9/3/2017

Ιδιότητες κλάσεων ισοδυναμίας

1. Κλειστότητα: αν προσθέσουμε δύο στοιχεία μιας κλάσης ισοδυναμίας, το αποτέλεσμα θα ανήκει και αυτό στην ίδια κλάση ισοδυναμίας. Πχ:

   $Z_7=0,1,2,3,4,5,6$
   $3+5(mod7)=8\,mod\,7=1$

2. Προσετεριστικότητα (a+b)+c(mod7)=a+(b+c)(mod7)
3. Ουδέτερο στοιχείο: αν προσθέσουμε το ουδέτερο στοιχείο με το α, μας δίνει α.
4. Συμμετρικό-Αντίστροφο στοιχείο: για κάθε α, υπάρχει α^{-1} που ανήκει στην ίδια κλάση ισοδυναμίας και αν το προσθέσουμε με το α μας δίνει το ουδέτερο στοιχείο.

Ομάδα

Αν ισχύουν αυτές οι ιδιότητες, τότε μια κλάση ισοδυναμίας λέγεται **ομάδα.** Π.χ. $(Z_n,+)$ είναι ομάδα, $(Z_n,*)$ δεν είναι ομάδα γιατί δεν ισχύει το συμμετρικό στοιχείο για το 0.

Αντίστροφος αριθμός και προϋπόθεση ύπαρξής του

$a\cdot a^{-1}\rightarrow a\cdot a^{-1}\equiv 1(modn)$ ή το α^{-1} είναι ο αριθμός εκείνος που αν τον πολλαπλασιάσουμε με το α και το διαιρέσουμε με το n μας δίνει υπόλοιπο 1.
<u>Όμως δεν υπάρχει πάντα κάποιος τέτοιος αριθμός!</u> $2x\equiv 1(mod\,8)$ δεν έχει λύση.

Γενικά: $a^{-1}=ax\equiv 1(modn)$ $\Rightarrow$ $ax=1+k\cdot n$ $\Rightarrow$ $a\cdot x-n\cdot k=1$ δηλαδή έχουμε γραμμικό συνδυασμό των α, n.

Άρα για να ισχύει η παραπάνω σχέση θα πρέπει gcd(a,n)=1, δηλαδή οι α και n να είναι πρώτοι μεταξύ τους.

Υπενθύμιση αλγορίθμου του Ευκλείδη: gcd(a,b)=gcd(b,amodb)
άρα σύμφωνα με την ιδιότητα του gcd υπάρχουν x,y ώστε:
$gcd(a,b)=ax+by\quad(1)$
$gcd(b,amodb)=bx'+(amodb)y'\quad(2)$
Τα πρώτα μέλη είναι ίσα, άρα θα είναι και τα δεύτερα, οπότε έχουμε:
$ax+by=bx'+(amodb)y'\Rightarrow$
$ax+by=bx'+(a-\lfloor a|b\rfloor b)y'\Rightarrow$
$ax+by=ay'+b(x'-\lfloor a|b\rfloor y')$
Άρα έχουμε $x=y'\ \ και\ \ y=x'-\lfloor a|b\rfloor y'$
Παράδειγμα για το gcd(31,7)=1:

α	b	gcd	x	y	
31	7	1	-2	9	$31\cdot(-2)+7\cdot y=1\Rightarrow 7\cdot y=63\Rightarrow y=9$
7	3	1	1	-2	$7\cdot 1+3\cdot y=1\Rightarrow 3\cdot y=-6\Rightarrow y=-2$
3	1	1	0	1	$3\cdot 0+1\cdot y=1\Rightarrow y=1$
1	0	1	1	0	$1\cdot 1+0\cdot y=1\Rightarrow y=0$

1. Υπολογίζουμε τα α και b από τον αλγόριθμο του Ευκλείδη.
2. Ο gcd(α,b) θα είναι το τελευταίο α.
3. Για κάθε γραμμή ισχύει ότι gcd(α,b)=αx+by και έτσι βρίσκουμε τα x και y από κάτω προς τα πάνω. Σε κάθε βήμα, $x_i=y_{i-1}$.
4. Στην πρώτη γραμμή, το x θα είναι το α^{-1}(modb) και το y το b^{-1}(moda)

Πλήθος στοιχείων ομάδας

Έστω $Z^*_n = \{a \in \mathbb{Z}_n\} : gcd(a,n)=1$ π.χ. $Z_8=\{0,1,2,3,4,5,6,7\}$ και $Z^*_8=\{1,3,5,7\}$, όπου Z^*_8 είναι ομάδα. Επίσης, Z^*_n είναι ομάδα.

Το πλήθος των στοιχείων της ομάδας Z_n είναι $|Z_n|=n$.

Το πλήθος των στοιχείων της ομάδας Z^*_n είναι $|Z^*_n|=\Phi(n)= n\prod_{p|n}(1-\frac{1}{p})$ π.χ.

$$\Phi(8)=8(1-\frac{1}{2})=4$$

Αν το n είναι γινόμενο μόνο δύο πρώτων, τότε

$$\Phi(n=pq)=n(1-\frac{1}{p})(1-\frac{1}{q})=(p-1)(q-1) \quad και \quad αν\ p=q \quad τότε \quad p(1-\frac{1}{p})=p-1$$

Προβλήματα

Έχουμε γενικά 3 τύπους προβλημάτων:

1. $ax \equiv b(modn)$ σχέση
2. $x \equiv a_i(modn_i)$ σύστημα
3. $\alpha^b \equiv x(modn)$ εκθέτης

Τα προβλήματα αυτά επιλύονται με τη βοήθεια των ομάδων.

1. Σχέση $ax \equiv b(modn)$
   a) Βρίσκω το gcd(α,n) και ελέγχω αν διαιρεί το b.
   b) Αν όχι, τότε δεν υπάρχει λύση. Αν ναι, τότε έχουμε gcd(α,n) σε πλήθος λύσεις.
   c) Η πρώτη λύση θα είναι $x_o=\frac{x \cdot b}{gcd(\alpha,n)}(modn)$ και οι υπόλοιπες θα είναι:

$$x_i=x_0+\frac{i \cdot n}{gcd(a,n)}(modn),\ i=1,2,\ldots gcd(a,n)-1$$

Παράδειγμα: $3x \equiv 6(mod\,9)$

a	b	gcd(a,b)	x	y	
3	9	3	1	0	$3\cdot 1+9\cdot y=3\Rightarrow y=0$
9	3	3	0	1	$9\cdot 0+3\cdot y=3\Rightarrow y=1$
3	0	3	1	0	$3\cdot 1+0\cdot y=3\Rightarrow y=0$

$$x_0=\frac{1\cdot 3}{gcd(3,9)}(mod\,9)=\frac{6}{3}(mod\,9)=2(mod\,9)=2$$
$$x_1=2+\frac{1\cdot 9}{gcd(3,9)}(mod\,9)=2+\frac{9}{3}(mod\,9)=5\,mod\,9=5$$
$$x_2=2+\frac{2\cdot 9}{gcd(3,9)}(mod\,9)=2+\frac{18}{3}(mod\,9)=8\,mod\,9=8$$

αλλά $3x\equiv 1(mod\,9)$ *δεν έχει λύση!!*

2. Σύστημα $x\equiv a_i(modn_i)$

Κινέζικο θεώρημα των υπολοίπων
Έστω x τέτοιο ώστε: $x\equiv 3(mod\,11),\ x\equiv 4(mod\,13),\ x\equiv 9(mod\,17).$ Ποιά είναι η τιμή του x;

Η κάθε σχέση γράφεται ως: $x\equiv a_i(modn_i),\ i=1,2,\ldots,k$ Προϋπόθεση για την ύπαρξη λύσης είναι για κάθε i,j, gcd(i,j)=1

1. $n=n_1n_2n_3\ldots n_k$
2. υπολογίζω τα $m_i=n/n_i$
3. υπολογίζω τα $c_i=m_i(m_i^{-1}\text{mod}n_i)$
4. $x=\sum_{i=1}^{k} a_ic_i(modn)$

Για το πρόβλημα που έχουμε:

1. $n=11\cdot 13\cdot 17=2431$
2. $m_1=221$, $m_2=187$, $m_3=143$
3. $c_1=221(221^{-1}\text{mod}11)=1$, $c_2=8$, $c_3=5$
4. $x=3\cdot 221\cdot 1+4\cdot 187\cdot 8+9\cdot 143\cdot 5(mod\,11\cdot 13\cdot 17)=927$