Ασκήσεις στην Θεωρία Αριθμών & Ομάδων

Αντώνης Αντωνόπουλος
CoReLab
aanton@corelab.ntua.gr

Άσκηση 1

Αν p πρώτος αριθμός, τότε $p = 2$ ή $p \equiv 1 \bmod 4$ ή $p \equiv 3 \bmod 4$.

Λύση

- Αν p άρτιος, τότε αναγκαστικά $p = 2$.
- Αν p περιττός, τότε η Ευκλείδεια Διαίρεση με το 4 δίνει: $p = 4k + r$, $0 \leq r \leq 3$.
  - Αν $r = 0$, τότε $p = 4k$ άτοπο.
  - Αν $r = 2$, τότε $p = 4k + 2 = 2(2k + 1)$, άτοπο.

  Άρα είτε $r = 1$ είτε $r = 3$, οπότε προκύπτει το ζητούμενο.

$\square$

Άσκηση 2

Ένας ακέραιος της μορφής $2^p - 1$, με p πρώτο, ονομάζεται *πρώτος του Mersenne*. Δείξτε ότι:

1. Αν $2^p - 1$ είναι πρώτος, τότε και ο p είναι πρώτος. Ισχύει και το αντίστροφο;
2. Αν $a, b \in \mathbb{N}$, τότε $2^a - 1 | 2^{ab} - 1$.

Λύση

1. Έστω, προς απαγωγή σε άτοπο, ότι ο $2^p - 1$ είναι πρώτος ενώ ο p *δεν* είναι. Τότε $\exists\, x, y > 1 : p = x \cdot y$. Άρα:

   $2^p - 1 = 2^{xy} - 1 = (2^x)^y - 1 = (2^x - 1)[2^{x(y-1)} + 2^{x(y-2)} + \cdots + 2^x + 1]$

   (χρησιμοποιώντας την γνωστή ταυτότητα $\alpha^n - \beta^n = (\alpha - \beta)[\alpha^{n-1} + \alpha^{n-2}\beta + \alpha^{n-3}\beta^2 + \cdots + \alpha\beta^{n-2} + \beta^{n-1}]$). Οπότε, παραγοντοποιήσαμε τον $2^p - 1$ σε γινόμενο δύο αριθμών μεγαλύτερων του 1, άρα είναι σύνθετος, άτοπο. Άρα ο p είναι πρώτος.

2. Έχουμε $2^{ab} - 1 = (2^a)^b - 1^b$.
   Λόγω της γνωστής ταυτότητας:

   $$\alpha^n - \beta^n = (\alpha - \beta)[\alpha^{n-1} + \alpha^{n-2}\beta + \alpha^{n-3}\beta^2 + \cdots + \alpha\beta^{n-2} + \beta^{n-1}] \Rightarrow$$

   $$\alpha - \beta | \alpha^n - \beta^n$$

   Άρα $2^a - 1 | (2^a)^b - 1^b$.

(Παρατηρήστε ότι μπορούμε να χρησιμοποιήσουμε το υποερώτημα 2. για να συνάγουμε το 1.: $2^p - 1 = 2^{xy} - 1$, και λόγω του 2. έχουμε ότι $2^x - 1 | 2^{xy} - 1$, άρα ο $2^p - 1$ *δεν* είναι πρώτος, άτοπο.)

$\square$

Άσκηση 3

1. Έστω $a, b \in \mathbb{N}$, με $a, b > 1$. Αν οι αναλύσεις των a, b σε γινόμενο πρώτων παραγόντων είναι: $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ και $b = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$ όπου p_i πρώτοι, δείξτε ότι:

$$(a, b) = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

όπου $t_i = \min\{e_i, h_i\}$, $i = 1, 2, \ldots, k$.

2. Δείξτε ότι $(a, b)^n = (a^n, b^n)$.

Λύση

1. Έστω $d = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, με $t_i = \min\{e_i, h_i\}$, όπως στην εκφώνηση. Αφού $\min\{e_i, h_i\} \le e_i$ και $\min\{e_i, h_i\} \le h_i$, θα έχουμε $d|a$ και $d|b$. Άρα ο d είναι κοινός διαιρέτης των a, b. Για να αποδείξουμε ότι είναι ο ΜΚΔ τους, πρέπει να δείξουμε ότι για κάθε d', με $d'|a \wedge d'|b$ έχουμε ότι $d' \le d$.

   Έστω $d' = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$. Αφού $d'|a \Rightarrow s_i \le e_i$, και αφού $d'|b \Rightarrow s_i \le h_i$, άρα και $s_i \le \min\{e_i, h_i\} \Rightarrow s_i \le t_i \Rightarrow p_i^{s_i} \le p_i^{t_i} \Rightarrow$

$$p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \le p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} \Rightarrow d' \le d$$

2. Αν $a = 1$, τότε $(1, b^n) = 1^n = (1, b)^n$, και ομοίως για $b = 1$. Έστω λοιπόν ότι $a, b > 1$: Θεωρούμε τις αναλύσεις των a, b σε γινόμενο πρώτων παραγόντων όπως στο προηγούμενο ερώτημα:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
$$b = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$$

   όπως και τον ΜΚΔ τους $d = (a, b) = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, με $t_i = \min\{e_i, h_i\}$, $i = 1, 2, \ldots, k$.

   Έχουμε $a^n = p_1^{ne_1} p_2^{ne_2} \cdots p_k^{ne_k}$ και $b^n = p_1^{nh_1} p_2^{nh_2} \cdots p_k^{nh_k}$, και αν $D = (a^n, b^n)$, τότε $D = p_1^{w_1} p_2^{w_2} \cdots p_k^{w_k}$, όπου $w_i = \min\{ne_i, nh_i\} = n \cdot \min\{e_i, h_i\} = nt_i$.Άρα:

$$D = p_1^{w_1} p_2^{w_2} \cdots p_k^{w_k} = p_1^{nt_1} p_2^{nt_2} \cdots p_k^{nt_k} = (p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k})^n = d^n$$

   Άρα $(a, b)^n = (a^n, b^n)$.

$\square$

Άσκηση 4

Έστω $a, b \in \mathbb{Z}$, τέτοιοι ώστε $ab \equiv 1 \bmod m$. Δείξτε ότι οι a, b έχουν την ίδια τάξη.

Λύση

Έστω z η τάξη του a και w η τάξη του b, με $z \neq w$. Τότε:

$$ab \equiv 1 \bmod m \Rightarrow ab - 1 = km, k \in \mathbb{Z} \Rightarrow ab + (-k)m = 1 \Rightarrow$$

$$(a, m) = 1 \wedge (b, m) = 1$$

Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $z < w$, άρα έχουμε:

$$a^z \equiv 1 \bmod m \ \wedge \ b^w \equiv 1 \bmod m \Rightarrow a^z b^w \equiv 1 \bmod m$$

$$\Rightarrow (a^z b^z) b^{w-z} \equiv 1 \bmod m \tag{1}$$

Αφού, εξ' υποθέσεως, $ab \equiv 1 \bmod m$, τότε και $(ab)^z \equiv 1 \bmod m$, άρα από την (1) έχουμε ότι $b^{w-z} \equiv 1 \bmod m$, που είναι *άτοπο*, αφού $w - z < z$, υποθέσαμε ότι η τάξη του b είναι w (δηλ. ο *ελάχιστος* θετικός ακέραιος για τον οποίο $b^w \equiv 1 \bmod m$). Άρα $z = w$. □

Άσκηση 5

Δείξτε ότι αν μια ομάδα $(G, *)$ έχει ως τάξη πρώτο αριθμό, τότε είναι κυκλική.

Λύση

Έστω ότι $|G| = p$, για p πρώτο. Αν $p = 1$, τότε $G = \{e\}$, που είναι κυκλική. Οπότε, έστω $p > 1$. Θεωρούμε ένα $x \in G, x \neq e$, και έστω k η τάξη του x.
Από το θ. Lagrange, γνωρίζουμε ότι η τάξη του στοιχείου μιας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας, οπότε $k|p$, και επειδή p πρώτος & $k \neq 1$ (αλλιώς $x^k = x = e$, άτοπο) έχουμε ότι $k = p$, το οποίο σημαίνει ότι το x είναι γεννήτορας της $(G, *)$, άρα είναι κυκλική. □

Άσκηση 6

Να δείξετε ότι η ισοτιμία $x^2 + 1 \equiv 0 \bmod p$, p περιττός πρώτος, έχει λύση αν και μόνο αν $p = 4k + 1, k \in \mathbb{Z}$.

Λύση

($\Rightarrow$) Έστω ότι η ισοτιμία $x^2 + 1 \equiv 0 \bmod p$ έχει λύση. Τότε, το -1 είναι τετραγωνικό υπόλοιπο modulo p. Οπότε $\left(\frac{-1}{p}\right) = 1 = (-1)^{\frac{p-1}{2}}$, άρα ο αριθμός $\frac{p-1}{2}$ είναι άρτιος, δηλαδή $\frac{p-1}{2} = 2k, k \in \mathbb{Z} \Rightarrow p = 4k + 1, k \in \mathbb{Z}$.

($\Leftarrow$) Έστω ότι $p = 4k + 1, k \in \mathbb{Z} \Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$, και επειδή p πρώτος: $\left(\frac{-1}{p}\right) = 1$, άρα το (-1) είναι τετραγωνικό υπόλοιπό, δηλαδή η εξίσωση $x^2 + 1 \equiv 0 \bmod p$ έχει λύση. $\square$

Άσκηση 7

Έστω η ομάδα $(G, \cdot)$. Αν $|G| = 3$, τότε:

1. Η ομάδα $(G, \cdot)$ είναι αβελιανή.
2. Αν $a \in G$, τότε $G = \{e, a, a^2\}$.

Λύση

Έστω $G = \{e, a, b\}$.

1. Από τον ορισμό του ουδέτερου στοιχείου, έχουμε ότι $a \cdot e = e \cdot a = a$ και $b \cdot e = e \cdot b = b$. Αρκεί, λοιπόν, να δείξουμε ότι $a \cdot b = b \cdot a$. Έχουμε 3 δυνατές περιπτώσεις:

   - $a \cdot b = a$
   - $a \cdot b = b$
   - $a \cdot b = e$

   Αναλυτικά:

   - $\mathbf{a} \cdot \mathbf{b} = \mathbf{a}$: Τότε $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot a \Rightarrow (a^{-1} \cdot a) \cdot b = e \Rightarrow e \cdot b = e \Rightarrow b = e$, άτοπο.
   - $\mathbf{a} \cdot \mathbf{b} = \mathbf{b}$: Τότε $(a \cdot b) \cdot b^{-1} = b \cdot b^{-1} \Rightarrow a \cdot (b \cdot b^{-1}) = e \Rightarrow a \cdot e = e \Rightarrow a = e$, άτοπο.

- $\mathbf{a \cdot b = e}$: Τότε $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot e \Rightarrow e \cdot b = a^{-1} \Rightarrow b = a^{-1} \Rightarrow b \cdot a = a^{-1} \cdot a \Rightarrow b \cdot a = e$, άρα $a \cdot b = b \cdot a$.

Άρα, οι $\binom{3}{2}$ συνδυασμοί στοιχείων είναι οι:

$$a \cdot e = e \cdot a$$

$$b \cdot e = e \cdot b$$

$$a \cdot b = b \cdot a$$

Άρα η $(G, \cdot)$ είναι αβελιανή.

2. Θα δείξουμε ότι $b = a^2$:

   - Έστω ότι $a^2 = a$: Τότε, $a = e$, άτοπο.
   - Έστω ότι $a^2 = e$: Τότε, αφού γνωρίζουμε από το 1. ότι $a \cdot b = e$, έχουμε ότι $a \cdot b = a^2 \Rightarrow a = b$, άτοπο.

   Άρα, $a^2 = b$, και $G = \{e, a, b\} = \{e, a, a^2\}$.

$\square$

Άσκηση 8

Δείξτε ότι αν ο $n > 1$ δεν έχει πρώτο διαιρέτη μικρότερο ή ίσο του $\sqrt{n}$, τότε ο n είναι πρώτος. (*Το κόσκινο του Ερατοσθένη*)

Λύση

Έστω ότι ο n είναι σύνθετος. Τότε, $n = xy, x, y > 1$. Αν $x > \sqrt{n} \wedge y > \sqrt{n} \Rightarrow n = xy > \sqrt{n} \cdot \sqrt{n} = n$, άτοπο. Άρα, $x \leq \sqrt{n} \vee y \leq \sqrt{n}$. Έστω $x \leq \sqrt{n}$. Τότε είτε ο x είναι πρώτος, είτε έχει πρώτο διαιρέτη $\leq \sqrt{n}$. $\square$

Άσκηση 9

Αν οι p και $2p-1$ είναι πρώτοι αριθμοί (*λέγονται και πρώτοι της Germaine*), δείξτε ότι $\phi(n) = \phi(n+2)$, όπου $n = 2(2p-1)$.

Λύση

Έχουμε ότι $\phi(n+2) = \phi(4p) = \phi(4)\phi(p) = 2(p-1)$.
Επειδή $2p-1$ πρώτος, έχουμε ότι $(2, 2p-1) = 1$, άρα: $\phi(n) = \phi(2(2p-1)) = \phi(2)\phi(2p-1) = 2p-2 = 2(p-1)$.
Άρα $\phi(n) = \phi(n+2) = 2(p-1)$. □

Άσκηση 10

Αν το στοιχείο a μιας ομάδας $(G, \cdot)$ έχει τάξη n, δείξτε ότι:

1. το στοιχείο a^k έχει τάξη $\frac{n}{(n,k)}$.
2. $|\langle a\rangle / \langle a^k\rangle| = (n, k)$

(*Συμβολίζουμε με* $\langle a\rangle$ *την κυκλική ομάδα που παράγεται από το* a.)

Λύση

1. Έστω x η τάξη του a^k, και $d = (n, k)$. Τότε έχουμε ότι $n = \lambda d$ και $k = \mu d$, με $(\lambda, \mu) = 1$ (*γιατί;*).

   Έχουμε ότι $(a^k)^\lambda = a^{k\lambda} = a^{\mu d\lambda} = (a^{d\lambda})^\mu = (a^n)^\mu = e^\mu = e$

   Επίσης, από την στιγμή που η τάξη του a^k είναι x, έχουμε ότι, αφού η τάξη του a είναι n:
   $$(a^k)^x = a^{kx} = e \Rightarrow n|kx$$

   Άρα $n|kx \Rightarrow \lambda d|kx \Rightarrow \lambda d|\mu dx \Rightarrow \lambda|\mu x$, και επειδή $(\lambda, \mu) = 1$ έχουμε ότι $\lambda|\mu x \Rightarrow \lambda|x$.

   Επειδή όμως $(a^k)^\lambda = 1$, έχουμε και ότι $x|\lambda$.

   Άρα, έχουμε ότι:

   $$\lambda|x \ \wedge \ x|\lambda \Rightarrow x = \lambda = \frac{n}{d} = \frac{n}{(n,k)}$$

2. Η ομάδα $\langle a^k \rangle$ είναι *υποομάδα* της $\langle a \rangle$ (*γιατί;*).
   Χρησιμοποιώντας το θ. Lagrange, έχουμε ότι:

$$|\langle a \rangle| = |\langle a \rangle / \langle a^k \rangle| \cdot |\langle a^k \rangle|$$

.

$\square$