

19/10/2016

→ $1 < p$ πρώτος \Leftrightarrow διαιρείται μόνο από $\pm 1, \pm p$
→ a σύνθετος $\Leftrightarrow \exists \beta$ και $\gamma, |\beta|, |\gamma| \neq 1$ ώστε
 $a = \beta \cdot \gamma$

→ Κάθε μη μηδενικό σύνθετος διαιρεί το 0

Θεώρημα

Κάθε φυσικός > 1 διαιρείται από ταυτόσημο έναν πρώτο
Απόδειξη \rightarrow αναγωγή

Διότητες 1) $a|b$ και $b|c \Rightarrow a|c$

απόδειξη: $a|b \Rightarrow b = a \cdot a', a', b' \in \mathbb{Z}$

$b|c \Rightarrow c = b \cdot b'$

$c = b \cdot b' = a \cdot a' \cdot b' \Leftrightarrow a|c$

2) $a|b$ και $b|a \Rightarrow |a| = |b|$

απόδειξη: $a|b \Leftrightarrow b = a \cdot a' \quad \left. \begin{array}{l} b|a \Leftrightarrow a = b \cdot b' \end{array} \right\} \begin{array}{l} b = b \cdot b' \cdot a \Rightarrow \\ \Rightarrow |b| = |b| \cdot |b'| \cdot |a'| \Leftrightarrow \end{array}$

3) $a|b \Rightarrow |a| \leq |b|$

$$4) \text{ } a|b \text{ και } a|c \Rightarrow a|b \pm c$$

$$\text{απόδειξη: } \left. \begin{array}{l} a|b \Leftrightarrow b = a \cdot a' \\ a|c \Leftrightarrow c = a \cdot a'' \end{array} \right\} b \pm c = a \cdot a' \pm a \cdot a'' = a(a' \pm a'')$$

$$5) \text{ } a|b \pm c \not\Rightarrow a|b \text{ και } a|c$$

$\neq |2 \pm 5 \Rightarrow \neq |2 \quad \text{και} \quad \neq |5$

$$6) \text{ } a|b \Rightarrow a|b \cdot c \quad a|b \cdot c \not\Rightarrow a|b$$

$$a|b \Leftrightarrow b = a \cdot a' \Rightarrow bc = a \cdot a' \cdot c \Leftrightarrow a|bc$$

$15|3 \cdot 5 \Rightarrow 15|3 \quad \text{αυτε} \quad 15 \nmid 5$

7) Πότε ισχύει $a|b \cdot c \Rightarrow a|b \text{ ή } a|c$;

Απάντηση: Αν $|a|$ πρώτος $\Rightarrow a|b \cdot c \Rightarrow a|b \text{ ή } a|c$

$$8) \text{ } a|b \Rightarrow a^2|b^2$$

9) Ένας αμέριστος διαιρείται από το 3 ή το 9 αν το άθροισμα των ψηφίων του διαιρείται από το 3 ή από το 9.

Απόδειξη: στο λημμα βλάβη της γενικότητας

$$a = a_k \dots a_2 a_1 a_0 = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$$

ψηφία στο δεκαδικό σύστημα

$$a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0 = \underbrace{(a_k + a_{k-1} + \dots + a_0)}_{\text{διαίρεται με το 3}}$$

$$a_k (10^k - 1) = a_k (10 - 1) \left(\dots \right)$$

διαίρεται με το 3

Άρα $3|A$ και $3|(a_k + \dots + a_0) \Rightarrow 3|A + (a_k + \dots + a_0)$
 $\Rightarrow 3|a$

Άσκηση

10) Ένας αριθμός αμέραιος διαίρεται από το 4 ή 5 αν τα δύο τελευταία ψηφία του διαγράφονται από το 4 ή 5.

Ορισμός

Δύο αμέραιοι a και b ονομάζονται πρώτοι μεταξύ τους ή πρώτοι προς αλληλούς, αν οι μόνοι κοινοί διαιρέτες είναι το ± 1

$$(a, b) = 1 \sim (b, a) = 1$$

π.χ. $(-14, 15) = 1$, $(-14, -15) = 1$

ΜΑΘΗΜΑΤΙΚΗ ΕΠΙΣΤΗΜΗ

Έστω μια πρόταση $p(n)$ της οποίας η αληθεία εξαρτάται από την μεταβλητή n , η οποία παίρνει τιμές $a \leq n$ για κάποιον φυσικό a .

Αν τα ενοστά 2 βήματα είναι αληθή τότε η $p(n)$ είναι αληθής $\forall n \geq a$

1) $p(a)$ αληθής. Το εφεξής

2) Αν η $p(k)$ είναι αληθής $\xrightarrow[\text{πρόσβαση}]{\text{τότε}}$ ότι και η $p(k+1)$ είναι αληθής.

π.χ. 1) Για $n \geq 0$, δείξτε $\sum_{i=0}^n r^i = \frac{r^{n+1} - 1}{r - 1}$ $r \neq 1$

α) Εξετάσω $n=0$: $\sum_{i=0}^0 r^i = r^0 = 1 = \frac{r^1 - 1}{r - 1} = 1$ αληθές

$n=1$: $\sum_{i=0}^1 r^i = \frac{r^{1+1} - 1}{r - 1}$ β) $\frac{r^2 - 1}{r - 1} = r + 1$

$\sum_{i=0}^1 r^i = r^0 + r^1 = 1 + r$

Υποθέτουμε ότι $\sum_{i=0}^k r^i = \frac{r^{k+1} - 1}{r - 1}$

Θέλουμε να δείξουμε ότι $\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}$

$\sum_{i=0}^{k+1} r^i = \sum_{i=0}^k r^i + r^{k+1} = \frac{r^{k+1} - 1}{r - 1} + r^{k+1} =$

$= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r - 1} = \frac{r^{k+2} - 1}{r - 1}$

2) Για $n \geq 1$ δείξτε ότι $3 \mid 2^{2n} - 1$

Με μαθηματική επαγωγή

$n=1$: $2^{2 \cdot 1} - 1 = 2^2 - 1 = 3$ δείχνει

$n=2$: $2^{2 \cdot 2} - 1 = 2^4 - 1 = 16 - 1 = 15$, δείχνει

Υποθέτουμε ότι ισχύει για $n=k$

$3 \mid 2^{2k} - 1$. Θα δείξουμε ότι $3 \mid 2^{2(k+1)} - 1$

$$2^{2^{k+1}} - 1 = 2^{2^k + 2^k} - 1 = 2^{2^k} \cdot 2^{2^k} - 1 = 4 \cdot 2^{2^k} - 1 \quad \textcircled{+}$$

$$3 \mid 2^{2^k} - 1 = 3a \quad \textcircled{+} \quad 3 \cdot 2^{2^k} + 2^{2^k} - 1 =$$

$$\text{ισχύει} \quad \Leftarrow 3 \cdot 2^k + 3a = 3(2^k + a)$$

Εφαρμογές : Για $n \geq 3$ ισχύει $2^n < 2n+1$

$$\sum_{i=1}^n (2i+1) = n^2$$

$$\text{Για } n \geq 1 \text{ ισχύει } \sqrt{n} < \sum_{i=1}^n \frac{1}{\sqrt{i}}$$

Ισχυρή Μαθηματική Έπαρση

- Έστω $p(n)$ μια πρόταση της οποίας η αληθεία εξαρτάται από τη μεταβλητή n η οποία παίρνει τιμές από κάποιους υποσύνολο των φυσικών. Έστω a και b σταθεροί φυσικοί με $a \leq b$. Αν ισχύουν τα δύο επόμενα βήματα τότε η $P(n)$ είναι αληθής $\forall n \geq a$.
- Οι προτάσεις $p(a), p(a+1), \dots, p(b)$ είναι αληθείς (το δείχνουμε)
- Για κάθε $k \geq b$, αν η $P(k)$ είναι αληθής για όλα τα $a \leq i < k$ και αυτό συνεπάγεται ότι και η $p(k)$ είναι αληθής.

Θεώρημα

Κάθε φυσικός $n > 1$ διαιρείται από κάποιο πρώτο.

Απόδειξη: Με ισχυρή μαθηματική επαγωγή.

$P(n)$: 0 n διαιρείται από κάποιο πρώτο

Για $n=2$: $p(2)$ αληθής, $p(3)$ αληθής, $p(4)$ αληθής

Θα υποθέσουμε ότι η πρότασή μας είναι αληθής για i με $2 \leq i < k$

Θα το αποδείξουμε για $P(k)$.

Δηλαδή πρέπει να αποδείξουμε ότι υπάρχει p πρώτος με $p|k$

k πρώτος \Rightarrow ισχύει $p=k|k$

k σύνθετος $\Leftrightarrow k=a \cdot b$ με $a, b \neq 1$.

παράγωγος ιδιότητα (\Leftarrow)

$$a|k \Rightarrow a \leq k$$

$$b|k \Rightarrow b \leq k$$

$$\Rightarrow a < k$$

(δεν ισχύει $k=a \cdot b$)

$a < k$ εφαρμόζεται η υπόθεση στο a .

Δηλαδή υπάρχει p πρώτος με $p|a$ και $a|k \Rightarrow p|k \Leftrightarrow p(k)$ αληθής.

Θεώρημα

Η δεσμη Μαθηματική επαγωγή είναι ισοδύναμη με την Αντι Μαθηματική Επαγωγή. (Goursat and Beirna)

Θεώρημα (Ευκλείδης)

Το πλήθος των πρώτων είναι άπειρο.

Απόδειξη

Υποθέτουμε ότι υπάρχουν μόνο πεπερασμένοι πρώτοι

$$a_1, a_2, a_3, \dots, a_k$$

" 2 " 3 " 5

$$0 \text{ αριθμός } q = a_1 \cdot a_2 \cdot \dots \cdot a_k + 1 = \prod_{i=1}^k a_i + 1$$

$$0 \ q \neq a_i, \forall i \quad q \neq 1$$

$$\text{όρα } q \text{ άπυτος} \Rightarrow \exists a_i \mid q$$

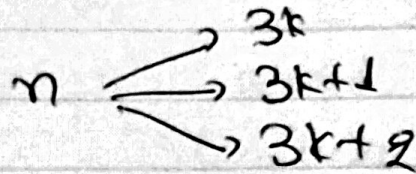
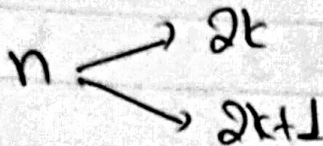
$$\left. \begin{array}{l} a_i \mid a_i \Rightarrow a_i \mid \prod_{j=1}^k a_j \\ a_i \mid q \end{array} \right\} a_i \mid q - \prod_{j=1}^k a_j$$

$$q - \prod_{j=1}^k a_j = \prod_{j=1}^k a_j + 1 - \prod_{j=1}^k a_j = 1$$

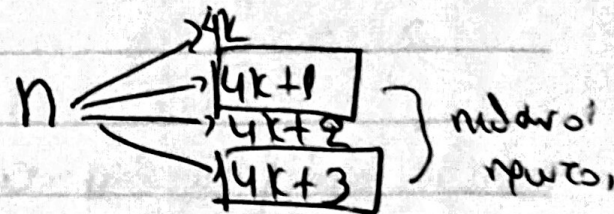
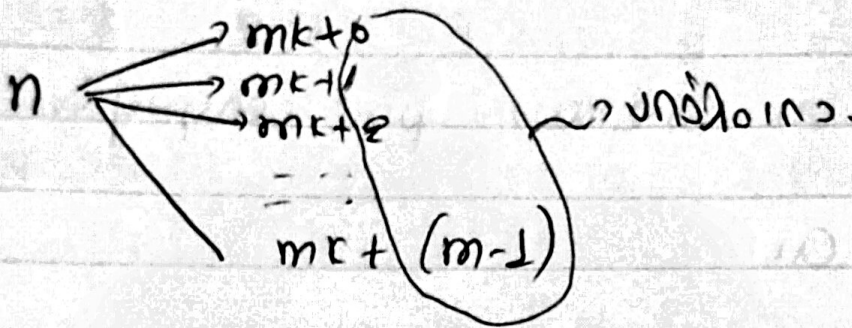
$$\underline{a_i = 1 \text{ άτοπο}}$$

Παραδείγματα

$$n \in \mathbb{N}$$



$$m \in \mathbb{N}, n \geq m$$



Πρόταση

Έστω $n \geq 4$ και πρώτος
Υπάρχουν άσπιοι πρώτοι μορφής
 $4k+1$ και $4k+3$.