Exámen parcial 1 – soluciones

1. *a*) (5 pts) Sea $p \in \mathbb{Z}$. Define: p es un primo.

   ▷ Un entero p es primo si $p > 1$ y sus únicos divisores positivos son 1 y p. □

   b) (20 pts) Demuestra: existe una infinidad de primos de la forma $4k+3$, $k \in \mathbb{Z}$.

   ▷ Demostramos para todo $n > 0$, que si $p_1, \ldots, p_n$ son n primos distintos de la forma $4k+3$, entonces existe un primo distinto de estos n primos, que es de la forma $4k+3$.
   Sea $M = 4p_1p_2\cdots p_n + 3$. Si es primo hemos terminado ya que es de la forma requirida y es mayor a cada uno de los p_i. Si M no es primo entonces es un producto de primos (por el teorema fundamental de arítmetica: "todo entero mayor que 1 es el producto de primos de manera única, salvo el orden". La únicidad aquí de hecho no se usa). Digamos $M = q_1q_2\cdots q_m$.
   Notemos ahora que $p_i \neq q_j$ para todo $1 \leq i \leq n$, $1 \leq j \leq m$. Esto es porque $M \equiv 0 \mod q_j$ y $M \equiv 1 \mod p_i$. Así que basta ver que uno de los q_j es de la forma $4k+3$.
   Si no, entonces todos los q_j son de la forma $4k+1$. (Notamos que con la excepción de 2, todo primo es impar, así que es de la forma $4k+3$ o $4k+1$. Ninguno de los q_j puede ser 2, ya que M, por su defínción, es impar). Tendremos entonces que por un lado

   $$M = 4p_1\cdots p_n + 3 \equiv 3 \mod 4,$$

   y por otro lado

   $$M = q_1\cdots q_m \equiv 1\cdot 1\cdots 1 = 1 \mod 4,$$

   lo cual nos lleva a una contradicción, así que alguno de los q_j es de la forma $4k+3$ y es distinto de todos los p_i's. □

2. *a*) (5 pts) Sean $a, b \in \mathbb{Z}$. Define: a, b son primos relativos.

   ▷ a, b son primos relativos si su máximo común divisor es 1. Es decir, para todo entero d, si $d|a, b \implies d \leq 1$. □

   b) (20 pts) Demuestra: si $p \in \mathbb{Z}$ es un primo entonces $a^p \equiv a \mod p$ para todo $a \in \mathbb{Z}$.

   ▷ Si $p|a \implies a \equiv 0 \mod p \implies a^p \equiv 0^p \equiv 0 \equiv a \mod p$.
   Si p no divide a a entonces a es primo relativo con p (porque los únicos divisores positivos de p son 1 y p), y entonces a tiene un recíproco mod p (según el teorema demostrado en la tarea: "si $a, n \in \mathbb{Z}$, $n > 1$, son primos relativos, entonces a tiene un recíproco mod n). Tenemos entonces un entero b tal que $ab \equiv 1 \mod p$. Tomemos ahora las p clases de congruencias mod p:

   $$[0], [1], [2], [3], \ldots, [p-1].$$

   Multiplicamos cada una por $[a]$ y obtenemos

   $$[0], [a], [2a], [3a], \ldots, [a(p-1)].$$

   Veremos ahora que estas p clases son todas distintas. Si $[ia] = [ja]$, con $0 \leq i \leq j \leq p-1$, entonces multiplicando ambos lados por $[b]$, $[iab] = [jab]$, pero $[ab] = [1]$, entonces tendremos $[i] = [j]$. Pero esto es imposible, ya que $[0], [1], [2], [3], \ldots, [p-1]$ son todos distintos.
   Concluimos entonces que las p clases $[0], [a], [2a], [3a], \ldots, [a(p-1)]$ coinciden con las p clases $[0], [1], [2], [3], \ldots, [p-1]$ (capaz en otro orden). Eliminando $[0]$ de ambos conjuntos de clases, tenemos que $\{[a], [2a], [3a], \ldots, [a(p-1)]\} = \{[1], [2], [3], \ldots, [p-1]\} \implies [a][2a][3a]\cdots[a(p-1)] = [1][2][3]\cdots[p-1] \implies [a^{p-1}][1][2][3]\cdots[p-1] = [1][2][3]\cdots[p-1]$, y multiplicando la última igualdad por los recíprocos de $[1], [2], [3], \ldots, [p-1]$ se obtiene $[a^{p-1}] = [1]$. Multiplicando ambos lados por $[a]$ se obtiene $[a^p] = [a]$, ó $a^p \equiv a \mod p$. □

3. (50 pts, 5 pts cada inciso) Hay que responder "Cierto" o "Falso" a cada uno de los incisos abajo, y luego dar una explicación *breve* (1-2 frases, no tienes que dar una demostración formal completa.)

a) Existe un entero positivo k tal que $2^k \equiv 3 \mod 1000$.

▷ Falso, ya que $2^k \equiv 3 \mod 1000 \implies 2^k \equiv 3 \mod 2$, pero $2^k \equiv 0 \mod 2$ y $3 \equiv 1 \mod 2$. □

b) Para todo enteros positivos m, n, si m tiene un recíproco mod n entonces n tiene un recíproco mod m.

▷ Cierto, ya que ambas condiciones son equivalentes a que m, n son primos relativos (una relación que obviamente no depende del orden de m, n). □

c) Para todo entero n en el rango $1 \leq n \leq 2008$, la representación de n en base 2 requiere no más que 10 dígitos.

▷ Falso, ya que $2^{10} = 1024$ requiere 11 dígitos. □

d) Para todo entero n, si 22 y 23 dividen a n entonces $22 \cdot 23$ también divide a n.

▷ Cierto, ya que $22, 23$ son primos relativos (como cualquier dos enteros positivos sucesivos), así que por el teorema chino de residuos, $n \equiv 0 \mod 22$, $n \equiv 0 \mod 23 \iff n \equiv 0 \mod 22 \cdot 23$. □

e) Existe un entero n tal que $n^{99} \equiv 100 \mod 101$.

▷ Cierto, ya que $100^{99} \equiv -1^{99} \equiv -1 \equiv 100 \mod 101$.

f) Existe un entero n tal que $n^{99} \equiv 2008 \mod 101$.

▷ Cierto. Como $99^2 \equiv (-1)^2 \equiv 1 \mod 100$, existe un entero positivo k tal que $99^2 = 1 + 100k$. Tomamos ahora cualquier entero n tal que $n \equiv 2008^{99} \mod 101$, y tenemos (por el teorema de Fermat, problema 2b) que $n^{99} \equiv (2008^{99})^{99} \equiv 2008^{99^2} \equiv 2008^{1+100k} \equiv (2008^{100})^k 2008 \equiv 2008 \mod 101$. □

g) Para todo enteros positivos m, n, su mínimo común múltiplo divide a mn.

▷ Cierto, ya que $mn = (m, n)[m, n]$. □

h) 3 divide a $1 + 2 + 2^2 + 2^3 + \cdots + 2^{2008}$.

▷ Falso. $2 \equiv -1 \mod 3 \implies 1+2+2^2+2^3+\cdots+2^{2008} \equiv 1+(-1)+(-1)^2+(-1)^3+(-1)^{2008} \equiv 1 \mod 3$. □

i) Sean $p_1 < p_2 < \ldots < p_{1000}$ primos distintos. Existe un entero $k > 1$ tal que k^2 divide a $p_1 p_2 \cdots p_{1000}$.

▷ Falso, ya que en la factorización en primos de k^2 cada primo aparece un número par de veces (2 o más) mientras que en la factorización de $p_1 p_2 \cdots p_{1000}$ cada primo aparece una sola vez . □

j) Existen enteros positivos a, b tal que $3^a = 5^b$.

▷ Falso, por el teorema funadmental de la aritmética. □