Διακριτά Μαθηματικά ΙΙ

Χρήστος Νομικός

Τμήμα Μηχανικών Η/Υ και Πληροφορικής
Πανεπιστήμιο Ιωαννίνων

MMXXIII

Περιεχόμενα

Περιεχόμενα

Η πράξη της αφαίρεσης στους ακέραιους αριθμούς είναι η αντίστροφη πράξη της πρόσθεσης: αν $a + b = c$, τότε $c - a = b$ και $c - b = a$.

Για οποιουσδήποτε ακέραιους αριθμούς a, c, υπάρχει πάντα ένας ακέραιος αριθμός b τέτοιος ώστε $a + b = c$.

Συνεπώς η διαφορά $c - a$ ορίζεται για οποιοδήποτε ζεύγος ακεραίων.

Αντίστοιχα θέλουμε να ορίσουμε τη διαίρεση ως την αντίστροφη πράξη του πολλαπλασιασμού: αν $q \cdot d = a$, τότε θα πρέπει $a \operatorname{div} d = q$ και $a \operatorname{div} q = d$.

Ωστόσο υπάρχουν ακέραιοι αριθμοί a, d, για τους οποίους δεν υπάρχει ακέραιος αριθμός q τέτοιος ώστε $q \cdot d = a$.

Ορισμός

Έστω a, d δύο ακέραιοι αριθμοί. Λέμε ότι ο d διαιρεί τον a αν $d \neq 0$ και υπάρχει ακέραιος q τέτοιος ώστε $q \cdot d = a$. Αν ο d διαιρεί το a τότε ο λέμε ότι ο d είναι διαιρέτης ή παράγοντας του a και ότι ο a είναι πολλαπλάσιο του d. Γράφουμε $d \mid a$ για να δηλώσουμε ότι ο d διαιρεί τον a και $d \nmid a$ για να δηλώσουμε ότι ο d δεν διαιρεί τον a.

Παράδειγμα

Ισχύει $4 \mid 20$, καθώς $5 \cdot 4 = 20$

Αντίθετα $5 \nmid 12$.

Πράγματι για κάθε ακέραιο k ισχύει $k \leq 2$ ή $k \geq 3$. Αν $k \leq 2$ τότε $k \cdot 5 \leq 2 \cdot 5 = 10 < 12$ αν $k \geq 3$ τότε $k \cdot 5 \geq 3 \cdot 5 = 15 > 12$. Συνεπώς για κάθε ακέραιο k ισχύει $k \cdot 5 \neq 12$.

Λήμμα

Για οποιουσδήποτε ακεραίους αριθμούς a, b, d ισχύουν τα παρακάτω:

(α) αν $d \mid a$ και $d \mid b$ τότε $d \mid a + b$

(β) αν $d \mid a$ τότε $d \mid a \cdot b$

(γ) αν $d \mid a$ και $a \mid b$ τότε $d \mid b$

(δ) αν $d \mid a$ και $b \neq 0$ τότε $d \cdot b \mid a \cdot b$

Απόδειξη

(α) Αν $d \mid a$ και $d \mid b$, τότε $d \neq 0$ και υπάρχουν ακέραιοι q_1, q_2 τέτοιοι ώστε $q_1 \cdot d = a$ και $q_2 \cdot d = b$.

Συνεδυάζοντας τις δύο παραπάνω ισότητες, προκύπτει ότι $q_1 \cdot d + q_2 \cdot d = a + b$ που ισοδυναμεί με $(q_1 + q_2) \cdot d = a + b$.

Άρα για $q = q_1 + q_2$ ισχύει $q \cdot d = a + b$. Επίσης ισχύει $d \neq 0$. Συνεπώς $d \mid a + b$.

Απόδειξη (συνέχεια)

(β) Αν $d \mid a$, τότε $d \neq 0$ και υπάρχει ακέραιος q' τέτοιος ώστε $q' \cdot d = a$.

Από την παραπάνω ισότητα, προκύπτει ότι $(q' \cdot d) \cdot b = a \cdot b$ που ισοδυναμεί με $(q' \cdot b) \cdot d = a \cdot b$.

Άρα για $q = q' \cdot b$ ισχύει $q \cdot d = a \cdot b$. Επίσης ισχύει $d \neq 0$. Συνεπώς $d \mid a \cdot b$.

Απόδειξη (συνέχεια)

Η απόδειξη των (γ) και (δ) αφήνεται σαν άσκηση. □

Θα ορίσουμε τη πράξη της ακέραιας διαίρεσης έτσι ώστε να εφαρμόζεται σε όλα τα ζεύγη ακεραίων a, d με $d > 0$.

Ορισμός

Έστω δύο ακέραιοι a, d με $d > 0$. Το πηλίκο της διαίρεσης του a με το d είναι ο αριθμός $a \operatorname{div} d = \max\{k \in \mathbb{Z} : k \cdot d \leq a\}$. Το υπόλοιπο της διαίρεσης του a με το d είναι ο αριθμός $a \bmod d = a - (a \operatorname{div} d) \cdot d$. Ο αριθμός a ονομάζεται διαιρετέος και ο d ονομάζεται διαιρέτης.

Παρατηρούμε ότι για κάθε ακέραιο a, το σύνολο $\{k \in \mathbb{Z} : k \cdot d \leq a\}$ είναι μη κενό και έχει μέγιστο στοιχείο, καθώς τα στοιχεία του είναι άνω φραγμένα από κάποιον ακέραιο:

- αν $a > 0$, τότε $0 \cdot d \leq a$ (δηλαδή το 0 είναι στοιχείο του συνόλου) και $k \cdot d \leq a$ συνεπάγεται $k < a + 1$ (δηλαδή το $a + 1$ είναι άνω φράγμα για τα στοιχεία του συνόλου).
- αν $a \leq 0$, τότε $a \cdot d \leq a$ (δηλαδή το a είναι στοιχείο του συνόλου) και $k \cdot d \leq a$ συνεπάγεται $k \leq 0$ (δηλαδή το 0 είναι άνω φράγμα για τα στοιχεία του συνόλου).

Συνεπώς το a div d είναι καλά ορισμένο.

Θεώρημα

Για οποιουσδήποτε ακέραιους a, d με $d > 0$, ισχύει

$$0 \leq a \bmod d \leq d - 1$$

Απόδειξη

Από τον ορισμό του $a \operatorname{div} d$ ισχύει $(a \operatorname{div} d) \cdot d \leq a$ και άρα

$$a \bmod d = a - (a \operatorname{div} d) \cdot d \geq 0$$

Θα δείξουμε ότι $a \bmod d \leq d - 1$ με απαγωγή σε άτοπο.

Απόδειξη (συνέχεια)

Έστω ότι $a \bmod d > d - 1$ που συνεπάγεται $a \bmod d \geq d$.

Τότε:

$$\begin{aligned} a - (a \operatorname{div} d) \cdot d = a \bmod d \geq d \quad &\Rightarrow \quad a - (a \operatorname{div} d) \cdot d - d \geq 0 \\ &\Rightarrow \quad a - ((a \operatorname{div} d) + 1) \cdot d \geq 0 \\ &\Rightarrow \quad ((a \operatorname{div} d) + 1) \cdot d \leq a \end{aligned}$$

Αυτό είναι ότοπο, καθώς ο μέγιστος ακέραιος k για τον οποίο ισχύει $k \cdot d \leq a$ είναι το $(a \operatorname{div} d)$.

Άρα $a \bmod d \leq d - 1$. □

Θεώρημα

Έστω δύο ακέραιοι a, d με $d > 0$. Τότε οι μοναδικές ακέραιες τιμές q και r για τις οποίες ισχύει $0 \leq r \leq d - 1$ και $a = q \cdot d + r$ είναι $q = a \text{ div } d$ και $r = a \bmod d$.

Απόδειξη

Αφήνεται σαν άσκηση.

Ορισμός

Έστω a, b δύο ακέραιοι και m ένας θετικός ακέραιος. Λέμε ότι ο αριθμός a είναι ισοϋπόλοιπος του b modulo m, το οποίο συμβολίζεται $a \equiv b \ (mod \ m)$, αν $a \bmod m = b \bmod m$. Αν $a \bmod m \neq b \bmod m$ γράφουμε $a \not\equiv b \ (mod \ m)$.

Η σχέση $a \equiv b \ (mod \ m)$ ονομάζεται ισοτιμία και ο αριθμός m μέτρο της ισοτιμίας.

Το $a \equiv b \ (mod \ m)$ διαφέρει από το $a \bmod m = b$.

Για παράδειγμα για $a = 15$, $b = 31$ και $m = 2$, το πρώτο γίνεται $15 \equiv 31 \ (mod \ 2)$, το οποίο αληθεύει επειδή $15 \bmod 2 = 31 \bmod 2 = 1$, ενώ το δεύτερο γίνεται $15 \bmod 2 = 31$, το οποίο δεν αληθεύει.

Το $\equiv \ (mod \ m)$ είναι μία σχέση επι του συνόλου των ακεραίων, ενώ το $\bmod$ είναι μία αριθμητική πράξη.

Θεώρημα

Για οποιουσδήποτε ακεραίους a, b, m με $m \geq 1$, ισχύει $a \equiv b \ (mod \ m)$ αν και μόνο αν $m \mid a - b$.

Απόδειξη

Έστω $q_1 = (a \text{ div } m)$, $r_1 = (a \text{ mod } m)$, $q_2 = (b \text{ div } m)$ και $r_2 = (b \text{ mod } m)$.

Τότε $a = q_1 \cdot m + r_1$ και $b = q_2 \cdot m + r_2$.

Απόδειξη (συνέχεια)

Για τη μία κατεύθυνση, έστω $a \equiv b \ (mod \ m)$. Τότε ισχύει $r_1 = r_2$.

Συνεπώς

$$\begin{aligned} a - b &= q_1 \cdot m + r_1 - q_2 \cdot m - r_2 \\ &= q_1 \cdot m - q_2 \cdot m + r_1 - r_2 \\ &= (q_1 - q_2) \cdot m \end{aligned}$$

Άρα $a - b = q \cdot m$, για $q = q_1 - q_2$, που συνεπάγεται $m \mid a - b$.

Απόδειξη (συνέχεια)

Για την αντίστροφη κατεύθυνση, έστω $m \mid a - b$. Τότε υπάρχει σταθερά q' τέτοια ώστε

$$\begin{aligned} a - b = q' \cdot m &\Leftrightarrow q_1 \cdot m + r_1 - q_2 \cdot m - r_2 = q' \cdot m \\ &\Leftrightarrow r_1 - r_2 = q' \cdot m - q_1 \cdot m + q_2 \cdot m \\ &\Leftrightarrow r_1 - r_2 = (q' - q_1 + q_2) \cdot m \end{aligned}$$

Έστω $q = (q' - q_1 + q_2)$. Συνεπώς $r_1 - r_2 = q \cdot m$.

Απόδειξη (συνέχεια)

Ισχύει $0 \leq r_1 \leq m-1$ και $0 \leq r_2 \leq m-1$, που συνεπάγεται $-(m-1) \leq r_1 - r_2 \leq m-1$.

Θα δείξουμε ότι η μοναδική τιμή του q για την οποία μπορεί να ισχύει η ισότητα $r_1 - r_2 = q \cdot m$ είναι η τιμή 0.

Απόδειξη (συνέχεια)

Πράγματι, για κάθε ακέραιο $k \leq -1$ ισχύει
$k \cdot m \leq -m < -(m-1) \leq r_1 - r_2$, που συνεπάγεται $k \cdot m \neq r_1 - r_2$.

Ομοίως, για κάθε ακέραιο $k \geq 1$ ισχύει $k \cdot m \geq m > m - 1 \geq r_1 - r_2$,
που συνεπάγεται $k \cdot m \neq r_1 - r_2$.

Συνεπώς $q = 0$ και άρα $r_i - r_2 = 0 \cdot m = 0$ που ισοδυναμεί $r_1 = r_2$. Άρα
$a \bmod m = b \bmod m$. □

Πόρισμα

Για οποιουσδήποτε ακεραίους a, b, m με $m \geq 1$, ισχύει $a \equiv b \ (mod \ m)$ αν και μόνο αν υπάρχει ακέραιος q τέτοιος ώστε $a = b + q \cdot m$.

Πόρισμα

Για οποιουσδήποτε ακεραίους a, m με $m \geq 1$, ισχύει $a \equiv (a \bmod m)\ (mod\ m)$.

Απόδειξη

Είναι $(a \bmod m) = a - (a \operatorname{div} m) \cdot m$ που ισοδυναμεί $a - (a \bmod m) = (a \operatorname{div} m) \cdot m$. Άρα $m \mid a - (a \bmod m)$, που συνεπάγεται $a \equiv (a \bmod m)\ (mod\ m)$, από το προηγούμενο θεώρημα. □

Θεώρημα

Έστω a, b, c, d, m ακέραιοι αριθμοί με $m \geq 1$. Αν $a \equiv b \ (mod \ m)$ και $c \equiv d \ (mod \ m)$, τότε $a + c \equiv b + d \ (mod \ m)$ και $a \cdot c \equiv b \cdot d \ (mod \ m)$.

Απόδειξη

Έστω ότι $a \equiv b \ (mod \ m)$ και $c \equiv d \ (mod \ m)$. Τότε $m \mid (a - b)$ και $m \mid (c - d)$, σύμφωνα με το προηγούμενο θεώρημα.

Από της ιδότητες της σχέσης $\mid$ προκύπτει ότι $m \mid (a - b) + (c - d)$.

Όμως $(a - b) + (c - d) = (a + c) - (b + d)$. Άρα $m \mid (a + c) - (b + d)$ που συνεπάγεται $a + c \equiv b + d \ (mod \ m)$, σύμφωνα με το προηγούμενο θεώρημα.

Απόδειξη (συνέχεια)

Επίσης από το προηγούμενο πόρισμα προκύπτει ότι, αν $a \equiv b \ (mod \ m)$ και $c \equiv d \ (mod \ m)$, τότε υπάρχουν σταθερές ακέραιοι q_1 και q_2, τέτοιοι ώστε $a = b + q_1 \cdot m$ και $c = d + q_2 \cdot m$.

Άρα

$$\begin{aligned} a \cdot c &= (b + q_1 \cdot m) \cdot (d + q_2 \cdot m) \\ &= b \cdot d + b \cdot q_2 \cdot m + q_1 \cdot m \cdot d + q_1 \cdot q_2 \cdot m^2 \\ &= b \cdot d + (b \cdot q_2 + q_1 \cdot d + q_1 \cdot q_2 \cdot m) \cdot m \end{aligned}$$

Συνεπώς για $q = b \cdot q_2 + q_1 \cdot d + q_1 \cdot q_2 \cdot m$ ισχύει $a \cdot c = b \cdot d + q \cdot m$.
Από το προηγούμενο πόρισμα προκύπτει ότι $a \cdot c \equiv b \cdot d \ (mod \ m)$. □

Πόρισμα

Έστω a, b, m ακέραιοι αριθμοί με $m \geq 1$. Τότε,
$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$ και
$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

Απόδειξη

Ισχύει $a \equiv (a \bmod m) \ (mod\ m)$ και $b \equiv (b \bmod m) \ (mod\ m)$.

Από το προηγούμενο θεώρημα προκύπτει ότι
$(a + b) \equiv ((a \bmod m) + (b \bmod m)) \ (mod\ m)$ και
$(a \cdot b) \equiv ((a \bmod m) \cdot (b \bmod m)) \ (mod\ m)$.

Οι δύο ισότητες προκύπτουν από τον ορισμό του $\equiv \ (mod\ m)$. □

Αν $c \cdot a \equiv c \cdot b \ (mod\ m)$, τότε ενδέχεται να ισχύει $a \not\equiv b \ (mod\ m)$.

Για παράδειγμα, αν $c = 2$, $a = 7$, $b = 11$ και $m = 8$, ισχύει
$c \cdot a \bmod m = 2 \cdot 7 \bmod 8 = 14 \bmod 8 = 6$ και
$c \cdot b \bmod m = 2 \cdot 11 \bmod 8 = 22 \bmod 8 = 6$, που συνεπάγεται
$c \cdot a \equiv c \cdot b \ (mod\ m)$.

Ωστόσο, $a \bmod m = 7 \bmod 8 = 7$ και $b \bmod m = 11 \bmod 8 = 3$, που συνεπάγεται $a \not\equiv b \ (mod\ m)$.

Επίσης $b \equiv c \ (mod \ m)$, τότε ενδέχεται να ισχύει $a^b \not\equiv a^c \ (mod \ m)$.

Για παράδειγμα, αν $a = 2$, $b = 1$, $c = 5$ και $m = 4$, ισχύει $b \equiv c \ (mod \ m)$.

Ωστόσο, $a^b \bmod m = 2^1 \bmod 4 = 2 \bmod 4 = 2$ και $a^c \bmod 4 = 2^5 \bmod 4 = 32 \bmod 4 = 0$, που συνεπάγεται $a^b \not\equiv a^c \ (mod \ m)$.

Μέγιστος Κοινός Διαιρέτης

Ορισμός

Έστω δύο ακέραιοι αριθμοί a και b τέτοιοι ώστε $a \neq 0$ ή $b \neq 0$.
Ονομάζουμε μέγιστο κοινό διαιρέτη των a και b τον αριθμό
$\gcd(a, b) = \max\{d \in \mathbb{Z} : d \mid a \text{ και } d \mid b\}$.

Ο μέγιστος κοινός διαιρέτης είναι καλά ορισμένος, καθώς το σύνολο των κοινών διαιρετών δύο αριθμών είναι μη κενό και πεπερασμένο. Πράγματι για κάθε ακέραιο αριθμό n, ισχύει $1 \mid n$ και για καθε για κάθε ακέραιο αριθμό $n \neq 0$, ισχύει ότι αν $d \mid n$, τότε $-|n| \leq d \leq |n|$.

Παρατηρούμε επίσης ότι

- $\gcd(a, b) \geq 1$ (επειδή $1 \mid a$ και $1 \mid b$)
- $\gcd(a, b) = gcd(b, a)$
- $\gcd(a, 0) = gcd(0, a) = a$ (για $a > 0$)
- $\gcd(a, a) = a$ (για $a > 0$)
- $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(|a|, |b|)$

Ορισμός

Δύο ακέραιοι αριθμοί a και b τέτοιοι ώστε $a \neq b$ ονομάζονται σχετικά πρώτοι αν $\gcd(a, b) = 1$.

Στη συνέχεια θα περιγράψουμε τον αλγόριθμο του Ευκλείδη για υπολογισμό του μέγιστου κοινού διαιρέτη δύο αριθμών.

Επειδή $\gcd(a,b) = \gcd(|a|,|b|)$ και $\gcd(a,0) = gcd(0,a) = a$ για $a > 0$, θα περιορισούμε στην περίπτωση όπου $a, b > 0$.

Ο αλγόριθμος του Ευκλείδη βασίζεται στα παρακάτω λήμματα:

Λήμμα

Για οποιουσδήποτε ακεραίους αριθμούς a, b, d με $b \geq a$, ισχύει ότι $d \mid a$ και $d \mid b$ αν και μόνο αν $d \mid a$ και $d \mid b - a$.

Απόδειξη

Αν $d \mid a$ και $d \mid b$, τότε $d \neq 0$ και υπάρχουν ακέραιοι q_1, q_2 τέτοιοι ώστε $q_1 \cdot d = a$ και $q_2 \cdot d = b$.

Συνδυάζοντας τις δύο παραπάνω ισότητες, προκύπτει ότι $q_2 \cdot d - q_1 \cdot d = b - a$ που ισοδυναμεί με $(q_2 - q_1) \cdot d = b - a$.

Άρα για $q = q_2 - q_1$ ισχύει $q \cdot d = b - c$, που συνεπάγεται $d \mid b - a$. Επίσης από την υπόθεση ισχύει $d \mid a$.

Απόδειξη (συνέχεια)

Αντίστροφα, αν $d \mid a$ και $d \mid b - a$, τότε $d \neq 0$ και υπάρχουν ακέραιοι q_1, q_2 τέτοιοι ώστε $q_1 \cdot d = a$ και $q_2 \cdot d = b - a$.

Συνδυάζοντας τις δύο παραπάνω ισότητες, προκύπτει ότι $q_1 \cdot d + q_2 \cdot d = a + (b - a) = b$ που ισοδυναμεί με $(q_1 + q_2) \cdot d = b$.

Άρα για $q = q_1 + q_2$ ισχύει $q \cdot d = b$, που συνεπάγεται $d \mid b$. Επίσης από την υπόθεση ισχύει $d \mid a$. □

Λήμμα

Για οποιουσδήποτε ακεραίους αριθμούς a, b με $b \geq a$, ισχύει ότι $\gcd(a, b) = gcd(a, b - a)$.

Απόδειξη

Από το προηγούμενο λήμμα προκύπτει ότι τα σύνολα

$$\{d \in \mathbb{Z} : d \mid a \text{ και } d \mid b\}$$

και

$$\{d \in \mathbb{Z} : d \mid a \text{ και } d \mid b - a\}$$

είναι ίσα.

Άρα και τα μέγιστα στοιχεία των δύο συνόλων είναι ίσα, που συνεπάγεται ότι $\gcd(a, b) = gcd(a, b - a)$. □

Ο αλγόριθμος του Ευκλείδη για να υπολογίσει το μέγιστο κοινό διαίρέτη δύο θετικών αριθμών a και b, ενώσο οι αριθμοί είναι διαφορετικοί μεταξύ τους, αντικαθιστά τον μεγαλύτερο με τη διαφορά τους.

Αν προκύψουν δύο αριθμοί που είναι ίσοι, τότε η τιμή τους είναι ο μέγιστος κοινός διαρέτης των αρχικών αριθμών.

Στη συνέχεια θα περιγράψουμε τον αλγόριθμο του Ευκλείδη σε μορφή ψευδοκώδικα και θα αποδείξουμε την ορθότητά του.

Αλγόριθμος του Ευκλείδη για εύρεση του Μέγιστου Κοινού Διαιρέτη

Είσοδος: θετικοί ακέραιοι αριθμοί A,B

while A $\neq$ B do
    if A $<$ B
        then B $\leftarrow$ B-A
        else A $\leftarrow$ A-B
return A

Θεώρημα

Αν οι αρχικές τιμές των παραμέτρων A και B είναι $a > 0$ και $b > 0$, τότε ο αλγόριθμος του Ευκλείδη τερματίζει, επιστρέφοντας το μέγιστο κοινό διαιρέτη των a και b.

Απόδειξη

Έστω a_i, b_i οι τιμές των μεταβλητών A και B μετά από i επαναλήψεις του βρόχου while.

Θα αποδείξουμε με επαγωγή στο i ότι αν ο βρόχος εκτελέσει τουλάχιστον i επαναλήψεις τότε

- $a_i > 0$ και $b_i > 0$
- $a_i + b_i \leq a + b - i$
- $\gcd(a_i, b_i) = \gcd(a, b)$

Απόδειξη (συνέχεια)

Για $i = 0$, δεν έχει εκτελεστεί καμία επανάληψη του βρόχου while και οι παράμετροι A και B έχουν τις αρχικές τους τιμές. Συνεπώς:

- $a_0 = a > 0$ και $b_0 = b > 0$
- $a_0 + b_0 = a + b \leq a + b - 0$
- $\gcd(a_0, b_0) = \gcd(a, b)$

Συνεπώς ο ισχυρισμός μας ισχύει για $i = 0$.

Απόδειξη (συνέχεια)

Έστω ότι ο ισχυρισμός μας ισχύει για $i = k$ επαναλήψεις. Θα δείξουμε ότι ισχύει και για $i = k + 1$ επαναλήψεις.

Επειδή η εκτέλεση του βρόχου δεν ολοκληρώθηκε μετά από τις k επαναλήψεις, έχουμε $a_k \neq b_k$.

Αν $b_k > a_k$ τότε

- $b_{k+1} = b_k - a_k > 0$. Επίσης $a_{k+1} = a_k > 0$ από επαγωγική υπόθεση.
- $a_{k+1} + b_{k+1} = a_k + (b_k - a_k) = (a_k + b_k) - a_k \leq a + b - k - a_k \leq a + b - k - 1 = a + b - (k + 1)$, όπου η πρώτη ανισότητα ισχύει από την επαγωγική υπόθεση.
- $\gcd(a_{k+1}, b_{k+1}) = \gcd(a_k, b_k - a_k) = \gcd(a_k, b_k) = \gcd(a, b)$, όπου η δεύτερη ισότητα ισχύει από το προηγούμενο λήμμα και η τρίτη από την επαγωγική υπόθεση.

Απόδειξη (συνέχεια)

Συνεπώς αν ο $b_k > a_k$ ο ισχυρισμός μας αληθεύει και για $i = k + 1$.

Με τον ίδιο τρόπο αποδεικνύεται ότι ο ισχυριμός μας αληθεύει για $i = k + 1$, στην περίπτωση όπου $a_k > b_k$.

Απόδειξη (συνέχεια)

Συνεπώς ο ισχυρισμός μας ισχύει για οποιοδήποτε πλήθος επαναλήψεων i.

Συμπεράινουμε ότι ο αλγόριθμος τερματίζει μετά από την ℓ-οστή επανάληψη του βρόχου while, για κάποιο $\ell < a + b$.

Πράγματι έστω $c = a + b$. Αν ο αλγόριθμος δεν τερμάτιζε σε λιγότερες από c επαναλήψεις του βρόχου while τότε μετά την c-οστή επανάληψη θα ίσχυε $a_c > 0$, $b_c > 0$ και $a_c + b_c \leq a + b - c = a + b - (a + b) = 0$, το οποίο είναι άτοπο.

Απόδειξη (συνέχεια)

Επειδή ο βρόχος τερματίζει μετά από την ℓ-οστή επανάληψη του, ισχύει $a_\ell = b_\ell$ και άρα η επιστρεφόμενη τιμή είναι
$a_\ell = \gcd(a_\ell, a_\ell) = \gcd(a_\ell, b_\ell) = \gcd(a, b)$. □

Έστω ότι $b > a$, $q = b \text{ div } a$ και $r = b \bmod a$. Τότε ισχύει $b = qa + r$ και $q \geq 1$.

Αν $r > 0$, τότε οι τιμές των μεταβλητών A και B μετά από κάθε μία από τις πρώτες q επαναλήψεις του βρόχου *for* είναι:

$$a_1 = a_2 = \cdots = a_q$$

και

$$b_1 = (q-1)a + r, b_2 = (q-2)a + r, \ldots, b_q = r$$

Συνεπώς θα μπορούσαμε να παρακάμψουμε τις $q-1$ πρώτες επαναλήψεις του βρόχου while, αν αντικαθιστούσαμε την εντολή B $\leftarrow$ B-A με την εντολή B $\leftarrow$ B mod A και την εντολή A $\leftarrow$ A-B με την εντολή A $\leftarrow$ A mod B.

Η παρατήρηση αυτή οδηγεί σε μία γρηγορότερη εκδοχή του αλγόριθμου του Ευκλείδη, η οποία βασίζεται στα επόμενα λήμματα.

Λήμμα

Για οποιουσδήποτε ακεραίους αριθμούς a, b, d με $a > 0$, ισχύει ότι $d \mid a$ και $d \mid b$ αν και μόνο αν $d \mid a$ και $d \mid b \bmod a$.

Απόδειξη

Έστω $q = b \operatorname{div} a$ και $r = b \bmod a$. Τότε $b = q \cdot a + r$.

Απόδειξη (συνέχεια)

Αν $d \mid a$ και $d \mid b$, τότε $d \neq 0$ και υπάρχουν ακέραιοι q_1, q_2 τέτοιοι ώστε $q_1 \cdot d = a$ και $q_2 \cdot d = b = q \cdot a + r$.

Λαμβάνοντας υπόψη τις παραπάνω ισότητες, προκύπτει ότι
$r = (q \cdot a + r) - q \cdot a = b - q \cdot a = q_2 \cdot d - q \cdot q_1 \cdot d = (q_2 - q \cdot q_1) \cdot d$.

Άρα για $q' = q_2 - q \cdot q_1$ ισχύει $q' \cdot d = r = b \bmod a$, που συνεπάγεται $d \mid b \bmod a$. Επίσης από την υπόθεση ισχύει $d \mid a$.

Απόδειξη (συνέχεια)

Αντίστροφα, αν $d \mid a$ και $d \mid b \bmod a$, τότε υπάρχουν ακέραιοι q_1, q_2 τέτοιοι ώστε $q_1 \cdot d = a$ και $q_2 \cdot d = b \bmod a = r$.

Λαμβάνοντας υπόψη τις δύο παραπάνω ισότητες, προκύπτει ότι $b = q \cdot a + r = q \cdot q_1 \cdot d + q_2 \cdot d = (q \cdot q_1 + q_2) \cdot d$.

Άρα για $q' = q \cdot q_1 + q_2$ ισχύει $q' \cdot d = b$, που συνεπάγεται $d \mid b$. Επίσης από την υπόθεση ισχύει $d \mid a$. □

Λήμμα

Για οποιουσδήποτε ακεραίους αριθμούς a, b με $a > 0$, ισχύει ότι $\gcd(a, b) = gcd(a, b \bmod a)$

Απόδειξη

Από το προηγούμενο λήμμα προκύπτει ότι τα σύνολα

$$\{d \in \mathbb{Z} : d \mid a \text{ και } d \mid b\}$$

και

$$\{d \in \mathbb{Z} : d \mid a \text{ και } d \mid b \bmod a\}$$

είναι ίσα.

Άρα και τα μέγιστα στοιχεία των δύο συνόλων είναι ίσα, που συνεπάγεται ότι $\gcd(a, b) = gcd(a, b \bmod a)$. □

Ο βελτιωμένος αλγόριθμος του Ευκλείδη, για να υπολογίσει το μέγιστο κοινό διαίρέτη δύο θετικών αριθμών a και b, ενώσο κανένας από τους δύο δεν είναι 0, αντικαθιστά τον μεγαλύτερο από τους δύο με το υπόλοιπο της διαίρεσής του με τον μικρότερο από τους δύο.

Αν προκύψουν δύο αριθμοί που ο ένας είναι 0, τότε ο άλλος είναι ο μέγιστος κοινός διαιρέτης των αρχικών αριθμών.

Παρακάτω φαίνεται ο βελτιωμένος αλγόριθμος σε μορφή ψευδοκώδικα.

Αλγόριθμος του Ευκλείδη για εύρεση του Μέγιστου Κοινού Διαιρέτη (βελτιωμένη έκδοση)

Είσοδος: θετικοί ακέραιοι αριθμοί A,B

while $A \neq 0$ and $B \neq 0$ do
    if $A < B$
        then $B \leftarrow B \bmod A$
        else $A \leftarrow A \bmod B$
return max(A,B)

Θεώρημα

Αν οι αρχικές τιμές των παραμέτρων A και B είναι $a > 0$ και $b > 0$, τότε ο βελτιωμένος αλγόριθμος του Ευκλείδη τερματίζει, επιστρέφοντας το μέγιστο κοινό διαιρέτη των a και b.

Απόδειξη

Έστω a_i, b_i οι τιμές των μεταβλητών A και B μετά από i επαναλήψεις του βρόχου while.

Μπορούμε αποδείξουμε με επαγωγή στο i ότι αν ο βρόχος εκτελέσει τουλάχιστον i επαναλήψεις τότε

- $a_i \geq 0$ και $b_i \geq 0$
- $1 \leq a_i + b_i \leq a + b - i$
- $\gcd(a_i, b_i) = \gcd(a, b)$

Απόδειξη (συνέχεια)

Ο αλγόριθμος τερματίζει μετά από την ℓ-οστή επανάληψη του βρόχου while, για κάποιο $\ell < a + b$.

Πράγματι έστω $c = a + b$. Αν ο αλγόριθμος δεν τερμάτιζε σε λιγότερες από c επαναλήψεις του βρόχου while τότε μετά την c-οστή επανάληψη θα ίσχυει $1 \leq a_c + b_c \leq a + b - c = a + b - (a + b) = 0$, το οποίο είναι άτοπο.

Απόδειξη (συνέχεια)

Επειδή ο βρόχος τερματίζει μετά από την ℓ-οστή επανάληψη του, ισχύει $a_\ell = 0$ ή $b_\ell = 0$ και άρα η επιστρεφόμενη τιμή είναι ο μέγιστος κοινος διαρέτης των a και b. □

Θεώρημα (Bézout)

Έστω δύο θετικοί ακέραιοι αριθμοί a και b. Τότε υπάρχουν ακέραιοι s και t τέτοιοι ώστε $\gcd(a, b) = s \cdot a + t \cdot b$.

Απόδειξη

Θα αποδείξουμε το θεώρημα με ισχυρή επαγωγή στο άθροισμα $n = a + b$.

Η μικρότερη τιμή που μπορεί να πάρει το $a + b$ όταν a και b είναι θετικοί ακέραιοι είναι 2.

Για $a + b = 2$, ισχύει $a = b = 1$ και
$\gcd(a, b) = \gcd(1, 1) = 1 = 1 \cdot 1 + 0 \cdot 1 = 1 \cdot a + 0 \cdot b$.

Συνεπώς η ισότητα $\gcd(a, b) = s \cdot a + t \cdot b$ ισχύει για $s = 1$ και $t = 0$.

Απόδειξη (συνέχεια)

Ας υποθέσουμε ότι ο ισχυρισμός αληθεύει όταν $a + b \leq k$.

Έστω δύο αριθμοί a, b με $a + b = k + 1$. Μπορούμε χωρίς βλάβη της γενικότητας, να θεωρήσουμε ότι $a < b$ (καθώς $\gcd(a, b) = \gcd(b, a)$). Διακρίνουμε δύο περιπτώσεις.

Απόδειξη (συνέχεια)

Περίπτωση 1η: $a \mid b$. Τότε $\gcd(a, b) = a$. Άρα $\gcd(a, b) = 1 \cdot a + 0 \cdot b$, συνεπώς η ισότητα $\gcd(a, b) = s \cdot a + t \cdot b$ ισχύει για $s = 1$ και $t = 0$.

Απόδειξη (συνέχεια)

Περίπτωση 2η: $a \nmid b$. Τότε $0 < b \bmod a < b$. Συνεπώς $a + (b \bmod a) < a + b$ που συνεπάγεται $a + (b \bmod a) \leq k$.

Από την επαγωγική υπόθεση, προκύπτει ότι υπάρχουν ακέραιοι s', t' τέτοιοι ώστε $\gcd(a, b \bmod a) = s' \cdot a + t' \cdot (b \bmod a)$.

Επιπλέον έχουμε δείξει ότι $\gcd(a, b) = \gcd(a, b \bmod a)$.

Απόδειξη (συνέχεια)

Συνδυάζοντας τις παραπάνω ισότητες και λαμβάνοντας υπόψη τον ορισμό του mod έχουμε:

$$\begin{aligned} \gcd(a,b) &= s' \cdot a + t' \cdot (b \bmod a) \\ &= s' \cdot a + t' \cdot (b - (b \operatorname{div} a) \cdot a) \\ &= (s' - (b \operatorname{div} a) \cdot t') \cdot a + t' \cdot b \end{aligned}$$

Συνεπώς η ισότητα $\gcd(a,b) = s \cdot a + t \cdot b$ ισχύει για $s = s' - (b \operatorname{div} a) \cdot t'$ και $t = t'$.

Η ισότητα $\gcd(a, b) = s \cdot a + t \cdot b$ ονομάζεται ταυτότητα Bézout και οι ακέραιοι s και t συντελεστές Bézout.

Οι συντελεστές Bézout μπορούν να υπολογιστούν από τις ακολουθίες τιμών $a_0, a_1, \ldots, a_\ell$ και $b_0, b_1, \ldots, b_\ell$ των μεταβλητών A και B στον αλγόριθμο του Ευκλείδη, όταν εκτελείται με είσοδο a, b.

Θα περιγράψουμε τη διαδικασία υπολογισμού των συντελεστών Bézout με βάση την βελτιωμένη έκδοση του αλγόριθμου.

Για κάθε i, $0 \leq i \leq \ell$ θα βρούμε συντελεστές s_i και t_i, τέτοιους ώστε $\gcd(a, b) = s_i \cdot a_i + t_i \cdot b_i$.

Ο υπολογισμός θα γίνει ξεκινώντας από $i = \ell$ και προχωρώντας αντίστροφα.

Για $i = \ell$, γνωρίζουμε ότο $\gcd(a, b) = \max(a_\ell, b_\ell)$.

Αν $\gcd(a, b) = a_\ell$ τότε $\gcd(a, b) = 1 \cdot a_\ell + 0 \cdot b_\ell$, άρα ισχύει $\gcd(a, b) = s_\ell \cdot a_\ell + t_\ell \cdot b_\ell$ για $s_\ell = 1$ και $t_\ell = 0$.

Αντίστοιχα, αν $\gcd(a, b) = b_\ell$ τότε $\gcd(a, b) = 0 \cdot a_\ell + 1 \cdot b_\ell$, άρα ισχύει $\gcd(a, b) = s_\ell \cdot a_\ell + t_\ell \cdot b_\ell$ για $s_\ell = 0$ και $t_\ell = 1$.

Οι συντελεστές s_i και t_i για $0 \leq i < \ell$ υπολογίζονται με βάση τους s_{i+1} και t_{i+1} με τον παρακάτω τρόπο:

Αν $a_{i+1} = a_i$, τότε ισχύει $b_{i+1} = b_i \bmod a_i$. Άρα

$$\begin{aligned} \gcd(a,b) &= s_{i+1} \cdot a_{i+1} + t_{i+1} \cdot b_{i+1} \\ &= s_{i+1} \cdot a_i + t_{i+1} \cdot (b_i \bmod a_i) \\ &= s_{i+1} \cdot a_i + t_{i+1} \cdot (b_i - (b_i \operatorname{div} a_i) \cdot a_i) \\ &= (s_{i+1} - (b_i \operatorname{div} a_i) \cdot t_{i+1}) \cdot a_i + t_{i+1} \cdot b_i \end{aligned}$$

Συνεπώς ισχύει $\gcd(a,b) = s_i \cdot a_i + t_i \cdot b_i$ για $s_i = s_{i+1} - (b_i \operatorname{div} a_i) \cdot t_{i+1}$ και $t_i = t_{i+1}$.

Αν $b_{i+1} = b_i$, τότε ισχύει $a_{i+1} = a_i \bmod b_i$. Άρα

$$\begin{aligned}
\gcd(a, b) &= s_{i+1} \cdot a_{i+1} + t_{i+1} \cdot b_{i+1} \\
&= s_{i+1} \cdot (a_i \bmod b_i) + t_{i+1} \cdot b_i \\
&= s_{i+1} \cdot (a_i - (a_i \operatorname{div} b_i) \cdot b_i) + t_{i+1} \cdot b_i \\
&= s_{i+1} \cdot a_i + (t_{i+1} - (a_i \operatorname{div} b_i) \cdot s_{i+1}) \cdot b_i
\end{aligned}$$

Συνεπώς ισχύει $\gcd(a, b) = s_i \cdot a_i + t_i \cdot b_i$ για $s_i = s_{i+1}$ και $t_i = t_{i+1} - (a_i \operatorname{div} b_i) \cdot s_{i+1}$.

Για $i = 0$ έχουμε $\gcd(a, b) = s_0 \cdot a_0 + t_0 \cdot b_0 = s_0 \cdot a + t_0 \cdot b$ (επειδή $a_0 = a$ και $b_0 = b$).

Οι συντελεστές Bézout για τους αριθμούς a και b είναι οι $s = s_0$ και $t = t_0$.