Εθνικό Μετσόβιο Πολυτεχνείο

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Διονύσης Ζήνδρος Αντώνης Αναστασόπουλος

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

28 Νοεμβρίου 2011

Θεωρία αριθμών

Από τις σημειώσεις [Ζάχος]: Κεφάλαιο 6, σελίδα 145.

Διαιρετότητα

$$a|b \stackrel{\text{def}}{=} \exists c \in \mathbb{Z} : b = ca$$

Ιδιότητες

1. $a|0$
2. Κάθε αριθμός μεγαλύτερος του 1 έχει τουλάχιστον δύο διαιρέτες: το 1 και τον εαυτό του
3. $a|b \Rightarrow a|(bc)$
4. $a|b \wedge b|a \Rightarrow a|c$
5. $a|b \wedge b|a \Leftrightarrow |a| = |b|$
6. $a|b \wedge a|c \Rightarrow a|(b + c)$
7. $a|b \wedge a|c \Rightarrow a|(bx + cy)$
8. $a|b \wedge b > 0 \Rightarrow a \leq b$

Πρώτος αριθμός

$$a \in \mathbb{N} \text{ πρώτος} \stackrel{\text{def}}{=} \forall b \in \mathbb{N} : 1 < b < a \Rightarrow b \nmid a$$

Γνωστοί πρώτοι

1. $2, 3, 5, ..., 1997, 1999, 2003, 2011, ...$
2. Ο μεγαλύτερος γνωστός πρώτος το 2011: $2^{43112609} - 1$ [GIMPS]

Σχετικά πρώτοι

$$a \text{ coprime } b \stackrel{\text{def}}{=} gcd(a, b) = 1$$

Μέγιστος Κοινός Διαιρέτης

$$(a, b) \stackrel{\text{def}}{=}$$
$$gcd(a, b) \stackrel{\text{def}}{=} \max\{c \in \mathbb{Z} : c|a \wedge c|b\}$$

Ο καλύτερος αλγόριθμος που γνωρίζουμε ακόμα και σήμερα για την εύρεσή του είναι ο αλγόριθμος του Ευκλείδη:

- $gcd(a, b) = b$, αν $b|a$ και $a > b$
- $gcd(a, b) = gcd(a \mod b, b)$, αν $b \nmid a$ και $a > b$
- $gcd(a, b) = gcd(b, a)$, αλλιώς

Αλγεβρικές δομές

Ομάδες

Abelian group ή αντιμεταθετική ομάδα λέγεται ένα ζεύγος $(G, *)$ τέτοιο ώστε για $a, b, c \in G$:

- $a * (b * c) = (a * b) * c$
- $a * b = b * a$
- $\exists! e \in G : \forall a : a * e = a$
- $\forall a \in a^{-1} \in G : a * a^{-1} = e$

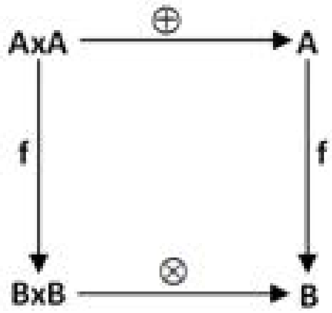
Αλγεβρική δομή

Αλγεβρική δομή λέγεται μία n-άδα $(A; f_1, f_2, f_3, \ldots)$ όπου A ένα σύνολο (domain) και $f_1, f_2, f_3, \ldots$ πράξεις (δηλαδή συναρτήσεις κλειστές εντός του A) με 0 ή περισσότερα ορίσματα με πεδίο ορισμού το A.

Ομομορφισμός

Μία συνάρτηση $f : A \to B$ ανάμεσα σε δύο αλγεβρικές δομές $(A, \oplus)$ και $(B, \otimes)$ ονομάζεται ομομορφισμός αν απεικονίζει τη μία αλγεβρική δομή στην άλλη ως εξής:

$$f(a \oplus b) = f(a) \otimes f(b)$$



Από τον ορισμό προκύπτει άμεσα ότι:

$$\begin{aligned} f(e_A \oplus b) &= f(e_A) \otimes f(b) \\ f(b) &= e_B \otimes f(b) \\ f(e_A) &= e_B \end{aligned}$$

Δακτύλιος

$$\begin{aligned} &(R, +, *) \text{ δακτύλιος} \stackrel{\text{def}}{=} \\ &\qquad (R, +) \text{ αντιμεταθετική ομάδα} \\ &\qquad \wedge \forall a, b, c \in R : \\ &\qquad a * (b + c) = (a * b + a * c) \\ &\qquad \wedge (b + c) * a = b * a + c * a \end{aligned}$$

Σώμα

$$\begin{aligned} &(F, +, *) \text{ σώμα } \stackrel{\text{def}}{=} \\ &\qquad (F, +) \text{ αντιμεταθετική ομάδα} \\ &\qquad \wedge (F - \{e_+\}, *) \text{ αντιμεταθετική ομάδα} \\ &\qquad \wedge \forall a, b, c \in F : a * (b + c) = a * b + a * c \end{aligned}$$

Υποομάδα

$$(S, *) \text{ υποομάδα της } (G, *) \stackrel{\text{def}}{=} S \subseteq G \wedge (S, *) \text{ ομάδα}$$

Κυκλική ομάδα

$$(G, *) \text{ κυκλική} \stackrel{\text{def}}{=} \exists g \in (G, *) : \forall x \in G : \exists y \in \mathbb{N} : x = g^y$$

Τάξη

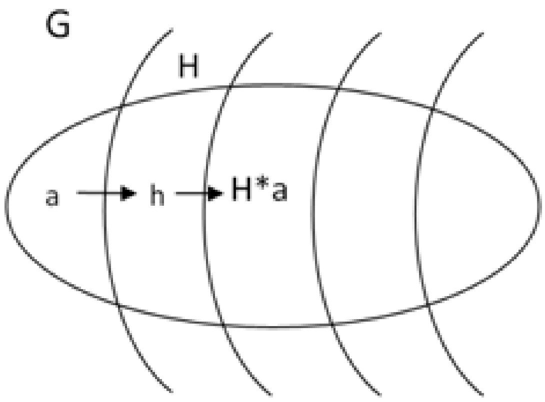
$$a^1 \stackrel{\text{def}}{=} a$$
$$a^n \stackrel{\text{def}}{=} a^{n-1} * a$$
$$\text{τάξη } a \stackrel{\text{def}}{=} min\{y \in \mathbb{N} : a^y = e\}$$

Γεννήτορας

$$a \text{ γεννήτορας της } G \stackrel{\text{def}}{=} \text{τάξη } a = |G|$$

Coset

$$H * a = \{h * a : h \in H, a \in G\} \stackrel{\text{def}}{=} \text{ δεξί σύμπλοκο (coset) της } H \text{ στη } G$$
$$\text{για } H \text{ υποομάδα της } (G, *).$$



Quotient group

Το σύνολο $\{G/H\}$ είναι ομάδα με πράξη $(H * a) * (H * b) = H * (a * b)$.

Lagrange

Αν H υποομάδα της πεπερασμένης ομάδας G τότε

$$|G| = |G/H| * |H|$$

Ο δακτύλιος $\mathbb{Z}_m$

Το σύνολο ακεραίων modulo m : $\{0, 1, 2, ..., m-1\}$.

Ισοδύναμα $\mathbb{Z}_m = \{a \mod m | a \in \mathbb{Z}\}$

Υπόλοιπο

$$a \equiv_m b \stackrel{\text{def}}{=}$$

$$a \equiv b \pmod m \stackrel{\text{def}}{=} m|(a-b)$$

Ιδιότητες υπολοίπου

1. $a \equiv a \pmod m$ (reflexive)
2. $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ (symmetric)
3. $a \equiv b \pmod m \wedge b \equiv c \pmod n \Rightarrow a \equiv c \pmod m$ (transitive)

Ιδιότητες κλάσεων

1. $[a] + [b] = [a + b]$
2. $[a].[b] = [a.b]$
3. $[a] + [b] = [b] + [a]$
4. $([a] + [b]) + [c] = [a] + ([b] + [c])$
5. $[a] + [0] = [a]$
6. $[a] + [-a] = [0]$
7. $[a].[b] = [b].[a]$
8. $([a].[b]).[c] = [a].([b].[c])$
9. $[a].([b] + [c]) = [a].[b] + [a].[c]$
10. $[a].[1] = [a]$

Ασκήσεις

1. Να αποδείξετε την Πρόταση 6.2, [Ζάχος] ς. 146
2. Άσκηση 6.8, [Ζάχος] ς. 147
3. Να αποδείξετε την ορθότητα του αλγορίθμου του Ευκλείδη, [Ζάχος] ς. 148
4. Να αποδείξετε την Πρόταση 6.15, [Ζάχος] ς. 149
5. Να αποδείξετε το Πόρισμα 6.17, [Ζάχος] ς. 149
6. Να αποδείξετε το Θεώρημα 6.19, [Ζάχος] ς. 149
7. Άσκηση 6.37, [Ζάχος] ς. 154
8. Άσκηση 6.40, [Ζάχος] ς. 155

Βιβλιογραφία

1. [Ζάχος]: Ε. Ζάχος, «Σημειώσεις στη Θεωρία Αριθμων και την Κρυπτογραφία», 2007
2. [GIMPS]:: «Great Internet Mersenne Prime Search», 1996 - 2011