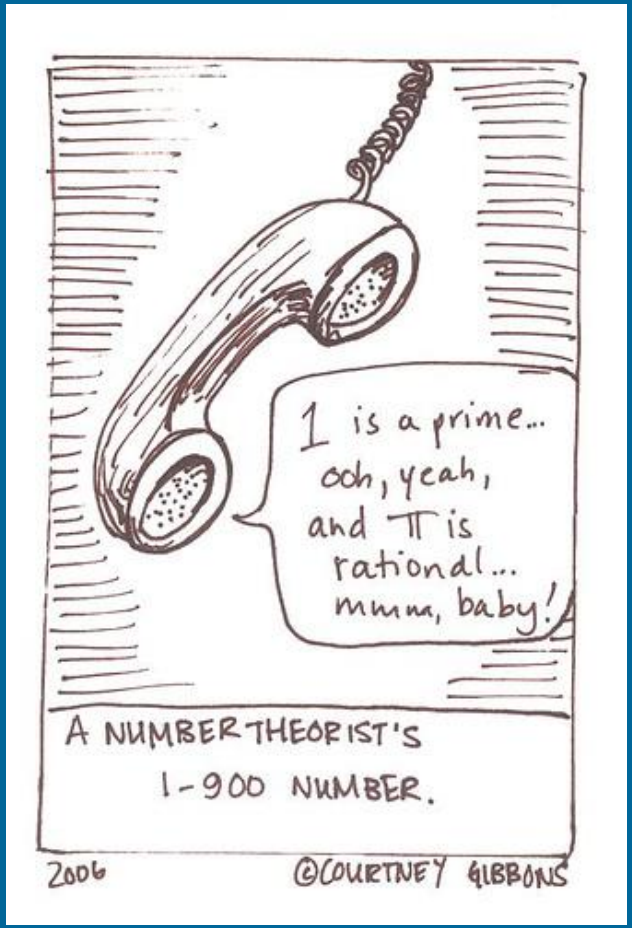
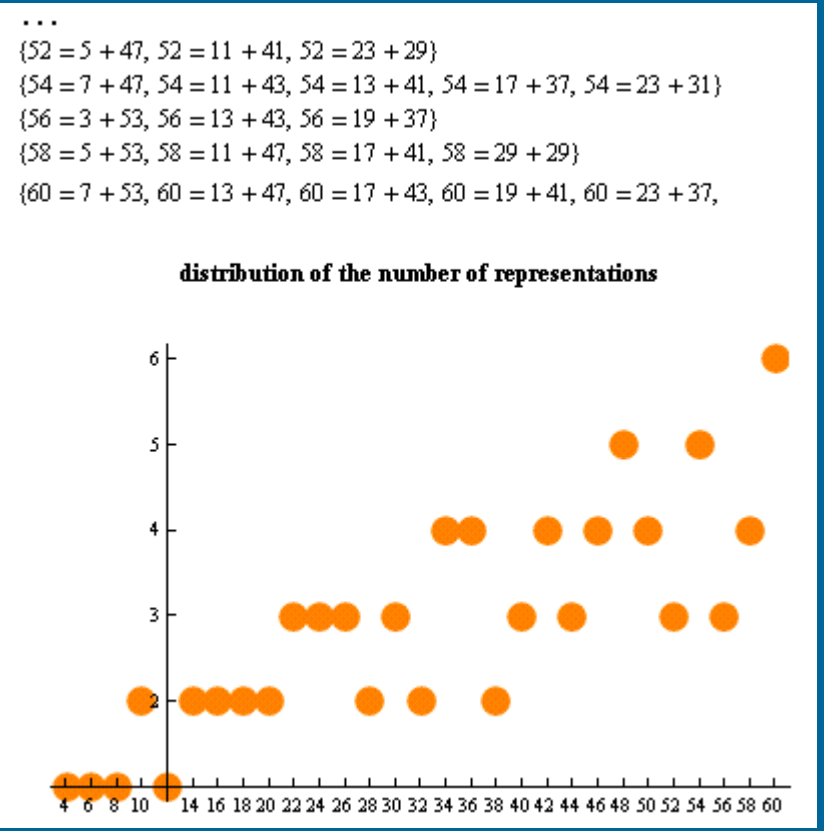


ΒΑΣΙΚΆ ΣΤΟΙΧΕΊΑ ΘΕΩΡΊΑΣ ΑΡΙΘΜΏΝ

Θεωρία Αριθμών

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



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:

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

Ελάχιστο Κοινό Πολλαπλάσιο:

ΕΚΠ(x,y) = ελάχιστο $k \geq 1 : x \mid k$ 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:

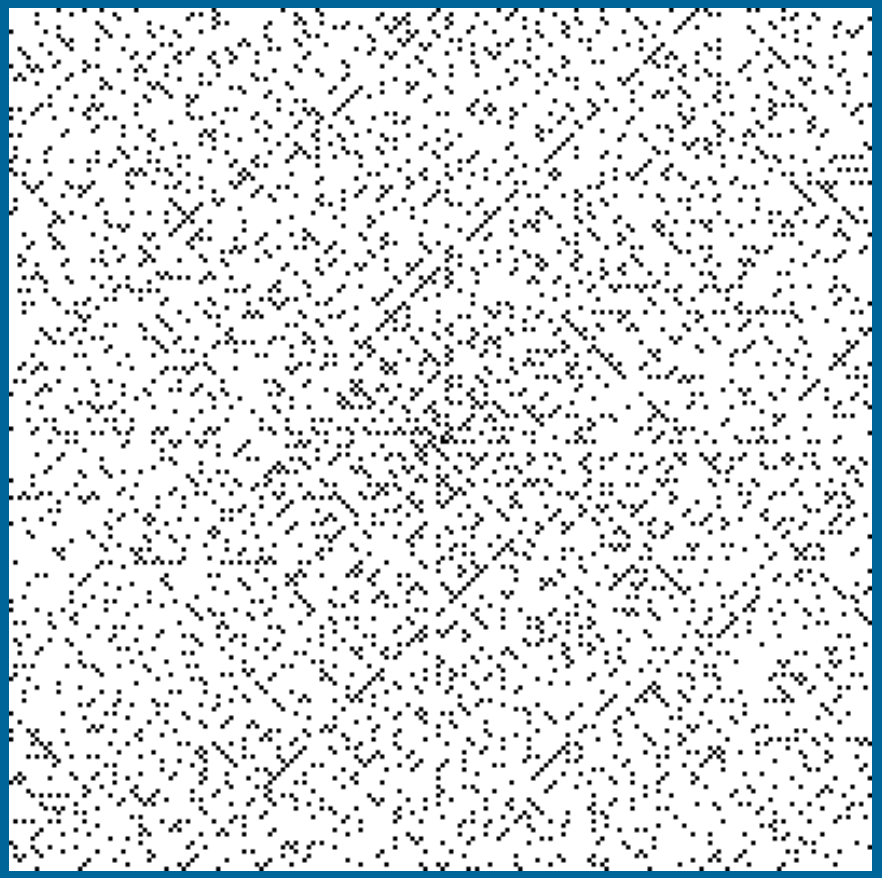
Κάθε θετικός ακέραιος μπορεί να γραφεί με μοναδικό τρόπο σαν πρώτος αριθμός ή σαν γινόμενο πρώτων αριθμών όπου οι πρώτοι παράγοντες γράφονται σε σειρά μη ελαττούμενου μεγέθους.

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.

$$a \bmod n = r$$

$$\Leftrightarrow$$

$$a = dn + r \text{ για κάποιον ακέραιο } d$$

Απόδειξη

Αν a,b και n είναι ακέραιοι αριθμοί τότε ο a είναι ισοδύναμος του b *modulo* n αν ο ***n διαιρεί το a-b***.

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

$31 \equiv 81 \pmod 2$

$31 \equiv_2 81$

Επίσης:

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

$31 \equiv 80 \pmod 7$

$31 \equiv_7 80$

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 $p \mid a_1 \times a_2 \times \ldots \times a_n$, 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 κάποιο 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

Παράδειγμα (2)

- $a = 35731$, $b = 25689$

a	b	q	r	
35731	24689	1	11042	$q = 35731/24689 = 1$
				$r = 35731 - 1 \times 24689$
24689	11042	2	2,605	$q = 24689/11042 = 2$
				$r = 24689 - 2 \times 11042$
11042	2605	4	622	$q = 11042/2605 = 4$
				$r = 11042 - 4 \times 2605$
2605	622	4	117	$q = 2605/622 = 4$; $r = 2605 - 4 \times 622$
622	117	5	37	$q = 622/117 = 5$; $r = 622 - 5 \times 117$
117	37	3	6	$q = 117/37 = 3$; $r = 117 - 3 \times 37$
37	6	6	1	$q = 37/6 = 6$; $r = 37 - 6 \times 6$
6	1	6	0	$q = 6/1 = 6$; $r = 6 - 6 \times 1$

Ψευδοκώδικας

```
///εύρεση μκδ των a και b
rprev = 1; r = 1;

while r != 0
    rprev = r;
    r = a % b;
    print 'a = ', a, 'b =', b, 'q = ', a div b, 'r = ', r, endline;
    a = b;
    b = r;

return rprev;
```

Πίσω στο mod…

Κλάσεις Ισοδυναμίας mod 3

[0] = { …, -6, -3, 0, 3, 6, ..}
[1] = { …, -5, -2, 1, 4, 7, ..}
[2] = { …, -4, -1, 2, 5, 8, ..}

[-6] = { …, -6, -3, 0, 3, 6, ..} = [0]
[7] = { …, -5, -2, 1, 4, 7, ..} = [1]
[-1] = { …, -4, -1, 2, 5, 8, ..} = [2]

Γιατί μας ενδιαφέρει;

Επειδή μπορούμε να αντικαταστήσουμε οποιοδήποτε μέλος της κλάσης με άλλο μέλος της όταν κάνουμε πρόσθεση ή πολλαπλασιασμό mod *n* και το αποτέλεσμα δεν θα αλλάξει

Για να υπολογίσουμε: 249 * 504 mod 251

αρκεί -2 * 2 = -4 = 247

Μας ενδιαφέρει επίσης επειδή οι Υπολογιστές κάνουν αριθμητική 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:

$$x = ijk + y$$

$x = (ij)k + y$ και άρα $x \equiv_k y$

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

$Z_n = \{[0], [1], [2], \ldots, [n\text{-}1]\}$

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 $*_n$

Αποδείξεις ιδιοτήτων για διακριτά αντικείμενα

ΜΑΘΗΜΑΤΙΚΗ ΕΠΑΓΩΓΗ

Χρήση

Η Μαθηματική Επαγωγή χρησιμοποιείται μόνο για την απόδειξη αποτελεσμάτων που έχουν ληφθεί με κάποιο άλλο τρόπο.

- Δεν αποτελεί εργαλείο ανακάλυψης τύπων ή θεωρημάτων

Αρχή της μαθηματικής επαγωγής

- Ιδιότητα $P(n)$ στους φυσικούς αριθμούς
- Θέλουμε να δείξουμε ότι $\forall n\, P(n)$, όπου το πεδίο ορισμού είναι το σύνολο των θετικών ακέραιων

Αν $$\left[P(1) \wedge \forall s(P(s) \rightarrow P(s+1))\right] \rightarrow \forall n P(n)$$

(α) $P(k)$ αληθής για κάποιο $k \in N$

(β) Για κάθε $n \geq k$, αν η $P(n)$ είναι αληθής τότε και η $P(n+1)$ είναι αληθής

τότε η $P(n)$ είναι αληθής για κάθε $n \geq k$

Παράδειγμα

$P(n)=\{n^3+2n$ διαιρείται από το 3, $n \epsilon N\}$

$P(1)=1+2=3$ – ***Αληθές***

Έστω ότι ισχύει το $P(n-1)$

$P(n-1)= (n-1)^3+2(n-1)=n^3-3n^2+3n-1+2n-2=$

$n^3-3n^2+5n-3=3\kappa$ *για* $\kappa \epsilon N$

$P(n)= (n^3-3n^2+5n-3)+(3n^2-3n+3)=3\kappa+3(n^2-n+1)$

Αποδείχτηκε.

Παράδειγμα

- Να αποδειχθεί ότι $n < 2^n$.
- Αν ο p είναι πρώτος και $p \mid a_1 \times a_2 \times \ldots \times a_n$, όπου κάθε a_i είναι ακέραιος, τότε $p \mid a_i$ για κάποιο i.
- Να δειχτεί ότι το παρακάτω είναι ταυτολογία:

$$[(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \ldots \wedge (p_{n-1} \to p_n)] \to [(p_1 \wedge p_2 \wedge \ldots \wedge p_{n-1}) \to p_n]$$

Ισχυρή Επαγωγή

Αν

(α) $P(k)$ αληθής για κάποιο $k \epsilon N$

(β) Για κάθε $n \geq k$, αν οι $P(k), P(k+1),\ldots, P(n)$ είναι αληθείς τότε και η $P(n+1)$ είναι αληθής

τότε η $P(n)$ είναι αληθής για κάθε $n \geq k$

$$\left[P(1) \wedge \forall k((P(1) \wedge P(2) \wedge \ldots \wedge P(k)) \rightarrow P(k+1))\right] \rightarrow \forall n P(n)$$

Άσκηση

1. Να δειχτεί ότι αν ο *n* είναι ακέραιος >1 τότε μπορεί να γραφεί σαν γινόμενο πρώτων παραγόντων.

Ποιο είναι το Σφάλμα;

Απόδειξη ότι όλα τα άλογα έχουν το ίδιο χρώμα:

Έστω P(n) η πρόταση «Ένα σύνολο n αλόγων έχουν το ίδιο χρώμα»

P(1) προφανώς ισχύει.

Έστω P(k). Θεωρήστε οποιοδήποτε αριθμημένο σύνολο k+1 αλόγων. Τα πρώτα k άλογα έχουν το ίδιο χρώμα όπως και τα τελευταία k άλογα έχουν το ίδιο χρώμα. Επειδή αυτά τα δύο σύνολα επικαλύπτονται σημαίνει ότι και τα δύο σύνολα έχουν το ίδιο χρώμα και άρα η P(k+1) είναι αληθής.