

- a/b נקרא a חלק b אם $a = b \cdot c$ למה a/b נקרא a חלק b אם $a = b \cdot c$ למה a/b נקרא a חלק b אם $a = b \cdot c$

המשפט הראשון

אם a חלק b ו b חלק c אז a חלק c

המשפט השני

אם a חלק b ו a חלק c אז a חלק $b+c$

המשפט השלישי

אם a חלק b ו a חלק c אז a חלק $b \cdot c$

המשפט הרביעי

אם a חלק b ו a חלק c אז a חלק $b \cdot c$

המשפט החמישי

אם a חלק b ו a חלק c אז a חלק $b \cdot c$

$$b \cdot c = a \cdot d$$

המשפט השישי

אם a חלק b ו a חלק c אז a חלק $b \cdot c$

$$I = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

המשפט השביעי

אם a חלק b ו a חלק c אז a חלק $b \cdot c$

המשפט השמיני

אם a חלק b ו a חלק c אז a חלק $b \cdot c$

המשפט התשיעי

אם a חלק b ו a חלק c אז a חלק $b \cdot c$

Claim: יי, נניח $a, b \in \mathbb{Z}$ ו- $a \neq 0$.
 הוכחה: יהי $d = \gcd(a, b)$. אז $a = da'$ ו- $b = db'$ ו- $\gcd(a', b') = 1$.

אם a/b אינו מס' שלם, נניח כי $a/b \notin \mathbb{Z}$.

אם $a/b \in \mathbb{Z}$, אז $a = kb$ ו- $\gcd(a, b) = |b|$.
 אם $a/b \notin \mathbb{Z}$, נניח כי $a/b = q + r/b$ כאשר $0 < r < |b|$.

נניח כי $d = \gcd(a, b)$. אז $a = da'$ ו- $b = db'$ ו- $\gcd(a', b') = 1$.
 $c = ua + vb$

$a/b, a/c, a/bc$
 $\Downarrow$
 a/c

~~אם~~

תוצאה: כל מס' שלם c ש- $d \mid c$ ניתן לכתוב $c = ua + vb$ עבור איזורים מסוימים של u, v .

אם a, b אינם מתחלקים ב-1, אז $\gcd(a, b) > 1$.

נניח כי $d = \gcd(a, b)$. אז $a = da'$ ו- $b = db'$ ו- $\gcd(a', b') = 1$.
 אם a, b אינם מתחלקים ב-1, אז $d > 1$.

$\gcd(a, b) = \gcd(a, b) \iff \gcd(a, b) = a$ אם $b = 0$ ו- $\gcd(a, b) = b$ אם $a = 0$.

אם a, b אינם מתחלקים ב-1, אז $d > 1$.

אם a, b אינם מתחלקים ב-1, אז $d > 1$.

$\gcd(a, b) = r_{k+1}$

הוכחה: נניח כי $a = q_1 b + r_1$ ו- $b = q_2 r_1 + r_2$ ו- $r_1 = q_3 r_2 + r_3$ ו- $\vdots$ ו- $r_{k-1} = q_k r_k + r_{k+1}$ ו- $r_k = q_{k+1} r_{k+1} + 0$.

$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_k, r_{k+1}) = r_{k+1}$.

אם a, b אינם מתחלקים ב-1, אז $d > 1$.

$\gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, r_{i+2})$

$\gcd(a, b) = \dots = \gcd(r_{k+1}, 0) = r_{k+1}$.

~~אם~~

$a = q_1 b + r_1, 0 \leq r_1 < b$
 $b = q_2 r_1 + r_2, 0 \leq r_2 < r_1$
 $r_1 = q_3 r_2 + r_3, 0 \leq r_3 < r_2$
 $\vdots$
 $r_{k-1} = q_k r_k + r_{k+1}, 0 \leq r_{k+1} < r_k$
 $r_k = q_{k+1} r_{k+1} + 0$
 הוכחה: נניח כי $a = q_1 b + r_1$ ו- $b = q_2 r_1 + r_2$ ו- $r_1 = q_3 r_2 + r_3$ ו- $\vdots$ ו- $r_{k-1} = q_k r_k + r_{k+1}$ ו- $r_k = q_{k+1} r_{k+1} + 0$.

$$\textcircled{d} \text{cd}(a, b) = \vee a + \vee b$$

$$k_{k+1} = x_{k+1} - x_k, \quad k=1, 2, \dots, n-1$$

$$r_n = r_{n-2} - 2r_{n-1}, a=1, b=r_1, (b=r_0)$$

$$\text{Def. } \varphi: \mathcal{A} \rightarrow \mathcal{B} \text{ is a homomorphism if } \varphi(a+b) = \varphi(a) + \varphi(b) \text{ and } \varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a, b \in \mathcal{A}.$$
[illegible]

הנכח

(5) $\text{היתרון, } d \text{ נחלק, משותף. הוא } d \text{ מכמת היתרון } d \text{ כי } a \text{ ו- } b \text{ מתחלקים}$
 משותף בלתי-פשוט או $d \text{ חלקי } a \text{ ו- } b \text{ ו- } d < \min(a, b)$
 (א) $\text{נרשם } \gcd(a, b) = \alpha a + \beta b$ עבור a, b אי-זוגיים, נובע

10" 1/2 k, 10N 10 1/2 k 21. (2w)

^(אדמ"ק)
הו' כח' נ"ח ב' אלה ע' מ' מ' ק' מ' (אדמ"ק) - P1

$$Z_L = \frac{L}{j\omega} P_1 + 7$$

2. $\int_0^1 x^2 dx = \frac{1}{3}$

$\cdot P_{L+7} \quad p \sim p' \text{ הן } p \text{ ו-} p' \quad P_{L+7} = e^{-\frac{\pi}{2}} \left(\frac{1}{k_1 + i k_2}, \frac{1}{k_1 - i k_2} \right) q_c \quad (9)$

$$\gamma = \gamma_1 = \prod_{i=1}^L p_i \quad \gamma \leq 1 \quad p_i \in \mathbb{R} \quad (p_i, u_i(x)) \quad 1 \leq i \leq L$$

$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$

[illegible]

p_1, p_2 - זכר שוקר ה"ס האשון שאינו נמצא בשימוש קטל.

מלך'ה נקרא'ם קודען / ס'ר'י, וו'רן ית'רתי ה' ראשית שפ'ר'ה ו'ר'

p''/k or q''/k

משפט 1. יש אינסוף ראשוניים מהצורה $4k+3$.

$$q_L = p_1 \cdot p_2 \cdot \dots \cdot p_L - 1$$

$$q_L = 4k+3$$

~~אם q_L ראשוני וכן $q_L \equiv 3 \pmod{4}$, אז q_L ראשוני מהצורה $4k+3$.
אם q_L אינו ראשוני, אז q_L מתפרק למכפלה של ראשוניים, אבל אחד מהם חייב להיות מהצורה $4k+3$.~~

בן היתרה, הראשוניים p חייבים להיות מהצורה $4k+3$ או $4k+1$.
אם q_L אינו ראשוני, אז q_L מתפרק למכפלה של ראשוניים, אבל אחד מהם חייב להיות מהצורה $4k+3$.

משפט 2 (דיריכלט, 1837)

$$\text{אם } a, b \text{ זרים, אז } \lim_{x \rightarrow \infty} \frac{\pi(ax+b)}{\pi(ax)} = 1$$

$$\pi(x) \sim \frac{x}{\log x}$$

משפט 3 (המשפט הראשוני)

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x} = 1$$

מהקובץ A איננו נוסף 2 (הוא ראשוני).

$$p_L \leq 2^L$$

$$p_L \leq 2^L$$

$$p_L \leq 2^L$$

$$q_L = p_1 \cdot p_2 \cdot \dots \cdot p_L$$

$$p_L \leq p \leq q_L$$

$$= p_1 \cdot p_2 \cdot \dots \cdot p_L < 2^L$$

$$\pi(x) \geq \log_2(\log_2(x))$$