Congruències

Definicions i Propietats

Les congruències són molt útils per resoldre problemes i tractar diferents aspectes amb un altre punt de vista. La idea és adonar-nos que en dividir qualsevol nombre enter a entre n, el residu de la divisió ha de ser necessàriament un nombre $0 \leq r \leq n-1$. Així s'estableix de forma senzilla una classificació, per a cada n, dels nombres enters. Per exemple, per a $n = 4$ tendrem 4 classes d'equivalència que són:

$$[0] = \{\text{Nombres enters que en dividir-los per 4 el residu és 0.}\},$$

$$[1] = \{\text{Nombres enters que en dividir-los per 4 el residu és 1.}\},$$

$$[2] = \{\text{Nombres enters que en dividir-los per 4 el residu és 2.}\},$$

$$[3] = \{\text{Nombres enters que en dividir-los per 4 el residu és 3.}\}.$$

Observau que la classe del zero, [0] és el conjunt dels múltiples de 4.

Definició 1. *Dos nombres enters a i b són congruents mòdul n, fet que s'indica per*

$$a \equiv b \,(mod\, n)$$

si pertanyen a una mateixa classe d'equivalència (si el residu és el mateix en dividir-los per n).

Equivalentment,

Proposició 1. *Donats dos nombres enters a i b, $a \equiv b \,(mod\, n)$ si i només si $a \equiv b$ és múltiple de n. De l'exemple anterior, $3 \equiv 23 \,(mod\, 4)$, $28 \equiv 0 \,(mod\, 4)$, $42 \equiv -14 \,(mod\, 4)$.*

Proposició 2. *Sigui n un nombre enter qualsevol. Aleshores:*

i. $a \equiv a \,(mod\, n)$ *(Reflexivitat)*
ii. *Si* $a \equiv b \,(mod\, n)$ *aleshores* $b \equiv a (mod\, n)$. *(Conmutativitat)*
iii. *Si* $a \equiv b (mod\, n)$ *i* $b \equiv c (mod\, n)$ *aleshores* $a \equiv c (mod\, n)$. *(Transitivitat)*
iv. *Si* $a \equiv b \,(mod\, n)$ *aleshores* $mcd(a; n) = mcd(b; n)$.
v. *Si* $a \equiv b \,(mod\, n)$ *aleshores* $a + k \equiv b + k \,(mod\, n)$.

vi. *Si* $a \equiv b\,(mod\,n)$ *aleshores* $a \cdot k \equiv b \cdot k\,(mod\,n)$.

vii. *Si* $a \equiv b\,(mod\,n)$ *i* $c \equiv d\,(mod\,n)$ *aleshores* $a + c \equiv b + d$.

viii. *Si* $a \equiv b(mod\,n)$ *i* $c \equiv d\,(mod\,n) aleshores a \cdot c \equiv b \cdot d$.

ix. *Si* $c \cdot a \equiv c \cdot b\,(mod\,n)$ *i* $mcd(c; n) = 1$ *aleshores* $a \equiv b\,(mod\,n)$. *(Simplificació)*

Teorema 1 (**Petit Teorema de Fermat**). *Sigui p un nombre primer i sigui a un nombre enter que no sigui múltiple de p. Aleshores*

$$a^{p-1} \equiv 1\ (mod\ p).$$

Demostració. Considerem $a, 2a, 3a, \ldots, (p-1) \cdot a$. Provarem que si $a \cdot i \equiv a \cdot j\ (mod\ p)$ amb $0 < i, j \leq p-1$ llavors $i = j$.

Suposem que $a \cdot i \equiv a \cdot j\ (mod\,p)$ per algun $i \neq j$ amb $0 < i, j \leq p-1$. Podem suposar sense pèrdua de generalitat que $i > j$. Llavors $a \cdot (i-j) \equiv 0\ (mod\ p)$. Això vol dir que $p|a \cdot (i-j)$; però com que p no divideix a a llavors $p|(i-j)$, cosa impossible ja que $i - j < p$.

Llavors, d'una banda tenim que $a \cdot i \equiv r_i\ (mod\ p)$, per algun r_i tal que $0 < r_i \leq p-1$ i, a més $r_i \neq r_j$ quan $i \neq j$. Així doncs, cada un dels termes $a, 2a, \ldots, (p-1) \cdot a$ és congruent amb algun dels nombres $1, 2, \ldots, p-1$, no necessàriament amb aquest ordre.

I d'altra banda,

$$a \cdot 2a \cdot \ldots \cdot (p-1) \cdot a = a^{p-1} \cdot (1 \cdot 2 \cdots (p-1)) = a^{p-1} \cdot (p-1)!$$

Per tant,

$$a^{p-1} \cdot (p-1)! \equiv (p-1)!\ (mod\ p)$$

I com que $(p-1)!$ no és múltiple de p, podem simplificar i obtenim que

$$a^{p-1} \equiv 1\ (mod\ p).$$

□

Bibliografia utilitzada i recomanada

1. Sessió de preparació per a l'olimpiada matemàtica Aritmètica i congruències del 2013.(Jaume Monreal i Climent Cànaves)
2. Bujalance, Emilio i altres. Elementos de Matemàtica Discreta, Ed. Sanz y Torres, 1997.
3. García Capitán, F.J. Un pequeño Manual para la Resolución de Problemas
4. Moreno, M.A., Tellechea, E. Colectivo de Problemas resueltos para Estudiantes de Alto Rendimiento
5. *www.iecat.net/institucio/societats/SCMatematiques/index.asp* (publicacions electròniques)

Exercicis

Exercici 1. *Demostrau els criteris de divisibilitat següents:*

1. *Un nombre és divisible per 2 quan acaba en xifra parell.*
2. *Un nombre és divisible per 3 quan la suma de les seves xifres és també múltiple de 3.*
3. *Un nombre és divisible per 4 quan les dues darreres xifres és múltiple de 4.*
4. *Un nombre és divisible per 5 quan acaba en 0 o en 5.*
5. *Un nombre és divisible per 9 quan la suma de les seves xifres és també un múltiple de 9.*
6. *Un nombre és divisible per 10 quan acaba en zero.*
7. *Un nombre és divisible per 11 quan la suma de les xifres de posició senar menys la suma de la xifres de posició parell resulta un nombre múltiple de 11.*
8. *Un nombre és múltiple de 25 quan acaba en 00, 25, 50 o 75.*

Exercici 2. *Trobau tots els enters positius n tals que $2^n - 1$ és divisible per 7. Així mateix, demostrau que no existeix cap enter positiu tal que $2^n + 1$ sigui divisible per 7.*

Exercici 3. *Demostra que tot quadrat perfecte és congruent amb 0 o amb 1 mòdul 4.*

Exercici 4. ***(Olimpiades 2004)*** *Troba totes les possibles maneres d'escriure 2003 com a suma de dos quadrats de nombres enters positius.*

Exercici 5. *A l'illa de Camelot viuen 13 camaleons vermells, 15 verds i 17 grocs. Quan dos de diferent color es troben canvien al tercer color. Podria donar-se la situació que tots tinguin el mateix color?*

Exercici 6. *Provar que per qualsevol nombre primer p diferent de 2 i 5 existeix un múltiple de p que té totes les seves xifres formades per 9's.*

Exercici 7. ***(Fase local Catalunya Olimpiades 2001)*** *Trobeu el mínim nombre natural n que és múltiple de 3 i tal que, a més, $n+1$ és múltiple de 5, $n+2$ és múltiple de 7, $n+3$ és múltiple de 9 i $n+4$ és múltiple de 11.*

Exercici 8. ***(Fase local Catalunya Olimpiades 2004)*** *Trobeu tots els nombres enters m, n, solucions de l'equació $9^m = 4n^2 + 1$.*

Exercici 9. *Calcula el residu de la divisió del producte $2^{50} \cdot 41^{65}$ entre 7.*

Exercici 10. *Provar que si x, y són nombres enters i 3 divideix a $x^2 + y^2$, llavors 3 divideix a x i també 3 divideix a y*

Exercici 11. *Determinar x, y, z en el nombre $33xy49z$ per a que sigui múltiple de 693.*