Teoría de Códigos y Criptografía
Curso 2009-2010

Hoja 1 (Repaso)

1. Demostrar que existen infinitos enteros no representables como suma de tres cuadrados. (Sugerencia: Estudiar los cuadrados módulo 8).

2. Demostrar que si $(n-1)!+1 \equiv 0 \pmod{n}$ entonces n es primo.

3. Escribir una sola congruencia que sea equivalente al par de congruencias $x \equiv 1 \pmod{4}$ y $x \equiv 2 \pmod{3}$.

4. Demostrar que si p es primo $(p \neq 3)$ entonces $(p-2)2^{p-2}+1$ no es primo.

5. Demostrar que $2222^{5555} + 5555^{2222}$ es divisible por 7.

6. Probar que $n^7 - n$ es divisible entre 42, para cualquier entero n.

7. Probar que $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es un entero para todo n.

8. Oliana Molls trabaja cuatro días consecutivos y descansa uno. Betty trabaja dos y descansa uno. Sólo se ven los días de luna llena (uno de cada veintiocho días). Betty tuvo fiesta ayer, Oliana la tendrá pasado mañana y hace diez días había luna llena. ¿Cuántos días faltan par que se vean? ¿Cuántos días libres comunes habrán perdido mientras tanto por falta de luna llena?

9. Sea (a,b,c) una terna pitagórica, esto es, una solución en $\mathbb{Z}^3$ de la ecuación $X^2+Y^2=Z^2$. Demostrar lo siguiente:

i) al menos uno de los valores a, b o c es múltiplo de 3;

ii) abc es múltiplo de 4;

iii) al menos uno de los valores a, b o c es múltiplo de 5;

iv) $abc \equiv 0 \ (60)$.

10. Demostrar que si $(a,n)=1$ ó $(b,n)=1$ la ecuación $ax+by=c$ tiene exactamente n soluciones en $\mathbb{Z}/n\mathbb{Z}$.

11. Resolver las siguientes ecuaciones en números eneteros.
1) $2x+3y=-1$.
2) $7x-12y=4$.

12. Hallar el conjunto de soluciones de cada uno de los siguientes sistemas en $\mathbb{Z}/10\mathbb{Z}$.

$$\left.\begin{array}{r} x+y=\bar{5} \\ \bar{2}x+\bar{9}y=1 \end{array}\right\} \qquad \left.\begin{array}{r} \bar{2}x+4y=\bar{6} \\ x+y=\bar{4} \end{array}\right\} \qquad \left.\begin{array}{r} x+\bar{3}y=1 \\ \bar{3}x-y=\bar{3} \end{array}\right\}$$

13. Calcular:
a) $234^{432} \pmod{11}$; b) $145^{197} \pmod{13}$; c) $2025^{2025} \pmod{14}$; d) $4002^{4002} \pmod{35}$.

14. Hallar las raíces del polinomio siguiente en $\mathbb{Z}_5$.

$$X^{14} + X^{11} + X^{10} - 3X^5$$

15. Demostrar que $(n^5 - 1)n(n^5 + 1)$ es divisible por 22.

16. Resolver, si es posible, los siguientes sistemas de congruencias:

$$\left.\begin{array}{r} x \equiv 13 \pmod{91} \\ x \equiv -1 \pmod{119} \end{array}\right\} \qquad \left.\begin{array}{r} x \equiv -5 \pmod{77} \\ x \equiv 17 \pmod{143} \end{array}\right\}$$

17. ¿Cuántas unidades hay en $\mathbb{Z}/2310\mathbb{Z}$? ¿y en $\mathbb{Z}/1764\mathbb{Z}$?

18. Hallar $\phi(n)$ para $5 \leq n \leq 24$.

19. Demostrar que

$$\sum_{d|n} \phi(d) = n \qquad \text{para todo } n \in \mathbb{N},\ n > 0.$$

(En el sumatorio d recorre todos los divisores positivos de n.)

20. 1. Encontrar el inverso multiplicativo de $23 + 35\mathbb{Z}$ en $\mathbb{Z}_{35}$.
2. Encontrar el inverso multiplicativo de $13 + 46\mathbb{Z}$ en $\mathbb{Z}_{46}$.

21.

1. Probar que la composición de homomorfismos de grupos es un homomorfismo de grupos.
2. Si $f : G \to H$ es un isomorfismo de grupos, probar que $f^{-1} : H \to G$ es un isomorfismo. Así, si $G \cong H$, entonces $H \cong G$.
3. Si $G \cong H$ y $H \cong K$, probar que $G \cong K$.
4. Si G es un grupo, el conjunto de todos automorfismos de f lo denotaremos por $Aut(G)$. Demostrar que $Aut(G)$ es un grupo respecto la operación composición.

22. Decidir si los siguientes anllos son isomorfos $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ y $\mathbb{Z}/24\mathbb{Z}$.

23. Sean A_1 y A_2 dos anillos unitarios. Entonces,

$$U(A_1 \times A_2) = U(A_1) \times U(A_2).$$

24.
Demostrar que para la transformación afín

$$f : \begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \to & \mathbb{Z}/N\mathbb{Z} \\ x & \mapsto & ax + b \end{array},$$

donde a, b dos elementos de $\mathbb{Z}/N\mathbb{Z}$, las siguientes afirmaciones son equivalentes
a) a es inversible en $\mathbb{Z}/N\mathbb{Z}$;
b) f es biyectiva;
c) f es inyectiva.

25. Sean p y q dos primos. Demostrar que si a es coprimo con pq, entonces $a^{MCM(p-1,q-1)} \equiv 1 \pmod{pq}$.