Θεωρία Αριθμών V

Μέγιστος Κοινός Διαιρέτης
(Greatest Common Divisor)
Ελάχιστο Κοινό Πολλαπλάσιο
(Least Common Multiple)

Βαγγέλης Ψύχας

Μέγιστος Κοινός Διαιρέτης

✧ Έστω a, b δύο ακέραιοι, από τους οποίους ένας τουλάχιστον είναι διάφορος του μηδενός ($|a| + |b| \neq 0$). Ονομάζουμε **μέγιστο κοινό διαιρέτη** των a και b, τον θετικό ακέραιο d για τον οποίο ισχύουν τα παρακάτω:

α) $d|a$ και $d|b$ β) $(c|a$ και $c|b) \Rightarrow c \leq d$

- Ο μέγιστος κοινός διαιρέτης των a και b , συμβολίζεται με $\mu\kappa\delta(a,b)$ ή απλά (a,b).
(greatest common divisor $gcd(a,b)$)

- Ο μέγιστος κοινός διαιρέτης των a και b, είναι ο μεγαλύτερος από τους κοινούς διαιρέτες των a και b.

- Αν a, b είναι δύο ακέραιοι με $|a| + |b| \neq 0$, τότε υπάρχουν ακέραιοι k, m για τους οποίους ισχύει:
$$(a,b) = k \cdot a + m \cdot b.$$

- Κάθε παράσταση της μορφής $k \cdot a + m \cdot b$ λέγεται γραμμικός συνδυασμός των a και b .

Σχετικά Πρώτοι Αριθμοί

✧ Δύο ακέραιοι a, b για τους οποίους ισχύει: $|a| + |b| \neq 0$, θα λέγονται **σχετικά πρώτοι ή πρώτοι μεταξύ τους** τον (relatively prime), αν $(a, b) = 1$.

✧ Έστω a, b δύο ακέραιοι με $|a| + |b| \neq 0$. Τότε οι ακέραιοι a, b θα είναι **σχετικά πρώτοι** αν και μόνο αν υπάρχουν ακέραιοι k, m για τους οποίους ισχύει: $1 = k \cdot a + m \cdot b$.

Ιδιότητες μκδ

- $(a, b) = (|a|, |b|)$
- $(a, b) = d \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$
- $$\left.\begin{matrix} a|c \\ b|c \\ (a, b) = 1 \end{matrix}\right\} \Rightarrow ab|c$$
- $$\left.\begin{matrix} a|bc \\ (a, b) = 1 \end{matrix}\right\} \Rightarrow a|c$$
- $$(a, b) = d \Leftrightarrow \begin{cases} d|a \;\&\; d|b \\ \left.\begin{matrix} c|a \\ c|b \end{matrix}\right\} \Rightarrow c|d \end{cases}, \qquad (|a| + |b| \neq 0)$$

✧ Για κάθε θετικό ακέραιο n και για κάθε ακέραιο a, αποδείξτε ότι $(a, a+n)|n$ και κατά συνέπεια $(a, a+1) = 1$.

✧ Έστω $(a, a+n) = d$ τότε:

$$\left.\begin{array}{r} d|a \\ d|(a+n) \end{array}\right\} \Rightarrow d|(a+n-a) \Rightarrow d|n.$$

Αν τώρα υποθέσουμε ότι $(a, a+1) = d$,
τότε $d|1$, οπότε $d = \pm 1$.
Άρα $d = 1$, διότι $d = (a, a+1) > 0$.

♢ Αποδείξτε ότι: $\left.\begin{matrix}(a,b)=1\\(a,c)=1\end{matrix}\right\} \Rightarrow (a,bc)=1.$

♢ $\left.\begin{matrix}(a,b)=1 \Leftrightarrow ka+mb=1\\(a,c)=1 \Leftrightarrow na+lc=1\end{matrix}\right\} \overset{(\cdot)}{\Rightarrow} (ka+mb)\cdot(na+lc)=1 \Rightarrow$

$\Rightarrow ka\cdot na+ka\cdot lc+mb\cdot na+mb\cdot lc=1 \Rightarrow$

$\Rightarrow a(kna+klc+mnb)+bc(ml)=1 \Leftrightarrow (a,bc)=1.$

♢ Αποδείξτε ότι: $\left.\begin{matrix}(a,b)=1\\c|a\end{matrix}\right\} \Rightarrow (b,c)=1.$

♢ Έστω $(b,c)=d$. Τότε $d|b$ και $d|c$.

Επειδή όμως $c|a$, θα ισχύει: $d|b$ και $d|a$.

Άρα $d|(a,b)=1 \Leftrightarrow d|1 \Rightarrow d=1.$

$$\text{♢ Αποδείξτε ότι: } \left.\begin{matrix}(a,b)=1\\ a|bc\end{matrix}\right\} \Rightarrow a|c.$$

♢ Εφόσον $(a,b)=1$ θα υπάρχουν ακέραιοι αριθμοί k, m τέτοιοι ώστε: $ka+mb=1$.

Πολλαπλασιάζοντας την προηγούμενη ισότητα με c έχουμε:

$$kac+mbc=c.$$

$$\text{Γνωρίζουμε ότι: } \left.\begin{matrix}a|ac\\ a|bc\end{matrix}\right\} \Rightarrow a|(kac+mbc)=c.$$

$$a = qb + r \Rightarrow (a, b) = (b, r).$$

$$k > 0 \Rightarrow (ka, kb) = k(a, b).$$

$$k \neq 0 \Rightarrow (ka, kb) = |k|(a, b).$$

Ελάχιστο Κοινό Πολλαπλάσιο

✧ Ονομάζουμε **ελάχιστο κοινό πολλαπλάσιο** των μη μηδενικών ακεραίων a και b, τον θετικό ακέραιο m για τον οποίο ισχύουν τα παρακάτω:

α) $a|m$ και $b|m$ β) $(a|c \text{ και } b|c) \Rightarrow m \leq c$.

✧ Το ελάχιστο κοινό πολλαπλάσιο των a και b, συμβολίζεται με $\varepsilon\kappa\pi(a, b)$ ή $[a, b]$.

(least common multiple $lcm(a, b)$)

✧ Για τους θετικούς ακέραιους $\boldsymbol{a}$ και $\boldsymbol{b}$ ισχύουν:

- $(\boldsymbol{a}, \boldsymbol{b}) \cdot [\boldsymbol{a}, \boldsymbol{b}] = \boldsymbol{a} \cdot \boldsymbol{b}$
- $[\boldsymbol{a}, \boldsymbol{b}] = \boldsymbol{a} \cdot \boldsymbol{b} \Leftrightarrow (\boldsymbol{a}, \boldsymbol{b}) = \mathbf{1}$