Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ζωή Παρασκευοπούλου
Νίκος Γιανναράκης

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

9 Νοεμβρίου 2012 (v2)

1 Κυκλικές Ομάδες

Ορισμός. *Κυκλική Ομάδα*
Μια ομάδα G καλείται κυκλική αν υπάρχει στοιχείο $g \in G$ τέτοιο ώστε $G = < g >$ δηλαδή $\forall x \in G,\ \exists y : x = g^y$. Το στοιχείο g το ονομάζουμε γεννήτορα της G .

Ορισμός. *Τάξη Κυκλικής Ομάδας*
Τάξη μίας κυκλικής ομάδας $G = < g >$ ονομάζεται ο μικρότερος ακέραιος n τέτοιος ώστε $g^n = e$. Τότε $G = < g > = \{g^0, \cdots, g^{n-1}\}$ και $|G| = n$.

Θεώρημα 1. $< a^k > = < a^{gcd(n,k)} >$
Έστω a ένα στοιχείο τάξης n μιας ομάδας και k θετικός ακέραιος. Τότε $< a^k > = < a^{gcd(n,k)} >$ και $ord(a^k) = \frac{n}{gcd(n,k)}$.

Απόδειξη. Έστω $d = gcd(n, k)$ τότε $d|k \Rightarrow k = d \cdot r$ για κάποιο r. Έχουμε $a^k = a^{dr} = (a^d)^r$ επομένως λόγω κλειστότητας $< a^k > \subseteq < a^d >$. Απο επεκταταμένο αλγόριθμο ΜΚΔ μπορούμε να βρούμε s, t τέτοια ώστε $d = s \cdot n + t \cdot k$. Έτσι:

$$
\begin{aligned}
& a^d = a^{s\cdot n + t\cdot k} \\
\Rightarrow\ & a^d = (a^n)^s \cdot (a^k)^t \\
\Rightarrow\ & a^d = e \cdot (a^k)^t \in < a^k > && \text{από ορισμό τάξης } a^n = e \\
\Rightarrow\ & a^d = (a^k)^t \in < a^k > && \text{λόγω κλειστότητας} \\
\Rightarrow\ & < a^d > \subseteq < a^k >
\end{aligned}
$$

Αποδείξαμε επομένως ότι $< a^k > = < a^{gcd(n,k)} >$.

Θα δείξουμε ότι $ord(a^k) = \frac{n}{gcd(n,k)}$. Έχουμε ότι $(a^d)^{\frac{n}{d}} = a^n = e$ και από ορισμό τάξης $ord(a^d) \leq \frac{n}{d}$. Έστω $ord(a^d) < \frac{n}{d}$, θα πρέπει $(a^d)^{ord(a^d)} = e$. Όμως $d \cdot ord(a^d) < d \cdot \frac{n}{d} = n$ άρα καταλήγουμε σε άτοπο πάλι απο τον ορισμό της τάξης. Επομενως $ord(a^d) = \frac{n}{d}$ και επειδή όπως δείξαμε $< a^k > = < a^d >$, είναι $ord(a^k) = \frac{n}{d}$

□

Θεώρημα 2. *Θεμελιώδες Θεώρημα Κυκλικών Ομάδων*
Έστω G κυκλική ομάδα τάξης n. Τότε ισχύουν:

α.) Αν H είναι υποομάδα της G τότε η H είναι κυκλική.

β.) Η τάξη κάθε υποομάδας της G διαιρεί την τάξη της G.

γ.) Για κάθε θετικό διαιρέτη k του n έχουμε μια μοναδική υποομάδα τάξης k της G, συγκεκριμένα την $< a^{\frac{n}{k}} >$.

Απόδειξη.

α.) Αφού η G είναι κυκλικη υπάρχει στοιχείο $a \in G$ τέτοιο ώστε $< a >= G$, δηλαδή a γεννήτορας της G. Όλα τα στοιχεία της H θα ανήκουν στην G δηλαδή $\forall h \in H \ \exists k : \ h = a^k$. Αν $H = \{e\}$ τότε η H είναι κυκλική αφού $\{e\} = < e >$. Αν $H \neq \{e\}$ τότε υπάρχει $k > 0$ τέτοιο ώστε $a^k \in H$. Έστω $h_o = a^m$ και m ο μικρότερος θετικός ακέραιος για τον οποίο $h_o \in H$. Θα δείξουμε ότι $< h_o >= H$. 'Εχουμε:

- $< h_o > \subseteq H$
  Λόγω κλειστότητας ισχύει:

$$\forall h \in < h_o >, \exists k \in \mathbb{N} : h = (h_o)^k \Rightarrow h \in H$$

- $H \subseteq < h_o >$
  Θα πρέπει να δείξουμε ότι $\forall h \in H \Rightarrow h \in < a^m >$. Έστω $h = a^k$ στοιχείο της H. Έφαρμόζοντας τον αλγόριθμο της ακέραιας διαίρεσης μπορούμε να βρούμε q, r τέτοια ώστε $k = q \cdot m + r, 0 \leq r < m$. Τότε:

$$\begin{aligned} a^k &= a^{mq+r} = a^{mq} \cdot a^r \\ \Rightarrow a^r &= a^k \cdot (a^m)^{-q} = h \cdot h_0^{-q} \end{aligned}$$

  Τα h_o^{-q}, h ανήκουν στην H επομένως $a^r \in H$. Αφού όμως m είναι ο μικρότερος θετικός για τον οποίο $a^m \in H$ και $0 \leq r < m$ θα πρέπει $r = 0$. Επομένως $h = a^k = a^{mq} = h_o^q \in < h_o >$.

Έχουμε συνεπώς ότι $< h_o >= H$ άρα εξ'ορισμού H κυκλική με γεννήτορα h_o.

β.) Άπο τον ορισμό της τάξης της ομάδας έχουμε $a^n = e$. Όπως δείξαμε αν m ο μικρότερος θετικός ακέραιος για τον οποίο $a^m \in H$ τότε $H = < a^m >$. Έστω $n = q \cdot m + r, \ 0 \leq r < m$. Έχουμε

$$\begin{aligned} a^r &= a^n \cdot (a^m)^{-q} \\ \Rightarrow a^r &= e \cdot (a^m)^{-q} \\ \Rightarrow a^r &= (a^m)^{-q} \end{aligned}$$

Το a^m ανήκει στην H άρα απο κλειστότητα $a^r = (a^m)^{-q}$ ανήκει επίσης στην H. Όμως m ο μικρότερος θετικός ακέραιος για τον οποίο $a^m \in H$ και

$0 \leq r < m$, άρα πρέπει $r = 0$. Έτσι $n = mq$ και

$$ord(H) = ord(a^m) = \frac{n}{gcd(n,m)} \qquad \text{απο } \textit{Θεώρημα 1}$$
$$\Rightarrow ord(H) = \frac{n}{m} = q$$
$$\Rightarrow ord(H) \mid n$$

γ.) Έστω k διαιρέτης του n. Τότε :

$$ord(a^{\frac{n}{k}}) = \frac{n}{gcd(n, \frac{n}{k})} \qquad \text{από } \textit{Θεώρημα 1}$$
$$\Rightarrow ord(a^{\frac{n}{k}}) = \frac{n}{\frac{n}{k}}$$
$$\Rightarrow ord(a^{\frac{n}{k}}) = k$$

Έστω υποομάδα H με $ord(H) = k$. Από *α.)* και *β.)* έχουμε $H = < a^m >$ και $m|n$. Κάνοντας πάλι χρήση του *Θεωρήματος 1* έχουμε ότι $ord(H) = ord(a^m) = \frac{n}{gcd(n,m)} = \frac{n}{m}$. Άρα $k = \frac{n}{m}$ ή $m = \frac{n}{k}$ και επομένως $H = < a^m > = < a^{\frac{n}{k}} >$.

Πόρισμα. *Όλα τα στοιχεία τάξης d ανήκουν στην $< a^{\frac{n}{d}} >$*

□

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

Sti06 : D. Stinson: Cryptography: Theory and Practice, 3rd edition, CRC Press, 2005.

Gal09 : Joseph A. Gallian: Contemporary Abstract Algebra