

Introducción a la Teoría de Números  
2. Congruencias – entrega 17/9

1. Mostrar que si  $a$  y  $b$  son enteros y  $p$  es un primo, entonces

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

2. Encontrar cuatro sistemas completos de restos módulo 7 cuyos elementos satisfagan (1) ser no negativos, (2) ser impares, (3) ser pares, (4) ser primos.
3. Encontrar criterios para la divisibilidad de un entero por 5, 9 y 11, y demostrar cada uno de estos criterios.
4. \* (De la competencia Putnam 1988). Se define una secuencia de enteros decimales de la siguiente forma:  $a_1 = 0$ ,  $a_2 = 1$ , y  $a_{n+2}$  se obtiene escribiendo los dígitos de  $a_{n+1}$  seguidos inmediatamente por los de  $a_n$ . Por ejemplo  $a_3 = 10$ ,  $a_4 = 101$ , y  $a_5 = 10110$ . Se quiere determinar los  $n$  tales que  $a_n$  es múltiplo de 11 de la siguiente forma:
- (a) Encontrar el menor  $n > 1$  tal que  $a_n$  es divisible entre 11.
  - (b) Probar que  $a_n$  es divisible entre 11 si y sólo si  $n \equiv 1 \pmod{6}$ .
5. Encontrar un entero  $x$  tal que  $37x \equiv 1 \pmod{101}$ .
6. ¿Cuál es el orden de 2 módulo 17?
7. Sea  $p$  un primo. Probar que  $\mathbb{Z}/p\mathbb{Z}$  es un cuerpo.
8. Probar que si  $n > 4$  es compuesto entonces  $(n - 1)! \equiv 0 \pmod{n}$ .
9. ¿Para qué valores de  $n$  es  $\varphi(n)$  impar?
10. Siete estudiantes de matemática tratan de compartir una gran cantidad de libros de matemática equitativamente. Desafortunadamente, sobran seis libros, y en la pelea uno de los estudiantes es expulsado. Los restantes seis estudiantes todavía son incapaces de repartir los libros ya que sobran dos, nuevamente pelean, y otro es expulsado. Cuando los restantes cinco reparten los libros, sobra uno, y es solamente después de expulsar otro estudiante que logran repartir equitativamente los libros. ¿Cuál es el mínimo número de libros que hace esto posible?
11. Encontrar las cuatro soluciones a la ecuación
- $$x^2 - 1 \equiv 0 \pmod{35}$$
12. Usar la fórmula para  $\varphi(n)$  para dar una demostración de que hay infinitos primos. [Sugerencia: si  $p_1, p_2, \dots, p_t$  fueran todos los primos, entonces  $\varphi(p_1 p_2 \cdots p_t) = 1$ ].
13. \* Probar que hay una raíz primitiva módulo  $p^2$ , donde  $p$  es primo.
14. \* Si  $p$  es un primo impar, probar que existe una raíz primitiva módulo  $p^n$ .
15. Encontrar una raíz primitiva módulo 125.
16. \* Caracterizar aquellos enteros  $n$  tales que existe una raíz primitiva módulo  $n$  (en términos de su factorización).