Modulos

Entrenamientos Nacionales Diciembre 2022

Emmanuel Buenrostro

December 2022

.

§1 Principios

Definición:

$$a \equiv b \mod n \text{ si } n|a-b$$

Propiedades: Si $a \equiv b \mod n$ y $c \equiv d \mod n$:

1. $a + c \equiv b + d \mod n$
2. $a - c \equiv b - d \mod n$
3. $ac \equiv bd \mod n$
4. $a^x \equiv b^x \mod n$
5. Se puede dividir? $\frac{a}{c} \equiv \frac{b}{d} \mod n$ es cierto si $c|a, d|b$ y que $(c, n) = 1 \Rightarrow (d, n) = 1$.
6. En caso de que no sean primos relativos

$$10 \equiv 6 \mod 4$$

Dividimos entre 2

$$5 \equiv 3 \mod 2$$

Cuando $a^c \equiv b^d$ mod n:

$$a^c \equiv b^d \mod n \text{ funciona si } c \equiv d \mod \phi(n)$$

§2 Pequeño Teorema Fermat

Theorem 2.1 (Pequeño Teorema de Fermat)

. Si p es primo y $a \in \mathbb{Z}$ entonces

$$a^p \equiv a \mod p$$

Tambien generalmente conocido como

Theorem 2.2 (Pequeño Teorema de Fermat)
. Si p es primo y $a \in \mathbb{Z}$ y $(a,p)=1$ entonces

$$a^{p-1} \equiv 1 \bmod p$$

Prueba por inducción.
Notemos que $0^p \equiv 0 \bmod p.$ y $1^p \equiv 1 \bmod p$. Son nuestros casos base, ahora supongamos que para algun a se tiene que

$$a^p \equiv a \bmod p$$

entonces tenemos que por el binomio de newton

$$(a+1)^p = a^p + pa^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1$$

Pero $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ asi que para $1 \leq k \leq p-1$ se tiene que $p|\binom{p}{k}$, porque como $k < p$ entonces no hay ningun factor p en $k!$ y como $p-k \leq p-1 < p$ entonces tampoco tiene un factor p y no hay ningun factor p en el denominador pero si en el numerador porque es $p!$.

Entonces $\binom{p}{k}a^{p-k} \equiv 0 \bmod p$ para $k \geq 1$ (porque es multiplo de p) entonces queda que

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p$$

probando lo que queremos mediante inducción.

Prueba mas de números.

Notemos que para a tal que $p|a$ si cumple porque $a^p \equiv 0 \equiv a \bmod p$.

Para los a con $(p,a)=1$. se tiene que

$$\{a, 2a, 3a, \ldots, (p-1)a\}$$

es una permutación de

$$\{1, 2, 3, \ldots p-1\}$$

en mod p.

Prueba. Todos los números $a, 2a, 3a, \ldots, (p-1)a$ tiene distintos modulos p, ya que si hay dos iguales ia y ja con $i \neq j$ entonces

$$ia - ja = a(i-j) \equiv 0 \bmod p$$

y como $(a,p)=1$ entonces $i-j \equiv 0 \bmod p \Rightarrow i \equiv j \bmod p$, pero $1 \leq i,j \leq p-1$ entonces $i=j$, una contradicción. Entonces si es una permutación.

Asi que si multiplicamos todos se tiene que

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \bmod p$$

entonces

$$\Rightarrow (p-1)!a^{p-1} \equiv (p-1)! \bmod p$$

$$\Rightarrow a^{p-1} \equiv 1 \bmod p$$

Probando el teorema.

§3 Teorema de Euler

Theorem 3.1 (Teorema de Euler)
Si a es primo relativo con n entonces $a^{\phi(n)} \equiv 1 \bmod n$

Prueba parecida a la 2da de Fermat. Sea a un entero tal que $(a, n) = 1$.
Vamos a considerar el conjunto $S = \{ja : 1 \le j \le n \text{ y } (j, n) = 1\}$ y vamos a probar que es una permutación de los primos relativos a n.

- Los números ja pertenicientes a S son primos relativos a n, ya que es la multiplicacion de dos primos relativos a n, y entonces su multiplicación no comparte ningun factor con n.
- Hay $\phi(n)$ distintos modulos primos relativos a n por definición.
- Si hay dos $1 \le j_1, j_2 \le n$ distintos primos relativos a n tal que $j_1 a \equiv j_2 a \bmod n$ entonces $(j_1 - j_2)a \equiv 0 \bmod n$ entonces $n|(j_1 - j_2)a$ pero como $(a, n) = 1$ entonces $n|j_1 - j_2$ y $j_1 \equiv j_2 \bmod n$ pero como $1 \le j_1, j_2 \le n$ entonces $j_1 = j_2$ una contradicción.
- Entonces los $\phi(n)$ j son distintos y entonces hay $\phi(n)$ ja diferentes y son primos relativos con n entonces S si es una permutacion de los primos relativos con n en mod n.

Entonces

$$\prod_{(j,n)=1}^{n} ja \equiv \prod_{(j,n)=1}^{n} j \bmod n$$

$$\Rightarrow \prod_{(j,n)=1}^{n} ja = (\prod_{(j,n)=1}^{n} j)a^{\phi(n)} \equiv \prod_{(j,n)=1}^{n} j \bmod n$$

y como $\prod_{(j,n)=1}^{n} j$ es la multiplicación de primos relativos con n entonces es primo relativo con n y

$$a^{\phi(n)} \equiv 1 \bmod n$$

§4 Wilson

Theorem 4.1 (Teorema de Wilson)
Si p es primo entonces $(p-1)! \equiv -1 \bmod p$.

Prueba.

Sea a un entero con $1 \le a \le p-1$ y sea b su inverso multiplicativo mod p. $(1 \le b \le p-1)$.
Tenemos que $ab \equiv 1 \bmod p$ y como es una ecuacion lineal sabemos que $ax \equiv 1 \bmod p$ tiene una solucion unica mod p, entonces el inverso de a es b y viceversa.

Entonces separamos los números del 1 al $p-1$ en parejas de la forma (a, b) donde $ab \equiv 1 \bmod p$ excepto cuando se tiene que $a = b$ es decir es el inverso de si mismo.

$$a^2 \equiv 1 \bmod p$$

$$(a+1)(a-1) \equiv 0 \bmod p$$

$$a \equiv 1, -1 \bmod p$$

Entonces todos los números del 2 al $p-2$ se emparejan y su producto es 1 mod p. Asi que

$$(p-1)! = 1 \cdot (2 \cdot 3 \cdots (p-2)) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \bmod p$$

probando el teorema.

§5 Algoritmo de Euclides

Sea $a, b \in \mathbb{N}$ entonces podemos escribir

$$a = bq + r \text{ con } 0 < r < b$$

$$b = rq_1 + r_1 \text{ con } 0 < r_1 < r$$
$$r = r_1 q_2 + r_2 \text{ con } 0 < r_2 < r_1$$
$$\vdots$$

Como $r_i > r_{i+1}$ siempre va decendiendo, entonces en algun punto va a llegar a ser 0.

$$r_{n-1} = r_n q_{n+1} + r_{n+1} \text{ con } 0 < r_{n+1} < r_1$$
$$r_n = r_{n+1} q_{n+2} + 0$$

Entonces se tiene que $(a, b) = r_{n+1}$

§6 Identidad de Bezout

Theorem 6.1 (Identidad de Bezout)
Si $(a, b) = d$. Existen enteros x, y tales que

$$ax + by = d$$

Remark. En particular si $(a, b) = 1$ existen enteros x, y tales que

$$ax + by = 1$$

Esto se apoya con el Algoritmo de Euclides, veamos un ejemplo con $a = 11, b = 7$.

Example 6.2

$$11 = 7 \cdot 1 + 4$$
$$7 = 4 \cdot 1 + 3$$
$$4 = 3 \cdot 1 + 1$$
$$3 = 1 \cdot 3 + 0$$

De esta penultima se tiene que $(11, 7) = 1$ y podemos escribir

$$1 = 4(1) - 3(1)$$

pero de la anterior tenemos que $3 = 7(1) - 4(1)$ asi que sustituimos.

$$1 = 4(1) - (7(1) - 4(1))(1) = 4(1) - 7(1) + 4(1) = 4(2) - 7(1)$$

Y de la primera tenemos que $4 = 11(1) - 7(1)$ asi que podemos sustituirlo

$$1 = 4(2) - 7(1) = (11(1) - 7(1))(2) - 7(1) = 11(2) - 7(2) - 7(1) = 11(2) - 7(3)$$

Entonces para $a = 11, b = 7$ tenemos que $11(2) + 7(-3) = 1$ cumpliendo la identidad.

Otro lema que se puede demostrar con Bezout es el Lema de Euclides

Claim 6.3 (Lema de Euclides) — Sea p un primo, Si $p|ab \Rightarrow p|a$ o $p|b$.

Prueba.
Supongamos que $p|ab$ y $p \nmid a \Rightarrow (a, p) = 1$. Entonces por Bezout existen enteros x, y con

$$ax + py = 1 \Rightarrow abx + pby = b$$

Y como $p|ab \Rightarrow p|abx$ y $p|pby$ entonces $p|abx + pby = b$ probando el Lema.

§7 Resolver Ecuaciones Modulares

Primero veamos que para enteros $(a, n) = 1$ sabemos que existen enteros c y d tales que $ac + dn = 1 \Rightarrow ac = 1 - dn \Rightarrow ac \equiv 1 \mod n$ Entonces c es el inverso multiplicativo de a mod n.

Por ejemplo anteriormente sacamos que $11(2) + 7(-3) = 1$ Entonces $7(-3) \equiv 1 \mod 11$ y por lo que $c = -3$ es el inverso multiplicativo de 7 mod 11.

Asi que para resolver esta ecuacion:

$$ax \equiv b \mod n$$

Multiplicamos por c (el inverso de a).

$$acx \equiv bc \mod n$$

$$\Rightarrow x \equiv bc \mod n$$

Ya que $ac \equiv 1 \mod n$ por definición.

Ahora que pasa si no son primos relativos, digamos $(a, n) = d$, entonces escribimos $a = da'$ y $n = dn'$ entonces tenemos que

$$ax \equiv b \bmod n \Rightarrow da'x \equiv b \bmod dn'$$

y

$$dn'|da'x - b \Rightarrow d|da'x - b$$

y como $d|da'x$ entonces $d|b$, de lo contrario no tiene solución el sistema. Entonces escribimos $b = db'$.
Asi que la ecuacion queda:

$$da'x \equiv db' \bmod dn' \Rightarrow da'x - db' = (dn')k$$

para algun entero k y seguimos a (dividiendo entre d):

$$a'x - b' = n'k \Rightarrow a'x \equiv b \bmod n'$$

Y como $(a', n') = 1$ porque quitamos todos sus factores en comun al dividir entre su maximo comun divisor, entonces esta ecuacion tiene una unica solución mod n', y por lo tanto hay d soluciones mod n. Si la solucion mod n' es $x \equiv x_0$ mod n', entonces las d soluciones son

$$x_0, x_0 + n', x_0 + 2n', \ldots, x_0 + (d-1)n'$$

modulo n.

Tambien cuando el modulo es primo se vale pensar en fracciones, ejemplo con 7,11. Sacamos anteriormente que -3 es el inverso multiplicativo de 7 mod 11, entonces $7(-3) \equiv 1$ mod 11, y entonces podemos pensar a -3 como $\frac{1}{7}$ mod 11.

§8 Problemas de Ejemplo

Example 8.1 (IMO 2005/4)

Encuentra todos los enteros positivos que son primos relativos con todos los términos de la secuencia infinita

$$a_n = 2^n + 3^n + 6^n - 1, \ \ n \geq 1.$$

Solución.
El unico número que cumple es el 1.
Supongamos que algun otro número m cumpla con $m > 1$, entonces tiene algun primo p tal que $p|m$ y ese primo cumple. Entonces vamos a probar que $p|a_n$ para algun a_n. Primero para poder usar lo que hemos visto vamos a ver que pasa con $p = 2, 3$ porque son los factores q aparecen en 2,3 y 6 (todos los demas primos son primos relativos a estos números y podemos aplicar Fermat/Euler).

- $p = 2$ Notemos que $a_1 = 2 + 3 + 6 - 1 = 10$ y $2|10$ entonces si cumple.
- $p = 3$ Notemos que $a_2 = 4 + 9 + 36 - 1 = 48$ y $3|48$ entonces si cumple.

Entonces ahora para $p > 3$ queremos que $2^n + 3^n + 6^n - 1 \equiv 0 \bmod p$.
Primeramente lo que intentariamos seria usar Fermat (porque p es primo), entonces intentamos con $n = p - 1$ pero queda

$$2^{p-1} + 3^{p-1} + 6^{p-1} - 1 \equiv 1 + 1 + 1 - 1 \equiv 2 \bmod p$$

entonces no cumple, ahora podemos usar lo de la idea de usar fracciones, y vemos que si $n = -1$ tenemos que

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{3} - 1 = 0$$

entonces si cumple, pero como $n \geq 1$ no podemos usar esto, asi que tenemos que encontrar un número que sea masomenos esto, el cual como $x^{p-1} \equiv 1 \bmod p$, vamos a sumarle $p-1$ a el exponente y lo va a multiplicar por 1, entonces con $n = p-2$ tenemos que

$$2^{p-2}+3^{p-2}+6^{p-2}-1 = 2^{-1}\cdot 2^{p-1}+3^{-1}\cdot 3^{p-1}+6^{-1}\cdot 6^{p-1}-1 \equiv \frac{1}{2}\cdot 1+\frac{1}{3}\cdot 1+\frac{1}{6}\cdot 1-1 \equiv 0 \bmod p$$

cumpliendo la condicion y demostrando que para cada número existe uno con el que no sea primo relativo.

Example 8.2 (PUTNAM 2022/A3)

Sea p un primo mayor a 5. Sea $f(p)$ el número de secuencias infinitas $a_1, a_2, a_3, \ldots$ que satisfaces

1. $a_n \in \{1, 2, \ldots, p-1\}$ $\forall n \geq 1$
2. $a_n a_{n+2} \equiv 1 + a_{n+1} \bmod p$ $\forall n \geq 1$

Solución.
Como $a_n a_{n+2} \equiv 1 + a_{n+1} \bmod p$, y $(a_n, p) = 1$ porque por definicion $1 \leq a_n \leq p-1$ y entonces p no lo puede dividir, asi que $a_{n+2} \equiv \frac{1+a_{n+1}}{a_n} \bmod p$.
Entonces

- $a_3 \equiv \frac{1+a_2}{a_1} \bmod p$.
- $a_4 \equiv \frac{1+a_3}{a_2} \equiv \frac{1+\frac{1+a_2}{a_1}}{a_2} \equiv \frac{1+a_1+a_2}{a_1a_2} \bmod p$.
- $a_5 \equiv \frac{1+a_4}{a_3} \equiv \frac{1+\frac{1+a_1+a_2}{a_1a_2}}{a_3} \equiv \frac{1+a_1+a_2+a_1a_2}{a_1a_2a_3} \equiv \frac{(1+a_1)(1+a_2)}{a_2(1+a_2)} \equiv \frac{1+a_1}{a_2} \bmod p$.
- $a_6 \equiv \frac{1+a_5}{a_4} \equiv \frac{1+\frac{1+a_1}{a_2}}{\frac{1+a_1+a_2}{a_1a_2}} \equiv \frac{1+a_1+a_2}{\frac{1+a_1+a_2}{a_1}} \equiv a_1 \bmod p$.
- $a_7 \equiv \frac{1+a_6}{a_5} \equiv \frac{1+a_1}{\frac{1+a_1}{a_2}} \equiv a_2 \bmod p$.

Y como la sucesion se va escribiendo en base a los dos anteriores llegamos a una periodicidad y entonces escribimos toda la sucesion en base de a_1 y a_2. (Como $1 \leq a_n \leq p-1$ entonces a_n van a ser a lo que son congruentes mod p. (Es decir $a_3 = frac1 + a_2a_1$))
Pero nunca descartamos que no pueden ser 0 mod p (es la unica congruencia mod p que no se puede) Como $a_3 \neq 0$ entonces $1 + a_2 \neq 0 \Rightarrow a_2 \neq -1 \bmod p$.
Como $a_5 \neq 0$ entonces $1 + a_1 \neq 0 \Rightarrow a_1 \neq -1 \bmod p$.
Como $a_4 \neq 0$ entonces $1 + a_1 + a_2 \neq 0 \Rightarrow a_2 \neq -1 - a_1 \bmod p$.
Asi que $f(p) = (p-2)(p-3)$, porque tenemos $p-2$ formas de escoger a_1 ya que tenemos $p-1$ opciones originalmente pero no puede estar $p-1$, y para a_2 tenemos originalmente $p-1$ opciones pero como no puede ser $-1 \bmod p$ y tampoco puede ser $-1 - a_1$ y como a_1 no es ninguna de $0, -1$ entonces $-1 - a_1$ no es ninguna de las dos opciones que no pueden ser por lo que descartamos otra opcion y solo quedan $p-3$ opciones. Entonces

$$f(p) = (p-2)(p-3) = p^2 - 5p + 6 \equiv p^2 + 1 \bmod 5$$

Como $p > 5$, $p \not\equiv 0 \bmod 5$.
Y $p^2 \bmod 5$ puede ser $1^2, 2^2, 3^2, 4^2 \to 1, 4, 4, 1 \bmod 5$, entonces p^2+1 puede ser congruente a $1+1 \equiv 2 \bmod 5$ o $4+1 \equiv 0 \bmod 5$, demostrando el problema.

§8.1 Ejercicios de Practica

Exercise 8.3. Resuelve para x:

1. $12x \equiv 1 \bmod 23$
2. $x^2 \equiv 1 \bmod 23$
3. $x^2 \equiv 1 \bmod 8$
4. $x(x+5) \equiv 6 \bmod 10$

Exercise 8.4. Encuentra todos los primos p tales que $13^{2p-1} + 17$ es divisible por p.

Problem 8.5. Prueba que

$$(x-1^2)(x-2^2)(x-3^2)(x-4^2)(x-5^2)(x-6^2) \equiv x^6 - 1 \bmod 13$$

Problem 8.6. Encuentra todas las tripletas de enteros positivos (k, m, n) tal que $7^k = 9^m + 2^n$.

Problem 8.7. Prueba que si p y $8p-1$ son ambos primos entonces $8p+1$ es compuesto.

Problem 8.8. Sea $f(x_1, x_2, \ldots, x_n)$ un polinomio con coeficientes enteros. Prueba que

$$f(x_1, x_2, \ldots, x_n)^p \equiv f(x_1^p, x_2^p, \ldots, x_n^p) \bmod p$$

para p primo.

Problem 8.9 (IMO 1970/4)**.** Encuentra el conjunto de todos los enteros positivos n con la propiedad que el conjunto $\{n, n+1, n+2, n+3, n+4, n+5\}$ puede ser dividido en dos conjuntos tal que el producto de los numeros en un conjunto sea igual al producto de los numeros del otro conjunto.