Tarea num. 6 – soluciones

1. (a) Demuestra que el conjunto de números primos es infinito.

   ▷ Construimos, a partir de una lista finita de primos $p_1, p_2, p_3, \ldots, p_n$, un primo nuevo. Sea $N = (p_1 p_2 p_3 \ldots p_n) + 1$. Sea p el mínimo divisor positivo de N. Entonces p es primo, porque si $d|p$, $d > 1 \Longrightarrow d|N \Longrightarrow d = p$ (porque p es el mínimo divisor de N, por su definición). Pero este p es un primo nuevo ya que ninguno de los primos viejos divide a N. ◁

   (b) El ejercicio de la página 30 de las notas.

   ▷ Empezando de $p_1 = 2$, tenemos $p_2 = 2 + 1 = 3$, $p_3 = 2 \cdot 3 + 1 = 7$, $p_4 = 2 \cdot 3 \cdot 5 + 1 = 31$, $22 \cdot 3 \cdot 5 \cdot 31 + 1 = 931 = 7 \cdot 7 \cdot 19 \Longrightarrow p_5 = 7$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 31 + 1 = 6511 = 17 \cdot 383 \Longrightarrow p_6 = 17$. ◁

   (c) (Opcional) Demostrar que hay infinidad de primos de la forma $4k + 3$.

   ▷ Construimos, a partir de una lista finita de primos $p_1, p_2, p_3, \ldots, p_n$ de la forma $4k + 3$, un nuevo tal primo. Sea $N = 4(p_1 p_2 p_3 \ldots p_n) + 3$. Notamos que el producto de enteros de la forma $4k+1$ es un entero de la misma forma. Así que si escribimos a N como producto de primos, no pueden ser todos de la forma $4k+1$; así que existe un primo p de la forma $4k+3$ que divide a N. Este p debe ser nuevo ya que ninguno de los primos viejos divide a N. ◁

2. (a) Sea $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, donde $p_1, p_2, \ldots, p_k$ son primos distintos y $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$. Encuentra el número de divisores positivos de N. (Ejercicio de la pág. 32 de las notas.)

   ▷ Según el teorema fundamental de aritmética, si $n|N$, $n > 1$, entonces n es un producto de primos que dividen a N, así que $n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, donde $0 \leq \beta_1 \leq \alpha_1, \ldots, 0 \leq \beta_k \leq \alpha_k$. El número de los divisores positivos de N es entonces $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1)$. ◁

   (b) ¿Cuántos divisores positivos tiene 1000?

   ▷ $1000 = 2^3 \cdot 5^3 \Longrightarrow$ 1000 tiene $4 \cdot 4 = 16$ divisores positivos. ◁

3. Sea p un primo. Demuestra que para todo $a \in \mathbb{Z}$, $a^p \equiv a \mod p$.

   ▷ Si $a \equiv 0 \Longrightarrow a^p \equiv 0^p \equiv 0 \equiv a$ (todas son congruencias mod p). Si $[a] \neq 0$, consideramos los primeros p múltiplos de a: $0, a, 2a, 3a, \ldots, (p-1)a$. Ningun par de ellos es congruente, ya que $ka \equiv la \Longrightarrow k - l \equiv 0$, pero $0 \leq k - l \leq p - 1 \Longrightarrow k - l = 0 \Longrightarrow k = l$. Así que las clases de congruencia de estos p números son *todas* las clases de congruencia mod p. Así que si tomamos el producto de estos números (excepto 0), obtenemos $1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a(2a)(3a) \cdots [(p-1)a] \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)a^{p-1}$. Ahora los números $1, 2, 3, \ldots, p-1$ son invertibles mod p, así que tambien $(p-1)!$ lo es, así que la última congruencia implica $a^{p-1} \equiv 1$. Esta última multiplicamos por a y obtenemos $a^p \equiv a$. ◁

   Notas: 1. Este resultado se llama "el pequeño teorema de Fermat". Fue demostrado en el siglo 18 y forma la base para una aplicaciones reciente de la teoría de números a la criptología (codoficacion de información).

   2. El convesro de este resultado no es cierto: hay numeros $n \in \mathbb{Z}$, $n > 1$, que satisfacen $a^n \equiv a \mod n$, $\forall a \in \mathbb{Z}$, pero sin embargo no son primos.

4. Sean a, b dos enteros, $b > 0$.

   (a) Demuestra que existen $q, r \in \mathbb{Z}$ tal que $a = bq + r$, $0 \leq r < b$. ¿Son únicos estos q, r?

   ▷ Sea q la parte entera de a/b. Entonces $a/b = q + \alpha$, donde $0 \leq \alpha < 1$. Entonces $a = bq + b\alpha$. Toma $r = b\alpha$. Entonces $0 \leq \alpha < 1 \Longrightarrow 0 \leq r < b$. Unicidad: si $bq_1 + r_1 = bq_2 + r_2 \Longrightarrow b(q_1 - q_2) = (r_2 - r_1)$. Pero $|r_2 - r_1| < b$ y es un múltiplo de b, así que $r_2 - r_1 = 0$. Tenemos entonces $b(q_1 - q_2) = 0$. Como $b \neq 0 \Longrightarrow q_1 - q_2 = 0$.

   (b) Demuestra que si $a = bq + r$, $0 \leq r < b \Longrightarrow (a, b) = (b, r)$.

   ▷ Sea $d = (a, b)$. Entonces $d|a$, $d|b \Longrightarrow d|(a - bq) = r \Longrightarrow d \leq (b, r) = d'$. Por otro lado $d' = (b, r)$ satiface $d'|b$, $d'|r \Longrightarrow d'|bq + r = a \Longrightarrow d' \leq (a, b) = d$. Así que $d = d'$. ◁

   (c) Encuentra $(1804, 328)$.

   ▷ Aplicando el algoritmo de Euclides:

$$\begin{aligned} 1804 &= 328 \cdot 5 + 164, \\ 328 &= 164 \cdot 2 \\ \Longrightarrow (1804, 328) &= (328, 164) = 164. \end{aligned}$$

   ◁

(d) (Opcional) Escribe 2003 en base 7.

▷ Dividiendo sucesivamente por 7 (guardando al lado los residuos), $2003 = 7 \cdot 286 + 1$, $286 = 7 \cdot 40 + 6$, $40 = 7 \cdot 5 + 5$, obtenemos: $2003 = 5 \cdot 7^3 + 5 \cdot 7^2 + 6 \cdot 7 + 1$, así que 2003 se escribe en base 7 como 5561. ◁

(e) Demuestra que existen $x, y \in \mathbb{Z}$ tal que $(a, b) = ax + yb$.

▷ Aplicando el algoritmo de Euclides a (a, b), se obtiene $a = bq_1 + r_1$, $b = r_1q_2 + r_2$, $r_1 = r_2q_2 + r_3, \dots$, $r_{n-2} = r_{n-1}q_{n-1} + r_n$, $r_{n-1} = r_nq_n \implies (a, b) = r_n$. Ahora demostramos por inducción (finita) sobre k, $k = 1, 2, \dots, n$, que cada residuo $r_k = ax_k + by_k$, para unos $x_k, y_k \in \mathbb{Z}$; en particular, para $k = n$ obtenemos $(a, b) = r_n = ax_n + by_n$. Para $k = 1$ tenemos: $a = bq_1 + r_1 \implies r_1 = bq_1 - a \implies x_1 = -1,\ y = q_1$ cumplen. Ahora suponemos que $r_i = ax_i + by_i$, $i \leq k-1$; para r_k tenemos: $r_{k-2} = r_{k-1}q_{k-1} + r_k \implies r_k = r_{k-2} - r_{k-1}q_{k-1} = (ax_{k-2} + by_{k-2}) - (ax_{k-1} + by_{k-1})q_{k-1} = a(x_{k-2} - q_{k-1}x_{k-1}) + b(y_{k-2} - q_{k-1}y_{k-1})$, así que $x_k := x_{k-2} - q_{k-1}x_{k-1},\ y_k := y_{k-2} - q_{k-1}y_{k-1}$ cumplen.

◁

(f) Encuentra x, y del último inciso para $a = 1804$, $b = 328$.

▷ Del inciso c): $(1804, 328) = 164 = 1804 - 5 \cdot 328 \implies x = 1,\ y = -5$. ◁

(g) Concluye que si $(a, n) = 1$, $n > 1$, entonces $[a] \in \mathbb{Z}_n$ tiene inversa multiplicativa.

▷ Si $(a, n) = 1$ entonces, según el inciso anterior, existen $x, y \in \mathbb{Z}$ tal que $1 = ax + ny$, lo cual implica $ax - 1 \in n\mathbb{Z} \implies ax \equiv 1 \mod n$. En otras palabras, $[x] = [a]^{-1}$. ◁

(h) Concluye que $\mathbb{Z}_p$ es un campo si p es un primo.

▷ Ya sabemos que $\mathbb{Z}_p$ es un anillo (demostrado en clase). Falta ver que todo elemento de $\mathbb{Z}_p$ distinto de $[0]$ tiene inversa multiplicativa. Si $[a] \in \mathbb{Z}_p$, $[a] \neq [0] \implies p \nmid a$ (p no divide a a) $\implies (a, p) = 1$ (ya que el único divisor de p que es mayor que 1 es p mismo) $\implies [a]$ es invertible en $\mathbb{Z}_p$, por el inciso anterior.

(i) Encontrar todas las inversas multiplicativas en $\mathbb{Z}_{31}$.

▷ Denotamos las clases no nulas por $[1], [2], \dots, [30]$. Claramente, $[1]$ y $[30] = -[1]$ son sus propias inversas. Las demas 28 clases se parten en 14 parejas, cada clase con su inversa: $[2][16] = [3][21] = [4][8] = [5][25] = [6][26] = [7][9] = [10][28] = [11][17] = [12][13] = [14][20] = [15][29] = [18][19] = [22][24] = [1]$. Aquí estan los detalles de algunos de los cálculos.

$$\begin{aligned}
\frac{1}{2} &\equiv \frac{32}{2} = 16 \\
\frac{1}{3} &\equiv -\frac{30}{3} \equiv -10 \equiv 21, \\
\frac{1}{4} &\equiv \frac{32}{4} = 8, \\
\frac{1}{5} &\equiv -\frac{30}{5} = -6 \equiv 25, \\
\frac{1}{6} &\equiv -5 \equiv 26, \\
\frac{1}{7} &\equiv \frac{35-3}{7} \equiv 5 - \frac{3}{7} \implies \frac{4}{7} \equiv 5 \implies \frac{1}{7} \equiv \frac{5}{4} \equiv 5 \cdot 8 = 40 \equiv 9.
\end{aligned}$$