2^o Καλοκαιρινό σχολείο Μαθηματικών
Νάουσα 2008

Πρώτοι αριθμοί
και τα
Βασικά Θεωρήματά τους

Αλέξανδρος Γ. Συγκελάκης
ags@math.uoc.gr

Αύγουστος 2008

Στη μνήμη του δασκάλου μου, Χάρη Βαφειάδη...

ΠΡΟΛΟΓΟΣ

Το παρόν άρθρο είναι μία συγκέντρωση κάποιων βασικών προτάσεων και παραδειγμάτων από τη θεωρία των πρώτων αριθμών. Σε καμία περίπτωση δεν επικαλείται ο συγγραφέας του άρθρου την πρωτοτυπία των περιεχομένων, τα οποία βρίσκονται στα βιβλία της βιβλιογραφίας που παρατίθεται στο τέλος του παρόντος, στη συλλογή μαθηματικών διαγωνισμών του γράφοντος και σε αρκετά βιβλία στοιχειώδους Θεωρίας Αριθμών. Παρά ταύτα, καταβλήθηκε ιδιαίτερη προσπάθεια ώστε η παρουσίαση της ύλης να είναι διαβαθμισμένη και όλα τα περιεχόμενα να περιέχουν ασκήσεις προσιτές σε μικρούς αλλά και μεγάλους μαθητές με ενδιαφέρον για τα μαθηματικά και ειδικά τους Μαθηματικούς Διαγωνισμούς - Ολυμπιάδες. Με μεγάλη χαρά θα δεχτώ στο *email* μου **ags@math.uoc.gr**, τις υποδείξεις σας, καθώς επίσης και τα σχόλια - κριτικές σας. Μοναδικός υπεύθυνος για τα γραφόμενα, είναι ο συγγραφέας που έκανε την επιλογή των προτάσεων και των ασκήσεων από τα βιβλία της βιβλιογραφίας. Τελειώνοντας, θα ήθελα να ευχαριστήσω τον Καθηγητή του Πανεπιστημίου Κρήτης κο Μιχάλη Λάμπρου για την πολύτιμη συμβολή του στις διορθώσεις του παρόντος.

Αλέξανδρος Γ. Συγκελάκης
Αύγουστος 2008

ΣΥΜΒΟΛΙΣΜΟΙ

$a|b$: «Ο a διαιρεί τον b» δηλαδή υπάρχει $k \in \mathbb{Z}$, τέτοιος ώστε $b = k \cdot a$.

$p^k \| a$: «Το p^k είναι η μεγαλύτερη δύναμη του p που διαιρεί το a.» Δηλαδή το p^k διαιρεί ακριβώς το a (αρα $p^k|a$ ενώ $p^{k+1} \nmid a$).

$a \nmid b$: «Ο a δεν διαιρεί τον b ».

$\min\{a_1, \ldots, a_n\}$: Ο μικρότερος μεταξύ των αριθμών $a_1, \ldots a_n$.

$\max\{a_1, \ldots, a_n\}$: Ο μεγαλύτερος μεταξύ των αριθμών $a_1, \ldots a_n$.

$(a_1, \ldots, a_n)$: Ο Μ.Κ.Δ. των αριθμών $a_1, \ldots a_n$.

$[a_1, \ldots, a_n]$: Το Ε.Κ.Π. των αριθμών $a_1, \ldots a_n$.

$n!$: Διαβάζεται «n παραγοντικό» και ορίζεται να είναι $n! = 1 \cdot 2 \cdot \cdots n$ $n \geq 2$ και 0!=1, 1!=1.

$a \equiv b \pmod{n}$: «Ο a είναι ισότιμος με τον b $modulo$ n (ή κατά μέτρο n) » δηλαδή $n|(a-b)$.

$\mathbb{Z}$: Το σύνολο των ακεραιών αριθμών $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

$\mathbb{N}$: Το σύνολο των φυσικών αριθμών $\{0, 1, 2, 3 \ldots\}$.

$\exists$: Ο υπαρξιακός ποσοδείκτης. Διαβάζεται «Υπάρχει» (τουλάχιστον ένα).

$\forall$: Ο καθολικός ποσοδείκτης. Διαβάζεται «Για κάθε».

$|a|$: «Απόλυτη τιμή του αριθμού a» δηλαδή $|a| = \begin{cases} a, & \text{εάν } a \geq 0 \\ -a, & \text{εάν } a < 0 \end{cases}$

1 Οι πρώτοι αριθμοί και τα Βασικά Θεωρήματά τους

Περίληψη

Στο παρόν άρθρο θα προσπαθήσουμε να συνοψίσουμε μερικά από τα βασικότερα θεωρήματα για τους πρώτους αριθμούς, συνοδευόμενα από αρκετά εισαγωγικά παραδείγματα καθώς και προβλήματα που έχουν τεθεί κατά καιρούς σε Μαθηματικούς Διαγωνισμούς και Ολυμπιάδες. Οι αποδείξεις των περισσοτέρων θεωρημάτων παραλείπονται καθώς μπορούν να βρεθούν σε όλα σχεδόν τα κλασικά βιβλία της στοιχειώδους Θεωρίας Αριθμών. Ενδεικτικά αναφέρονται τα βιβλία που υπάρχουν στη βιβλιογραφία στο τέλος του άρθρου.

Ορισμός 1.1 *Ένας θετικός ακέραιος $p > 1$ καλείται **πρώτος** εάν οι μόνοι διαιρέτες του είναι οι ακέραιοι ± 1 και $\pm p$. Ένας πρώτος αριθμός που είναι διαιρέτης ενός ακέραιου m καλείται **πρώτος διαιρέτης** ή **πρώτος παράγοντας** του m. Ένας θετικός ακέραιος $n > 1$ που δεν είναι πρώτος, καλείται **σύνθετος**. Σε αυτή την περίπτωση υπάρχουν φυσικοί αριθμοί d, e τέτοιοι, ώστε*

$$n = d \cdot e \ \text{ και } \ 1 < d \leq e < n.$$

(Το 2 είναι ο μοναδικός άρτιος πρώτος αριθμός).

Πρόταση 1.1 *Κάθε ακέραιος αριθμός $a > 1$ έχει ένα τουλάχιστον πρώτο διαιρέτη.*

Παράδειγμα 1.1 *Να βρείτε όλους τους θετικούς ακεραίους n για τους οποίους οι αριθμοί $3n-4,\ 4n-5, 5n-3$ είναι όλοι πρώτοι αριθμοί.*

Λύση:

Το άθροισμα των 3 αριθμών είναι άρτιος, συνεπώς τουλάχιστον ένας από αυτούς είναι άρτιος. Ο μοναδικός άρτιος πρώτος είναι το 2. Μόνο οι $3n-4$ και $5n-3$ μπορεί να είναι άρτιοι. Λύνοντας λοιπόν τις εξισώσεις $3n-4=2$ και $5n-3=2$ παίρνουμε $n=2$ και $n=1$, αντίστοιχα. Μόνο για $n=2$ οι τρεις παραπάνω αριθμοί είναι πρώτοι άρα είναι και η μοναδική λύση.

□

Παράδειγμα 1.2 *($AHSME$ 1976) Εάν οι p και q είναι πρώτοι και το τριώνυμο $x^2 - px + q = 0$ έχει διακεκριμένες θετικές ακέραιες ρίζες, να βρείτε τα p και q.*

Λύση:

Έστω x_1 και x_2 με $x_1 < x_2$, οι δύο διακεκριμένες θετικές ακέραιες ρίζες. Τότε $x^2 - px + q = (x - x_1)(x - x_2)$, το οποίο δίνει ότι $p = x_1 + x_2$ και $q = x_1x_2$. Καθώς ο q είναι πρώτος, άρα $x_1 = 1$. Συνεπώς οι $q = x_2$ και $p = x_2 + 1$ είναι διαδοχικοί πρώτοι αριθμοί, άρα $q = 2$ και $p = 3$.

□

Παράδειγμα 1.3 *(ARML 2003) Να βρείτε το μεγαλύτερο διαιρέτη του αριθμού 1001001001 που δεν ξεπερνά το 10000.*

Λύση:

Έχουμε

$$1001001001 = 1001 \cdot 10^6 + 1001 = 1001 \cdot (10^6 + 1) = 7 \cdot 11 \cdot 13 \cdot (10^6 + 1).$$

Ας σημειωθεί ότι

$$x^6 + 1 = (x^2)^3 + 1 = (x^2 + 1)(x^4 - x^2 + 1).$$

Άρα $10^6+1 = 101 \cdot 9901$, άρα $1001001001 = 7 \cdot 11 \cdot 13 \cdot 101 \cdot 9901$. Δεν είναι δύσκολο τώρα να ελέγξουμε ότι κανένας συνδυασμός των 7,11,13 και 101 δεν φτιάχνει γινόμενο που να ξεπερνά το 9901 και να είναι μικρότερο του 1000, άρα η απάντηση είναι 9901.

□

Παράδειγμα 1.4 *Έστω n ένας θετικός ακέραιος. Να αποδειχθεί ότι ο $3^{2^n} + 1$ διαιρείται από το 2 αλλά όχι από το 4* [1].

Απόδειξη:

Καταρχήν, ο 3^{2^n} είναι περιττός και ο $3^{2^n} + 1$ είναι άρτιος. Επίσης,

$$3^{2^n} = (3^2)^{2^{n-1}} = 9^{2^{n-1}} = (8 + 1)^{2^n}.$$

Από το διώνυμο του Νεύτωνα

$$(x+y)^m = x^m + \binom{m}{1}x^{m-1}y + \binom{m}{2}x^{m-2}y^2 + \cdots + \binom{m}{m-1}xy^{m-1} + y^m,$$

για $x = 8,\ y = 1$ και $m = 2^{n-1}$, όλοι οι όροι του αθροίσματος πλην του τελευταίου (που είναι $y^m = 1$), είναι πολλαπλάσια του 8 (τα οποία είναι

[1] Δηλαδή $2 \| 3^{2^n} + 1$.

πολλαπλάσια του 4). Συνεπώς το υπόλοιπο του 3^{2^n} όταν διαιρεθεί με το 4 είναι ίσο με 1, και το υπόλοιπο του $3^{2^n}+1$ με το 4 είναι ίσο με 2.

Παρατήρηση: *Φυσικά το παραπάνω πρόβλημα απλοποιείται εάν κάνουμε χρήση ισοτιμιών $modulo\ 4$.*

□

Παράδειγμα 1.5 *Να βρεθεί το n έτσι ώστε $2^n \| 3^{1024}-1$.*

Λύση:

Η απάντηση είναι 12. Ας σημειώσουμε ότι $1024 = 2^{10}$ και $x^2-y^2 = (x-y)(x+y)$. Τότε, έχουμε

$$\begin{aligned} 3^{2^{10}}-1 &= \left(3^{2^9}+1\right)\left(3^{2^9}-1\right) = \left(3^{2^9}+1\right)\left(3^{2^8}+1\right)\left(3^{2^8}-1\right) \\ &= \cdots = \left(3^{2^9}+1\right)\left(3^{2^8}+1\right)\cdots\left(3^{2^1}+1\right)\left(3^{2^0}+1\right)(3-1) \end{aligned}$$

Όμως από το παράδειγμα 1.4, έχουμε $2\|3^{2^k}+1$ για θετικούς ακεραίους k. Συνεπώς η απάντηση είναι 9+2+1=12.

□

Η ακόλουθη Πρόταση είναι πολύ χρήσιμη σε ασκήσεις στις οποίες χρειαζόμαστε την αναπαράσταση ενός πρώτου αριθμού (Κοιτάξτε, για παράδειγμα, την προτεινόμενη άσκηση στο τέλος του Παραδείγματος (1.26)).

Πρόταση 1.2 *Κάθε πρώτος αριθμός είναι είτε της μορφής $6k+1$ είτε της μορφής $6k+5$.*

Πρόταση 1.3 ***(Βασική Πρόταση)***

(i) *Αν ο $p \neq 3$ είναι πρώτος τότε $p^2 \equiv 1 \pmod 3$.*

(ii) *Αν ο $p \neq 2$ είναι πρώτος τότε $p^2 \equiv 1 \pmod 8$.*

(iii) *Αν ο $p > 3$ είναι πρώτος τότε $p^2 \equiv 1 \pmod{12}$.*

(iv) *Για κάθε πρώτο $p > 3$ ισχύει ότι $p \equiv \pm 1 \pmod 6$ (Αναδιατύπωση της Πρότασης 1.2).*

Θεώρημα 1.1 *Το πλήθος των πρώτων είναι άπειρο.*

Απόδειξη: [2]

Ας υποθέσουμε ότι $p_1, \ldots, p_n$ είναι όλοι οι πρώτοι αριθμοί. Θεωρούμε τον αριθμό

$$A = p_1 \cdots p_n + 1.$$

Σύμφωνα με την Πρόταση (1.1), υπάρχει πρώτος p τέτοιος, ώστε $p|A$. Καθώς $p_1, \ldots, p_n$ είναι όλοι οι πρώτοι, έχουμε $p = p_j$ για κάποιο δείκτη j με $1 \leq j \leq n$. Επομένως $p|A$ και $p|p_1 \cdots p_n$ απ' όπου παίρνουμε $p|1$ που είναι άτοπο. Συνεπώς, το πλήθος των πρώτων είναι άπειρο.

□

Πρόταση 1.4 *Εάν με p_n συμβολίσουμε του n-οστό πρώτο αριθμό, τότε ισχύει (απόδειξη με επαγωγή)*

$$p_n \leq 2^{2^{n-1}}.$$

Παράδειγμα 1.6 *Για κάθε φυσικό αριθμό $n > 1$ υπάρχουν n διαδοχικοί φυσικοί αριθμοί, κανείς από τους οποίους δεν είναι πρώτος αριθμός.*

Απόδειξη:

Αρκεί να θεωρήσουμε τους εξής n διαδοχικούς φυσικούς αριθμούς

$$(n+1)! + 2,\ (n+1)! + 3,\ \cdots, (n+1)! + (n+1).$$

Κανείς από τους αριθμούς αυτούς δεν είναι πρώτος, διότι για κάθε $m = 2, 3, \cdots, n+1$, ο αριθμός $(n+1)! + m$ διαιρείται δια του m [3].

Παρατήρηση: *Από το παραπάνω παράδειγμα προκύπτει ότι στο σύνολο των φυσικών αριθμών, υπάρχουν όσο μεγάλα κενά πρώτων αριθμών θέλουμε.*

Ωστόσο, ανοικτό παραμένει το ερώτημα αν μπορούμε με κάποιο άλλο τρόπο (εκτός από εξαντλητική απαρίθμηση) να βρούμε τους μικρότερους διαδοχικούς αριθμούς που να έχουν το επιθυμητό κενό. Αυτή είναι εύλογη ερώτηση αν αναλογιστούμε ότι το παραγοντικό μεγαλώνει πολύ γρήγορα. Να αναφέρουμε ότι π.χ. με τον παραπάνω τρόπο, για να προσδιορίσουμε 5 διαδοχικούς σύνθετους αριθμούς, μπορούμε να πάρουμε τους αριθμούς

[2] Πρόκειται για μία πολύ όμορφη απόδειξη η οποία οφείλεται στον Ευκλείδη και την οποία παραθέτουμε για ιστορικούς λόγους.

[3] Επίσης οι αριθμοί $(n+1)! - (n+1), \ldots, (n+1)! - 3, (n+1)! - 2$ είναι αποδεκτοί.

6!+2, 6!+3, 6!+4, 6!+4, 6!+6 δηλαδή τους αριθμούς 722,723,724,725,726. Όμως οι 5 πρώτοι διαδοχικοί φυσικοί αριθμοί που συναντάμε είναι οι 24,25,26,27,28 (ασφαλώς πολύ μικρότεροι από εκείνους που προκύπτουν με την παραπάνω μέθοδο).

□

Η Πρόταση που ακολουθεί μας δίνει ένα τρόπο για να ελέγχουμε εάν ένας φυσικός αριθμός είναι πρώτος.

Πρόταση 1.5 *Κάθε σύνθετος φυσικός αριθμός $a > 1$, έχει ένα τουλάχιστον πρώτο διαιρέτη p, με $p \leq \sqrt{a}$.*

Πόρισμα 1.1 *Εάν ένας φυσικός αριθμός $a > 1$ δεν διαιρείται από κανένα πρώτο p, με $p \leq \sqrt{n}$, τότε ο αριθμός a είναι πρώτος.*

Παράδειγμα 1.7 *Θα εξετάσουμε έαν ο ακέραιος 383 είναι πρώτος. Έχουμε $19 < \sqrt{383} < 20$. Οι πρώτοι που είναι ≤ 19 είναι οι 2,3,5,7,11,13,17 και 19. Με έλεγχο διαπιστώνουμε ότι κανένας από αυτούς δεν διαιρεί το 383. Επομένως ο αριθμός 383 είναι πρώτος.*

Πρόταση 1.6 *Έστω a, b ακέραιοι $\neq 0, 1$ και p ένας πρώτος. Εάν $p|ab$ τότε $p|a$ ή $p|b$.*

Γενίκευση: *Έστω $a_1, \ldots, a_n$ ακέραιοι $\neq 0, 1$ και p ένας πρώτος. Εάν $p|a_1 \cdots a_n$ τότε $p|a_m$ για κάποιο δείκτη m ($1 \leq m \leq n$).*

Το ακόλουθο Θεώρημα είναι ένα από τα σημαντικότερα της Θεωρίας Αριθμών και είναι γνωστό ως το **Θεμελιώδες Θεώρημα της Αριθμητικής**.

Θεώρημα 1.2 ***(Θεμελιώδες Θεώρημα της Αριθμητικής)*** *Κάθε φυσικός $a > 1$ αναλύεται σε γινόμενο πρώτων κατά ένα και μόνο τρόπο, αν παραβλέψουμε την τάξη των παραγόντων στο γινόμενο.*

Ορισμός 1.2 *Σύμφωνα με το παραπάνω Θεώρημα, εάν a είναι ένας φυσικός > 1, τότε υπάρχουν διαφορετικοί πρώτοι $p_1, \ldots, p_k$ και φυσικοί $a_1, \ldots, a_k > 0$ έτσι, ώστε*

$$a = p_1^{a_1} \cdots p_k^{a_k}.$$

*Η παραπάνω γραφή του a θα καλείται **πρωτογενής ανάλυση** του a.*

Πρόταση 1.7 *Έστω a ένας φυσικός > 1 και $a = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής του ανάλυση. Ο φυσικός αριθμός d διαιρεί τον a, αν και μόνο αν, $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ με $0 \leq \beta_i \leq a_i$ $(i = 1, \ldots, k)$.*

Πρόταση 1.8 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι με*

$$|a_1| = p_1^{a_{11}} \cdots p_k^{a_{1k}}, \ldots, |a_n| = p_1^{a_{n1}} \cdots p_k^{a_{nk}}$$

όπου $p_1, \ldots, p_k$ είναι πρώτοι και a_{ij} φυσικοί αριθμοί $(i = 1, \ldots, n, j = 1, \ldots, k)$. Τότε

$$(a_1, \ldots, a_n) = p_1^{d_1} \cdots p_k^{d_k},$$

όπου $d_j = \min\{a_{1j}, \ldots, a_{nj}\}$ $(j = 1, \ldots, k)$.

Πόρισμα 1.2 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι και $m \in \mathbb{N}$. Τότε*

$$(a_1^m, \ldots, a_n^m) = (a_1, \ldots, a_n)^m.$$

Ορισμός 1.3 *Δύο ακέραιοι αριθμοί a, b θα καλούνται **πρώτοι μεταξύ τους**, εάν $(a, b) = 1$.*

Πρόταση 1.9 ***(ταυτότητα Bezout)*** *Οι ακέραιοι αριθμοί a και b είναι πρώτοι μεταξύ τους, αν και μόνο αν υπάρχουν ακέραιοι r και s τέτοιοι, ώστε να ισχύει*

$$r \cdot a + s \cdot b = 1.$$

Πρόταση 1.10 *Έστω $a, b_1, \cdots, b_n$ $(n \geq 2)$ μη μηδενικοί ακέραιοι και οι $b_1, \cdots, b_n$ πρώτοι μεταξύ τους ανά δύο. Τότε*

$$(a, b_1, \ldots, b_n) = (a, b_1) \cdots (a, b_n).$$

Πόρισμα 1.3 *Έστω $a, b_1, \ldots, b_n$ $(n \geq 2)$ μη μηδενικοί ακέραιοι και οι $b_1, \ldots, b_n$ ανά δύο πρώτοι μεταξύ τους. Εάν $b_1|a, \ldots, b_n|a$ τότε $b_1 \cdots b_n|a$.*

Παράδειγμα 1.8 *Έστω n ένας περιττός ακέραιος > 1. Να δείξετε ότι*

$$24|n(n^2 - 1).$$

Απόδειξη :

Ο ακέραιος $A = n(n^2-1) = (n-1)n(n+1)$ *είναι γινόμενο τριών διαδοχικών ακεραίων συνεπώς είναι πολλαπλάσιο του 3, δηλαδή* $3|A$. *Επειδή ο ακέραιος* n *είναι περιττός* > 1, *υπάρχει* $k \in \mathbb{N}$ *με* $k \neq 0$ *έτσι, ώστε* $n = 2k+1$. *Οπότε*

$$A = 4k(k+1)(2k+1).$$

Ένας από τους φυσικούς $k, k+1$ *είναι άρτιος άρα* $8|A$. *Τέλος, καθώς* $(3,8) = 1$, *το Πόρισμα* 1.3 *δίνει το ζητούμενο* $24|A$.

□

Πρόταση 1.11 *Έστω* $a_1, \ldots, a_n$ *μη μηδενικοί ακέραιοι με*

$$|a_1| = p_1^{a_{11}} \cdots p_k^{a_{1k}}, \ldots, |a_n| = p_1^{a_{n1}} \cdots p_k^{a_{nk}}$$

όπου $p_1, \ldots, p_k$ *είναι πρώτοι και* a_{ij} *φυσικοί αριθμοί (*$i = 1, \ldots, n \ \ , \ \ j = 1, \ldots, k$*). Τότε*

$$[a_1, \ldots, a_n] = p_1^{c_1} \cdots p_k^{c_k},$$

όπου $c_j = \max\{a_{1j}, \ldots, a_{nj}\}$ $(j = 1, \ldots, k)$.

Πόρισμα 1.4 *Έστω* $a_1, \ldots, a_n$ *μη μηδενικοί ακέραιοι και* $m \in \mathbb{N}$. *Τότε*

$$[a_1^m, \ldots, a_n^m] = [a_1, \ldots, a_n]^m.$$

Παράδειγμα 1.9 *Οι Προτάσεις* 1.8, 1.11 *είναι πολύ χρήσιμες για την εύρεση του Μ.Κ.Δ. και Ε.Κ.Π. δύο ή περισσοτέρων φυσικών στην περίπτωση που γνωρίζουμε την πρωτογενή τους ανάλυση. Για τον Μ.Κ.Δ. αρκεί να πάρουμε το γινόμενο όλων των πρώτων που εμφανίζονται στην πρωτογενή ανάλυση κάθε αριθμού υψωμένο στη μικρότερη δύναμη (εάν κάποιος πρώτος δεν εμφανίζεται στην πρωτογενή ανάλυση του αριθμού, τότε θεωρούμε ότι εμφανίζεται με εκθέτη 0, συνεπώς αυτός ο εκθέτης είναι και ο μικρότερος που εμφανίζεται για τον ευ λόγω πρώτο). Για το Ε.Κ.Π. αρκεί να πάρουμε το γινόμενο όλων των πρώτων που εμφανίζονται στην πρωτογενή ανάλυση κάθε αριθμού υψωμένο στη μεγαλύτερη δύναμη. Έτσι, ο Μ.Κ.Δ. των αριθμών* $49000 = 2^3 \cdot 5^3 \cdot 7^2$, $36400 = 2^4 \cdot 5^2 \cdot 7 \cdot 13$, $27500 = 2^2 \cdot 5^4 \cdot 11$ *είναι* $2^2 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13^0 = 100$. *ενώ το Ε.Κ.Π. των ίδιων είναι* $2^4 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 = 70070000$.

Πρόταση 1.12 *Έστω* a, b *δύο μη μηδενικοί ακέραιοι. Τότε*

$$(a,b) \cdot [a,b] = |ab|.$$

Παρατήρηση: *Για περισσότερους από δύο ακεραίους,* ***δεν ισχύει*** *ανάλογη σχέση με την παραπάνω. Δηλαδή γενικά, έχουμε*

$$(a_1, \ldots, a_n) \cdot [a_1, \ldots, a_n] \neq |a_1 \cdots a_n| \quad \textit{για} \quad n > 2.$$

Για παράδειγμα, $(6, 8, 10) \cdot [6, 8, 10] = 2 \cdot 120 = 240 \neq 480 = 6 \cdot 8 \cdot 10$.

Παράδειγμα 1.10 *Να αποδειχθεί ότι ο αριθμός* $2^{4n+2}+1$ *δεν είναι πρώτος αν* $n \geq 1$.

Απόδειξη:

Ισχύει

$$\begin{aligned} 2^{4n+2}+1 &= (2^{2n+1})^2+1 = (2^{2n+1}+1)^2 - 2\cdot 2^{2n+1} = (2^{2n+1}+1)^2 - 2^{2n+2} \\ &= (2^{2n+1}+1)^2 - (2^{n+1})^2 = (2^{2n+1}+2^{n+1}+1)(2^{2n+1}-2^{n+1}+1). \end{aligned}$$

Για $n > 0$ *ισχύει*

$$2^{2n+1} + 2^{n+1} + 1 > 1$$

και

$$2^{2n+1} - 2^{n+1} + 1 = 2^{n+1}(2^n - 1) + 1 > 1,$$

απ' όπου προκύπτει ότι ο δοσμένος αριθμός είναι σύνθετος.

□

Παράδειγμα 1.11 *Να αποδειχθεί ότι ο αριθμός* $n^4 + 4$ *δεν είναι πρώτος αν* $n > 1$.

Απόδειξη:

Ισχύει ότι:

$$n^4+4 = (n^2)^2+2^2 = (n^2+2)^2-4n^2 = (n^2+2)^2-(2n)^2 = (n^2+2n+2)(n^2-2n+2).$$

και κάθε ένας παράγοντας του τελευταίου γινομένου είναι > 1.

□

Παράδειγμα 1.12 *Να αποδειχθεί ότι υπάρχουν άπειροι πρώτοι της μορφής* $6m + 5$.

Απόδειξη:

Έστω ότι υπάρχουν πεπερασμένου πλήθους πρώτοι $p_1, \ldots, p_r$ *της μορφής* $6m + 5$. *Τότε ο φυσικός αριθμός* $s = 6p_1 \cdots p_r - 1$ *θα έχει ένα πρώτο*

διαιρέτη q της μορφής $6m+5$, αφού διαφορετικά (λόγω της Πρότασης 1.2 όλοι οι πρώτοι διαιρέτες του θα ήταν της μορφής $6m+1$ και συνεπώς και το γινόμενό τους s θα ήταν της ίδιας μορφής, άτοπο, διότι ο s είναι της μορφής $6m+5$. Άρα, υπάρχει $k \in \{1,2,\ldots,r\}$, τέτοιος ώστε $q = 6m+5 = p_k$, οπότε $q|6p_1 \cdots p_r$ άρα $q|1$, άτοπο.

Άσκηση: *Να αποδειχθεί ότι υπάρχουν άπειροι πρώτοι της μορφής $4m+3$.*

□

Παράδειγμα 1.13 *(Ευκλείδης 1995) Να προσδιορίσετε τους πρώτους αριθμούς p, q για τους οποίους ο αριθμός $p^{p+1} + q^{q+1}$ είναι πρώτος.*

Λύση:

Εάν p, q και οι δύο άρτιοι ή και οι δύο περιττοί, τότε ο αριθμός $p^{p+1} + q^{q+1}$ είναι άρτιος > 2 άρα όχι πρώτος. Άρα ο ένας είναι το 2 και ο άλλος είναι περιττός. Χωρίς βλάβη της γενικότητος μπορούμε να υποθέσουμε ότι $p = 2$ και $q \equiv 0, 1, -1 \pmod 3$ και περιττός. Εάν $q \equiv 1 \pmod 3$, τότε $p^{p+1} + q^{q+1} \equiv 8 + 1 \equiv 0 \pmod 3$, άτοπο. Εάν $q \equiv -1 \pmod 3$, τότε $p^{p+1} + q^{q+1} \equiv 8 + 1 \equiv 0 \pmod 3$ (διότι q περιττός άρα $q+1$ άρτιος), άτοπο. Τέλος, εάν $q \equiv 0 \pmod 3$ τότε επειδή ο q είναι πρώτος, θα είναι $q = 3$ κι έτσι $p^{p+1} + q^{q+1} = 89$ που είναι πρώτος. Άρα η μοναδική δεκτή λύση είναι $p = 2,\ q = 3$ (ή $p = 3,\ q = 2$).

□

Παράδειγμα 1.14 *(Προταθέν στην Διεθνή Ολυμπιάδα) Πότε ο αριθμός $(p-1)! + 1$ είναι δύναμη του p όπου p πρώτος αριθμός;*

Λύση:

Για $p = 2, 3, 5$ ο αριθμός $(p-1)! + 1$ είναι δύναμη των $2, 3, 5$ αντίστοιχα ($2^1, 3^1, 5^2$ αντίστοιχα).

Έστω τώρα $p > 5$. Προφανώς, ισχύουν οι συνεπαγωγές

$$p-1 = 2k > 4 \Rightarrow k > 2 \Rightarrow p-1 = 2k > k+2 \Rightarrow k < p-3 \Rightarrow$$

$$2 < k < p-3 \Rightarrow 2k|(p-2)! \Rightarrow p-1|(p-2)! \Rightarrow (p-1)^2|(p-1)!,$$

οπότε για κάποιο A είναι $(p-1)! = A \cdot (p-1)^2$. Εάν τώρα

$(p-1)!+1 = p^n$ τότε $(p-1)!+1 = (1+(p-1))^n = 1+n(p-1)+(p-1)^2 \cdot B$ άρα

$(p-1)! = n(p-1) + (p-1)^2 \cdot B$ *άρα* $n(p-1) = (p-1)! - (p-1)^2 \cdot B =$ $= (p-1)^2 \cdot A - (p-1)^2 \cdot B = (p-1)^2(A-B)$ *άρα* $n = (p-1)(A-B)$ *οπότε* $p-1|n$ *δηλαδή* $p-1 \leq n$ *που σημαίνει* $(p-1)! + 1 \geq p^{p-1}$, *άτοπο αφού ισχύει*

$$(p-1)! \leq (p-1)^{p-2} < p^{p-2} < p^{p-1} - 1 \Rightarrow (p-1)! + 1 < p^{p-1}.$$

□

Παράδειγμα 1.15 *(Ρωσσία 2001) Να βρεθούν όλοι οι πρώτοι* p *και* q *τέτοιοι, ώστε* $p + q = (p-q)^3$.

Λύση:

Επειδή $(p-q)^3 = p + q \neq 0$, *οι* p, q *είναι διακεκριμένοι και συνεπώς πρώτοι μεταξύ τους.*

Επειδή $p - q \equiv 2p \pmod{p+q}$, *παίρνοντας την δοσμένη εξίσωση* $modulo\,(p+q)$ *έχουμε* $0 \equiv 8p^3 \pmod{p+q}$. *Επειδή οι* p,q *είναι πρώτοι μεταξύ τους, άρα το ίδιο συμβαίνει και για τους* $p, p+q$. *Συνεπώς* $0 \equiv 8 \pmod{p+q}$, *δηλαδή* $8|p+q$.

Ομοίως, παίρνοντας την παραπάνω εξίσωση $modulo\,(p-q)$, *παίρνουμε* $2p \equiv 0 \pmod{p-q}$ *και επειδή οι* p, q *είναι πρώτοι μεταξύ τους, το ίδιο συμβαίνει και για τους* $p, p-q$. *Άρα* $2 \equiv 0 \pmod{p-q}$, *δηλαδή* $2|p-q$.

Συνεπώς προκύπτει ότι $(p,q) = (3,5)$ *ή* $(5,3)$ *και μόνο το τελευταίο ζεύγος ικανοποιεί την δοσμένη εξίσωση.*

Παρατήρηση: *Υπάρχει και μία άλλη προσέγγιση του εν λόγω θέματος. Θέτουτας* $p - q = a$ *παίρνουμε* $p + q = a^3$. *Συνεπώς* $p = \dfrac{a^3 + a}{2}$ *και* $q = \dfrac{a^3 - a}{2}$. *Αυτή η μέθοδος είναι πολύ διαδεδομένη στην επίλυση διοφαντικών εξισώσεων.*

□

Παράδειγμα 1.16 *(Baltic 2001) Έστω* a *ένας περιττός ακέραιος. Να αποδείξετε ότι οι αριθμοί* $a^{2^n} + 2^{2^n}$ *και* $a^{2^m} + 2^{2^m}$ *είναι πρώτοι μεταξύ τους, για όλους τους θετικούς ακεραίους* n *και* m *με* $n \neq m$.

Απόδειξη:

Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $m > n$. *Για κάθε πρώτο* p *που διαιρεί τον* $a^{2^n} + 2^{2^n}$, *έχουμε*

$$a^{2^n} \equiv -2^{2^n} \pmod{p}.$$

Υψώνοντας και τα δύο μέλη στο τετράγωνο $m-n$ φορές παίρνουμε

$$a^{2^m} \equiv 2^{2^m} \pmod{p}.$$

Επειδή ο a είναι περιττός, έχουμε $p \neq 2$. Συνεπώς, $2^{2^m} + 2^{2^m} = 2^{2^m+1} \not\equiv 0 \pmod{p}$ άρα

$$a^{2^m} \equiv 2^{2^m} \not\equiv -2^{2^m} \pmod{p}.$$

Άρα

$$p \not| \, a^{2^m} + 2^{2^m}$$

το οποίο αποδεικνύει αυτό που θέλαμε.

□

Παράδειγμα 1.17 *Εξετάστε εάν υπάρχουν άπειροι το πλήθος άρτιοι θετικοί ακέραιοι k τέτοιοι ώστε για κάθε πρώτο αριθμό p, ο αριθμός p^2+k να είναι σύνθετος.*

Λύση:

Η απάντηση είναι θετική.

Καταρχήν για $p=2$, ο p^2+k είναι πάντα σύνθετος για όλους τους άρτιους θετικούς ακεραίους.

Εάν $p>3$, τότε $p^2 \equiv 1 \pmod{3}$. Συνεπώς εάν ο k είναι άρτιος θετικός ακέραιος με $k \equiv 2 \pmod{3}$, τότε ο p^2+k είναι σύνθετος για όλους τους πρώτους $p>3$ (ο p^2+k είναι μεγαλύτερος από το 3 και διαιρείται με το 3).

Τέλος, σημειώνουμε ότι $3^2+k \equiv 0 \pmod{5}$ εάν $k \equiv 1 \pmod{5}$.

Έτσι, συγκεντρώνοντας όλα τα παραπάνω, καταλήγουμε στο ότι όλοι οι θετικοί ακέραιοι k με

$$\begin{cases} k \equiv 0 \pmod{2} \\ k \equiv 2 \pmod{3} \\ k \equiv 1 \pmod{5} \end{cases}$$

ή διαφορετικά $k \equiv 26 \pmod{30}$, ικανοποιούν τις απαιτήσεις του προβλήματος.

□

Παράδειγμα 1.18 *(Ρουμανία 2003) Θεωρούμε πρώτους αριθμούς $n_1 < n_2 < \cdots < n_{31}$. Αποδείξτε ότι εάν $30 | n_1^4 + n_2^4 + \cdots + n_{31}^4$, τότε μεταξύ αυτών των αριθμών μπορούμε να βρούμε 3 διαδοχικούς πρώτους.*

Απόδειξη :

Έστω $s = n_1^4 + n_2^4 + \cdots + n_{31}^4$. *Αρχικά ισχυριζόμαστε ότι* $n_1 = 2$. *Διαφορετικά, όλοι οι αριθμοί* $n_i,\ 1 \leq i \leq 31$ *είναι περιττοί, δηλαδή ο* s *είναι περιττός, άτοπο.*

Επίσης ισχυριζόμαστε ότι $n_2 = 3$. *Διαφορετικά, έχουμε* $n_i^4 \equiv 1 \pmod 3$ *για κάθε* $1 \leq i \leq 31$. *Προκύπτει λοιπόν ότι* $s \equiv 31 \equiv 1 \pmod 3$, *άτοπο.*

Τέλος θα δείξουμε ότι $n_3 = 5$. *Πράγματι, εάν* $n_3 \neq 5$, *τότε* $n_i^2 \equiv \pm 1 \pmod 5$ *και* $n_i^4 \equiv 1 \pmod 5$ *για κάθε* $1 \leq i \leq 31$. *Συνεπώς* $s \equiv 31 \equiv 1 \pmod 5$, *άτοπο.*

Έτσι δείξαμε ότι οι διαδοχικοί πρώτοι $2, 3, 5$ *εμφανίζονται στους δοσμένους πρώτους αριθμούς.*

□

Το παρακάτω Θεώρημα δίνει μία ικανή και αναγκαία συνθήκη για να είναι ένας φυσικός p πρώτος.

Θεώρημα 1.3 ***(Θεώρημα του Wilson)*** *Έναςακέραιος* $p > 1$ *είναι πρώτος, αν και μόνο αν, ισχύει*

$$(p-1)! \equiv -1 \pmod p.$$

Πόρισμα 1.5 *Για κάθε πρώτο αριθμό* p *ισχύει*

$$(p-2)! \equiv 1 \pmod p.$$

Παράδειγμα 1.19 *Εάν* $0 < s < p$, *όπου* p *πρώτος αριθμός, να αποδειχθεί ότι ισχύει*

$$(s-1)!(p-s)! + (-1)^{s-1} \equiv 0 \pmod p.$$

Απόδειξη :

Για $s = 1$ *η Πρόταση είναι αληθής λόγω του θεωρήματος* $Wilson$. *Υποθέτουμε ότι ισχύει*

$$(s-2)!(p-(s-1))! + (-1)^{s-2} \equiv 0 \pmod p$$

οπότε έχουμε τις συνεπαγωγές

$$\begin{aligned}
& (s-2)!(p-s+1)! + (-1)^{s-2} \equiv 0 \pmod p \\
\Rightarrow\ & (s-2)!(p-s)!(p-s+1) + (-1)^{s-2} \equiv 0 \pmod p \\
\Rightarrow\ & (s-2)!(p-s)!p - (s-2)!(p-s)!(s-1) + (-1)^{s-2} \equiv 0 \pmod p \\
\Rightarrow\ & -(s-2)!(s-1)(p-s)! + (-1)^{s-2} \equiv 0 \pmod p \\
\Rightarrow\ & (s-1)!(p-s)! - (-1)^{s-2} \equiv 0 \pmod p \\
\Rightarrow\ & (s-1)!(p-s)! + (-1)^{s-1} \equiv 0 \pmod p
\end{aligned}$$

άρα η Πρόταση ισχύει για κάθε s με $0 < s < p$.

Παρατήρηση: *Η Πρόταση ισχύει και για $s = p$. Πράγματι,*

$$(p-1)!0! + (-1)^{p-1} = (p-1)! + 1 \equiv 0 \pmod{p}.$$

□

Πρόταση 1.13 *Έστω p ένας περιττός πρώτος. Τότε*

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 = \begin{cases} -1 \pmod{p}, \text{αν } p \equiv 1 \pmod{4} \\ 1 \pmod{p}, \text{αν } p \equiv 3 \pmod{4} \end{cases}$$

Παράδειγμα 1.20 *Έστω p πρώτος > 2. Να δείξετε ότι*

$$(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}.$$

Απόδειξη:

Καθώς $1+2+\cdots+(p-1) = \dfrac{p(p-1)}{2}$, αρκεί να δείξουμε ότι

$$\frac{p(p-1)}{2} | (p-1)! - (p-1).$$

Από το Θεώρημα $Wilson$, έχουμε $(p-1)! \equiv -1 \pmod{p}$, απ' όπου $p|(p-1)! + 1$ και επομένως $p|(p-1)! - (p-1)$. Επίσης, $(p-1)! - (p-1) = (p-1)\left((p-2)! - 1\right)$, απ' όπου $p-1|(p-1)! - (p-1)$. Επειδή $(p, p-1) = 1$, παίρνουμε

$$p(p-1)|(p-1)! - (p-1).$$

Καθώς ο πρώτος p είναι περιττός, έπεται ότι ο αριθμός $(p-1)/2$ είναι ακέραιος και κατά συνέπεια ισχύει

$$\frac{p(p-1)}{2} | (p-1)! - (p-1).$$

□

Από τα σπουδαιότερα θεωρήματα της στοιχειώδους Θεωρίας Αριθμών είναι το ακόλουθο, που είναι γνωστό ως Μικρό Θεώρημα του $Fermat$

Θεώρημα 1.4 ***(Μικρό Θεώρημα Fermat)*** *Έστω p ένας πρώτος και a ένας ακέραιος με $p \nmid a$. Τότε*

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

Πόρισμα 1.6 *Έστω p ένας πρώτος. Τότε για κάθε $a \in \mathbb{Z}$ ισχύει*

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

Πρόταση 1.14 *Εάν p είναι ένας πρώτος αριθμός και $a_1, \ldots, a_n$ ακέραιοι αριθμοί, τότε ισχύει*

$$(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \pmod{p}.$$

Παράδειγμα 1.21 *Εάν για το φυσικό αριθμό n ισχύει*

$$5 \not| n-1,\ 5 \not| n,\ 5 \not| n+1,$$

να αποδειχθεί ότι $5|n^2+1$.

Απόδειξη:

Επειδή $5 \not| n$, από το Μικρό Θεώρημα του $Fermat$, ισχύει

$$n^4 \equiv 1 \pmod{5} \text{ άρα } (n-1)(n+1)(n^2+1) \equiv 0 \pmod{5}$$

οπότε, επειδή $5 \not| n-1,\ 5 \not| n+1$, έχουμε το ζητούμενο.

□

Η γενίκευση του Μικρού Θεωρήματος του $Fermat$ είναι γνωστό ως Θεώρημα $Euler$.

Θεώρημα 1.5 ***(Θεώρημα Euler)*** *Έστω n ένας φυσικός > 1 και a ένας ακέραιος τέτοιος, ώστε $(a, n) = 1$. Τότε*

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

Παράδειγμα 1.22 *Να υπολογίσετε το υπόλοιπο της διαίρεσης του 10^{6k+4}, όπου $k \in \mathbb{N}$, με το 7.*

Λύση:

Καθώς $(10, 7) = 1$, το Μικρό Θεώρημα $Fermat$ δίνει $10^6 \equiv 1 \pmod{7}$, απ' όπου $10^{6k} \equiv 1 \pmod{7}$. Επίσης

$$10^4 \equiv 3^4 = 9^2 \equiv 2^2 = 4 \pmod{7}.$$

Άρα

$$10^{6k+4} \equiv 4 \pmod{7}$$

και επομένως το ζητούμενο υπόλοιπο είναι το 4.

□

Παράδειγμα 1.23 *Να δείξετε ότι ο αριθμός* $\dfrac{7 \cdot 1968^{1968} - 3 \cdot 68^{78}}{10}$ *είναι ακέραιος.*

Απόδειξη :

Αρκεί να δείξουμε ότι

$$10 | 7 \cdot 1968^{1968} - 3 \cdot 68^{78}.$$

Το Μικρό Θεώρημα του $Fermat$ *δίνει* $3^4 \equiv 1 \pmod 5$. *Επομένως*

$$1968^{1968} \equiv 3^{1968} = \left(3^4\right)^{492} \equiv 1 \pmod 5.$$

Επίσης, έχουμε

$$68^{78} \equiv 3^{78} = 9 \cdot \left(3^4\right)^{19} \equiv 9 \equiv 4 \pmod 5,$$

οπότε

$$7 \cdot 1968^{1968} - 3 \cdot 68^{78} \equiv 7 - 3 \cdot 4 = -5 \equiv 0 \pmod 5.$$

Δηλαδή

$$5 | 7 \cdot 1968^{1968} - 3 \cdot 68^{78}.$$

Καθώς ο ακέραιος $7 \cdot 1968^{1968} - 3 \cdot 68^{78}$ *είναι άρτιος και* $(2, 5) = 1$ *παίρνουμε*

$$10 | 7 \cdot 1968^{1968} - 3 \cdot 68^{78}.$$

□

Παράδειγμα 1.24 *Να δείξετε ότι για κάθε ακέραιο* n *ισχύει*

$$2730 | n^{13} - n.$$

Απόδειξη :

Η πρωτογενής ανάλυση του 2730 είναι $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. *Καθώς οι ακέραιοι* $2, 3, 5, 7, 13$ *είναι πρώτοι μεταξύ τους ανά δύο αρκεί να δείξουμε ότι καθένας απ' αυτούς διαιρεί τον* $n^{13} - n$.

Παρατηρούμε ότι αν ο n *είναι άρτιος τότε και ο* $n^{13} - n$ *είναι άρτιος. Επίσης, εάν ο* n *είναι περιττός, τότε ο* $n^{13} - n$ *είναι άρτιος. Άρα για κάθε*

$n \in \mathbb{Z}$ *ισχύει* $2|n^{13} - n$. *Από το Πόρισμα* (1.6) *έχουμε ότι για κάθε* $n \in \mathbb{Z}$, *ισχύουν*

$$n^3 \equiv n \pmod 3,\ n^5 \equiv n \pmod 5,\ n^7 \equiv n \pmod 7,\ n^{13} \equiv n \pmod{13}.$$

Άρα

$$\begin{aligned} n^{13} &\equiv n \cdot \left(n^3\right)^4 \equiv n \cdot n^4 = n^3 \cdot n^2 \equiv n^3 \equiv n \pmod 3 \\ n^{13} &\equiv n^3 \cdot \left(n^5\right)^2 \equiv n^3 \cdot n^2 = n^5 \equiv n \pmod 5 \\ n^{13} &\equiv n^6 \cdot n^7 \equiv n^6 \cdot n = n^7 \equiv n \pmod 7 \end{aligned}$$

οπότε

$$3|n^{13} - n,\ \ 5|n^{13} - n,\ \ 7|n^{13} - n,\ \ 13|n^{13} - n.$$

□

Παράδειγμα 1.25 *Έστω* p *πρώτος. Να αποδείξετε ότι* $p|ab^p - ba^p$ *για όλους τους ακεραίους* a, b.

Απόδειξη:

Ας σημειώσουμε αρχικά ότι $ab^p - ba^p = ab(b^{p-1} - a^{p-1})$.

Εάν $p|ab$ *τότε* $p|ab^p - ba^p$, *ενώ εάν* $p \nmid ab$ *τότε* $(p, a) = (p, b) = 1$ *συνεπώς από το Μικρό Θεώρημα του* $Fermat$ *έχουμε* $b^{p-1} \equiv a^{p-1} \equiv 1 \pmod p$. *Άρα* $p|b^{p-1} - a^{p-1}$ *που δίνει ότι* $p|ab^p - ba^p$ *και έτσι σε κάθε περίπτωση* $p|ab^p - ba^p$.

□

Παράδειγμα 1.26 *(Εσωτερικός Διαγωνισμός Ε.Μ.Ε. 1995) Εάν* p *πρώτος αριθμός με* $p > 3$, *να αποδείξετε ότι* $20p|5^p - 4^p - 1$.

Απόδειξη:

Εάν $p = 5$ *τότε το αποτέλεσμα ισχύει. Έστω λοιπόν* $p \geq 7$. *Τότε*
$5^p - 4^p - 1 \equiv 0 - (-1)^p - 1 = 0 \pmod 5$
$5^p - 4^p - 1 \equiv 1^p - 0 - 1 = 0 \pmod 4$
και τέλος, λόγω του Πορίσματος 1.6, *παίρνουμε* $5^p \equiv 5 \pmod p$ *και* $4^p \equiv 4 \pmod p$ *άρα* $5^p - 4^p - 1 \equiv 5 - 4 - 1 = 0 \pmod p$ *και επειδή* $(4, 5, p) = 1$ *παίρνουμε ότι* $20p|5^p - 4^p - 1$.

Άσκηση: *(2ος Εσωτερικός διαγωνισμός Ε.Μ.Ε. 1989) Εάν* p *πρώτος να αποδείξετε ότι* $42p|3^p - 2^p - 1$. *(Υπόδειξη: Για να δείξετε ότι* $7|3^p - 2^p - 1$, *χρησιμοποιήστε την Πρόταση* 1.2*).*

□

Παράδειγμα 1.27 *Έστω $p \geq 7$ ένας πρώτος. Να αποδείξετε ότι ο αριθμός*

$$\underbrace{11\ldots1}_{p-1 \quad \text{μονάδες}}$$

διαιρείται από το p.

Απόδειξη:

Έχουμε

$$\underbrace{11\ldots1}_{p-1 \quad \text{μονάδες}} = \frac{10^{p-1}-1}{9}$$

και το συμπέρασμα προκύπτει από το Μικρό Θεώρημα του $Fermat$ [4].

□

Παράδειγμα 1.28 *Έστω p ένας πρώτος με $p > 5$. Να αποδείξετε ότι $p^8 \equiv 1 \pmod{240}$.*

Απόδειξη:

Η πρωτογενής ανάλυση του 240 είναι $240 = 2^4 \cdot 3 \cdot 5$. Από το Μικρό Θεώρημα του $Fermat$, έχουμε $p^2 \equiv 1 \pmod 3$ και $p^4 \equiv 1 \pmod 5$. Επειδή ένας θετικός ακέραιος είναι πρώτος προς το 2^4 αν και μόνο αν είναι περιττός $\phi(2^4) = 2^3$ και έτσι λόγω του θεωρήματος $Euler$, έχουμε $p^8 \equiv 1 \pmod{16}$. Συνεπώς $p^8 \equiv 1 \pmod m$ για $m = 3, 5, 16$ των οποίων το Ε.Κ.Π. είναι το 240 και έτσι $p^8 \equiv 1 \pmod{240}$.

Παρατήρηση: *Δεν είναι δύσκολο να δούμε ότι $n^4 \equiv 1 \pmod{16}$ για $n \equiv \pm1, \pm3, \pm5, \pm7 \pmod{16}$. Συνεπώς μπορούμε να βελτιώσουμε το αποτέλεσμα της άσκησης σε $p^4 \equiv 1 \pmod{240}$ για όλους τους πρώτους $p > 5$.*

□

Παράδειγμα 1.29 *Να αποδείξετε ότι για κάθε άρτιο θετικό ακέραιο n ισχύει*

$$n^2 - 1 | 2^{n!} - 1.$$

Απόδειξη:

[4] Ας σημειωθεί ότι $(10, p) = 1$

Θέτουμε $m = n + 1$. *Θέλουμε τότε να δείξουμε ότι* $m(m-2)|2^{(m-1)!} - 1$. *Επειδή* $\phi(m)|(m-1)!$, *έχουμε* $2^{\phi(m)} - 1|2^{(m-1)!} - 1$ *και από το θεώρημα του* $Euler$ *έχουμε* $m|2^{\phi(m)} - 1$. *Έτσι, προκύπτει ότι* $m|2^{(m-1)!} - 1$. *Όμοια,* $m - 2|2^{(m-1)!} - 1$ *και επειδή ο* m *είναι περιττός, παίρνουμε* $(m, m-2) = 1$, *άρα το ζητούμενο αποτέλεσμα.*

□

Παράδειγμα 1.30 *Έστω* p *ένας πρώτος της μορφής* $3k+2$ *ο οποίος διαιρεί το* $a^2 + ab + b^2$ *για κάποιους ακεραίους* a, b. *Αποδείξτε ότι οι* a, b *είναι και οι δύο διαιρετοί από το* p.

Απόδειξη:

Ας υποθέσουμε ότι ο p *δεν διαιρεί το* a. *Επειδή* $p|a^2 + ab + b^2$, *άρα ο* p *διαιρεί και το* $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$, *συνεπώς* $a^3 \equiv b^3 \pmod{p}$. *Άρα*

$$a^{3k} \equiv b^{3k} \pmod{p} \quad (1)$$

Συνεπώς ο p *δεν διαιρεί ούτε το* b. *Από το Μικρό Θεώρημα του* $Fermat$ *έχουμε* $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$, *ή*

$$a^{3k+1} \equiv b^{3k+1} \pmod{p} \quad (2)$$

Επειδή ο p *είναι πρώτος προς το* a, *και λόγω των* (1), (2) *παίρνουμε* $a \equiv b \pmod{p}$. *Το τελευταίο σε συνδυασμό με το* $a^2 + ab + b^2 \equiv 0 \pmod{p}$ *δίνει* $3a^2 \equiv 0 \pmod{p}$. *Έτσι, αφού* $p \neq 3$, *είναι* $p|a$, *άτοπο.*

□

Με όμοιο τρόπο όπως την παραπάνω να λύσετε την επόμενη άσκηση η οποία ήταν θέμα της 3ης Προκαταρτικής Φάσης της 13ης Εθνικής Μαθηματικής Ολυμπιάδας του 1996.

Άσκηση: Έστω p πρώτος αριθμός της μορφής $4k + 3$ ($k \in \mathbb{N}$). Εάν $x, y \in \mathbb{Z}$ και $p|x^2 + y^2$, να αποδείξετε ότι $p|x$ και $p|y$.

□

Παράδειγμα 1.31 *(Διεθνής Ολυμπιάδα Μαθηματικών 2005) Θεωρούμε την ακολουθία* $a_1, a_2, \ldots$ *που ορίζεται με τον τύπο*

$$a_n = 2^n + 3^n + 6^n - 1$$

για όλους τους θετικούς ακεραίους n. Να βρείτε τους θετικούς ακέραιους που είναι πρώτοι προς όλους τους όρους της ακολουθίας.

Λύση:

Η απάντηση είναι μόνο το 1. Αρκεί να δείξουμε ότι κάθε πρώτος p διαιρεί το a_n για κάποιο θετικό ακέραιο n. Ας σημειωθεί ότι οι $p = 2$ και $p = 3$ διαιρούν τον $a_2 = 48$.

Ας υποθέσουμε τώρα ότι $p \geq 5$. Τότε από το Μικρό Θεώρημα του $Fermat$ έχουμε $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod{p}$, οπότε

$$3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv 3 + 2 + 1 \equiv 0 \pmod{6}$$

δηλαδή $6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 0 \pmod{p}$, άρα $p|6a_{p-2}$. Επειδή $(p, 6) = 1$, έπεται ότι ο a_{p-2} διαιρείται από το p.

□

Παράδειγμα 1.32 *Εάν p είναι ένας πρώτος αριθμός, τότε οι αριθμοί*

$$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$$

διαιρούνται δια p.

Απόδειξη:

Για κάθε $s = 1, 2, \ldots, p-1$ ισχύει

$$\binom{p}{s} = \frac{p \cdot (p-1) \cdots (p-s+1)}{1 \cdot 2 \cdots s}$$

δηλαδή

$$1 \cdot 2 \cdots s \cdot \binom{p}{s} = p \cdot (p-1) \cdots (p-s+1).$$

Επειδή όμως $p|1 \cdot 2 \cdots s \cdot \binom{p}{s}$ και $p \not| 1 \cdot 2 \cdots s$, προκύπτει ότι

$$p| \binom{p}{s}.$$

□

Πρόταση 1.15 *Εάν p πρώτος, τότε*

$$x^{p-1} - 1 \equiv (x-1)(x-2) \cdots (x-(p-1)) \pmod{p}.$$

Πρόταση 1.16 *Έστω p περιττός πρώτος. Η ισοτιμία $x^2 \equiv -1 \pmod{p}$ έχει λύση αν και μόνο αν $p \equiv 1 \pmod{4}$.*

Βιβλιογραφία

[1] Δ. Πουλάκης, *Θεωρία Αριθμών*, Μία σύγχρονη θεώρηση της κλασικής Θεωρίας Αριθμών, Θεσσαλονίκη 1998.

[2] Κ. Λάκκη, *Θεωρία Αριθμών*, Θεσσαλονίκη 1991.

[3] Κ. Λάκκη, Γ. Τζιτζή, *Ασκήσεις Θεωρίας Αριθμών*, Θεσσαλονίκη 1991.

[4] Θ. Ν. Καζαντζή, *Θεωρία Αριθμών*, Εκδόσεις Μαθηματική Βιβλιοθήκη, Β΄ Έκδοση (1997).

[5] T. Andreescu, D. Andrica, Z. Feng, *104 Number Theory Problems, From the Training of the USA IMO Team*, $Birkhäuser$ 2007.