ΜΗΥΠ 416 – ΚΡΥΠΤΟΓΡΑΦΙΑ

Χρήστος Κακλαμάνης
Καθηγητής

Παύλος Σπυράκης
Καθηγητής

Μάιος 2002

Ασκήσεις

1. Δώστε όλες τις υποομάδες των Z_{11} και Z_{17}^*.

2. Έστω ότι υπάρχει ακέραιος n_0 τέτοιος ώστε να ισχύουν $gcd(p^{ab}, ab) = p$ για κάθε πρώτο $p \leq n_0$ και $gcd(p^{ab}, ab) = 1$ για κάθε πρώτο $p > n_0$. Δείξτε ότι $gcd(a, b) = 1$.

3. Είναι ομάδα το σύνολο Z_n εφοδιασμένο με την πράξη του πολλαπλασιασμού; Εξηγήστε.

4. Βρείτε τις λύσεις της εξίσωσης $21x = 12 \pmod{45}$.

5. Έστω m ένας σύνθετος ακέραιος. Δείξτε ότι τουλάχιστον $\sqrt{m}$ στοιχεία του Z_m δεν έχουν πολλαπλασιαστικό αντίστροφο.

6. Δείξτε ότι ανάμεσα σε δύο συνεχόμενους πρώτους υπάρχουν αυθαίρετα πολλοί ακέραιοι.

7. Δείξτε πώς μπορεί να υπολογιστεί το $\alpha^{-1} \mod n$ για κάθε $\alpha \in Z_n^*$, χρησιμοποιώντας την ρουτίνα MODULAR– EXPONENTIATION. Υποθέστε ότι γνωρίζετε το $\phi(n)$.

8. Δείξτε ότι $gcd(a, b) = 1$ αν και μόνο αν $gcd(ab, a + b) = 1$.

9. Δείξτε ότι $gcd(2^s - 1, 2^t - 1) = 1$ αν και μόνο αν $gcd(s, t) = 1$.

10. Λύστε το σύστημα εξισώσεων

$$x = 2 \pmod{3}$$
$$x = 5 \pmod{7}$$
$$x = 3 \pmod{11}$$

Παράδοση : Δευτέρα, 27/05/2002 ώρα 15:00

Άσκηση 1

Δώστε όλες τις υποομάδες των Z_{11} και Z_{17}^*

Λύση

Μπορούμε να παράγουμε μια υποομάδα από κάποιο στοιχείο a μια ομάδας με τον εξής τρόπο:

$$\langle a \rangle = \{ a^{(k)} : k \geq 1 \}$$

όπου $a^{(k)} = \bigoplus_{i=1}^{k} a = \underbrace{a \oplus a \oplus \cdots \oplus a}_{k}$ $\quad k \geq 1$

Εφαρμόζοντας το πιο πάνω για ομάδα Z_i, έχουμε:

$$a^{(k)} = k\,a \bmod i \qquad k \geq 1$$

Οπότε για το Z_{11}, έχουμε:

$Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ Άρα οι υποομάδες είναι

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle = \langle 9 \rangle = \langle 10 \rangle$

$= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Για μια ομάδα Z_i^*, έχουμε: $a^{(k)} = a^k \bmod i$

Έτσι για το Z_{17}^*, έχουμε:

$Z_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{2, 4, 8, 16, 15, 13, 9, 1\} = \langle 8 \rangle = \langle 9 \rangle = \langle 15 \rangle$

$\langle 3 \rangle = \langle 5 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 10 \rangle = \langle 11 \rangle = \langle 12 \rangle = \langle 14 \rangle =$

$= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

$\langle 4 \rangle = \langle 13 \rangle = \{1, 4, 13, 16\}$

$\langle 16 \rangle = \{16, 1\}$

∎

Άσκηση 2

Έστω ότι υπάρχει ακέραιος n_0 τέτοιος ώστε να ισχύουν $\gcd(p^{ab}, ab) = p$ για κάθε πρώτο $p \leq n_0$ και $\gcd(p^{ab}, ab) =$ για κάθε πρώτο $p > n_0$. Δείξτε ότι $\gcd(a, b) = 1$.

Λύση

Για να δείξουμε ότι a και b είναι πρώτα μεταξύ τους, αρκεί να δούμε την πληροφορία που "κρύβουν" τα 2 gcd που δίνονται για τιμές του $p \leq n_0$ και $p > n_0$.

Από το γεγονός ότι $\gcd(p^{ab}, ab) = p$ καταλαβαίνουμε ότι $ab \neq 1$ γιατί αλλιώς θα είχαμε για όλες τις τιμές του p το αποτέλεσμα που έχουμε όταν $p > n_0$, δηλ. $\gcd(p^{ab}, ab) = 1$.

Έτσι αφού $ab \geq 2$ συμβαίνει ότι και $p^{ab} \geq p^2$.

Επίσης από την θεωρία αριθμών ξέρουμε ότι το ab μπορεί να γραφεί σαν γινόμενο πρώτων υψωμένων σε κάποιες δυνάμεις, δηλ. $ab = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_k^{\varepsilon_k}$ με $\varepsilon_i = 1 - m$. Όμως από το γεγονός ότι $\gcd(p^{ab}, ab) = 1$ όταν $p > n_0$ καταλαβαίνουμε ότι το γινόμενο πρώτων που ~~δίνει~~ παράγει το ab δεν περιέχει πρώτο μεγαλύτερο ή ίσο με n_0 διαφορετικά p^{ab} και ab δεν θα είχαν πάντα πρώτο μεταξύ τους όπως συμβαίνει. Επίσης από το γεγονός ότι $\gcd(p^{ab}, ab) = p$ για $p \leq n_0$ συμβαίνει ότι το ab δεν περιέχει καμία πρώτο υψωμένο σε δύναμη $\varepsilon > 1$. Αν αυτό ~~[illegible]~~ μπορούσε να συμβεί τότε θα είχαμε το $\gcd(p^{ab}, ab)$ να ισούται με p^{ε}. Και όμως που δεν συμβαίνει.

Τελικά καταλήξαμε στο γεγονός ότι το ab είναι της μορφής: $ab = p_1 p_2 \dots p_k$ με $p_i \leq n_0$. Τα a και b με την σειρά τους χτίζονται σαν γινόμενα κάποιων από αυτούς τους πρώτους και το δεύτερο με τους υπόλοιπους. Άρα γιατί δεν έχουν κανένα κοινό πρώτο και είναι $a = p_1 p_2 \dots p_m$, $b = p_{m+1} \dots p_k$ τότε είναι πρώτοι μεταξύ τους και $\gcd(a, b) = 1$.

Άσκηση 3

Είναι ομάδα το σύνολο Z_n εφοδιασμένο με την πράξη του πολλαπλασιασμού; Εξηγήστε.

Λύση:

Για να είναι ένα σύνολο ομάδα ως προς μια πράξη πρέπει να είναι εφοδιασμένο με τις ιδιότητες της κλειστότητας, της προσεταιριστικότητας μεταξύ των στοιχείων του, να έχει μοναδιαίο στοιχείο και κάθε στοιχείο του να έχει αντίστροφο.

Πρέπει να δούμε αν ισχύουν οι πιο πάνω ιδιότητες για το σύνολο Z_n ως προς την πράξη του πολλαπλασιασμού.

Η κλειστότητα ισχύει αφού αν πολλαπλασιάσουμε $[a]_n, [b] \in Z$ τότε παίρνουμε $[ab]_n \in Z_n$.

Η προσεταιριστικότητα είναι εύκολο να διαπιστωθεί όπως και η υπαρξη μοναδιαίου στοιχείου όπως είναι το $[1]_n$ αφού $[a]_n [1]_n = [a \cdot 1]_n = [a]$

Για να έχει αντίστροφο ένα στοιχείο $[a]_n$ του Z_n πρέπει να ισχύει ότι υπάρχει $[b]_n$ τέτοιο ώστε $[a]_n [b]_n = [1]$

Άρα $[ab]_n = [1]_n \Rightarrow ab = 1 \mod n \Rightarrow n \mid (ab-1)$.

Εξετάζουμε αν ισχύει για το $[0]_n$ που ανήκει σε όλα τα Z.

Έχουμε: $n \mid (0-1) \Rightarrow n \mid -1 \Rightarrow n = 1$

Άρα αντίστροφο υπάρχει μόνο αν $n = 1$. Άρα το $[0]_n$ δεν έχει αντίστροφο για κάθε τιμή του n. Έτσι αφού έστω και ένα στοιχείο του Z_n $(n \neq 1)$ δεν έχει αντίστροφο τότε δεν ισχύει η τέταρτη ιδιότητα.

Άρα το σύνολο Z_n εφοδιασμένο με την πράξη του πολλ/μου <u>δεν</u> αποτελεί ομάδα.

Άσκηση 4

Βρείτε τις λύσεις της εξίσωσης $21X = 12 \pmod{45}$

Λύση

Θα βρούμε την λύση της εξίσωσης εφαρμόζοντας τύπους με τον αλγόριθμο MODULAR-LINEAR-EQUATION-SOLVER(a, b, n) όπως αυτός δίνεται στην θεωρία.

Έχουμε $a=21$, $b=12$ και $n=45$

Με αυτά σαν παράμετρους καλούμε τον Extended-Euclid(a,

Κατά την εκτέλεση του παίρνουμε τα πιο κάτω αποτελέσματα

a	b	$\lfloor a/b \rfloor$	d	x	y
21	45	0	3	-2	1
45	21	2	3	1	-2
21	3	7	3	0	1
3	0	–	3	1	0

Άρα η λύση της μας επιστρέφει $(d, x', y') = (3, -2, 1)$

Ο αλγόριθμος συνεχίζει αν $d \mid b$. Όντως είναι $3 \mid 45$ και έτσι αναθέτουμε στο X_0 την τιμή: $X_0 = x'(b/d) \bmod 45$

$X_0 = -2(4) \bmod 45$

$X_0 = 37$

Τέλος για τιμές του $i = 0$ έως $d-1 = 2$ έχουμε τις λύσεις

$X_0 + i(n/d) \bmod n \Rightarrow 37 + i\,15 \bmod 45$

Άρα οι λύσεις είναι $i=0 \Rightarrow 37$

$i=1 \Rightarrow 7$

$i=2 \Rightarrow 22$

Άσκηση 5

Έστω m ένας σύνθετος ακέραιος. Δείξτε ότι τουλάχιστον $\sqrt{m}$ στοιχεία του Z_m δεν έχουν πολλαπλασιαστικό αντίστροφο

Λύση

Γνωρίζουμε ότι το σύνολο Z_m^* είναι ομάδα μι φα τα απορέτητα χαρακτηριστικά. Άρα κάθε στοιχείο του έχει πολλαπλασιαστικό αντίστροφο.

Ξέρουμε επίσης ότι $Z_m^* \subset Z_m$. Άρα ο αριθμός στοιχείων του Z_m που δεν έχουν πολλαπλασιαστικό αντίστροφο είναι

$$|Z_m| - |Z_m^*| = m - \varphi(m) = m - m\prod_{p|m}\left(1-\frac{1}{p}\right) = A$$

Η συνάρτηση $\varphi(n)$ του Euler, ως γνωστό δίνει τον αριθμό στοιχείων μια Z_n^* ομάδας. Το p σε αυτήν συμβολίζει όλους τους πρώτους που διαιρούν το n.

Στην περίπτωση μας το m είναι σύνθετος άρα μπορεί να γραφεί σαν γινόμενο πρώτων αριθμών. Από αυτού για το γινόμενο στην σχέση $\varphi(m)$ κρατάμε μόνο τον μικρότερο από αυτούς K για το οποίο ισχύει $K \leq \sqrt{m}$, αφού αν δεν ήταν θα πολλαπλασιαζόταν με κάποιο μεγαλύτερο από $\sqrt{m}$ και θα πέρναμε αριθμό μεγαλύτερο από m.

Επομένως από την προηγούμενη σχέση έχουμε:

$$A = m - m\prod_{p|m}\left(1-\frac{1}{p}\right) \geq m - m\left(1-\frac{1}{K}\right) = \cancel{m} - \cancel{m} + \frac{m}{K} \geq \sqrt{m}$$

Άρα τελικά τα στοιχεία χωρίς πολ/κο αντίστροφο στο Z_m είναι τουλάχιστον $\sqrt{m}$

Άσκηση 6

Δείξτε ότι ανάμεσα σε δυο συνεχόμενους πρώτους υπάρχουν αυθαίρετα πολλοί ακέραιοι.

Λύση

Συμβολίζουμε τον σύνθετο αριθμό ανάμεσα σε 2 πρώτους αριθμούς με $g(p)$, που χωρίζουν τον p από τον επόμενο πρώτο. Άρα $p_{n+1} = g(p_n) + p_n$ ($g(p)$ είναι το πλήθος των σύνθετων)

Θέλουμε να δείξουμε ότι το $g(p)$ είναι αυθαίρετα μεγάλο.

Θεωρούμε ένα ακέραιο $n > 1$ και έστω η ακολουθία συνεχόμενων ακεραίων $n!+2, n!+3, n!+4 \dots n!+n$

Σε αυτή την ακολουθία έχουμε:

$$\left.\begin{array}{ll} n!+2 & \text{διαιρείται με το } 2 \\ n!+3 & \text{διαιρείται με το } 3 \\ \vdots & \\ n!+n & \text{διαιρείται με το } n \end{array}\right\} \Rightarrow \text{Οι αριθμοί } n!+2 \text{ έως το } n!+n \text{ είναι σύνθετοι}$$

Εάν πούμε ότι p είναι ο μεγαλύτερος πρώτος, που είναι μικρότερος από το $n!+2$ τότε μέχρι τον επόμενο πρώτο υπάρχουν $g(p) > n-1$ σύνθετοι αριθμοί.

Βρήκαμε λοιπόν ότι οι σύνθετοι αριθμοί ανάμεσα σε δυο συνεχόμενους πρώτους είναι αυθαίρετα πολλοί σε πλήθος και εξαρτώνται από το n.

Άσκηση 7

Δείξτε πώς μπορεί να υπολογιστεί το $a^{-1} \bmod n$ για κάθε $a \in Z_n^*$ χρησιμοποιώντας την ρουτίνα MODULAR-EXPONENTIA
Υποθέστε ότι γνωρίζετε το $\varphi(n)$

Λύση

Η πιο πάνω ρουτίνα παρέχει ένα τρόπο υπολογισμού του $a^b \bmod n$, όπου a και b είναι μη αρνητικοί ακέραιοι και n ένας θετικός ακέραιος.

Για να μπορεί να υπολογίσει το $a^{-1} \bmod n$ πρέπει να το φέρουμε σε μορφή, αποδεκτή από την ρουτίνα.

Έτσι αφού $a \in Z_n^*$ σημαίνει ότι a και n είναι πρώτοι μεταξύ τους. Δηλ. $\gcd(a, n) = 1$.

Σύμφωνα με το θεώρημα του Euler, για ακέραιο $n > 1$ και για κάθε $a \in Z_n^*$ ισχύει $a^{\varphi(n)} = 1 \pmod n$

Άρα μπορούμε να γράψουμε: $a^{\varphi(n)} a^{-1} \equiv a^{-1} \pmod n$

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

Το δεύτερο μέρος της ισότητας είναι αυτό που ψάχνουμε να υπολογίσουμε και βλέπουμε ότι: $a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$

Το δεύτερο μέρος της τελευταίας ισότητας μπορεί να υπολογιστεί από την MODULAR-EXPONENTIATION και επομένως μπορούμε να υπολογίσουμε το $a^{-1} \bmod n$, υπολογίζοντας το ίδιο πρώτα από, $a^{\varphi(n)-1} \bmod n$.

Άσκηση 8

Δείξτε ότι $\gcd(a,b)=1$ αν και μόνον αν $\gcd(ab, a+b)=1$

Λύση

Για να αποδείξουμε ότι το ζητούμενο ισχύει πρέπει να δείξουμε πως μπορούμε να πάμε από την πρώτη σχέση στη δεύτερη αλλά και το αντίστροφο.

Πρώτο μέρος ($\Leftarrow$): Αφού $\gcd(ab, a+b)=1$ τότε σύμφωνα με το θεώρημα η μικρότερη θετική τιμή του γραμμικού συνδυασμού των ab και $a+b$ είναι ίση με τον μέγιστο κοινό διαιρέτη τους. Δηλ. $abx+(a+b)y=1$
$\Rightarrow abx+ay+by=1 \Rightarrow a(bx+y)+by=1 \Rightarrow$ Έχουμε γραμμικό συνδυασμό των a και b που δίνει 1 που είναι ο μικρότερος θετικός. Άρα $\gcd(a,b)=1$.

Δεύτερο μέρος ($\Rightarrow$): Έστω ότι $\gcd(a,b)=1$. Αν θεωρήσουμε ότι $\gcd(a, a+b)\neq 1$ (δηλ. a και $a+b$ δεν είναι πρώτα μεταξύ τους) τότε υπάρχει ένα m τέτοιο ώστε (α) $k|a$, (β) $k|a+b$ και επομένως από το γράμμα έχουμε $k|(a+b-a) \Rightarrow k|b$ (γ). Συνδιάζοντας τα (α) και (γ) βρίσκουμε ότι $\gcd(a,b)\neq 1$ κάτι που έρχεται σε αντιπαράθεση με την αρχική υπόθεση. Επομένως $\gcd(a, a+b)=1$. Εργαζόμενοι με τον ίδιο τρόπο βρίσκουμε $\gcd(b, a+b)=1$.
Συνδιάζοντας τις δύο τελευταίες σχέσεις και από το θεώρημα συμπαιρένουμε: $\gcd(ab, a+b)=1$ αν $\gcd(a,b)=1$

Άσκηση 9

Δείξτε ότι $\gcd(2^s-1, 2^t-1)=1$ αν και μόνο αν $\gcd(s,t)=1$

Λύση

Ξεκινάμε από το ότι s και t είναι πρώτα μεταξύ τους. Τότε $\gcd(s,t)=1$ και επομένως $sx+ty=1$

Η ισότητα ισχύει αν τα 2 μέρη αποτελούν δυνάμεις στις οποίες υψώνουμε ένα ακέραιο a. $a^{sx+ty}=a^1$. Είναι προφανές ότι εμείς θέλουμε $a=2$. Άρα

$$2^{sx+ty}=2 \Rightarrow 2^{sx}2^{ty}=2 \Rightarrow 2^{sx}2^{ty}+2^{ty}-2^{ty}=2$$
$$\Rightarrow 2^{ty}(2^{sx}-1)+(2^{ty}-1)=1$$

Συνεχίζοντας τις πράξεις θα δούμε ότι υπάρχει γραμμικός συνδυασμός των 2^s-1 και 2^t-1 ώστε $\gcd(2^s-1, 2^t-1)=1$

Μπορούμε να δείξουμε το ζητούμενο και με άλλο τρόπο. Αν πούμε ότι s και t δεν είναι πρώτοι μεταξύ τους, τότε υπάρχει ακέραιος m ώστε $s=am$ και $t=bm$.

Τότε $2^s-1=2^{am}-1=(2^m-1)(2^{(a-1)m}+\dots+1)$ και
$2^t-1=2^{bm}-1=(2^m-1)(2^{(b-1)m}+\dots+1)$

Επομένως τόσο το 2^s-1 όσο και το 2^t-1 είναι πολλαπλάσια του (2^m-1). Αυτό όμως δεν μπορεί να ισχύει γιατί έχουμε $\gcd(2^s-1, 2^t-1)=1$. Επομένως και η αρχική υπόθεση ότι s και t δεν είναι πρώτοι μεταξύ τους δεν ισχύει και επομένως είναι $\gcd(s,t)=1$.

Άσκηση 10

Λύστε το σύστημα εξισώσεων

$x = 2 \pmod 3$

$x = 5 \pmod 7$

$x = 3 \pmod{11}$

Λύση

Λύγκυμα με το γνήμα αν έχουμε n_1, n_2 και n_3 πρώτους μεταξύ τους και $n = n_1 \cdot n_2 \cdot n_3$ τότε για οποιουσδήποτε ακεραίο a_1, a_2, a_3 τότε το σύστημα $x \equiv a_i \pmod{n_i}$ για $i = 1$ εως 3 έχει μια μοναδική λύση.

Στην περίπτωση μας έχουμε:

$n = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 7 \cdot 11 = 231$. Τα n_1, n_2, n_3 είναι πρώτα μεταξύ τους

Ένω για τις εξισώσεις έχουμε:

$x = 2 \pmod 3$ $\quad a_1 = 2 \quad n_1 = 3 \quad m_1 = n/n_1 = 77$

$x = 5 \pmod 7$ $\quad a_2 = 5 \quad n_2 = 7 \quad m_2 = n/n_2 = 33$

$x = 3 \pmod{11}$ $\quad a_3 = 3 \quad n_3 = 11 \quad m_3 = n/n_3 = 21$

Έτσι υπολογίζουμε τα c_i ($c_i = m_i (m_i^{-1} \bmod n)$)

$c_1 = 77 (2 \bmod 3) = 154$ $\quad$ Αφού $m_1^{-1} = 77^{-1} = 2 \pmod 3$

$c_2 = 33 (3 \bmod 7) = 99$ $\quad$ Αφού $m_2^{-1} = 33^{-1} = 3 \pmod 7$

$c_3 = 21 (10 \bmod 11) = 210$ $\quad$ Αφού $m_3^{-1} = 21^{-1} = 10 \pmod{11}$

Έτσι $x = 2 \cdot c_1 + 5 \cdot c_2 + 3 c_3 \pmod{231}$

$= 2 \cdot 154 + 5 \cdot 99 + 3 \cdot 210 \pmod{231}$

$= 1433 \bmod 231$

$= 47 \pmod{231}$

Άρα η απάντηση είναι $x = 47$ το οποίο επαληθεύει και τις 3 αρχικές εξισώσεις.