2^o Καλοκαιρινό σχολείο Μαθηματικών
Νάουσα 2008

Μικρό Θεώρημα του Fermat, η συνάρτηση του Euler και Μαθηματικοί Διαγωνισμοί

Αλέξανδρος Γ. Συγκελάκης
ags@math.uoc.gr

Αύγουστος 2008

1 Το μικρό Θεώρημα του Fermat και η γενίκευσή του

Θεώρημα 1.1 *Εάν p πρώτος και a ένας φυσικός αριθμός τότε:*

(i) $a^p \equiv a \pmod{p}$

(ii) *(Το μικρό θεώρημα του Fermat) εάν $(a,p)=1$ τότε*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Απόδειξη:

Σχόλιο: Υπάρχουν πολλές αποδείξεις του μικρού Θεωρήματος του Fermat . Επιλέξαμε αυτή η οποία χτίζει βήμα-βήμα την απόδειξη και είναι μέσα στις δυνατότητες ενός μαθητή με ενδιαφέρον για τα μαθηματικά.

(i) Θα κάνουμε χρήση της μαθηματικής επαγωγής. Για $a=1$ ισχύει τετριμμένα. Ας υποθέσουμε ότι $p|a^p-a$. Θα αποδείξουμε ότι $p|(a+1)^p-(a+1)$.

Απ'τον τύπο του διωνύμου του Newton [1], έχουμε

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Συνεπώς

$$(a+1)^p - a^p - 1 = \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a.$$

Όμως το p διαιρεί το δεξί μέλος [2] άρα και το αριστερό. Συνδιάζοντας αυτό με την επαγωγική υπόθεση, έχουμε ότι

$$p \mid [(a+1)^p - a^p - 1] + (a^p - a) = (a+1)^p - (a+1).$$

[1] $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

[2] Η απόδειξη αυτού αφήνεται ως άσκηση στους αναγνώστες. Τα δύο βήματα που χρειάζονται για την απόδειξη είναι:

(a) Το γινόμενο n διαδοχικών ακεραίων διαιρείται από το $n!$ και

(b) εαν p πρώτος, τότε οι $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ διαιρούνται από το p.

(ii) Προφανώς από το (i) έχουμε $p \mid a^p - a \Rightarrow p \mid a(a^{p-1} - 1)$ που σε συνδιασμό με το $(a, p) = 1$ δίνει το ζητούμενο

$$p \mid a^{p-1} - 1.$$

□

Παράδειγμα 1.1 (i) *Αφού* $(2, 11) = 1$ *και ο* 11 *είναι πρώτος, θα είναι* $2^{11-1} \equiv 1 \pmod{11}$. *Πράγματι όταν το* $2^{10} = 1024$ *διαιρεθεί με το* 11, *αφήνει υπόλοιπο* 1.

(ii) *Με μεγαλύτερα νούμερα: π.χ. οι αριθμοί* $2^3 * 5 * 11^2 = 4840$ *και* 101 *είναι πρώτοι μεταξύ τους και αφού ο* 101 *είναι πρώτος, έχουμε* $4840^{100} \equiv 1 \pmod{101}$.

□

Πόρισμα 1.1 *Εαν* p *πρώτος και* a *ένας φυσικός αριθμός με* $(a, p) = 1$, *και* d *είναι ο μικρότερος εκθέτης για τον οποίο ισχύει*

$$a^d \equiv 1 \pmod{p}$$

τότε $d \mid p - 1$.

Η απόδειξη αφήνεται ως άσκηση στους αναγνώστες.

□

2 Η συνάρτηση του Euler

Για δοσμένο φυσικό αριθμό $n \geq 1$, συμβολίζουμε με $\varphi(n)$ το πλήθος των φυσικών αριθμών των μικρότερων ή ίσων του n που είναι πρώτοι προς τον n. Με αυτό τον τρόπο ορίσαμε μία συνάρτηση

$$\varphi : \mathbb{N} \to \mathbb{N}$$

με

$$\varphi(n) = \sharp\{k \in \mathbb{N} \backslash k \leq n \ \text{ και } \ (a, n) = 1\}^{(3)}.$$

[3] Το σύμβολο $\sharp\{\ldots\}$ συμβολίζει το πλήθος των στοιχείων του συνόλου $\{\ldots\}$.

Παράδειγμα 2.1 $\varphi(9) = 6$ *διότι οι* 6 *αριθμοί* $1, 2, 4, 5, 7, 8$ *είναι μικρότεροι και πρώτοι προς το* 9.

□

Ιδιότητες της συνάρτησης Euler

(i) $\varphi(1) = 1$

(ii) Είναι φανερό ότι εάν $n = p$ πρώτος, τότε $\varphi(p) = p - 1$ καθώς όλοι οι αριθμοί οι μικρότεροι του p, δηλαδή οι $1, 2, \ldots, p-1$, είναι πρώτοι προς τον p.

(iii) Η συνάρτηση φ είναι πολλαπλασιαστική δηλαδή εαν $(m, n) = 1$, τότε

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

(Για παράδειγμα $\varphi(21) = \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = (3-1) \cdot (7-1) = 12$).

(iv) Εαν p πρώτος, τότε

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

[Απλά λογαριάστε το πλήθος των αριθμών που είναι μικρότεροι ή ίσοι του p^k και είναι πρώτοι προς τον p^k (ή αντίθετα, αφαιρέστε τα πολλαπλάσια του p τα οποία σε πλήθος είναι p^{k-1})].

(v) Γενικά, εαν $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ η ανάλυση του n σε πρώτους (διακεκριμένους μεταξύ τους) παράγοντες, χρησιμοποιήστε την ιδιότητα (iii) για να δείξετε ότι:

$$\begin{aligned} \varphi(n) &= p_1^{k_1-1}(p_1-1) \cdot p_2^{k_2-1}(p_2-1) \cdots p_l^{k_l-1}(p_l-1) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_l}\right) \\ &= n \prod_{i=1}^{l} \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

□

Παράδειγμα 2.2 *Είναι*

$$\begin{aligned}\varphi(1200) &= \varphi(2^2 \cdot 3^4 \cdot 5^2) = 1200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\ &= 1200 \cdot \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 320\end{aligned}$$

Άρα με αυτό τον τρόπο βρήκαμε, με πολύ απλό τρόπο, ότι το πλήθος των φυσικών που είναι μικρότεροι απ'το 1200 *και πρώτοι προς αυτόν είναι* 320.

□

Παράδειγμα 2.3 (i) *Να αποδειχθεί ότι οι φυσικοί αριθμοί* $n \in \mathbb{N}\backslash\{4\}$ *για τους οποίους ισχύει* $\varphi(n) \equiv 2 \pmod 4$ *είναι είτε της μορφής* $n = p^k$ *είτε της μορφής* $n = 2p^k$, *όπου* $k \in \mathbb{N}$ *και ο* p *ένας πρώτος με* $p \equiv 3 \pmod 4$.

(ii) *Να αποδειχθεί ότι δεν υπάρχει φυσικός αριθμός* n *με* $\varphi(n) = 14$.

Λύση:

(i) *Θα δείξουμε ότι στην ανάλυση του* n *σε πρώτους αριθμούς, δε γίνεται να υπάρχουν περισσότεροι από δύο διακεκριμένοι πρώτοι αριθμοί οι οποίοι να είναι* ≥ 3. *Γι'αυτό, ας υποθέσουμε αντίθετα, ότι*

$$n = p_1^{k_1}p_2^{k_2}\cdots p_l^{k_l},\ \ p_i \geq 3\ \forall i = 1,\ldots,l\ \ \textit{και}\ \ l \geq 2.$$

Τότε

$$\varphi(n) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_l^{k_l-1}(p_l-1)$$

Όμως, καθώς $l \geq 2$, *υπάρχουν τουλάχιστον* 2 *άρτιοι παράγοντες μεταξύ των* $(p_1-1),(p_2-1),\ldots,(p_l-1)$. *Άρα* $\varphi(n) \equiv 0 \pmod 4$, *άτοπο.*

Άρα

$$n = 2^r p^k.$$

Εαν $r \geq 3$ *(*$r \neq 2$ *διότι* $n \neq 4$*) , τότε*

$$\varphi(n) = 2^{r-1}p^{k-1}(p-1) \equiv 0 \pmod 4,\ \ \textit{άτοπο.}$$

Άρα, $r = 0, 1$ *(*$r \neq 2$ *διότι* $n \neq 4$*) συνεπώς*

$$n = p^k\ \ \textit{ή}\ \ n = 2p^k.$$

Έμεινε να δείξουμε ότι $p \equiv 3 \pmod 4$. *Εαν αντίθετα ήταν* $p \equiv 1 \pmod 4$[4], *τότε θα είχαμε (και στις δύο περιπτώσεις για τον* n*)*

$$\varphi(n) = p^k(p-1) \equiv 0 \pmod 4, \quad \textit{άτοπο.}$$

Έτσι αποδείχθηκε η ζητούμενη.

(ii) *Πρόκειται για άμεση εφαρμογή του πρώτου ερωτήματος.*

□

Δεν σταματάνε όμως εδώ οι πολύ σημαντικές εφαρμογές της συνάρτησης του Euler . Υπάρχουν πολλές ακόμη εφαρμογές και σπουδαία θεωρήματα που την χρησιμοποιούν. Κλείνουμε αυτή την παράγραφο με το Θεώρημα του Euler , χωρίς απόδειξη (καθώς υπάρχει σε πολλά κλασσικά βιβλία Θεωρίας Αριθμών), το οποίο αποτελεί γενίκευση του μικρού Θεωρήματος του Fermat .

Θεώρημα 2.1 *(Θεώρημα Euler) Εαν* a *είναι φυσικός πρώτος προς τον* n *τότε ισχύει*

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Παρατήρηση: Εαν $n = p$, τότε παίρνουμε το μικρό Θεώρημα του Fermat .

Παράδειγμα 2.4 *Επειδή* $\varphi(9) = 6$, *και* $(9,4) = 1$ *έχουμε ότι* $4^6 \equiv 1 \pmod 9$.

Πόρισμα 2.1 *Εαν* a *είναι φυσικός πρώτος προς του* n, *και* $k \equiv l \pmod{\varphi(n)}$, *τότε*

$$a^k \equiv a^l \pmod n.$$

Απόδειξη:

Ας υποθέσουμε χωρίς βλάβη της γενικότητας ότι $k \geq l$. Τότε λόγω της $k \equiv l \pmod{\varphi(n)}$, συμπεραίνουμε ότι υπάρχει ακέραιος π τέτοιος ώστε $k = \pi\varphi(n) + l$ άρα, λόγω και του θεωρήματος του Euler , έχουμε

$$a^k = a^l \left(a^{\varphi(n)}\right)^l \equiv a^l \cdot 1^l \equiv a^l \pmod n$$

□

[4]Προφανώς αφού $p \neq 2$, άρα p περιττός οπότε δεν γίνεται να είναι $p \equiv 0, 2 \pmod 4$

3 Μία χρήσιμη εφαρμογή του Θεωρήματος Euler σε μία κατηγορία ασκήσεων από Μαθηματικούς διαγωνισμούς

Ας δώσουμε μερικές ασκήσεις και τον τρόπο με τον οποίο μπορούμε να εργαστούμε ώστε να τις λύσουμε μεθοδικά και εύκολα με τα παραπάνω εφόδια .

Μία άσκηση της 6ης Εθνικής Μαθηματικής Ολυμπιάδας του 1989 ήταν :

Παράδειγμα 3.1 *Για ποιές τιμές του* $n \in \mathbb{N}$ *ο αριθμός* $1^n+2^n+3^n$ *διαιρείται με το* 7 ;

Σχόλιο : *Θα παρουσιάσουμε αρχικά (*1*η Λύση) την εξαιρετική λύση της συναδέλφου Ε. Μήτσιου που δημοσιεύθηκε τότε στο περιοδικό «Διάσταση» και κατόπιν (*2*η Λύση) κάνοντας χρήση της παραπάνω θεωρίας.*

1η Λύση (Ε. Μήτσιου)

Για $n = 1$ *η δοθείσα παράσταση δεν διαιρείται με το* 7*, για* $n = 2$ *διαιρείται με το* 7 *και για* $n = 3$ *δεν διαιρείται με το* 7.

- *Για* $n = 2k$ *έχουμε*

$$1^{2k}+2^{2k}+3^{2k} = 1+4^k+9^k = 1+4^k+\pi o\lambda.7+2^k = \pi o\lambda.7+1+2^k+4^k \quad (1)$$

{ *Εάν* $k = 3l$ *τότε η* (1) *γίνεται*

$$\begin{aligned} \pi o\lambda.7 + 1 + 2^{3l} + 4^{3l} &= \pi o\lambda.7 + 1 + 8^l + 64^l \\ &= \pi o\lambda.7 + 1 + \pi o\lambda.7 + 1^l + \pi o\lambda.7 + 1^l \\ &= \pi o\lambda.7 + 3 \end{aligned}$$

{ *Εάν* $k = 3l + 1$ *τοτε η* (1) *γίνεται*

$$\begin{aligned} \pi o\lambda.7 + 1 + 2^{3l+1} + 4^{3l+1} &= \pi o\lambda.7 + 1 + 2 \cdot 8^l + 1 \cdot 64^l \\ &= \pi o\lambda.7 + 1 + 2(\pi o\lambda.7 + 1^l) \\ &+ 4(\pi o\lambda.7 + 1^l) \\ &= \pi o\lambda.7 + 1 + 2 + 4 = \pi o\lambda.7 \end{aligned}$$

{ *Εάν* $k = 3l + 2$ *τοτε η* (1) *γίνεται*

$$\begin{aligned} \pi o\lambda.7 + 1 + 2^{3l+2} + 4^{3l+2} &= \pi o\lambda.7 + 1 + 4 \cdot 8^l + 16 \cdot 64^l \\ &= \pi o\lambda.7 + 1 + \pi o\lambda.7 + 4 \cdot 1^l \\ &+ \pi o\lambda.7 + 16 \cdot 1^l \\ &= \pi o\lambda.7 + 1 + 4 + 16 = \pi o\lambda.7 \end{aligned}$$

Άρα εάν $n = 2k$, *τότε πρέπει* $k = 3l + 1$ *ή* $k = 3l + 2$, *δηλαδή* $n = 6l + 2$ *ή* $n = 6l + 4$.

- *Για* $n = 2k + 1$ *έχουμε*

$$\begin{aligned} 1^{2k+1} + 2^{2k+1} + 3^{2k+1} &= 1 + 2 \cdot 4^k + 3 \cdot 9^k = 1 + 2 \cdot 4^k + \pi o\lambda.7 + 3 \cdot 2^k \\ &= \pi o\lambda.7 + 2(1 + 2^k + 4^k) + 2^k - 1 \end{aligned}$$

Βρήκαμε ότι αν $k = 3l + 1$ *ή* $k = 3l + 2$, *τότε* $1 + 2^k + 4^k = \pi o\lambda.7$, . *Θα εξετάσουμε το* $2^k - 1$ *για* $k = 3l + 1$ *ή* $k = 3l + 2$.

{ *Αν* $k = 3l + 1$ *τότε*

$$2^k - 1 = 2^{3l+1} - 1 = 2 \cdot 8^l - 1 = \pi o\lambda.7 + 2 \cdot 1^l - 1 = \pi o\lambda.7 + 1$$

άρα όχι $\pi o\lambda.7$

{ *Αν* $k = 3l + 2$ *τότε*

$$2^k - 1 = 2^{3l+2} - 1 = 4 \cdot 8^l - 1 = \pi o\lambda.7 + 4 \cdot 1^l - 1 = \pi o\lambda.7 + 3$$

άρα όχι $\pi o\lambda.7$

Άρα το $2^k - 1$ *είναι* $\pi o\lambda.7$ *για* $k = 3l$ *γιατί*

$$2^{3l} - 1 = 8^l - 1 = \pi o\lambda.7 + 1^l - 1 = \pi o\lambda.7$$

όμως τότε το $1^k + 2^k + 4^k$ *δεν είναι* $\pi o\lambda.7$. *Άρα τελικά πρέπει ο* n *να είναι* $\pi o\lambda.2$ *και όχι* $\pi o\lambda.3$, *δηλαδή πρέπει* $n = 6k + 2$ *ή* $n = 6k + 4$ *ή αλλιώς* $n = 6k \pm 2$.

2**η Λύση** *Αφού το* 7 *είναι πρώτος αριθμός και* $(7, 2) = 1 = (7, 3)$, *από το Μικρό Θεώρημα του Fermat ισχύει ότι*

$$2^{7-1} \equiv 1 \pmod 7 \text{ } \textit{οπότε} \text{ } 2^6 \equiv 1 \pmod 7$$

$$3^{7-1} \equiv 1 \pmod 7 \text{ } \textit{οπότε} \text{ } 3^6 \equiv 1 \pmod 7$$

Άρα, το υπόλοιπο του 2^n *με το* 7, *θα επαναλαμβάνεται το πολύ κάθε* 6 *βήματα και μάλιστα το βήμα της επανάληψης (Πόρισμα* 1.1), *θα είναι διαιρέτης του* 6 [5] *(δηλαδή* $1, 2, 3, 6$). *Όμοια και για το υπόλοιπο της*

[5] Σημειώστε πόσο φυσιολογικά έρχεται τώρα, ότι οι περιπτώσεις που πρέπει να πάρουμε για το n, είναι ως προς το υπόλοιπο που αφήνει όταν διαιρεθεί με το 6, κάτι που φαίνεται και στην 1η λύση.

διαίρεσης του 3^n *με το* 7. *Αυτό που μένει λοιπόν να κάνουμε για να δούμε εποπτικά τα παραπάνω, είναι ένας απλός πίνακας δυνάμεων για να βρούμε το* $1^n + 2^n + 3^n$ *για τις διάφορες τιμές του* υ, *όπου* $n = 6k + \upsilon$, $\upsilon = 0, 1, 2, 3, 4, 5$, *θα χρειαστούν το πολύ* 6 *βήματα για να δούμε τα δυνατά υπόλοιπα των* 2^n *και* 3^n *με το* 7.

$\upsilon = n \pmod 6$	0	1	2	3	4	5	*επανάληψη ανα*
$1^n \pmod 7$	1	1	1	1	1	1	1
$2^n \pmod 7$	1	2	4	1	2	4	3
$3^n \pmod 7$	1	3	2	6	4	5	6
$1^n + 2^n + 3^n \pmod 7$	3	6	0	1	0	3	–

Τώρα φαίνεται καθαρά από του παραπάνω πίνακα οτι ο αριθμός $1^n + 2^n + 3^n$ *είναι πολλαπλάσιο του* 7, *όταν το* n *έχει τη μορφή* $n = 6k + 2$ *ή* $6k + 4$. *(Ή ακόμη, ότι ο αριθμός* $1^n + 2^n + 3^n$, *διαιρούμενος με το* 7 *δεν αφήνει ποτέ υπόλοιπο* $2, 4, 5$.*)*

□

Η μέθοδος αυτή μπορεί να εφαρμοστεί και για πολυπλοκότερα προβλήματα τα οποία, όπως το παρακάτω, που χωρίς συγκεκριμένη στρατηγική, είναι δύσκολο να επιλυθούν.

Παράδειγμα 3.2 *Να βρεθούν όλα τα δυνατά υπόλοιπα της διαίρεσης του αριθμού* $A = 2 \cdot 3^n + 3 \cdot 7^{n+1} + 5^{3n+1} - 7$ *δια του* 11.

Λύση

Σχόλιο: Απλά θα προσαρμόσουμε τα δεδομένα στον πίνακα προσθέτοντας δύο ακόμη γραμμες για το $n + 1$ και το $3n + 1$ που εμφανίζονται ως εκθέτες στη δοθείσα παράσταση.

Αφού $(11, 3) = (11, 7) = (11, 5) = 1$, ο ρυθμός επανάληψης των $3^n, 7^n, 5^n$ θα είναι διαιρέτης του $\varphi(11) = 10$ (δηλαδή η επανάληψη τώρα θα είναι είτε ανά $1, 2, 5$ ή 10) και έτσι ο αντίστοιχος πίνακας γίνεται [6]

[6] Προφανώς δεν χρειάζονται οι γραμμές των $3^n \pmod{11}, 5^n \pmod{11}, 7^n \pmod{11}$ απλά μπαίνουν για να γίνει μια πρώτη σύγκριση.

$n \pmod{10}$	0	1	2	3	4	5	6	7	8	9	επανάληψη ανα
$n+1 \pmod{10}$	1	2	3	4	5	6	7	8	9	0	–
$3n+1 \pmod{10}$	1	4	7	0	3	6	9	2	5	8	–
$3^n \pmod{11}$	1	3	9	5	4	1	3	9	5	4	5
$2 \cdot 3^n \pmod{11}$	2	6	7	10	8	2	6	7	10	8	5
$7^n \pmod{11}$	1	7	5	2	3	10	4	6	9	8	10
$3 \cdot 7^{n+1} \pmod{11}$	10	4	6	9	8	1	7	5	2	3	10
$5^n \pmod{11}$	1	5	3	4	9	1	5	3	4	9	5
$5^{3n+1} \pmod{11}$	5	9	3	1	4	5	9	3	1	4	5
A	10	1	9	2	2	1	4	8	6	8	–

Συμπεραίνουμε ότι εαν ο n είναι της μορφής $n = 10k+2$, τότε όταν ο A διαιρεθεί με το 11, αφήνει υπόλοιπο 1. Έτσι, είναι έτοιμη μία (απαιτητική) άσκηση που μπορεί να δειχτεί πλέον με επαγωγή:

Άσκηση: Να αποδειχθεί ότι εαν το τελευταίο ψηφίο του αριθμού n είναι το 2, τότε ο A αφήνει υπόλοιπο 1 όταν διαιρεθεί με το 11.

□

Σχόλια:

1. Ασκήσεις όπως η παραπάνω αποδεικνύονται με επαγωγή εαν γνωρίζουμε όμως το αποτέλεσμα της διαίρεσης με τον αριθμό. Για παράδειγμα παίρνω μία άσκηση από το βιβλίο του αείμνηστου Θ.Ν. Καζαντζή, Θεωρία Αριθμών, Β΄ Έκδοση, Εκδόσεις Μαθηματική Βιβλιοθήκη, Θεσσαλονίκη 1998.

   Άσκηση Να δείξετε ότι εαν n φυσικός ≥ 1 τότε η παράσταση $2^{4n+1} - 2^{2n} - 1$ διαιρείται από το 9. Κατασκευάζοντας τον αντίστοιχο πίνακα, θα διαπιστώσουμε ότι αφού $(2,9) = 1$ και $\varphi(9) = 6$, τα υπόλοιπα της διαίρεσης του 2^n με το 9 θα επαναλαμβάνονται ανά αριθμό που είναι διαιρέτης του 6. Μπορεί για το συγκεκριμένο παράδειγμα (που η λύση με επαγωγή είναι πολύ εύκολη), η διαδικασία κατασκευής του πίνακα να είναι επίπονη, αλλά φανταστείτε ότι θα μπορούσατε με διάφορες δοκιμές να ανακαλύψετε μία τόσο συμμετρικά φτιαγμένη άσκηση!

2. Με τον παραπάνω τρόπο μπορείτε να κατασκευάσετε τις δικές σας ασκήσεις όπως την ακόλουθη που κατασκεύασα πριν από λίγο καιρό πειραματιζόμενος μπροστά στον υπολογιστή με την παραπάνω μέθοδο:

Άσκηση 1: Να δείξετε ότι εαν $n \neq 0 \pmod 6$ τότε

$$1^n + 2^n + 3^n + 4^n + 5^n + 6^n \equiv 0 \pmod 7.$$

Η λύση της είναι αρκετά απλή εαν κατασκευάσετε τον γνωστό πίνακα και αφήνεται ως άσκηση.

□

Ως γενίκευση αυτής της παρατήρησης μου γεννήθηκε το ερώτημα εαν ισχύει γενικά και το έθεσα ως προβληματισμό στο Forum [7]:

Άσκηση 2: Εαν $n \neq 0 \pmod{(p-1)}$ τότε

$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod p$$

Λύση: Λύση σε αυτό το πρόβλημα έδωσε (με εξαιρετικό τρόπο) ο Στέλιος, την οποία παραθέτω παρακάτω για να την απολαύσετε.

Κατάρχήν παρατηρούμε ότι

$$\begin{aligned} p^{n+2} &= p + \binom{n+2}{1}\left[1 + 2 + \cdots + (p-1)\right] \\ &+ \binom{n+2}{2}\left[1^2 + 2^2 + \cdots + (p-1)^2\right] \\ &+ \cdots + \binom{n+2}{n+1}\left[1^{n+1} + 2^{n+1} + \cdots + (p-1)^{n+1}\right] \end{aligned}$$

Άρα αν $p \mid [1^k + 2^k + \cdots + (p-1)^k]$ για κάθε $k = 1, 2, \cdots, n$, όπου $n \in \{1, 2, \cdots, (p-3)\}$, τότε $p \mid [(n+2)(1^{n+1} + 2^{n+1} + \cdots + (p-1)^{n+1})]$

και επειδή $n \in \{1, 2, \cdots, (p-3)\}$ θα ισχύει ότι ο p δεν διαιρεί το $(n+2)$. Συνεπώς $p \mid [1^{n+1} + 2^{n+1} + \cdots + (p-1)^{n+1}]$.

Επαγωγικά λοιπόν αποδεικνύουμε ότι επειδή $p \mid [1 + 2 + \cdots + (p-1)] = \dfrac{p(p-1)}{2}$ θα ισχύει ότι $p \mid [1^k + 2^k + \cdots + (p-1)^k]$ για κάθε $k = 1, 2, \cdots, (p-2)$

και αφού $a^{(p-1)m+u} \equiv (a^{p-1})^m a^u \equiv a^u \pmod p$ για κάθε a με $(a, p) = 1$ [8]

[7] $www.mathlinks.ro/Forum/viewtopic.php?t = 112234$

[8] διότι από το Μικρό Θεώρημα του Fermat ισχύει ότι $a^{p-1} \equiv 1 \pmod p$ αν $(a, p) = 1$

προκύπτει ότι $p \mid [1^n + 2^n + \cdots + (p-1)^n]$ για κάθε $n \in \mathbb{N}^*$ με $n \not\equiv 0 \pmod{p-1}$, όπου p πρώτος μεγαλύτερος του 2.

Σχόλιο: Στη βιβλιογραφία, έμαθα αργότερα, αναφέρεται ως Θεώρημα Chevalley-Warning του οποίου η απόδειξη δεν γίνεται συνήθως με στοιχειώδη τρόπο αφού τα μέσα που διαθέτει η Θεωρία Ομάδων, είναι πολύ ισχυρά και βγάζουν το επιθυμητό αποτέλεσμα της άσκησης σε δύο γραμμές. Αυτή όμως είναι και η αξία της λύσης του Στέλιου. Ότι με στοιχειώδη μέσα αποδεικνύει αυτή την Πρόταση.

□

Ακολουθεί μία πάρα πολύ καλή άσκηση από Μαθηματικό Διαγωνισμό με την οποία τελειώνουμε το άρθρο. Πριν δώσουμε την εκφώνηση δίνουμε ένα πολύ βασικό Λήμμα:

Λήμμα 3.1 *Κάθε πρώτος αριθμός $p > 3$, είναι της μορφής $6k+1$ ή $6k+5$ (Πάρτε ένα οποιοδήποτε φυσικό αριθμό n. Τότε $n = 6k + \upsilon,\ \upsilon = 0, 1, \ldots, 5$ και δείξτε (φανερό) ότι $\upsilon \neq 2, 3, 4$ εαν n πρώτος)*

Παράδειγμα 3.3 *(2ος Εσωτερικός Διαγωνισμός ΕΜΕ 1989)*

Να αποδειχθεί ότι εαν p πρώτος, τότε $42p \mid 3^p - 2^p - 1$.

Απόδειξη:

Αφού $42p = 2 \cdot 3 \cdot 7 \cdot p$ άρα αρκεί να δείξουμε οτι ο $A = 3^p - 2^p - 1$ είναι πολλαπλάσιο των πρώτων αριθμών $2, 3, 7, p$ [9]

(i) **Με το 2:** *Φανερά ο A είναι άρτιος άρα $A \equiv 0 \pmod{2}$.*

(ii) **Με το 3:** $A = 3^p - (2^p + 1) = 3^p - (2+1)(2^{p-1} + 2^{p-2} + \cdots + 2 + 1) \equiv 0 \pmod{3}$

(iii) **Με το p:** *Απ'το Θεώρημα 1.1(i) έχουμε*

$$3^p \equiv 3 \pmod{p} \text{ και } 2^p \equiv 2 \pmod{2}$$

Άρα

$$A = 3^p - 2^p - 1 \equiv 3 - 2 - 1 = 0 \pmod{p}.$$

(iv) **Με το 7:**

Σύμφωνα λοιπόν με το Λήμμα 3.1, κάθε πρώτος αριθμός είναι της μορφής $p = 6k + 1$ ή $p = 6k + 5$.

[9] Θυμίζουμε οτι εάν p, q είναι δύο διακεκριμένοι πρώτοι αριθμοί και n φυσικός, με $p \mid n$ και $q \mid n$ τότε $p \cdot q \mid n$.

- *Εαν* $p = 6k + 1$ *τότε λόγω του Μικρού Θεωρήματος του Fermat , αφού* $(2, 7) = 1$*, είναι*

  $2^6 \equiv 1 \pmod 7$ *άρα* $2^{6k} \equiv 1 \pmod 7$ *άρα* $2^{6k+1} \equiv 2 \pmod 7$

  Όμοια, αφού $(3, 7) = 1$ *έχουμε ότι*

  $$3^{6k+1} \equiv 3 \pmod 7$$

  και έτσι

  $$A = 3^p - 2^p - 1 \equiv 3 - 2 - 1 = 0 \pmod 7$$

- *Εαν* $p = 6k + 5$ *τότε λόγω όμοια όπως παραπάνω έχουμε*

  $$2^{6k+5} \equiv 2^5 = 32 \equiv 4 \pmod 7$$

  και

  $$3^{6k+5} \equiv 3^5 = 243 \equiv 5 \pmod 7$$

  Άρα τελικά

  $$A = 3^p - 2^p - 1 \equiv 5 - 4 - 1 = 0 \pmod 7$$

  Σε κάθε περίπτωση λοιπόν έχουμε $A \equiv 0 \pmod 7$

Σχόλιο: *Παρατηρήστε ότι* $(2, 7) = 1 = (3, 7)$ *και* $\varphi(7) = 6$ *άρα τα υπόλοιπα της διαίρεσης των* 2^k *και* 3^k *με το* 7*, σύμφωνα με όσα είπαμε παραπάνω, επαναλαμβάνονται ανά έναν αριθμό ο οποίος είναι διαιρέτης του* 6*. Φτιάξτε λοιπόν τον αντίστοιχο πίνακα, όπως έγινε στα παραπάνω παραδείγματα, για να δείξετε ότι στις περίπτωσεις* $p = 6k + 1, p = 6k + 5$ *έχουμε ότι* $A \equiv 0 \pmod 7$*. Δικαιολογείται λοιπόν με τα παραπάνω ο λόγος για τον οποίο χρειάστηκε να εργαστούμε* $\mod 6$ *και ο οποίος μας οδήγησε να καταλήξουμε στο (γενικό και πολύ χρήσιμο) Λήμμα* 3.1*.*

□