Guia para el exámen parcial 1 - unas soluciones

Fecha del exámen: miercoles, 4 oct, 2017.

Profesor: Gil Bor, CIMAT.

Definiciones:

- La *representación* de $a \in \mathbb{Z}$ en base n (un entero mayor que 1) es la expresión
$$n = \varepsilon \left(d_k d_{k-1} \dots d_1 d_0\right)_n ,$$
donde $\varepsilon \in \{1, -1\}$, $d_i \in \{0, 1, \dots, n-1\}$, $i = 0, 1, \dots k$, y $a = \varepsilon \left(d_0 + d_1 n + \dots + d_k n^k\right)$.
- Un *divisor* de un entero $n \in \mathbb{Z}$ es un entero $d \in \mathbb{Z}$ tal que (1) $d \neq 0$, (2) existe $k \in \mathbb{Z}$ tal que $n = dk$. Notación: $d|n$ ("d divide a n").
- El *máximo común divisor* de $a, b \in Z$ es el máximo $d \in \mathbb{Z}$ tal que $d|a$ y $d|b$. Notación: $d = (a, b)$.
- Dos enteros $a, b \in \mathbb{Z}$ son *primos relativos* si $(a, b) = 1$.
- Un *primo* es un entero $p \in \mathbb{Z}$ tal que (1) $p > 1$, (2) sus únicos divisores positivos son $1, p$.
- Sea $n \in \mathbb{Z}$, $n > 1$. Dos enteros $a, b \in \mathbb{Z}$ son *congruentes* módulo n si $n|a - b$; notación $a \equiv b \bmod n$. La *clase de congruencia* módulo n de $a \in \mathbb{Z}$ es el conjunto de enteros congruente a $a \bmod n$; notación: $[a]$. $\mathbb{Z}_n$ es el conjunto de las clases de congruencias $\bmod n$. La suma y el producto en $\mathbb{Z}_n$ están definidos por $[a] + [b] := [a + b]$, $[a][b] := [ab]$.
- Una *inversa multiplicativa* (recíproco) módulo n de un entero $a \in \mathbb{Z}$ es un entero $b \in \mathbb{Z}$ tal que $ab \equiv 1 \bmod n$. Una inversa multiplicativa de un elemento $[a] \in \mathbb{Z}_n$ es un elemento $[b] \in \mathbb{Z}_n$ tal que $[a][b] = [1]$.
- $\mathbb{Z}_n^*$ es el conjunto de los elementos en $\mathbb{Z}_n$ que tienen inversa multiplicativa.
- La función de Euler $\phi(n)$ es el número de elemento en $\mathbb{Z}_n^*$.

  Nota: un teorema improtante (ver abajo) afirma que $[a] \in \mathbb{Z}_n^*$ si y solo si $(a, n) = 1$. En unos libros se usa este teorema para dar una definición alternativa: $\phi(n)$ es el número de enteros $0 \leq a < n$ tal que $(a, n) = 1$.
- El *orden* de un elemento $[a] \in \mathbb{Z}_n^*$ es el mínimo entero $d > 0$ tal que $a^d \equiv 1 \bmod n$.
- Una *raíz primitiva* módulo n es un elemento $[a] \in \mathbb{Z}_n^*$ cuyo orden es $\phi(n)$.
- El logaritmo discreto $\log_a b \bmod n$, donde $[a]$ es una raíz primitiva módulo n y $[b] \in \mathbb{Z}_n^*$, es el mínimo entero $k \geq 0$ tal que $a^k \equiv b \bmod n$.

Teoremas: hay que saber las demostraciones de los siguientes teoremas.

1. El teorema fundamental de la aritmética: dado un entero $n > 1$ existe una única sucesión de primos $p_1 \leq p_2 \leq \dots \leq p_k$ tal que $n = p_1 p_2 \cdots p_k$.
2. Existe una infinidad de números primos.
3. División con resíduo: dados $a, n \in \mathbb{Z}$ con $n > 0$, existen únicos $k, r \in \mathbb{Z}$, con $0 \leq r < n$, tal que $a = nk + r$. Terminología: r es el resíduo de a módulo n.
4. El algoritmo de Euclides: dados dos enteros $a, b \in \mathbb{Z}$, con $|a| \geq |b| \geq 0$, se define una sucesión finita de enteros no negativos por $a_1 = |a|$, $a_2 = |b|$, y luego para $n \geq 2$, si $a_n > 0$, a_{n+1} es el resíduo de a_{n-1} módulo a_n; si $a_n = 0$ la sucesión termina en a_n. Entonces: (1) la sucesión es finita; es decir, $a_n = 0$ para algun n; (2) $(a, b) = a_{n-1}$.

5. El Teorema de Euler-Fermat: si $a, n \in \mathbb{Z}$, $n > 1$ y $(a, n) = 1$ entonces $a^{\phi(n)} \equiv 1 \text{ mód } n$.

6. El Teorema Chino de Residuos: dados n enteros positivos $m_1, \ldots, m_n$, tal que $(m_i, m_j) = 1$ para todo $1 \leq i < j \leq n$ ("primos relativos en pares"), y n enteros $a_1, \ldots a_n$, (1) existe una solución $x \in \mathbb{Z}$ al sistema de congruencias $x \equiv a_i \text{ mód } m_i$, $i = 1, \ldots n$; (2) la solución es única módulo $m_1 m_2 \cdots m_n$ (el conjunto de soluciones al sistema es una clase de congruencia módulo $m_1 m_2 \cdots m_n$).

   Reformulación: la función $\mathbb{Z}_n \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ que manda una clase $[x] \in \mathbb{Z}_n$ a $(c_1, \ldots, c_n)$, donde c_i es la clase de congruencia de $x \text{ mód } m_i$, es una biyección.

7. Sean $a, n \in \mathbb{Z}$, $n > 1$. Entonces $a \in \mathbb{Z}$ tiene un recíproco módulo n si y solo si $(a, n) = 1$. Reformulación: Dados $a, b \in \mathbb{Z}$, $ax + by = 1$ tiene una solución si y solo si $(a, b) = 1$.

8. $\phi(ab) = \phi(a)\phi(b)$ si $(a, b) = 1$.

Calcular (sin calculadora):

1. La representación en bases 2 y 3 de los siguientes números, dados en base 10: 2, 10, 11, 100.

   ▷ En base 2: se divide sucesivamente entre 2, hasta llegar a 0, y luego se lee la sucesión de residuos (escritos arriba de las flechas) de la derecha a la izquierda:

   $$100 \xrightarrow{0} 50 \xrightarrow{0} 25 \xrightarrow{1} 12 \xrightarrow{0} 6 \xrightarrow{0} 3 \xrightarrow{1} 1 \xrightarrow{1} 0.$$

   Así que $100 = (1100100)_2$.

   En base 3:

   $$100 \xrightarrow{1} 33 \xrightarrow{0} 11 \xrightarrow{2} 3 \xrightarrow{0} 1 \xrightarrow{1} 0.$$

   Así que $100 = (10201)_3$. □

2. La representación en bases 2 y 10 de los siguientes números, dados en base 3: 2, 10, 11, 100.

   ▷ $(100)_3 = 3^2 = 9 = 8 + 1 = (101)_2$. □

3. El mínimo y máximo posible número de dígitos necesarios para representar un número en base 2, si se requiere 100 dígitos para reperentarlo en base 10. (Nota: $\log_2 10 = 3.321928\ldots$)

   ▷ $n \in \mathbb{N}$ tiene 100 dígitos en base 10 si y solo si $10^{99} \leq n < 10^{100}$ y tiene d dígitos en base 2 si y solo si $2^{d-1} \leq n < 2^d$. Así que $2^{d_{min}-1} \leq 10^{99} < 2^{d_{min}}$, lo cual es equivalente a $d_{min} - 1 \leq 99 \log_2 10 < d_{min}$, o $d_{min} = [99 \log_2 10] + 1$. Ahora $99 \log_2 10 = 100 \log_2 10 - \log_2 10 = 332.19\ldots - 3.32\ldots = 329.8\ldots$, así que $d_{min} = 330$. Para calcular d_{max} observamos primero que 10^{100} no es una potencia de 2 (ninguna potencia de 2 termina con 0 en base 10), por lo que su número de dígitos en base 2 es el mismo que el número de digitos de $10^{100} - 1$ en base 2, o sea d_{max}. Así que $2^{d_{max}-1} \leq 10^{100} < 2^{d_{max}}$, por lo que $d_{max} = [100 \log_2 10] + 1 = 333$. □

4. El número de veces que aparece el dígito 7 en la lista de todos los números de 1 hasta 2017 en base 10. Mismo para base 9.

   ▷ Primero determinamos el número de veces que aparece 7 en el rango 0-999. Los números con menos de 3 dígitos les completamos con ceros en frente. De este modo todos los 10 dígitos aparecen el mísmo números de veces. En total son $1000 \times 3 = 3000$ dígitos, así que cada dígito aparece 300 veces. Luego en el rango 1000-1999 aparece 7 el mismo número de veces que en 0-999, y en 2000-2017 aparece 2 veces, así que la respuesta es 602 veces (en base 10). □

5.* La representación en base 2 de 0.1, 0.01, 1/3, $\sqrt{2}$ (primeros 5 dígitos).

   ▷ $0.1 = (0.0\overline{0011})_2$, $0.01 = (0.00\overline{0000101001111010111})_2$, $1/3 = 0.\overline{01}$, $\sqrt{2} = (1.01101\ldots)_2$. □

6. Todos los divisores (positivos y negativos) de: $10, -1, 0, 2^5$.

   ▷ $\text{Div}(10) = \{10, 5, 2, 1, -1, -2, -5, -10\}$, $\text{Div}(-1) = \{1, -1\}$, $\text{Div}(0) = \mathbb{Z} \setminus \{0\}$, $\text{Div}(2^5) = \{32, 16, 8, 4, 2, 1, -1, -2, -4, -8, -16, -32\}$.

7. El número de divisores positivos de 10^{10}.

   ▷ Son todos los números de la forma $2^a 5^b$, $0 \leq a, b \leq 10$, por lo que son $11^2 = 121$ divisores. □

8. El máximo común divisor de 2015 y 2017.

   ▷ El residuo de 2017 mód 2015 es 2, y de 2015 mód 2 es 1, por lo que $(2017, 2015) = 1$. □

9. El máximo común divisor y el mínimo comun múltiplo de 2015^{2017} y 2017^{2015}.

   ▷ 2017 es un primo que no divide a 2015, por lo que $(2015^{2017}, 2017^{2015}) = 1$ y sus mínimo comun múltiplo es su producto.

10. El recíproco de 61 módulo 117 y el recíproco de 117 módulo 61.

    ▷ $117 = 2{\cdot}61{-}5$, $61 = 12{\cdot}5{+}1$, $\implies 1 = 61{-}12{\cdot}5 = 61{-}12{\cdot}(2{\cdot}61{-}117) \equiv 61{\cdot}(1{-}24){+}117{\cdot}12 = 61 \cdot (-23) + 117 \cdot 12$, por lo que q $61^{-1} \equiv -23 \equiv 94 \text{ mód } 117$, y $117^{-1} \equiv 12 \text{ mód } 61$. □

11. Las raices primitivas módulo 17 y los logarítmos discretos $\log_r 16 \text{ mód } 17$, donde r es cada una de las raices primitivas módulo 17.

    ▷ El orden de un elemento divide a $\phi(17) = 16$, por lo que los ordenes posibles de elementos $1 < r < 17$ son $2, 4, 8, 16$. Ahora $2^4 = 16 \equiv -1 \implies 2^8 = 1 \implies \pm 2, \pm 4, \pm 8$ no son primitivos. Luego $3^4 = 81 \equiv 1 \implies \pm 3, \pm 6$ no son primitivos. Luego $5^2 = 25 \equiv 8 = 2^3 \implies 5^8 \equiv 2^{12} \equiv 2^4 \equiv -1 \implies \pm 5$ son primitivos. Luego $7^2 \equiv -2 \implies 7^8 \equiv 2^4 \equiv -1$ por lo que ± 7 son primitivos. Resumen: $\pm 5, \pm 7$ son las raices primitivas mód 17.

    $\log_{\pm 5} 16 = \log_{\pm 5}(-1) = 8$, $\log_{\pm 7}(-1) = 8$.

12. El resíduo de 2015^{2017} módulo 1001.

    ▷ Sea $x = 2015^{2017}$. Notamos que $1001 = 7 \cdot 11 \cdot 13$, así que basta calcular los residuos de $x \text{ mód } 7, 11, 13$. Módulo 7: $2015^{2017} \equiv (2015 \text{ mód } 7)^{2017} = (-1)^{2017} = -1$. Módulo 11: $2015^{2017} \equiv (2015 \text{ mód } 11)^{2017 \text{ mód } 10} = 2^7 = 7$; Mód 13: $2015^{2017} \equiv (2015 \text{ mód } 13)^{2017} = 0$; así que $x \equiv -1 \text{ mód } 7, x \equiv 7 \text{ mód } 11$ y $x \equiv 0 \text{ mód } 13 \implies x = 13y \equiv 2y \equiv 7 \equiv -4 \text{ mód } 11 \implies y \equiv -2 \text{ mód } 11 \implies x = 13(-2 + 11z) \equiv -1 \text{ mód } 7 \implies z \equiv -1 \text{ mód } 7 \implies x = 13(-2 + 11(-1)) = -13^2 \equiv 832 \text{ mód } 1001$.

13. El número de elementos en $\mathbb{Z}^*_{2016}$.

    ▷ $\#\mathbb{Z}^*_{2016} = \phi(2016) = \phi(2^5 3^2 7) = \phi(2^5)\phi(3^2)\phi(7) = (2^5 - 2^4)(3^2 - 3)6 = 576$.

14. Los ordenes del los elementos de $\mathbb{Z}^*_{18}$.

    ▷ $\phi(18) = \phi(2 \cdot 3^2) = \phi(2)\phi(3^2) = 1 \cdot 6 = 6$. Así que los ordenes posibles son 1, 2, 3, 6. $\mathbb{Z}^*_{18} = \{\pm 1, \pm 5, \pm 7\}$. Luego, $ord(1) = 1$, $ord(-1) = 2$, $5^2 \equiv 7, 5^3 \equiv -1 \implies (-5)^3 \equiv 1 \implies ord(5) = 6, ord(-5) = 3$, $7^3 \equiv 1 \implies (-7)^3 = -1 \implies ord(7) = 3, ord(-7) = 6$.

Demostrar:

1. Un número entero n es compuesto si y solo si tiene un divisor primo p en el rango $2 \leq p \leq \sqrt{n}$.

   ▷ Si n tiene un divisor primo $p < n$ entonces, por defínción, n es compuesto. En la otra dirección, si n es compuesto $\implies$ existen $a, b > 1$ tal que $n = ab$. Digamos $a \leq b$ y p es un divisor primo de $a \implies p \leq a = \sqrt{a^2} \leq \sqrt{ab} = \sqrt{n}$. □

2. Cada elemento de $\mathbb{Z}_n$ tiene a lo más un recíproco.

   ▷ Sean $[a], [b], [b'] \in \mathbb{Z}_n$ tal que $[a][b] = [a][b'] = [1] \implies [b'] = [1][b'] = ([b][a])[b'] = [b]([a][b']) = [b][1] = [b]$. □

3. 13 divide a $4^{2n+1} + 3^{n+2}$ para todo entero $n \geq 0$.

   ▷ Por inducción sobre n. Para $n = 0$, $4^{2\cdot 0+1}+3^{0+2} = 4+9 = 13$. Luego, suponiendo para n, para $n+1$ tenemos $4^{2(n+1)+1}+3^{(n+1)+2} = 4^{2n+1}\cdot 16+3^{n+2}3 \equiv 4^{2n+1}\cdot 3+3^{n+2}3 = (4^{2n+1}+3^{n+2})3 \equiv 0 \cdot 3 = 0 \mod 13$. □

4. Si $a, b, c \in \mathbb{Z}$ satisfacen $a^2 + b^2 = c^2$ entonces 60 divide a abc.

   ▷ Notamos que $60 = 3 \cdot 4 \cdot 5 \implies$ basta demostrar que $abc \equiv 0$ módulo 3,4 y 5 (usando el Teorema Chino de Resíduos). Módulo 3, los cuadrados son 0 y 1, luego $1 + 1 \not\equiv 1 \implies$ uno (por lo menos) de a^2, b^2, c^2 es $\equiv 0$. Pero $x^2 \equiv 0 \mod 3 \implies x \equiv 0 \mod 3 \implies$ uno de a, b, c es $\equiv 0 \mod 3 \implies abc \equiv 0 \mod 3$. Módulo 5 es similar: los cuadrados son $0, \pm 1$, luego $\pm 1 \pm 1 \not\equiv \pm 1 \implies$ uno de a^2, b^2, c^2 es $\equiv 0 \implies$ uno de a, b, c es $\equiv 0 \mod 5 \implies abc \equiv 0 \mod 5$. Módulo 4 el mismo argumento no funciona porqué $2^2 + 2^2 \equiv 2^2 \mod 4$. Pasamos a módulo 8. Los cuadrados son $0, 1, 4$ así que uno de a^2, b^2, c^2 es $\equiv 0 \mod 8$. Luego, $x^2 \equiv 0 \mod 8 \implies x \equiv 0$ o $4 \mod 8 \implies x \equiv 0 \mod 4$. □

5. Si a, b son enteros positivos, entonces $ab/(a, b)$ es su mínimo común múltiple.

6. Si $a, b, c \in \mathbb{Z}$ y $a \neq 0$ entonces $a|bc, (a, b) = 1$, implica $a|c$.

7. Si $n = am + r$ entonces $(n, a) = (a, r)$.

8. En la sucesión 1,1,2,3,5,8,13,..., (cada término, empezando con el tercero, es la suma de los dos anteriores), cada dos elementos consecutivos son primos relativos.

9. Hay una infinidad de primos de la forma $4k + 3$, $k \in \mathbb{Z}$.

   ▷ Construimos por inducción una sucesión infinita de primos de esta forma, empezando con $p_1 = 3$. Si ya tenemos a $p_1, \ldots, p_n$, definimos a $P := (p_1 \cdots p_n)^2 + 2$. Claramente, $P \equiv 3 \mod 4$ y $P > p_i$, $i = 1, \ldots, n$, así que si P es primo, es un primo nuevo de la forma $4k + 3$ y podemos definir $p_{n+1} = P$. Si P no es primo, examinamos a sus divisores primos. Como P es impar, todos sus divisores primos son impares, de la forma $4k+1$ o $4k+3$. Si todos fueron de la forma $4k + 1$ entonces tambien P seria de esta forma; así que P tiene un divisor primo, digamos p, de la forma $4k + 3$. Luego p no puede ser ninguno de los $p_1, \ldots, p_n$, ya que $P \equiv 0 \mod p$ y $P \equiv 2 \not\equiv 0 \mod p_i$, $i = 1, \ldots, n$. Así que podemos definir $p_{n+1} = p$. □

10.* Hay una infinidad de primos de la forma $4k + 1$, $k \in \mathbb{Z}$.

11. 9973 es un primo.

12. Si $n = p_1^{\alpha_1} p_2^{\alpha_1} \cdots p_m^{\alpha_m}$ es la descomposición de un entero $n > 1$ en producto de primos, donde $p_1, \ldots, p_m$ son primos distintos, entonces

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right).$$

   ▷ $\phi(n) = \phi(p_1^{\alpha_1} \cdots p_m^{\alpha_m}) = \phi(p_1^{\alpha_1}) \cdots \phi(p_m^{\alpha_m}) = p_1^{\alpha_1}(1-\frac{1}{p_1}) \cdots p_m^{\alpha_1}(1-\frac{1}{p_m}) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right)$.

Cierto o Falso

1. Si $d, a, b \in \mathbb{Z}$, $d \neq 0$, $d|ab$, entonces $d|a$ ó $d|b$.

   ▷ Falso. $4|2 \cdot 2$.

2. Si $a \not\equiv 0 \mod n$ entonces a tiene un recíproco $\mod n$.

   ▷ Falso. $2 \not\equiv 0 \mod 4$ pero no tiene recíproco $\mod 4$.

3. $(a, b) = (a, a + b)$ para todo $a, b \in \mathbb{Z}$.

   ▷ Cierto: $\{a, b\}$ y $\{a, a + b\}$ tienen los mismo divisores comunes.

4. Si $a^p \equiv a \mod p$ para todo $a \in \mathbb{Z}$ entonces p es primo.

   ▷ Falso. Los compuestos que satisfacen esto se llaman los *números de Carmichael*. El más pequeño es $561 = 3 \cdot 11 \cdot 17$. En 1994 se demostró que hay una infinidad de ellos.

5. Existen enteros x, y tal que $79x + 2018y = 1$.

   ▷ Cierto, ya que 79 es primo.

6. Existe en la sucesión $1, 3, 9, 27, \ldots$ (las potencias de 3) un número que termina con 00001.

   ▷ Cierto. $(3, 10^5) = 1 \implies 3^{\phi(10^5)} \equiv 1 \mod 10^5$.