19/10/2016

→ $1<p$ πρώτος ⇔ διαιρείται μόνο από $\pm 1, \pm p$

→ a σύνθετος ⇔ $\exists\ \beta$ και γ, $|\beta|, |\gamma| \neq 1$ ώστε
$$a = \beta \cdot \gamma$$

→ Κάθε μη μηδενικός ακέραιος διαιρεί το 0

Θεώρημα

Κάθε φυσικός >1 διαιρείται από τουλάχιστον έναν πρώτο

Απόδειξη → παρακάτω

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

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

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

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

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

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

$\Rightarrow |b| = |b| \cdot \underbrace{|b'| \cdot |a'|}_{1} \Leftrightarrow$

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

4) $a|b$ και $a|c \Rightarrow a|b \pm c$

<u>Απόδειξη</u>: $a|b \Leftrightarrow b = a \cdot a'$, $a|c \Leftrightarrow c = a \cdot a'$ $\Big\}$ $b \pm c = a \cdot a' \pm a \cdot a''$ $= a(a' \pm a'')$

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

$7|2+5 \Rightarrow 7|2$ ή $7|5$

6) $a|b \Rightarrow a|b \cdot c$ $\qquad$ $a|b \cdot c \not\Rightarrow a|b$

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

$15|3 \cdot 5 \Rightarrow 15 \nmid 3$ ούτε $15 \nmid 5$

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

<u>Απάντηση</u>: Αν $|a|$ πρώτος $\Rightarrow a|b \cdot c \Rightarrow a|b$ ή $a|c$

8) $a|b \Rightarrow a^2 | b^2$

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

<u>Απόδειξη</u>: $a > 0$ χωρίς βλάβη της γενικότητας

$a = \underbrace{a_k \ldots a_2 a_1 a_0}_{\text{ψηφία στο δεκαδικό σύστημα}} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 10 + a_0$

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

$a_k (10^k - 1^k) = a_k \underbrace{(10-1)}_{\text{διαιρείται με το 3}} (\_\_\_\_\_\_)$

Άρα $3/A$ και $3/(a_k + \ldots + a_0) \Rightarrow 3/A + (a_k + \ldots + a_0)$
$\Rightarrow 3/a$

Άσκηση

1) Ένας αριθμός ακέραιος διαιρείται από το 4 ή 5 αν τα δύο τελευταία ψηφία του διαιρούνται από το 4 ή 5.

Ορισμός

Δύο ακέραιοι α και β καλούνται πρώτοι μεταξύ τους ή πρώτοι προς αλλήλους, αν οι μόνοι κοινοί διαιρέτες είναι το ± 1

$(a,\beta) = 1 \rightsquigarrow (\text{ΜΚΔ}) = 1$

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

ΜΑΘΗΜΑΤΙΚΗ ΕΠΑΓΩΓΗ

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

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

1) $P(a)$ αληθής. Το εξετάζω

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

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

0) Εξετάζω $n=0$: $\sum_{0}^{0} r^i = r^0 = 1 = \frac{r^1-1}{r-1} = 1$ αληθής

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

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

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 $n \geq 1$ ισχύει ότι $3 | 2^{2n}-1$

Με Μαθηματική επαγωγή

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

$n=2$: $2^{2\cdot 2}-1 = 2^4-1 = 16-1 = 15$. ισχύει

Υποθέτουμε ότι ισχύει για $n=k$

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

$$2^{2(k+1)}-1=2^{2k+2}-1=2^{2k}\cdot 2^{2}-1=4\cdot 2^{2k}-1 \overset{(+)}{=}$$

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

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

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

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

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

Ισχυρή Μαθηματική Επαγωγή

- Έστω $p(n)$ μια πρόταση της οποίας η αλήθεια εξαρτάται από τη μεταβλητή n η οποία παίρνει τιμές από κάποιο 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 $p(a)$, $p(a+1)$, ..., $p(b)$ είναι αληθείς (το δείχνουμε)
- Για κάθε $k>b$, αν η $P(i)$ 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.

$P(n)$: Ο 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 $p|k$

$k \to$ πρώτος $\Rightarrow$ ισχύει $p=k|k$

ή

$k \to$ σύνθετος $\Leftrightarrow k=a\cdot b$ με $\boxed{a,b \neq 1}$

$$\left.\begin{array}{l} a|k \overset{\text{παραπάνω ιδιότητα } (\leftarrow)}{\Rightarrow} a \leq k \\ b|k \Rightarrow b \leq k \\ \text{(δεν ισχύει το = γιατί } k=a\cdot b) \end{array}\right\} \Rightarrow a<k$$

$a<k$ εφαρμόζεται η υπόθεση στο a.
Δηλαδή υπάρχει p πρώτος με $p|a$ και $a|k \Rightarrow p|k \Leftrightarrow p(k)$ αληθής.

Θεώρημα

Η ισχυρή Μαθηματική επαγωγή είναι ισοδύναμη με την Απλή Μαθηματική Επαγωγή. (χωρίς απόδειξη)

Θεώρημα (Ευκλείδης)

Το πλήθος των πρώτων είναι άπειρο.

Απόδειξη

Υποθέτουμε ότι υπάρχουν μόνο πεπερασμένοι πρώτοι

$$a_1, a_2, a_3, \dots, a_k$$
$$a_1 = 2,\quad a_2 = 3,\quad a_3 = 5$$

Ο αριθμός $q = a_1 \cdot a_2 \cdots a_k + 1 = \prod_{i=1}^{k} a_i + 1$.

Ο $q \neq a_i,\ \forall i$ $q > a_i$

άρα q σύνθετος $\Rightarrow \exists a_i \mid q$

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

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

$a_i = 1$ άτοπο

Παρατήρηση

$n \in \mathbb{N}$

$n \to 2k$
$n \to 2k+1$

$n \to 3k$
$n \to 3k+1$
$n \to 3k+2$

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

$n \to mk+0$
$n \to mk+1$
$n \to mk+2$
$\vdots$
$n \to mk+(m-1)$

→ υπόλοιπο.

$n \to 4k$
$n \to \boxed{4k+1}$
$n \to 4k+2$
$n \to \boxed{4k+3}$

$\left.\begin{matrix} 4k+1 \\ 4k+3 \end{matrix}\right\}$ πιθανοί πρώτοι

Πρόταση

Έστω $n > 4$ και πρώτος.
Υπάρχουν άπειροι πρώτοι μορφής $4k+1$ και $4k+3$.