Material para exámen parcial 1

Fecha del exámen: viernes, 12 sept, 2008

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 la 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 $\phi(n)$.

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

- El teorema fundamental de la aritmética (unicidad en $\mathbb{Z}$ de factorización en primos).
- La existencia de infinidad de primos.
- Pequeño teorema de Fermat y el teorema de Euler-Fermat.
- El algoritmo de Euclides para el máximo común divisor de dos enteros.
- La sucesión 3,7,11,... (los enteros positivos de la forma $4k+3$) contiene una infinidad de primos.
- El algoritmo de Euclides (para encontrar el máximo común divisor de dos enteros).

Problemas: hay que saber resolver todos los problemas de la tarea 1 hasta 5. Aquí hay problemas adicionales del tipo que aparecerá en el examen.

1. Encuentra la cardinalidad del conjunto de los números $n \in \mathbb{Z}$ tal que: (1) $0 \leq n \leq 2008$ (2) en la representación de n en la base 3 no se usa el dígito 1.
2. Encuentra a todos los divisores de: 24, -1, 0.
3. Si $n > 1$ es un entero compuesto (=no primo) entonces tiene un divisor primo p, $2 \leq p \leq \sqrt{n}$. (En otras palabras, para demostrar que un entero $n > 1$ es primo, basta verificar que ninguno de los primos $\leq \sqrt{n}$ divide a n).
4. Cada $c \in \mathbb{Z}_n$ tiene a lo más un recíproco. En otras palabras, $ax \equiv ay \equiv 1 \pmod{n} \Longrightarrow x \equiv y \pmod{n}$.
5. Demuestra por inducción que 13 divide a $4^{2n+1} + 3^{n+2}$ para todo entero $n \geq 0$.
6. Si $a, b, c \in \mathbb{Z}$ satisfacen $a^2 + b^2 = c^2$ entonces 60 divide a abc.

   Sugerencia: basta demostrar que $abc \equiv 0$ mod 3,4 y 5. Por ejemplo, mod 3, basta ver que alguno de a, b, c es $\equiv 0$ mod 3. Si no, tendremos que $a^2 \equiv b^2 \equiv c^2 \equiv 1$ mod 3, pero entonces tendremos $1 + 1 \equiv 1$ mod 3.
7. Encuentra el máximo común divisor de 2006^{2008} y 2008^{2006}.
8. Si a, b son enteros positivos, entonces $ab/(a, b)$ es su mínimo común múltiple.
9. Para cuáles pares de enteros a, b lo siguiente es siempre cierto: si un entero n es divisible entre a y b entonces es divisible entre ab.
10. Cierto o falso: existen enteros x, y tal que $79x + 2008y = 1$.
11. Si $n = am + r$ entonces $(n, a) = (a, r)$.
12. Usa el algorítmo de euclides para encontrar el máximo común divisor de 2008 y 3008.
13. Demuestra que en la "sucesión de Fibonacci", 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.
14. Cierto o falso: entre los números de la sucesión $1, 3, 9, 27, \ldots$ (las potencias de 3) existe un número que termina con $0 \ldots 0001$ (un millon de 0's y luego un 1).