בס"ד



תורת המספרים

בס"ד

חלוקה עם שארית

$\mathbb{Z}$ הקבוצה של כל המספרים השלמים

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

3 פעולות חשבון: $+, -, \times$

~~$\div$~~

$41 = 12 \cdot 3 + 5$

שארית

$0 < 5 < 12$



12



12



12

5 שארית





41

$12 \cdot 3 = 36$

משפט יהי $a,b\in\mathbb{Z}$ קיימים $q,r\in\mathbb{Z}$ יחידים: $a=bq+r$ כאשר $0\le r<|b|$

הסבר: a,b נתונים $a\div b$

נניח $a=bq+r$

$a=bq_1+r_1$

$\Downarrow$ יחידות

$\begin{cases} q_1=q \\ r_1=r \end{cases}$

הסיכה: $0\le r<|b|$

$0\le r_1<|b|$

$a = 17$

$b = 6$

$17 \div 6$

$17 - 6 = 11$

$11 - 6 = 5 < 6$

$17 - 6 \cdot 2 = 5$

$q = 2$

$r = 5$

$17 = 6 \cdot 2 + 5$

דרך 1:

$6 \cdot k < 17$

k הוא מספר שלם גדול מ-1

$6 \cdot 2 = 12 < 17$

$6 \cdot 3 = 18 > 17$

$200 \div 6$

דרך 1:

$6 \cdot k < 200$

$6 \cdot (k+1) > 200$

$6 \cdot 35 = 3 \cdot 70 = 210 > 200$

$r = a - b \cdot q = 200 - 198 = 2 \quad <= \quad q = 33 \quad <= \quad 6 \cdot 33 = 198 < 200$

$200 = 6 \cdot 33 + 2$

$\frac{200}{6} = \frac{100}{3} = 33.333\ldots$:2 :3

$6 \cdot 33 < 200$

$q = 33$

$a = 517$

$b = 9$

$517 \div 9$

$\frac{517}{9} = 57.44\ldots$

$q = 57$

$r = 517 - 513 = 4$

$57(10-1) = 570 - 57$

513

$517 = 9 \cdot 57 + 4$

מספרים ראשוניים ופירוק לגורמים

$\mathbb{N}$ = קבוצת כל המספרים השלמים בין 1 ל-

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

$a, b \in \mathbb{N}$

a מחלק את b אם קיים $c \in \mathbb{N}$ כך ש: $b = ac$

סימון: $a \mid b$

$p \in \mathbb{N}$ מספר ראשוני אם $p \neq 1$ ו-

$$\left(a \mid p \Rightarrow \begin{array}{l} a = p \\ \text{או} \\ a = 1 \end{array} \right)$$

$5 \mid 10$

$4 \mid 12$

$2 \mid 5786$

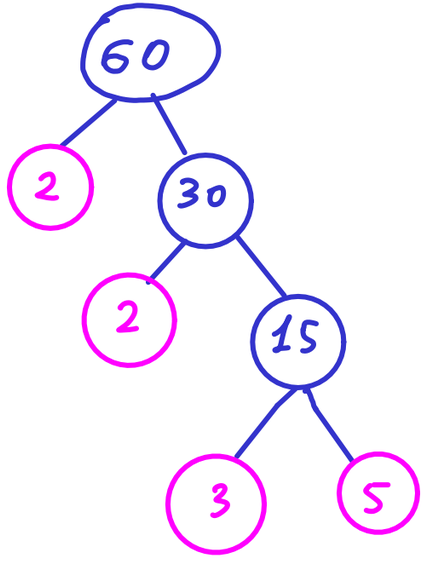
$2 \nmid 5787$

לכן p ראשוני אם ורק אם ל-p יש 2 מחלקים בדיוק (אם"מ)

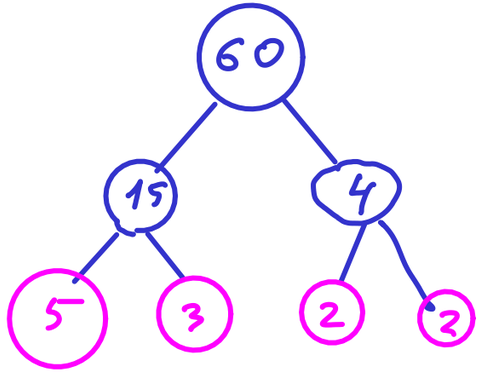
לפי הגדרה, 1 הוא/אינו מספר ראשוני

אלו בונים ל-60 ?

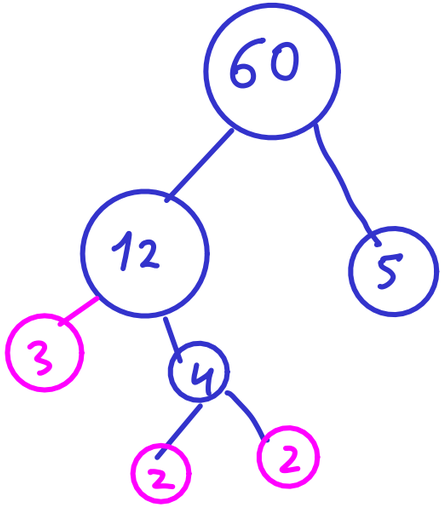
מתלק = גורם



$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$



$60 = 5 \cdot 3 \cdot 2 \cdot 2 = 5 \cdot 3 \cdot 2^2 = 2^2 \cdot 3 \cdot 5$



$60 = 3 \cdot 2 \cdot 2 \cdot 5 = 3 \cdot 2^2 \cdot 5 = 2^2 \cdot 3 \cdot 5$

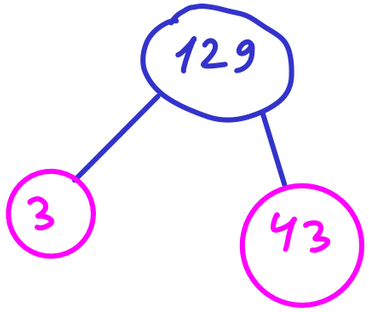
2, 3, 5, 7, 11, 13, 17, 19, 23

129

$\sqrt{129} \approx 11.36\ldots$

? $3 \mid 129$ מתי אפשר לעצור במיון של מספרים

$\frac{129}{3} = 43$



$\sqrt{43} \approx 6.56$

2, 3, 5, 7

$43 = 7 \cdot 6 + 1$

$129 = 3 \cdot 43$

מסקנה: 43 ראשוני

$p_1, \ldots, p_k$ $\quad p_1 \cdots p_k + 1$