25/5/2017 – Επαναληπτικό μάθημα

Θεωρία Αριθμών

Υπάρχουν δύο είδη συνόλων που μας ενδιαφέρουν:

- $Z_n=\{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$ ή αλλιώς $Z_n=\{0, 1, 2, \ldots, n-1\}$ δηλαδή το σύνολο που περιέχει όλα τα δυνατά υπόλοιπα της διαίρεσης με το n. Το πλήθος των στοιχείων αυτών είναι $|Z_n|=n$.
- $Z_n^*=\{\alpha \in Z_n : \gcd(\alpha,n)=1\}$ δηλαδή το υποσύνολο του Z_n το οποίο περιλαμβάνει όλα τα υπόλοιπα που έχουν μέγιστο κοινό διαιρέτη με το n το 1 (ή αλλιώς είναι αμοιβαία πρώτοι με το n). Το πλήθος τους είναι $|Z_n^*|=\varphi(n)= n\cdot\prod_{p|n}\left(1-\frac{1}{p}\right)$ όπου p πρώτοι και p|n όλοι οι πρώτοι που διαιρούν το n.

Τα σύνολα αυτά λέγονται κλάσεις ισοδυναμίας. Μας ενδιαφέρουν επειδή για αυτά ισχύει η ιδιότητα: $[\alpha_n]+[b_n]=[c_n]$ για κάθε $[\alpha_n], [b_n], [c_n] \in Z_n$.

Τα στοιχεία που ανήκουν στην ίδια υποομάδα λέγονται ταυτόσημα (αφήνουν το ίδιο υπόλοιπο αν τα διαιρέσουμε με το n).

Πχ. για n=10	15	+	25	(mod10)=0
	5	+	5	(mod10)=0
	-15	+	105	(mod10)=0
	ταυτόσημοι		ταυτόσημοι	
για n=7	10	•	20	(mod7)=4
	3	•	6	(mod7)=4
	7003	•	70006	(mod7)=4
	ταυτόσημοι		ταυτόσημοι	

ΠΡΟΣΟΧΗ αυτό δεν ισχύει για την ύψωση σε δύναμη.

Για κάθε n και κάθε $\alpha \in Z_n^*$ ισχύει ότι $\alpha^{\varphi(n)} \equiv 1(\text{mod}n)$.
Για κάθε πρώτο p και κάθε $\alpha \in Z_p^*$ ισχύει ότι $\alpha^{p-1} \equiv 1(\text{mod}n)$.

Γεννήτορας είναι ένας αριθμός ο οποίος αν τον υψώσουμε σε δυνάμεις θα παράγει όλα τα στοιχεία του Z_n^*. Για κάθε γεννήτορα g του Z_n^* ισχύει ότι:
$g^x \equiv g^y(\text{mod}n) \iff x \equiv y\ (\text{mod}\varphi(n))$
Γενικά ισχύει ότι αν $x \equiv y\ (\text{mod}\varphi(n)) \implies a^x \equiv a^y\ (\text{mod}n)$

Έχουμε 3 τύπους πράξεων:

1. $ax \equiv b(\text{mod}n)$
2. $x \equiv a_1(\text{mod}n_1)$
   $x \equiv a_2(\text{mod}n_2)$
   …
   $x \equiv a_k(\text{mod}n_k)$
3. $a^b \equiv x(\text{mod}n)$

1. Για να έχει λύση θα πρέπει $\gcd(a,n)|b$. Αν ισχύει θα έχουμε $\gcd(a,n)$ σε πλήθος λύσεις.

Παράδειγμα: $27x \equiv 6 (\mathrm{mod} 33)$

aa	b	πηλίκο	gcd	x'	y'	
27	33	0	3	5		$3=27\bullet 5+33\bullet y' \Longrightarrow y'=-4$
33	27	1	3	-4	5	
27	6	4	3	1	-4	
6	3	2	3	0	1	
3	0	-	3	1	0	

Η βασική λύση είναι $x_0 = 5 \cdot \frac{6}{3} (mod\, 33) = 10 (mod\, 33)$

Οι υπόλοιπες λύσεις είναι: $x_1 = 1 \cdot \frac{33}{3} (mod\, 33) = 21 (mod\, 33)$

$x_2 = 2 \cdot \frac{33}{3} (mod\, 33) = 32 (mod\, 33)$

<u>Θέμα Ιουνίου 2016 (2 μονάδες)</u>

Ποιο είναι το αποτέλεσμα της ύψωσης $3^{98765432109} (\mathrm{mod} 101)$;

- $\varphi(101) = 101\left(1 - \frac{1}{101}\right) = 100$
- $98765432109 \bmod 100 = 9$
- $3^{98765432109} = 3^9 (\mathrm{mod} 101)$
- γράφουμε τη δυαδική αναπαράσταση του εκθέτη και εφαρμόζουμε τον αλγόριθμο (μάθημα 4ο)
  $<9>_{10} \longrightarrow <1001>_2$
  d=1
  <u>1</u>001
  d=1
  d=1•3=3
  1<u>0</u>01
  d=9
  10<u>0</u>1
  d=81
  100<u>1</u>
  $d=81^2 \bmod 101$
  $d=3\bullet 81^2 \bmod 101$

Παράδειγμα κινέζικου θεωρήματος των υπολοίπων, μάθημα 3ο.