Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

# Θεωρία Αριθμών

*Επιμέλεια σημειώσεων:*
Ελένη Λιτσα
Νίκος Μελισσαρης

*Διδάσκοντες:*
Στάθης Ζαχος
Άρης Παγουρτζης

21 Νοεμβρίου 2011

Έστω $a, b \in \mathbb{Z}$, λέμε ότι ο $a$ διαιρεί τον $b$ και γράφουμε $a|b$ αν $\exists c \in \mathbb{Z}$ τέτοιο ώστε $b = c \cdot a$. Αντίστοιχα, λέμε ότι ο $a$ δεν διαιρεί τον $b$ και γράφουμε $a \nmid b$ αν $\nexists c \in \mathbb{Z}$ τέτοιο ώστε $b = c \cdot a$.

Ιδιότητες:

- $a|0$
- $0|a \Leftrightarrow a = 0$
- $a|b \wedge b|c \Rightarrow a|c$
- $a|b \Rightarrow a|bc$
- $a|b \wedge a|c \Rightarrow a|(b + c)$
- $a|b \wedge b|a \Rightarrow a = \pm b$
- $a|b \wedge b > 0 \Rightarrow a \leq b$

**Θεμελιώδες Θεώρημα της Αριθμητικής:**
*Κάθε αριθμός $n \in \mathbb{Z}_+$ μεγαλύτερος της μονάδας γράφεται με μοναδικό τρόπο σαν γινόμενο πρώτων αριθμών.*

Απόδειξη:

1. *Ανάλυση σε γινόμενο πρώτων:*
   Για $n = 2$ προφανώς ισχύει.
   Έστω ότι για κάθε φυσικό αριθμό $n$ με $n \geq 2$, υπάρχουν πρώτοι αριθμοί $p_1, ..., p_m$ έτσι ώστε $n = p_1...p_m$. Αν ο αριθμός $n$ είναι πρώτος τότε προφανώς η πρόταση ισχύει. Αν ο $n$ είναι σύνθετος, τότε υπάρχουν $a, b \in \mathbb{N}$ τέτοια ώστε $n = a \cdot b$ με $1 < a \leq b < n$. Τότε από επαγωγική υπόθεση οι $b, c$ γράφονται ως γινόμενο πρώτων άρα και ο $n$ γράφεται ως γινόμενο πρώτων.

2. *Μοναδικότητα:*
   Έστω ότι υπάρχουν δύο διαφορετικές γραφές για τον $n$, έστω δηλαδή $n = p_1...p_k = q_1...q_l$, με $k \leq l$. Το $p_1$ διαιρεί το $n$ επομένως, $p_1|q_1...q_l$ και άρα $p_1|q_j$ για κάποιο δείκτη $j$. Και επειδή ο $q_j$ είναι πρώτος προκύπτει πως $p_1 = q_j$. Με την ίδια διαδικάσία βρίσκουμε πως κάθε πρώτος $p_i$ της πρώτης γραφής ταυτίζεται με κάποιον $q_j$ της δεύτερης γραφής, επομένως οι δύο γραφές ταυτίζονται.

**Θεώρημα ακέραιης διαίρεσης:**
*Για κάθε $a, b \in \mathbb{Z}$ με $b \neq 0$ υπάρχουν μοναδικά $q, r$ τέτοια ώστε $a = q \cdot b + r$*

**Θεώρημα :**
*Ο Μ.Κ.Δ. δύο αριθμών μπορεί να γραφεί σαν γραμμικός συνδυασμός τους. Δηλαδή, έστω $a, b \in \mathbb{Z}$ και $d = gcd(a, b)$ τότε υπάρχουν μοναδικά $\kappa, \lambda \in \mathbb{Z}$ τέτοια ώστε $d = \kappa a + \lambda b$. Ισοδύναμα, αν το $d$ είναι ο ελάχιστος μη αρνητικός αριθμός για τον οποίο $d = \kappa a + \lambda b$ τότε $d = gcd(a, b)$.*

Απόδειξη:

Έστω $I = \{xa + yb | x, y \in \mathbb{Z}\}$ και $d = min(\{t \in I | t > 0\})$

- $d|a$ και $d|b$
  απόδειξη:
  Έστω $d \nmid a$ τότε $a = qd + r$ με $0 < r < d$
  αλλά $r = a - qd = a - q\kappa a - q\lambda b \in I$ άτοπο.
  Όμοια και για $d|b$.

- είναι ο μέγιστος
  Έστω ότι υπάρχει $d'$ τέτοιο ώστε $d'|a$ και $d'|b$.
  Τότε θα ισχύουν $a = a'd'$ και $b = b'd'$.
  Επομένως, $d = (\kappa a' + \lambda b')d' \Rightarrow d' \leq d$ άτοπο.

**Θεώρημα :**
*Αν $c|ab \wedge gcd(c, a) = 1$ τότε $c|b$*

Απόδειξη:

$gcd(c, a) = 1 \Rightarrow \exists s, t \in \mathbb{Z}$ τέτοια ώστε $as + ct = 1$. Πολλαπλασιάζοντας και τα δύο μέλη της ισότητας με $b$ παίρνουμε $abs + bct = b$. Αλλά $c|ab$ επομένως $ab = \lambda c$ άρα αντικαθιστώντας στην προηγούμενη εξίσωση παίρνουμε $s\lambda ct + tbc = b \Rightarrow (s\lambda t + tb)c = b \Rightarrow c|b$

**Θεώρημα :**
*Αν $p$ πρώτος αριθμός και $p|ab$ τότε $(p|a) \vee (p|b)$*

Απόδειξη:

Θα ισχύει $gcd(p, a) = 1$ ή $gcd(p, a) = p$

Αν $gcd(p, a) = p$ τότε $(p|a)$
Αν $gcd(p, a) = 1$ τότε $(p|a)$ σύμφωνα με το προηγούμενο θεώρημα.

**Θεώρημα :**
*Εάν* $gcd(a, n) = 1$ *τότε υπάρχει* $a^{-1}$ *τέτοιο ώστε* $a \cdot a^{-1}(mod\, n) = 1$

Απόδειξη:

$gcd(a, n) = 1 \Rightarrow 1 = \kappa a + \lambda n \Rightarrow 1 = \kappa a\, (mod\, n) \Rightarrow \kappa = a^{-1}$