Las Matemáticas son la Reina de las Ciencias y la Teoría de Números es la Reina de las Matemáticas. (Die Mathematik ist die Königin der Wissenschaften und die Zahlentheorie ist die Königin der Mathematik.). - Carl Friedrich Gauss

Problema 1. Demuestren que n y $n+1$ son números coprimos para todo $n \geq 1$.

Problema 2. Utilice las propiedades de divisibilidad de los números enteros para demostrar que las únicas soluciones para $y^2 = x(x+1)(x+2)$ con $x, y \in \mathbb{Z}$ son $(0,0)$, $(-1,0)$ y $(-2,0)$. (Pista: si a y b son primos relativos y ab es un cuadrado, entonces a es un cuadrado y b es un cuadrado).

Problema 3. Encuentre todas las ternas pitagóricas (a,b,c), es decir, $a,b,c \in \mathbb{Z}$ y $a^2+b^2=c^2$, tales que b^2+c^2 es un cuadrado perfecto. En otras palabras, encuentre todos los números enteros a,b,c,d tales que (a,b,c) y (b,c,d) sean ambos ternas pitagóricas. (Pista: puedes asumir que $y^2 = x(x+1)(x+2)$ no tiene puntos racionales distintos de $(0,0)$, $(-1,0)$ y $(-2,0)$.)

Problema 4. Sea $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, con $a_i \in \mathbb{Z}$. Demuestren que si $x = \frac{p}{q} \in \mathbb{Q}$, con $\gcd(p,q) = 1$, es una solución de $f(x) = 0$, entonces a_n es un múltiplo p y a_0 es un múltiplo de q.

Problema 5. Sea C la cónica definida por $x^2 - 2y^2 = 1$.

1. Encuentre todos los puntos racionales de C. (Pista: el punto $O = (1,0)$ pertenece a C. Sea $L(t)$ la línea que pasa por O y tiene pendiente $t \in \mathbb{Q}$. Entonces $L(t) \cap C$ contiene dos puntos de racionales, O y Q. Encuentren las coordenadas de Q en términos de t.)

2. Sea $\alpha = 1 + \sqrt{2}$. Calcule $\alpha^2 = a + b\sqrt{2}$ y $\alpha^4 = c + d\sqrt{2}$ y verifique que (a,b) y (c,d) son puntos integrales de $C : x^2 - 2y^2 = 1$. (Nota: de hecho, si $\alpha^{2n} = e + f\sqrt{2}$, entonces $(e,f) \in C$ y los coeficientes de α^{2n+1} son una solución de $x^2 - 2y^2 = -1$.)

Problema 6. Sea $C/\mathbb{Q}$ una curva afín (plana).

1. Supongamos que $C/\mathbb{Q}$ está dado por una ecuación de la forma

$$C : xy^2 + ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{1}$$

   Encuentre un cambio invertible de variables que lleve la ecuación de C a una de la forma $xy^2 + gx^2 + hxy + jx + ky + l = 0$. (Pista: considere un cambio de variables $X = x + \lambda$, $Y = y$).

2. Supongamos que $C'/\mathbb{Q}$ está dado por una ecuación de la forma

$$C' : xy^2 + ax^2 + bxy + cx + dy + e = 0. \tag{2}$$

   Encuentre un cambio invertible de variables que lleve la ecuación de C' a una de la forma $y^2 + \alpha xy + \beta y = x^3 + \gamma x^2 + \delta x + \eta$. (Pista: multiplica (2) por x y considera el cambio de las variables $X = x$ y $Y = xy$. Asegúrate de que, al final, los coeficientes de y^2 y x^3 equivalen a 1.)

3. Supongamos que $C''/\mathbb{Q}$ es una curva dada por una ecuación de la forma

$$C'' : y^2 + axy + by = x^3 + cx^2 + dx + e. \tag{3}$$

   Encuentre un cambio invertible de variables que lleve la ecuación de C'' a una de la forma $y^2 = x^3 + Ax + B$. (Pista: hágalo en dos pasos. Primero elimine los términos xy e y. Luego elimine el término x^2).

4. Sea $E/\mathbb{Q} : y^2 + 43xy - 210y = x^3 - 210x^2$. Encuentre un cambio invertible de variables que lleve la ecuación de E a una de la forma $y^2 = x^3 + Ax + B$.

Problema 7. Sean C y E curvas definidas, respectivamente, por $C : V^2 = U^4 + 1$ y $E : y^2 = x^3 - 4x$. Sea ψ la función definido por

$$\psi(U, V) = \left(\frac{2(V+1)}{U^2}, \frac{4(V+1)}{U^3} \right).$$

1. Demuestre que si $U \neq 0$ y $(U, V) \in C(\mathbb{Q})$, entonces $\psi(U, V) \in E(\mathbb{Q})$.
2. Encuentra una función inversa para ψ; es decir, encuentre $\varphi : E \to C$ tal que $\varphi(\psi(U, V)) = (U, V)$.

A continuación, trabajamos en coordenadas proyectivas. Sea $C : W^2V^2 = U^4 + W^4$ y $E : zy^2 = x^3 - 4xz^2$.

(3) Escribe la definición de ψ en coordenadas proyectivas; es decir, ¿qué es $\psi([U, V, W])$?

(4) Demuestre que $\psi([0, 1, 1]) = [0, 1, 0] = \mathcal{O}$.

(5) Demuestre que $\psi([0, -1, 1]) = [0, 0, 1]$.
(*Pista: Demuestre que* $\psi([U, V, W]) = [2U^2, 4UW, W(V - W)]$.)

Problema 8. Utilice SageMath (también llamado CoCalc) o Magma (o otro programa) para resolver los siguientes problemas:

1. Encuentre $3Q$, donde $E : y^2 = x^3 - 25x$ y $Q = (-4, 6)$. Usa $3Q$ para encontrar un nuevo triángulo rectángulo con lados racionales y un área igual a 5.
2. Sea $y^2 = x(x + 5)(x + 10)$ y $P = (-9, 6)$. Encuentre nP para $n = 1, \ldots, 12$. Compare las coordenadas x de nP con la lista dada durante el curso y escriba los siguientes tres números que pertenecen a la lista.

Problema 9. Sea $E/\mathbb{Q}$ una curva elíptica dada por una ecuación de Weierstrass de la forma $y^2 = f(x)$, donde $f(x) \in \mathbb{Z}[x]$ es un polinomio cúbico mónico con raíces distintas (sobre $\mathbb{C}$).

1. Demuestre que $P = (x, y) \in E$ es un punto de torsión de orden exacto 2 si y solo si $y = 0$ y $f(x) = 0$.
2. Sea $E(\mathbb{Q})[2]$ el subgrupo de $E(\mathbb{Q})$ formado por aquellos puntos racionales $P \in E(\mathbb{Q})$ tales que $2P = \mathcal{O}$. Demuestre que el tamaño de $E(\mathbb{Q})[2]$ puede ser 1, 2 o 4.
3. Da ejemplos de tres curvas elípticas definidas sobre $\mathbb{Q}$ donde el tamaño de $E(\mathbb{Q})[2]$ es 1, 2 y 4, respectivamente.

Problema 10. Sea $E_t : y^2 + (1 - t)xy - ty = x^3 - tx^2$ con $t \in \mathbb{Q}$ y $\Delta_t = t^5(t^2 - 11t - 1) \neq 0$. Cada curva E_t tiene un subgrupo isomorfo a $\mathbb{Z}/5\mathbb{Z}$. Utilice SageMath o Magma para encontrar curvas elípticas con torsión $\mathbb{Z}/5\mathbb{Z}$ y rango 0, 1 y 2. Además, intente encontrar una curva elíptica E_t con rango r, lo más alto posible. (Nota: el rango más alto conocido para una curva elíptica con torsión $\mathbb{Z}/5\mathbb{Z}$ es 9, descubierto por Klagsburn en 2020.)

Problema 11. Sea $p \geq 2$ un primo y $E_p : y^2 = x^3 + p^2$. Demuestre que no existe un punto de torsión $P \in E_p(\mathbb{Q})$ con $y(P)$ igual a

$$y = \pm 1,\ \pm p^2,\ \pm 3p,\ \pm 3p^2,\ \text{o}\ \pm 3.$$

Demuestre que $Q = (0, p)$ es un punto de torsión de orden exacto 3. Concluya que $\{\mathcal{O}, Q, 2Q\}$ son los únicos puntos de torsión en $E_p(\mathbb{Q})$. (Nota: para $p = 3$, el punto $(-2, 1) \in E_3(\mathbb{Q})$. Demuestre que *no* es un punto de torsión.)

Problema 12. 1. Primero demuestre que si $f(x)$ es un polinomio, $f'(x)$ es su derivada, y $f(\delta) = f'(\delta) = 0$, entonces $f(x)$ tiene una raíz doble en δ.

2. Demuestre que si $y^2 = f(x)$ es singular, donde $f(x) \in K[x]$ es un polinomio cúbico mónico, entonces la singularidad debe ocurrir en $(\delta, 0)$, donde δ es una raíz de $f(x)$.

3. Demuestre que $(\delta, 0)$ es singular si y solo si δ es una raíz doble de $f(x)$. Por lo tanto $D = 0$ si y sólo si E es singular.

Problema 13. Sea $E/\mathbb{Q} : y^2 = x^3 + 3$. Encuentre todos los puntos de $\widetilde{E}(\mathbb{F}_7)$ y verifique que N_7 satisface la cota de Hasse.

Problema 14. Sea $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ y sea $p \geq 3$ un primo de mala reducción para $E/\mathbb{Q}$. Demuestre que $E(\mathbb{F}_p)$ tiene un punto singular único.

Problema 15. Sea $E : y^2 = x^3 - 10081x$. Utilice SageMath o Magma para encontrar un conjunto mínimo de generadores para el subgrupo que abarca todos estos puntos en E:

$$(0,0),\ (-100,90),\ \left(\frac{10081}{100}, \frac{90729}{1000}\right),\ (-17,408)$$

$$\left(\frac{907137}{6889}, -\frac{559000596}{571787}\right),\ \left(\frac{1681}{16}, \frac{20295}{64}\right), \left(\frac{833}{4}, \frac{21063}{8}\right)$$

$$\left(-\frac{161296}{1681}, \frac{19960380}{68921}\right), \left(-\frac{6790208}{168921}, -\frac{40498852616}{69426531}\right).$$

(Pista: use un teorema del curso para determinar el rango de $E/\mathbb{Q}$.)

Problema 16. Sea $E : y^2 = x^3 + Ax + B$ una curva elíptica con $A, B \in \mathbb{Q}$, y supongamos $P = (x_0, y_0)$ es un punto en E, con $y_0 \neq 0$.

1. Demuestre que la coordenada x de $2P$ está dada por

$$x(2P) = \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4y_0^2}.$$

2. Encuentra una fórmula para $y(2P)$ en términos de x_0 y y_0.

Problema 17. La curva $E/\mathbb{Q} : y^2 = x^3 - 157^2x$ tiene un punto racional Q con coordenada $x = x(Q)$ dada por

$$x = \left(\frac{2244035177043369699245575130906748631609484720 41}{1782466453785771917605107035793432714003296 1660}\right)^2.$$

Demuestre que existe un punto $P \in E(\mathbb{Q})$ tal que $2P = Q$. Encuentra las coordenadas de P. (Sugerencia: use SageMath o Magma y haga el ejercicio 16.)

Problema 18. Sea $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$ con $e_i \in \mathbb{Q}$, distinto, y tal que $e_1+e_2+e_3 = 0$. Además, supongamos que $e_1 - e_2 = n^2$ y $e_1 - e_3 = m^2$ son cuadrados. Este ejercicio muestra que, bajo estos supuestos, existe un punto $P = (x_0, y_0)$ tal que $2P = (e_1, 0)$, es decir, P es un punto de orden exacto 4.

1. Demuestre que $e_1 = \frac{n^2+m^2}{3}$, $e_2 = \frac{m^2-2n^2}{3}$, $e_3 = \frac{n^2-2m^2}{3}$.

2. Encuentre A y B, en términos de n y m, tales que $x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$. (Pista: SageMath o Magma pueden ser de gran ayuda aquí).

3. Sea $p(x) = x^4 - 2Ax^2 - 8Bx + A^2 - 4(x^3 + Ax + B)e_1$. Demuestre que $p(x_0) = 0$ si y solo si $x(2P) = e_1$, y por lo tanto $2P = (e_1, 0)$. (Pista: utilice el ejercicio 16.)

4. Expresa todos los coeficientes de $p(x)$ en términos de n y m. (Sugerencia: use SageMath o Magma).

5. Factorizar $p(x)$ para $(n, m) = (3, 6),\ (3, 12),\ (9, 12), \ldots$.

6. Supongo que $p(x) = (x - a)^2(x - b)^2$ para algunos a y b. Exprese todos los coeficientes de $p(x)$ en términos de a y b.

7. Finalmente, compare los coeficientes de $p(x)$ en términos de a, b y n, m y encuentre las raíces de $p(x)$ en términos de n, m. (Pista: compare primero el coeficiente de x^3 y luego el coeficiente de x^2.)

8. Escribe $P = (x_0, y_0)$ en términos de n y m.

Problema 19. Sean e_1, e_2, e_3 tres números enteros distintos. Demuestre que $\Delta = (e_1 - e_2)(e_2 - e_3)(e_1 - e_3)$ siempre es par.

Problema 20. En este ejercicio estudiamos la estructura del cociente $G/2G$, donde G es un grupo abeliano finito.

1. Sea $p \geq 2$ un primo y sea $G = \mathbb{Z}/p^e\mathbb{Z}$, con $e \geq 1$. Demuestre que $G/2G$ es trivial si y sólo si $p > 2$.

2. Demuestre que, si $G = \mathbb{Z}/2^e\mathbb{Z}$ y $e \geq 1$, entonces $G/2G \cong \mathbb{Z}/2\mathbb{Z}$.

3. Finalmente, sea G un grupo abeliano finito arbitrario. Definimos $G[2^\infty]$ como la componente primaria 2 de G, es decir,

$$G[2^\infty] = \{g \in G : 2^n \cdot g = 0 \text{ para algunos } n \geq 1\}.$$

   En otras palabras, $G[2^\infty]$ es el subgrupo de G formado por aquellos elementos de G cuyo orden es una potencia de 2. Pruebe que

$$G[2^\infty] \cong \mathbb{Z}/2^{e_1}\mathbb{Z} \oplus \mathbb{Z}/2^{e_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2^{e_r}\mathbb{Z}$$

   para algunos $r \geq 0$ y $e_i \geq 1$ (aquí $r = 0$ significa que $G[2^\infty]$ es trivial). Demuestre también que $G/2G \cong (\mathbb{Z}/2\mathbb{Z})^r$.

Problema 21. Demuestre que el espacio

$$C : \begin{cases} 2Y^2 - X^2 = 34, \\ Y^2 - Z^2 = 34 \end{cases}$$

no tiene soluciones racionales con $X, Y, Z \in \mathbb{Q}$. (Pista: modifique el sistema para que no haya potencias de 2 en ninguno de los denominadores, luego trabaje en módulo 8.)

Problema 22. Para las siguientes curvas elípticas, utilice el método de 2-descenso para encontrar la rango de $E/\mathbb{Q}$ y generadores de $E(\mathbb{Q})/2E(\mathbb{Q})$.

1. $E : y^2 = x^3 - 14931x + 220590$.

2. $E : y^2 = x^3 - x^2 - 6x$.

3. $E : y^2 = x^3 - 37636x$.

4. $E : y^2 = x^3 - 962x^2 + 148417x$.

Problema 23. Encuentre el rango y los generadores de los puntos racionales en la curva elíptica $y^2 = x(x + 5)(x + 10)$.

Problema 24. (Curvas elípticas con rango no trivial). El objetivo aquí es una forma sistemática de encontrar curvas de rango al menos $r \geq 0$ sin usar tablas de curvas elípticas:

1. (Fácil) Encuentre 3 curvas elípticas no isomorfas sobre $\mathbb{Q}$ con rango ≥ 2. Debe demostrar que el rango es de al menos 2. (Para mostrar independencia lineal, puede usar SageMath o Magma para calcular la matriz de altura).

2. (Aceptable) Encuentre 3 curvas elípticas no isomorfas sobre $\mathbb{Q}$ con rango ≥ 3.

3. (Dificultad media) Encuentre 3 curvas elípticas no isomorfas sobre $\mathbb{Q}$ con rango ≥ 6. Si es así, entonces probablemente puedas encontrar curvas de rango de $3 \geq 8$ también.

4. (Significantemente más difícil) Encuentre 3 elíptica no isomorfa curvas sobre $\mathbb{Q}$ de rango ≥ 10.

5. (¡Serías famoso!) Encuentre una curva elíptica sobre $\mathbb{Q}$ de rango ≥ 29.

Problema 25. Sea E una curva elíptica y supongamos que las imágenes de los puntos

$$P_1, P_2, \ldots, P_n \in E(\mathbb{Q})$$

en $E(\mathbb{Q})/2E(\mathbb{Q})$ genera el grupo $E(\mathbb{Q})/2E(\mathbb{Q})$. Sea G el subgrupo de $E(\mathbb{Q})$ generado por $P_1, P_2, \ldots, P_n$.

1. Demuestre que el índice de G en $E(\mathbb{Q})$ es finito, es decir, el grupo cociente $E(\mathbb{Q})/G$ es finito.

2. Demuestre que, dependiendo de la elección de los generadores $\{P_i\}$ del cociente $E(\mathbb{Q})/2E(\mathbb{Q})$, el tamaño de $E(\mathbb{Q})/G$ puede ser arbitrariamente grande.

Problema 26. El último teorema de Fermat muestra que $x^3 + y^3 = z^3$ no tiene soluciones enteras con $xyz \neq 0$. Encuentre el primer $d \geq 1$ tal que $x^3 + y^3 = dz^3$ tenga infinitas soluciones no triviales, encuentre un generador para las soluciones y escriba algunos ejemplos.

Problema 27. Encuentre la solución mas sencilla con números enteros $a, b, c \in \mathbb{Z}$ tales que

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = 4.$$

Problema 28. Encuentre la solución mas sencilla con números naturales $a, b, c \in \mathbb{N}$ tales que

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = 4.$$

Problema 29. Sea E la curva $y^2 = x^3 - 2$ definida sobre $\mathbb{F}_{17}$, y sea $P = (3, 5)$. ¿Puedes resolver el problema de logaritmo discreto de curva elíptica $x \cdot P = (13, 11)$? En otras palabras, encuentre un número entero $x \geq 1$ tal que $x \cdot P = (13, 11)$ en $E(\mathbb{F}_{17})$.

Problema 30. Sea E la curva $y^2 = x^3 - 2$ definida sobre $\mathbb{F}_{103}$, y sea $P = (3, 5)$.

1. Demuestre que el orden de P en $E(\mathbb{F}_{103})$ es 91.

2. Resuelve el problema de logaritmo discreto de curva elíptica $x \cdot P = (102, 93)$ en $E(\mathbb{F}_{103})$.

3. Demuestre que P es un generador de $E(\mathbb{F}_{103})$, es decir, si $Q \in E(\mathbb{F}_{103})$, entonces el problema de logaritmo discreto de curva elíptica $x \cdot P = Q$ siempre tiene solución.

(Sugerencia: utilice una computadora y el software Magma o SageMath.)

Problema 31. Sea $p = 541$ (que es un primo) y sea E la curva elíptica $y^2 = x^3 + x + 1$ definida sobre $\mathbb{F}_{541}$. Sea $P = (72, 70)$ en $E(\mathbb{F}_{541})$. La siguiente es una lista de los múltiplos $n \cdot P$ para $1 \leq n \leq 59$, en orden:

$$
\begin{gathered}
(72,70),(424,71),(9,110),(338,159),(255,123),\\
(161,528),(147,468),(168,416),(480,353),(454,92),\\
(360,174),(264,41),(152,438),(468,56),(437,44),\\
(68,447),(459,293),(115,326),(328,507),(278,318),\\
(113,117),(534,456),(307,277),(1,57,1),(491,440),\\
(107,249),(465,115),(67,517),(301,61),(301,480),\\
(67,24),(465,426),(107,292),(491,101),(1,484),\\
(307,264),(534,85),(113,424),(278,223),(328,34),\\
(115,215),(459,248),(68,94),(437,497),(468,485),\\
(152,103),(264,500),(360,367,1),(454,449),(480,188),\\
(168,125),(147,73),(161,13),(255,418),(338,382),\\
(9,431),(424,470),(72,471),(0:1:0),
\end{gathered}
$$

donde $(0 : 1 : 0)$ es $\mathcal{O}$, el punto en el infinito. En otras palabras, $P = (72, 70)$, $2P = (424, 71)$, $3P = (9, 110)$, ..., $6P = (161, 528)$, etc.

1. Verifica que el orden de P en $E(\mathbb{F}_{541})$ sea 59.

2. Rey y Finn quieren establecer una curva elíptica de intercambio de claves Diffie-Hellman con $p = 541$ y E y P como se indicó anteriormente. Rey elige $a = 10$ como su número entero secreto. ¿Qué punto A debería enviar Rey a Finn?

3. A continuación, Rey recibe $B = (459, 293)$ de Finn. Determina el punto secreto que comparten Rey y Finn.

4. El general Hux intercepta una comunicación entre Rey y Finn (no la de las partes (2) y (3), pero usando los mismos p, E y P. Hux ahora sabe que Rey envió $A = (534, 456)$ a Finn, y Finn envió $B = (255, 123)$ a Rey. Explica cómo Hux ahora puede encontrar el punto secreto que comparten Rey y Finn.