Guia para el exámen parcial 1

Fecha del exámen: miercoles, 4 oct, 2017.

Profesor: Gil Bor, CIMAT.

Definiciones: hay que saber las definiciones precisas de todos los siguientes términos, y conocer ejemplos concretos de cada uno.

> La representación de un entero en base n; un *divisor* de un entero; el *máximo común divisor* de dos enteros; dos enteros que son *primos relativos*; un *primo*; congruencia mod n de dos enteros; la clase de congruencia mod n de un entero; $\mathbb{Z}_n$ y la definición de suma y producto en ello; *recíproco* (o inversa multiplicativa) de un elemento en $\mathbb{Z}_n$; $\mathbb{Z}_n^*$; la función de Euler $\phi(n)$. Orden de un elemento en $\mathbb{Z}_n^*$. Raíz primitiva módulo n y logarítmo discreto.

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

1. El teorema fundamental de la aritmética (existencia y unicidad de la factorización de un entero en primos).
   Nota: no hemos demostrado la unicidad en clase. Hay que aprenderla de tu texto favorito. Por ejemplo, la p.12 de las notas de Teoria de Numeros (escritas por mi) en la página del curso.
2. La existencia de infinidad de primos.
3. El algoritmo de Euclides para el máximo común divisor de dos enteros.
4. El teorema de Euler-Fermat: si $(a,n)=1$ entonces $a^{\phi(n)} \equiv 1 \mod n$.
5. El Teorema Chino de residuos.
6. $a \in \mathbb{Z}$ tiene un recíproco módulo n si y solo si $(a,n)=1$.
7. $a, b \in \mathbb{Z}$ son primos relativos si y solo si existen $x, y \in \mathbb{Z}$ tal que $ax+by=1$.

Calcular (sin calculadora):

1. La representación en bases 2 y 3 de los siguientes números, dados en base 10: 2, 10, 11, 100.
2. La representación en bases 2 y 10 de los siguientes números, dados en base 3: 2, 10, 11, 100.
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: $\log_2 10 = 3.321928\ldots$)
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.
5. * La representación en base 2 de 0.1, 0.01, 1/3, $\sqrt{2}$ (primeros 5 dígitos).
6. Todos los divisores (positivos y negativos) de: $10, -1, 0, 10, 2^5$.
7. El número de divisores positivos de 10^{10}.
8. El máximo común divisor de 2015 y 2017.
9. El máximo común divisor y el mínimo comun múltiplo de 2015^{2017} y 2017^{2015}.
10. El recíproco de 61 módulo 117 y el recíproco de 171 módulo 61.
11. Las raices primitivas módulo 17 y los logarítmos discretos $\log_r 16 \mod 17$, donde r es cada una de las raices primitivas módulo 17.
12. El resíduo de 2015^{2017} módulo 1001.
13. El número de elementos en $\mathbb{Z}_{2016}^*$.
14. Los ordenes del los elementos de $\mathbb{Z}_{18}^*$.

Demostrar:

1. Un número entero n es compuesto si y solo si tiene un divisor primo p en el rango $2 \le p \le \sqrt{n}$.
2. Cada elemento de $\mathbb{Z}_n$ tiene a lo más un recíproco.

3. 13 divide a $4^{2n+1} + 3^{n+2}$ para todo entero $n \geq 0$.
4. Si $a, b, c \in \mathbb{Z}$ satisfacen $a^2 + b^2 = c^2$ entonces 60 divide a abc.
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 $4k + 3$, $k \in \mathbb{Z}$.
10. * Hay una infinidad de primos de la forma $4k + 1$, $k \in \mathbb{Z}$.
11. 9973 es un primo.
12. Si $n = p_1^{\alpha_1} p_2^{\alpha_1} p_2 \cdots p_m^{\alpha_m}$ es la descomposición de un entero $n > 1$ en producto de primos, donde $p_1, \ldots, p_m$ son primos distintos, entonces

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

Cierto o Falso

1. Si $d, a, b \in \mathbb{Z}$, $d \neq 0$, $d|ab$, entonces $d|a$ ó $d|b$.
2. Si $a \not\equiv 0 \mod n$ entonces a tiene un recíproco $\mod n$.
3. $(a, b) = (a, a + b)$ para todo $a, b \in \mathbb{Z}$.
4. Si $a^p \equiv a \mod p$ para todo $a \in \mathbb{Z}$ entonces p es primo.
5. Existen enteros x, y tal que $79x + 2018y = 1$.
6. Existe en la sucesión $1, 3, 9, 27, \ldots$ (las potencias de 3) un número que termina con 00001.