da por reciprocidad cuadrática, y por propiedades 4 y 5, notando que $\left(\frac{p}{2}\right)_K = \left(\frac{2}{p}\right)_L$ para $p > 2$ primo, y que $\left(\frac{p}{-1}\right)_K = -1 = \left(\frac{-1}{p}\right)_L$.

Si $p \equiv 3 \pmod 4$ es primo, entonces $\left(\frac{-p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ notando nuevamente que $\left(\frac{-p}{2}\right)_K = \left(\frac{2}{p}\right)_L$, que $\left(\frac{-p}{-1}\right)_K = 1 = \left(\frac{-1}{p}\right)_L$ y aplicando reciprocidad cuadrática.

Solución

Es inmediato que $\chi_4(n) := \left(\frac{-4}{n}\right)_K$ es un caracter primitivo módulo 4. Así mismo, χ_8 y χ_{-8} son caracteres y son primitivos pues $\chi_8(q) = 1$ para un primo $q \equiv 1 \pmod 8$ y $\chi_8(q) = -1$ para $q \equiv 5 \pmod 8$. Similarmente, $\chi_{-8}(3) = 1 \neq -1 = \chi_{-8}(7)$.

Si $d = p \equiv 1 \pmod 4$ es primo, entonces $\left(\frac{p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ pues la igualdad se da por reciprocidad cuadrática, y por propiedades 4 y 5, notando que $\left(\frac{p}{2}\right)_K = \left(\frac{2}{p}\right)_L$ para $p > 2$ primo, y que $\left(\frac{p}{-1}\right)_K = -1 = \left(\frac{-1}{p}\right)_L$.

Si $p \equiv 3 \pmod 4$ es primo, entonces $\left(\frac{-p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ notando nuevamente que $\left(\frac{-p}{2}\right)_K = \left(\frac{2}{p}\right)_L$, que $\left(\frac{-p}{-1}\right)_K = 1 = \left(\frac{-1}{p}\right)_L$ y aplicando reciprocidad cuadrática.

Sean pues d_1, d_2 enteros coprimos que satisfagan (a) y (b), y sea $d := d_1 d_2$. Basta notar ahora que $\chi_d(n) = \chi_{d_1}(n)\chi_{d_2}(n)$ para ver que χ_d es un caracter primitivo por inducción sobre $|d|$ (usando el ejercicio anterior).

Solución

Es inmediato que $\chi_4(n) := \left(\frac{-4}{n}\right)_K$ es un caracter primitivo módulo 4. Así mismo, χ_8 y χ_{-8} son caracteres y son primitivos pues $\chi_8(q) = 1$ para un primo $q \equiv 1 \pmod 8$ y $\chi_8(q) = -1$ para $q \equiv 5 \pmod 8$. Similarmente, $\chi_{-8}(3) = 1 \neq -1 = \chi_{-8}(7)$.

Si $d = p \equiv 1 \pmod 4$ es primo, entonces $\left(\frac{p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ pues la igualdad se da por reciprocidad cuadrática, y por propiedades 4 y 5, notando que $\left(\frac{p}{2}\right)_K = \left(\frac{2}{p}\right)_L$ para $p > 2$ primo, y que $\left(\frac{p}{-1}\right)_K = -1 = \left(\frac{-1}{p}\right)_L$.

Si $p \equiv 3 \pmod 4$ es primo, entonces $\left(\frac{-p}{n}\right)_K = \left(\frac{n}{p}\right)_L$ notando nuevamente que $\left(\frac{-p}{2}\right)_K = \left(\frac{2}{p}\right)_L$, que $\left(\frac{-p}{-1}\right)_K = 1 = \left(\frac{-1}{p}\right)_L$ y aplicando reciprocidad cuadrática.

Sean pues d_1, d_2 enteros coprimos que satisfagan (a) y (b), y sea $d := d_1 d_2$. Basta notar ahora que $\chi_d(n) = \chi_{d_1}(n)\chi_{d_2}(n)$ para ver que χ_d es un caracter primitivo por inducción sobre $|d|$ (usando el ejercicio anterior). En efecto, coinciden en $\chi_d(2)$ por propiedad 3; coinciden en $\chi_d(p)$ para un primo $p > 2$ por 4 y evidentemente también en -1.

Series de Dirichlet

Problema

Pruebe que

$$\frac{1}{x}\sum_{n\leq x}\sigma(n) = \frac{\pi^2}{12}x^2 + O(\log x).$$

(Recuerde que

$$\sigma(n) := \sum_{\substack{d|n \\ d>0}} d.)$$

Solución

Expandamos

$$\sum_{n \leq x} \sigma(n) \quad = \quad \sum_{n \leq x} \sum_{dm=n} d = \sum_{1 \leq dm \leq x} d$$

Solución

Expandamos

$$\begin{aligned}\sum_{n\leq x}\sigma(n) &= \sum_{n\leq x}\sum_{dm=n} d = \sum_{1\leq dm\leq x} d \\ &= \sum_{m\leq x}\sum_{\substack{d\\ dm\leq x}} d\end{aligned}$$

Solución

Expandamos

$$\begin{aligned}\sum_{n\leq x}\sigma(n) &= \sum_{n\leq x}\sum_{dm=n} d = \sum_{1\leq dm\leq x} d \\ &= \sum_{m\leq x}\sum_{\substack{d\\ dm\leq x}} d = \frac{1}{2}\sum_{m\leq x}\left\lfloor\frac{x}{m}\right\rfloor\left(\left\lfloor\frac{x}{m}\right\rfloor+1\right)\end{aligned}$$

Solución

Expandamos

$$\begin{aligned}
\sum_{n\leq x}\sigma(n) &= \sum_{n\leq x}\sum_{dm=n} d = \sum_{1\leq dm\leq x} d \\
&= \sum_{m\leq x}\sum_{\substack{d\\ dm\leq x}} d = \frac{1}{2}\sum_{m\leq x}\left\lfloor\frac{x}{m}\right\rfloor\left(\left\lfloor\frac{x}{m}\right\rfloor+1\right) \\
&= \frac{1}{2}\sum_{m\leq x}\frac{x^2}{m^2} + O\left(x\sum_{m\leq x}\frac{1}{m}\right).
\end{aligned}$$

Solución

Expandamos

$$\begin{aligned}\sum_{n\leq x}\sigma(n) &= \sum_{n\leq x}\sum_{dm=n} d = \sum_{1\leq dm\leq x} d \\ &= \sum_{m\leq x}\sum_{\substack{d\\ dm\leq x}} d = \frac{1}{2}\sum_{m\leq x}\left\lfloor\frac{x}{m}\right\rfloor\left(\left\lfloor\frac{x}{m}\right\rfloor+1\right) \\ &= \frac{1}{2}\sum_{m\leq x}\frac{x^2}{m^2} + O\left(x\sum_{m\leq x}\frac{1}{m}\right).\end{aligned}$$

El primer término es $x^2\sum_{m\leq x}\frac{1}{m^2} = x^2\zeta(2)+O(x)$

Solución

Expandamos

$$\begin{aligned}\sum_{n\leq x}\sigma(n) &= \sum_{n\leq x}\sum_{dm=n} d = \sum_{1\leq dm\leq x} d \\ &= \sum_{m\leq x}\sum_{\substack{d\\ dm\leq x}} d = \frac{1}{2}\sum_{m\leq x}\left\lfloor\frac{x}{m}\right\rfloor\left(\left\lfloor\frac{x}{m}\right\rfloor+1\right) \\ &= \frac{1}{2}\sum_{m\leq x}\frac{x^2}{m^2} + O\left(x\sum_{m\leq x}\frac{1}{m}\right).\end{aligned}$$

El primer término es $x^2\sum_{m\leq x}\frac{1}{m^2} = x^2\zeta(2)+O(x)$ pues

$$\sum_{m>x}\frac{1}{m^2} \leq \int_{x-1}^{\infty}\frac{1}{t^2}\,dt = \frac{1}{x-1} \sim \frac{1}{x};$$

Solución

Expandamos

$$\begin{aligned}\sum_{n\leq x}\sigma(n) &= \sum_{n\leq x}\sum_{dm=n} d = \sum_{1\leq dm\leq x} d \\ &= \sum_{m\leq x}\sum_{\substack{d\\ dm\leq x}} d = \frac{1}{2}\sum_{m\leq x}\left\lfloor\frac{x}{m}\right\rfloor\left(\left\lfloor\frac{x}{m}\right\rfloor+1\right) \\ &= \frac{1}{2}\sum_{m\leq x}\frac{x^2}{m^2} + O\left(x\sum_{m\leq x}\frac{1}{m}\right).\end{aligned}$$

El primer término es $x^2\sum_{m\leq x}\frac{1}{m^2} = x^2\zeta(2)+O(x)$ pues

$$\sum_{m>x}\frac{1}{m^2} \leq \int_{x-1}^{\infty}\frac{1}{t^2}\,dt = \frac{1}{x-1} \sim \frac{1}{x};$$

el segundo término es $\sum_{m\leq x}\frac{1}{m} = \log x + \gamma + O(\frac{1}{x})$. Se concluye el enunciado.

Curvas elípticas

Problema

Calcule todos los puntos racionales de torsión de la curva elíptica $E: \ y^2 = x^3 + px$ para un primo p.

Solución

Primero comenzamos por calcular el discriminante del polinomio cúbico $f(x) := x^3 + px$

Solución

Primero comenzamos por calcular el discriminante del polinomio cúbico $f(x) := x^3 + px$ dado por el determinante

$$D := \mathrm{Res}(f, f') = \begin{vmatrix} 1 & 0 & p & 0 & \\ & 1 & 0 & p & 0 \\ 3 & 0 & p & & \\ & 3 & 0 & p & \\ & & 3 & 0 & p \end{vmatrix} = 4p^3.$$

Solución

Primero comenzamos por calcular el discriminante del polinomio cúbico $f(x) := x^3 + px$ dado por el determinante

$$D := \mathrm{Res}(f, f') = \begin{vmatrix} 1 & 0 & p & 0 & \\ & 1 & 0 & p & 0 \\ 3 & 0 & p & & \\ & 3 & 0 & p & \\ & & 3 & 0 & p \end{vmatrix} = 4p^3.$$

Ahora bien, el teorema de Nagell-Lutz dice que si $(x, y) \in E(\mathbb{Q})$ es de torsión, entonces $y = 0$ o $y \mid D$. En el segundo caso, nos da que $y = \pm 2^a p^b$ con $a \leq 2$ y $b \leq 3$.

Solución

Primero comenzamos por calcular el discriminante del polinomio cúbico $f(x) := x^3 + px$ dado por el determinante

$$D := \mathrm{Res}(f, f') = \begin{vmatrix} 1 & 0 & p & 0 & \\ & 1 & 0 & p & 0 \\ 3 & 0 & p & & \\ & 3 & 0 & p & \\ & & 3 & 0 & p \end{vmatrix} = 4p^3.$$

Ahora bien, el teorema de Nagell-Lutz dice que si $(x, y) \in E(\mathbb{Q})$ es de torsión, entonces $y = 0$ o $y \mid D$. En el segundo caso, nos da que $y = \pm 2^a p^b$ con $a \leq 2$ y $b \leq 3$.
Si $a = 0$ (i.e., $y = \pm p^b$), entonces resolvemos la ecuación diofántica $p^{2b} = x(x^2 + p)$.

Solución

Primero comenzamos por calcular el discriminante del polinomio cúbico $f(x) := x^3 + px$ dado por el determinante

$$D := \mathrm{Res}(f, f') = \begin{vmatrix} 1 & 0 & p & 0 & \\ & 1 & 0 & p & 0 \\ 3 & 0 & p & & \\ & 3 & 0 & p & \\ & & 3 & 0 & p \end{vmatrix} = 4p^3.$$

Ahora bien, el teorema de Nagell-Lutz dice que si $(x, y) \in E(\mathbb{Q})$ es de torsión, entonces $y = 0$ o $y \mid D$. En el segundo caso, nos da que $y = \pm 2^a p^b$ con $a \leq 2$ y $b \leq 3$.
Si $a = 0$ (i.e., $y = \pm p^b$), entonces resolvemos la ecuación diofántica $p^{2b} = x(x^2 + p)$. Note que $x^2 + p \geq p > 1$, de modo que $b > 0$. Mirando congruencias módulo p, obtenemos $x^3 \equiv 0 \ (p)$, es decir, $x = pu$ y obtenemos

$$p^{2b-2} = u(pu^2 + 1),$$

como u y $pu^2 + 1$ son coprimos (¿por qué?), se sigue que $u = \pm 1$ o $pu^2 + 1 = \pm 1$. El segundo caso implica $u = 0$, lo que es absurdo.

Solución

Primero comenzamos por calcular el discriminante del polinomio cúbico $f(x) := x^3 + px$ dado por el determinante

$$D := \mathrm{Res}(f, f') = \begin{vmatrix} 1 & 0 & p & 0 & \\ & 1 & 0 & p & 0 \\ 3 & 0 & p & & \\ & 3 & 0 & p & \\ & & 3 & 0 & p \end{vmatrix} = 4p^3.$$

Ahora bien, el teorema de Nagell-Lutz dice que si $(x, y) \in E(\mathbb{Q})$ es de torsión, entonces $y = 0$ o $y \mid D$. En el segundo caso, nos da que $y = \pm 2^a p^b$ con $a \leq 2$ y $b \leq 3$.
Si $a = 0$ (i.e., $y = \pm p^b$), entonces resolvemos la ecuación diofántica $p^{2b} = x(x^2 + p)$. Note que $x^2 + p \geq p > 1$, de modo que $b > 0$. Mirando congruencias módulo p, obtenemos $x^3 \equiv 0 \ (p)$, es decir, $x = pu$ y obtenemos

$$p^{2b-2} = u(pu^2 + 1),$$

como u y $pu^2 + 1$ son coprimos (¿por qué?), se sigue que $u = \pm 1$ o $pu^2 + 1 = \pm 1$. El segundo caso implica $u = 0$, lo que es absurdo.
Si $u = \pm 1$, entonces $pu^2 + 1 = p + 1 = p^{2b-2}$ lo que es imposible.

Solución (cont.)

Si $a \in \{1, 2\}$, entonces obtenemos $4^a p^{2b} = x(x^2 + p)$. Nuevamente, mirando módulo p se sigue que $x = pu$ y tenemos la ecuación

$$4^a p^{2b-2} = u(pu^2 + 1).$$

Solución (cont.)

Si $a \in \{1, 2\}$, entonces obtenemos $4^a p^{2b} = x(x^2 + p)$. Nuevamente, mirando módulo p se sigue que $x = pu$ y tenemos la ecuación

$$4^a p^{2b-2} = u(pu^2 + 1).$$

Igual que antes, u y $pu^2 + 1$ son coprimos, y $p \nmid pu^2 + 1$, así que $pu^2 + 1 \in \{4, 16\}$.

Solución (cont.)

Si $a \in \{1, 2\}$, entonces obtenemos $4^a p^{2b} = x(x^2 + p)$. Nuevamente, mirando módulo p se sigue que $x = pu$ y tenemos la ecuación

$$4^a p^{2b-2} = u(pu^2 + 1).$$

Igual que antes, u y $pu^2 + 1$ son coprimos, y $p \nmid pu^2 + 1$, así que $pu^2 + 1 \in \{4, 16\}$. Por inspección solo nos deja $p = 3$ y $u = \pm 1$, lo que a su vez implica $b = 0$.

Solución (cont.)

Si $a \in \{1, 2\}$, entonces obtenemos $4^a p^{2b} = x(x^2 + p)$. Nuevamente, mirando módulo p se sigue que $x = pu$ y tenemos la ecuación

$$4^a p^{2b-2} = u(pu^2 + 1).$$

Igual que antes, u y $pu^2 + 1$ son coprimos, y $p \nmid pu^2 + 1$, así que $pu^2 + 1 \in \{4, 16\}$. Por inspección solo nos deja $p = 3$ y $u = \pm 1$, lo que a su vez implica $b = 0$.
Esto nos dice que los únicos puntos de torsión de $E(\mathbb{Q})$ son $(0, 0)$ en general, y posiblemente $P := (3, \pm 6)$ cuando la ecuación es $y^2 = x^3 + 3x$.

Solución (cont.)

Si $a \in \{1, 2\}$, entonces obtenemos $4^a p^{2b} = x(x^2 + p)$. Nuevamente, mirando módulo p se sigue que $x = pu$ y tenemos la ecuación

$$4^a p^{2b-2} = u(pu^2 + 1).$$

Igual que antes, u y $pu^2 + 1$ son coprimos, y $p \nmid pu^2 + 1$, así que $pu^2 + 1 \in \{4, 16\}$. Por inspección solo nos deja $p = 3$ y $u = \pm 1$, lo que a su vez implica $b = 0$.
Esto nos dice que los únicos puntos de torsión de $E(\mathbb{Q})$ son $(0, 0)$ en general, y posiblemente $P := (3, \pm 6)$ cuando la ecuación es $y^2 = x^3 + 3x$.
Finalmente, operamos P consigo mismo para ver que sea de torsión:

$$2P = \left(\frac{1}{4}, \pm\frac{7}{8}\right) \notin E(\mathbb{Q})_{tors}.$$

Así que $E(\mathbb{Q})_{tors} = \{(0, 0), o\}$