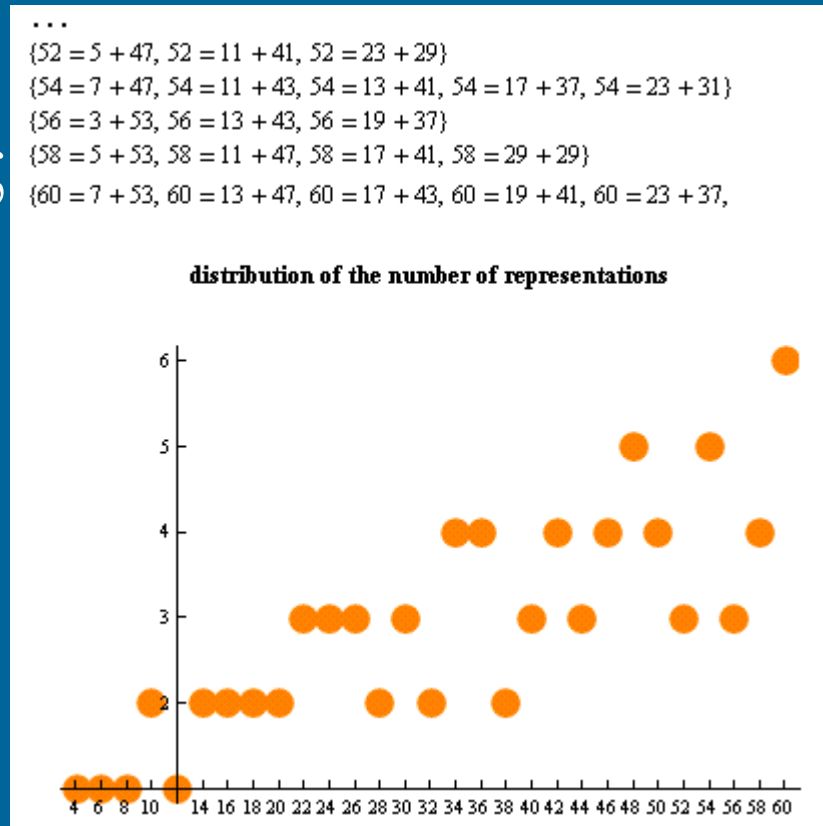


ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

Θεωρία Αριθμών

- Κλάδος μαθηματικών που ασχολείται με τους ακέραιους και τις ιδιότητές τους.
- Πολλά και εξαιρετικά δύσκολα προβλήματα – Εικασία του Goldbach



Κάποιες Εφαρμογές που θα Δούμε

- Συναρτήσεις Κατακερματισμού (Hashing Functions)
- Ψευδοτυχαίοι Αριθμοί
- Ψηφίο Ελέγχου

Η Διαίρεση

Ένας ακέραιος a διαιρεί τον b όταν υπάρχει c έτσι ώστε $b=ac$.

$a \rightarrow$ παράγοντας του b

$b \rightarrow$ πολλαπλάσιο του a

$$a \mid b \equiv \exists c(ac=b)$$

$$a \nmid b \equiv \forall c(ac \neq b)$$

Ιδιότητες

1. Αν $a \mid b$ και $a \mid c$ τότε $a \mid (b+c)$
2. Αν $a \mid b$ τότε $a \mid bc$ για όλους τους ακεραίους c
3. Αν $a \mid b$ και $b \mid c$ τότε $a \mid c$

Πόρισμα:

Αν $a \mid b$ και $a \mid c$ τότε $a \mid (mb+nc)$ όπου m και n ακέραιοι.

Βασικοί Ορισμοί

Μέγιστος Κοινός Διαιρέτης:

$$\text{ΜΚΔ}(x,y) = \text{μέγιστο } k \geq 1 : k \mid x \text{ και } k \mid y$$

Ελάχιστο Κοινό Πολλαπλάσιο:

$$\text{ΕΚΠ}(x,y) = \text{ελάχιστο } k \geq 1 : x \mid k \text{ και } y \mid k$$

Πρώτοι Αριθμοί

Ένας θετικός ακέραιος p λέγεται *πρώτος* αν οι μόνοι θετικοί του παράγοντες είναι το 1 και το p . Αν ένας θετικός ακέραιος δεν είναι πρώτος λέγεται *σύνθετος*.

Θεμελιώδες θεώρημα αριθμητικής:

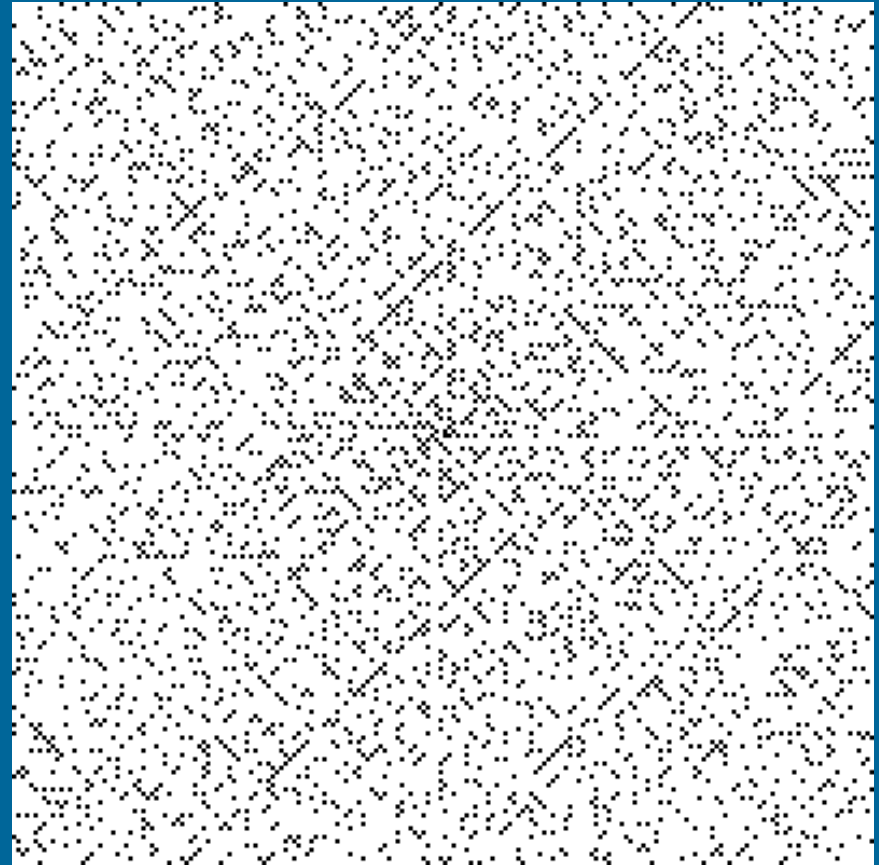
Κάθε θετικός ακέραιος μπορεί να γραφεί με μοναδικό τρόπο σαν πρώτος αριθμός ή σαν γινόμενο πρώτων αριθμών όπου οι πρώτοι παράγοντες γράφονται σε σειρά μη ελαττούμενου μεγέθους.

Θεωρήματα

1. Αν ο n είναι σύνθετος ακέραιος, τότε ο n έχει διαιρέτη πρώτο αριθμό μικρότερο από ή ίσο με $n^{1/2}$. (Απόδειξη)
 1. Να δειχτεί ότι ο 101 είναι πρώτος.
2. Υπάρχουν άπειροι πρώτοι αριθμοί. (Απόδειξη)

Πρώτοι Αριθμοί – ???

- Ο λόγος του πλήθους των πρώτων αριθμών, που δεν είναι μεγαλύτεροι από x και του $x/\ln x$ πλησιάζει το 1, καθώς το x αυξάνει χωρίς φράγμα. (Χωρίς απόδειξη :-)



Βαθμιδωτή Αριθμητική

$(a \bmod n)$ είναι το υπόλοιπο της διαίρεσης του a από το n .

$$a \bmod n = r$$



$a = dn + r$ για κάποιον ακέραιο d Απόδειξη

Αν a, b και n είναι ακέραιοι αριθμοί τότε ο a είναι ισοδύναμος του $b \bmod n$ αν ο n διαιρεί το $a-b$.

$$a \equiv b \pmod{n}$$

$$31 \equiv 81 \pmod{2}$$

$$31 \equiv_2 81$$

Επίσης:

$$a \equiv b \pmod{n} \leftrightarrow a \bmod n = b \bmod n$$

$$31 \equiv 80 \pmod{7}$$

$$31 \equiv_7 80$$

Συναρτήσεις Κατακερματισμού

Ορισμός: Μία **συνάρτηση κατακερματισμού** h αναθέτει μία θέση μνήμης $h(k)$ στην εγγραφή που έχει το k ως κλειδί.

- Μία κοινή συνάρτηση είναι η $h(k) = k \bmod m$, όπου m είναι το πλήθος των θέσεων μνήμης.

Παράδειγμα: Έστω $h(k) = k \bmod 111$. Αυτή η συνάρτηση αναθέτει τις εγγραφές των πελατών με ΑΦΜ ως κλειδιά, σε θέσεις μνήμης με τον εξής τρόπο:

$$h(064212848) = 064212848 \bmod 111 = 14$$

$$h(037149212) = 037149212 \bmod 111 = 65$$

$h(107405723) = 107405723 \bmod 111 = 14$, αλλά αφού η θέση 14 είναι ήδη πιασμένη, η εγγραφή θα ανατεθεί στην επόμενη διαθέσιμη θέση μνήμης, δηλαδή την 15.

Συναρτήσεις Κατακερματισμού

- Οι συναρτήσεις κατακερματισμού δεν είναι 1-προς-1, αφού ο τομέας αναφοράς των κλειδιών είναι μεγαλύτερος από το πλήθος των θέσεων μνήμης. Όταν περισσότερα από ένα κλειδιά ανατίθενται στην ίδια θέση μνήμης τότε έχουμε **σύγκρουση**. Στο προηγούμενο παράδειγμα λύσαμε τη σύγκρουση αναθέτοντας το κλειδί στην πρώτη διαθέσιμη θέση.
- Για την επίλυση μίας σύγκρουσης, μπορούμε να χρησιμοποιήσουμε μία **συνάρτηση γραμμικής ανίχνευσης**: $h(k,i) = (h(k) + i) \bmod m$, όπου το i παίρνει τιμές από το 0 μέχρι το $m - 1$.
- Υπάρχουν και άλλες μέθοδοι για επίλυση συγκρούσεων αλλά περισσότερα στο μάθημα «Δομές Δεδομένων»

Μέγιστος Κοινός Διαιρέτης

a, b είναι
σχετικά πρώτοι
αν $\gcd(a,b)=1$

Αν οι a και b είναι θετικοί ακέραιοι, τότε υπάρχουν ακέραιοι s και t έτσι ώστε ο μέγιστος κοινός διαιρέτης των a και b $\gcd(a,b)=sa+tb$.

Αποτελέσματα:

1. Αν $\gcd(a,b)=1$ και $a \mid bc$, τότε $a \mid c$
2. Αν ο p είναι πρώτος και $p \mid a_1 \times a_2 \times \dots \times a_n$, όπου κάθε a_i είναι ακέραιος, τότε $p \mid a_i$ για κάποιο i . (με επαγωγή)
3. Αν $ac \equiv bc \pmod{m}$ και $\gcd(c,m)=1$ τότε $a \equiv b \pmod{m}$

Ο Αλγόριθμος του Ευκλείδη

- Δοθέντων θετικών ακεραίων a και b , να βρούμε τον μέγιστο κοινό διαιρέτη
- Ιδέα:
 - Αν ο x είναι ο μέγιστος κοινός διαιρέτης των a και b , τότε το x διαιρεί το $r = a - kb$, για οποιοδήποτε k .
 - Μειώνει το πρόβλημα στην εύρεση του μεγαλύτερου x που διαιρεί τα r και b
 - Επανάληψη

Παράδειγμα (1)

- $a = 15, b = 12$

a	b	q	r	
15	12	1	3	$q = 15/12 = 1$ $r = 15 - 1 \times 12$
12	3	4	0	$q = 12/3 = 4$ $r = 12 - 4 \times 3$

- Άρα $\mu\kappa\delta(15, 12) = 3$
 - Το b για το οποίο το r είναι 0

Πίσω στο mod...

Κλάσεις Ισοδυναμίας mod 3

$$[0] = \{ \dots, -6, -3, 0, 3, 6, \dots \}$$

$$[1] = \{ \dots, -5, -2, 1, 4, 7, \dots \}$$

$$[2] = \{ \dots, -4, -1, 2, 5, 8, \dots \}$$

$$[-6] = \{ \dots, -6, -3, 0, 3, 6, \dots \} = [0]$$

$$[7] = \{ \dots, -5, -2, 1, 4, 7, \dots \} = [1]$$

$$[-1] = \{ \dots, -4, -1, 2, 5, 8, \dots \} = [2]$$

Αναπαράσταση Συστήματος mod 3

Πεπερασμένο σύνολο $S = \{0, 1, 2\}$

+ και * ορίζονται στο S :

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Σημειογραφεία

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

Πράξεις $+_n$ και $*_n$:

$$a +_n b = (a + b \bmod n)$$

$$a *_n b = (a * b \bmod n)$$

Ιδιότητες Πράξεων

[“Κλειστότητα”]

$$x, y \in Z_n \Rightarrow x +_n y \in Z_n$$

[“Προσεταιριστική”]

$$x, y, z \in Z_n \Rightarrow (x +_n y) +_n z = x +_n (y +_n z)$$

[“Αντιμεταθετική”]

$$x, y \in Z_n \Rightarrow x +_n y = y +_n x$$

Παρόμοιες Ιδιότητες και για $*_n$

Γιατί μας ενδιαφέρει;

Επειδή μπορούμε να αντικαταστήσουμε οποιοδήποτε μέλος της κλάσης με άλλο μέλος της όταν κάνουμε πρόσθεση ή πολλαπλασιασμό $\text{mod } n$ και το αποτέλεσμα δεν θα αλλάξει

Για να υπολογίσουμε: $249 * 504 \text{ mod } 251$

αρκεί $-2 * 2 = -4 = 247$

Μας ενδιαφέρει επίσης επειδή οι Υπολογιστές κάνουν αριθμητική $\text{mod } n$, όπου n είναι 2^{32} ή 2^{64} .

Ιδιότητες

$$a \equiv b \pmod{m} \leftrightarrow \exists k(a=b+km)$$

Έστω ότι ο m είναι θετικός ακέραιος. Αν

$$a \equiv b \pmod{m}$$

και

$$c \equiv d \pmod{m},$$

τότε

$$a+c \equiv b+d \pmod{m} \text{ και } ac \equiv bd \pmod{m}$$

Ιδιότητες (2)

Αν $(x \equiv_n y)$ και $(k \mid n)$, τότε : $x \equiv_k y$

Παράδειγμα: $10 \equiv_6 16 \Rightarrow 10 \equiv_3 16$

Απόδειξη:

$x \equiv_n y$ αν και μόνο αν $x = in + y$ για κάποιο ακέραιο i

Έστω $n = jk$ Τότε:

$$x = ijk + y$$

$$x = (ij)k + y \quad \text{και άρα } x \equiv_k y$$

Ψευδοτυχαίοι Αριθμοί

- Οι *ψευδοτυχαίοι αριθμοί* δεν είναι πραγματικά τυχαίοι αφού παράγονται με συστηματικές μεθόδους.
- Η γραμμική αναλογική μέθοδος χρησιμοποιείται συχνά για την παραγωγή τέτοιων αριθμών.
- Απαιτούνται 4 ακέραιοι: ο συντελεστής m , ο πολλαπλασιαστής a , η αύξηση c , και ο σπόρος x_0 , όπου $2 \leq a < m, 0 \leq c < m, 0 \leq x_0 < m$.
- Παράγουμε μία ακολουθία ψευδοτυχαίων αριθμών $\{x_n\}, 0 \leq x_n < m$ χρησιμοποιώντας αναδρομικά την εξής συνάρτηση:

$$x_{n+1} = (ax_n + c) \bmod m$$

Ψευδοτυχαίοι Αριθμοί

Παράδειγμα: Βρείτε την ακολουθία ψευδοτυχαίων αριθμών που παράγεται από τη γραμμική αναλογική μέθοδο όπου $m = 9$, $a = 7$, $c = 4$, και $x_0 = 3$.

Λύση: Υπολογίζουμε διαδοχικά την $x_{n+1} = (7x_n + 4) \bmod 9$, $x_0 = 3$.

$$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,$$

$$x_2 = 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,$$

$$x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,$$

$$x_4 = 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$$

$$x_5 = 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$$

$$x_6 = 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$$

$$x_7 = 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$$

$$x_8 = 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$$

$$x_9 = 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$$

Η παραγόμενη ακολουθία είναι η 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,...

Η ακολουθία επαναλαμβάνεται μετά από 9 όρους.

Συνήθως, οι γλώσσες προγραμματισμού χρησιμοποιούν τη γραμμική αναλογική μέθοδο με $c = 0$. Μία τέτοια γεννήτρια ψευδοτυχαίων αριθμών που έχει $m=2^{31} - 1$ και $a = 7^5 = 16,807$, παράγει μία ακολουθία με $2^{31} - 2$ αριθμούς πριν επαναληφθεί.

Ψηφίο Ελέγχου: UPCs

Μία κοινή μέθοδος για ανίχνευση λαθών σε ακολουθίες ψηφίων είναι η πρόσθεση ενός επιπλέον ψηφίου στο τέλος, το οποίο υπολογίζεται από μία συνάρτηση. Αν το τελικό ψηφίο είναι λάθος, τότε η ακολουθία δεν είναι σωστή.

Παράδειγμα: Τα εμπορικά προϊόντα αναγνωρίζονται από τους *Universal Product Codes* (*UPCs*). Συνήθως αυτοί έχουν 12 δεκαδικά ψηφία με το τελευταίο να είναι ψηφίο ελέγχου που καθορίζεται ως εξής:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$$

- Έστω ότι τα πρώτα 11 ψηφία του UPC είναι 79357343104. Ποιο είναι το ψηφίο ελέγχου;
- Είναι ο 041331021641 ένα έγκυρο UPC?

Λύση:

- $3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10}$
 $21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$
 $98 + x_{12} \equiv 0 \pmod{10}$
 $x_{12} \equiv 2 \pmod{10}$ Άρα το ψηφίο ελέγχου είναι το 2.
- $3 \cdot 0 + 4 + 3 \cdot 1 + 3 + 3 \cdot 3 + 1 + 3 \cdot 0 + 2 + 3 \cdot 1 + 6 + 3 \cdot 4 + 1 \equiv 0 \pmod{10}$
 $0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv 0 \pmod{10}$
Άρα ο 041331021641 δεν είναι έγκυρο UPC.

Ψηφίο Ελέγχου: ISBNs

Τα βιβλία αναγνωρίζονται από έναν δεκαψήφιο αριθμό: *International Standard Book Number* (ISBN-10). Τα πρώτα 9 ψηφία καθορίζονται από τη γλώσσα, τον εκδότη και το βιβλίο. Το δέκατο ψηφίο είναι ψηφίο ελέγχου που καθορίζεται ως εξής:

$$x_{10} = \sum_{i=1}^9 ix_i \pmod{11}$$

Η εγκυρότητα ενός ISBN-10 αριθμού μπορεί να ελεγχθεί:

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$$

- a) Έστω ότι τα πρώτα 9 ψηφία ενός ISBN-10 είναι 007288008. Ποιο είναι το ψηφίο ελέγχου;
b) Είναι το 084930149X ένας έγκυρος κωδικός ISBN10; Το X ανήκει στο {0,1,...,10}.

Λύση:

- a. $X_{10} \equiv 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 \pmod{11}$.
 $X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$.
 $X_{10} \equiv 189 \equiv 2 \pmod{11}$. Άρα, $X_{10} = 2$.
- b. $1 \cdot 0 + 2 \cdot 8 + 3 \cdot 4 + 4 \cdot 9 + 5 \cdot 3 + 6 \cdot 0 + 7 \cdot 1 + 8 \cdot 4 + 9 \cdot 9 + 10 \cdot 10 =$
 $0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$
Άρα ο 084930149X δεν είναι έγκυρος ISBN-10 αριθμός.

Θέμα 6^ο: (0,5 Μονάδες) (2/2/2017)

Όταν ένας $n \in \mathbb{Z}$ διαιρεθεί με το 7 τότε το υπόλοιπο είναι 4. Ποιο είναι το υπόλοιπο αν ο $5n$ διαιρεθεί με το 7;

Θέμα 4^ο: (1,5 Μονάδες) (15/9/2017)

Να αποδείξετε με αντίφαση την εξής πρόταση: Για κάθε ακέραιο a και έναν πρώτο αριθμό p , αν $p \mid a$ τότε $p \nmid (a + 1)$.