ΜΗΥΠ 416 – ΚΡΥΠΤΟΓΡΑΦΙΑ

Χρήστος Κακλαμάνης
Καθηγητής

Παύλος Σπυράκης
Καθηγητής

Μάιος 2003

Ασκήσεις

1. Δώστε όλες τις υποομάδες των Z_{11} και Z_{15}^*.

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 $33x = 12 \pmod{60}$.

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

9. Λύστε το σύστημα εξισώσεων

$$\begin{aligned} x &= 4 \pmod{5} \\ x &= 1 \pmod{9} \\ x &= 2 \pmod{11} \end{aligned}$$

10. Δείξτε ότι

    (α′) Αν α και β είναι άρτιοι, τότε $gcd(\alpha, \beta) = 2 \cdot gcd(\alpha/2, \beta/2)$.

    (β′) Αν α είναι περιττός και β είναι άρτιος, τότε $gcd(\alpha, \beta) = gcd(\alpha, \beta/2)$.

    (γ′) Αν α και β είναι περιττοί, τότε $gcd(\alpha, \beta) = gcd((\alpha - \beta)/2, \beta)$.

Παράδοση : Παρασκευή, 23/05/2003 ώρα 15:00

ΑΣΚΗΣΗ 1:

Δώστε όλες τις υποομάδες των Z_{11} και Z_{15}^*.

Λύση:

Γνωρίζουμε από το Θεώρημα 33.14 που λέει ότι αν $(S, \oplus)$ είναι μία πεπερασμένη ομάδα και S' ένα οποιοδήποτε υποσύνολο του S έτσι ώστε $(a \oplus b) \in S'$ $\forall a, b \in S'$, τότε $(S', \oplus)$ είναι μία υποομάδα της $(S, \oplus)$ ($\oplus$: κάποια operation).

Το παραπάνω Θεώρημα μας δίνει ένα τρόπο να παράγουμε μια υποομάδα κάποιας ομάδας $(S, \oplus)$, επιλέγοντας κάποιο στοιχείο $a \in S$ και παίρνοντας όλα τα στοιχεία που μπορούν να παραχθούν από το a, χρησιμοποιώντας τον πράξ. $\oplus$.

Τα στοιχεία παράγονται με τον εξής τρόπο:

$$a^{(k)} = \bigoplus_{i=1}^{k} a = \underbrace{a \oplus a \oplus \ldots \oplus a}_{k \text{ φορές}}, \quad k \geq 1, \ a \in S.$$

Για την ομάδα Z_n, έχουμε $\boxed{a^{(k)} = ka \bmod n}$ και $\langle a \rangle = \{a^{(k)} : k \geq 1\}$ υποομάδα που παράγεται από το a.

και αφού η ομάδα S είναι πεπερασμένη, $\langle a \rangle$ είναι πεπερασμένο υποσύνολο του S και ισχύει η προσεταιριστική ιδιότητα: $a^{(i)} \oplus a^{(j)} = a^{(i+j)}$, τότε η $\langle a \rangle$ είναι κλειστή ως προς τις πράξ. $\oplus$ και σύμφωνα με το πιο πάνω Θεώρημα (33.14), $\langle a \rangle$ αποτελεί υποομάδα της S.

Συγκεκριμένα για την Z_{11} έχουμε:

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

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

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

Για την ομάδα Z_n^*, έχουμε $\boxed{a^{(k)} = a^k \bmod n}$ και $\langle a \rangle = \{a^{(k)} : k \geq 1\}$.

Συγκεκριμένα για την Z_{15}^*, έχουμε:

$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Άρα οι υποομάδες είναι οι ακόλουθες:

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

$\langle 2 \rangle = \{1, 2, 4, 8\}$.

$\langle 4 \rangle = \{1, 4\}$.

$\langle 7 \rangle = \{1, 4, 7, 13\}$.

$\langle 8 \rangle = \{1, 4, 2, 8\} = \langle 2 \rangle$.

$\langle 11 \rangle = \{1, 11\}$.

$\langle 13 \rangle = \{1, 4, 7, 13\} = \langle 7 \rangle$.

$\langle 14 \rangle = \{1, 14\}$.

Ερώτημα 2

Για να δείξουμε ότι α και b είναι μεταξύ τους πρώτοι αριθμοί, θα χρησιμοποιήσουμε το gcd που μας δίνει η εκφώνηση για $p \leq n_0$ και $p > n_0$

Από το $\gcd(p^{\alpha b}, \alpha b) = p$ συμπεραίνουμε ότι $ab \neq 1$. Σε διαφορετική περίπτωση θα προέκυπτε $\gcd(p^{\alpha b}, \alpha b) = 1$, το αποτέλεσμα δηλαδή για $p > n_0$. Άρα $ab \geq 2$, από το οποίο $p^{\alpha b} \geq p^2$.

Σύμφωνα με τη Θεωρία Αριθμών γράφουμε το αb ως γινόμενο πρώτων υψωμένων σε κάποια δύναμη.

$$\alpha \cdot b = p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdots p_k^{\varepsilon_k}, \quad \varepsilon_i = 1-m.$$

Από τη δεύτερη συνθήκη, $\gcd(p^{\alpha b}, \alpha b) = 1$ για $p > n_0$, συμπεραίνουμε ότι το γινόμενο πρώτων που δίνει το αb δεν περιέχει πρώτο αριθμό μεγαλύτερο ή ίσο με n_0. Σε διαφορετική περίπτωση το αb, $p^{\alpha b}$ δεν θα ήταν πάντα πρώτα μεταξύ τους, όπως μας δείχνει η συνθήκη ότι ισχύει.

Επίσης αφού $\gcd(p^{\alpha b}, \alpha b) = p$, $p \leq n_0$, προκύπτει ότι το αb δεν περιέχει κανένα πρώτο υψωμένο σε δύναμη $\varepsilon > 1$. Σε αντίθετη περίπτωση θα προέκυπτε η δύναμη και στον gcd και θα είχαμε $\gcd(p^{\alpha b}, \alpha b) = p^{\varepsilon}$.

Από τα παραπάνω τελικά έχουμε καταλήξει ότι το αb είναι $\alpha b = p_1 \cdot p_2 \cdot p_3 \cdots p_k$, $p_i \leq n_0$. Τα α και b συνεπώς θα γράφονται το μεν α ως γινόμενο κάποιων εκ των p_i και το b ως γινόμενο των υπολοίπων p_i. Αφού λοιπόν δεν έχουν κανένα κοινό πρώτο και $\alpha = p_1 \cdot p_2 \cdots p_m$, $b = p_{m+1} \cdots p_k$ θα είναι και co-primes και συνεπώς $\gcd(\alpha, b) = 1$

Ερώτημα 3

Για να αποτελεί ένα σύνολο σώμα ως προς μια πράξη, πρέπει να είναι εφοδιασμένο με τις εξής ιδιότητες:

α) Κλειστότητα

β) Προσεταιριστική μεταξύ των στοιχείων του

γ) Ύπαρξη ουδετέρου στοιχείου.

δ) Ύπαρξη αντίστροφου για κάθε στοιχείο

Θα εξετάσουμε το σύνολο Z_n με τις ισχύ των πιο πάνω ιδιοτήτων, ως προς την πράξη του πολλαπλασιασμού

α) ισχύει: $[a]_n [b] \in Z_n \Rightarrow [ab]_n \in Z_n$

β) και γ) ισχύουν αφού για ουδέτερο στοιχείο το $[1]_n$ έχουμε $[a]_n [1]_n = [a \cdot 1]_n = [a]$

δ) Για να έχει πολλαπλασιαστικό αντίστροφο ένα στοιχείο $[a]_n$ του Z_n θα πρέπει να υπάρχει στοιχείο $[b]_n$ τέτοιο ώστε $[a]_n [b]_n = [1] \Rightarrow [ab]_n = [1]_n \Rightarrow ab \equiv 1 \bmod n$
$\Rightarrow n \mid (ab-1)$ *

Θα εξετάσουμε την * για το στοιχείο $[0]_n$ που ανήκει σε όλα τα Z_n.

$n \mid (ab-1) \overset{ab=0}{\Longrightarrow} n \mid (-1) \Rightarrow n = 1$

Άρα η ύπαρξη αντιστρόφου ισχύει μόνο για $n=1$. Συνεπώς το στοιχείο $[0]_n$ δεν έχει αντίστροφο για κάθε n. Έτσι προκύπτει ότι για $n \neq 1$ υπάρχει κάποιο στοιχείο του Z_n για το οποίο δεν υπάρχει αντίστροφος. Άρα η δ) δεν ισχύει

Συνεπώς το σύνολο Z_n εφοδιασμένο με την πράξη του πολλαπλασιασμού ΔΕΝ αποτελεί σώμα

ΑΣΚΗΣΗ 4:

Βρείτε τις λύσεις της εξίσωσης $33x = 12 \pmod{60}$.

Λύση:

Για να βρούμε τις λύσεις της εξίσωσης $33x = 12 \pmod{60}$ χρησιμοποιούμε τον αλγόριθμο MODULAR-LINEAR-EQUATION-SOLVER (a, b, n)

```
(d, x', y') ← EXTENDED-EUCLID (a, n)
if d|b
    then x0 ← x'(b/d) mod n
        for i ← 0 to d-1
            do print (x0 + i(n/d)) mod n
    else print "no solutions".
```

με $a=33$, $b=12$ και $n=60$.

Ο πιο πάνω αλγόριθμος καλεί τον EXTENDED-EUCLID (a, n):

```
if n=0
    then return (a, 1, 0)
(d', x', y') ← EXTENDED-EUCLID (n, a mod n)
(d, x, y) ← (d', y', x' - ⌊a/n⌋ y')
return (d, x, y)
```

Κατά την εκτέλεση του παίρνουμε τα πιο κάτω αποτελέσματα:

a	n	$\lfloor a/n \rfloor$	d	x_0	y_0
33	60	0	3	-9	5
60	33	1	3	5	-9
33	27	1	3	-4	5
27	6	4	3	1	-4
6	3	2	3	0	1
3	0	-	3	1	0

$\gcd(a,n) = \gcd(33, 60) = 3 = d$

Άρα υπάρχουν 3 λύσεις.

Επίσης ισχύει $\gcd(a,n) = 3 = 33x_0 + 60y$

$\therefore$ Άρα η κλήση της EXTENDED-EUCLID μας επιστρέφει $(3, -9, 5)$.

Στην συνέχεια ο αλγόριθμος MODULAR-LINEAR-EQUATION-SOLVER εξετάζει αν το d διαιρεί το b. Στην περίπτωση μας $3|12 = 4$. Αν δεν το διαιρούσε, ο αλγόριθμος μας θα τερμάτιζε εκτυπώνοντας "no solutions", δηλαδή ότι δεν υπάρχουν λύσεις. Στην συνέχεια αναθέτουμε στο x_0 την τιμή $x_0 = x'(b/d) \bmod 60 = -9(12/3) \bmod 60 = -36 \bmod 60 = 24$

Η πιο πάνω λύση υποδηλώνει ότι υπάρχουν συνολικά $d-1$ (2) λύσεις, που τις βρίσκουμε για $i=0$ έως $d-1=2$: $(x_0 + i(n/d)) \bmod n = (24 + i\,20) \bmod 60$.

Άρα οι λύσεις είναι:

για $i=0 \Rightarrow x_1 = x_0 = 24$ //

για $i=1 \Rightarrow x_2 = (24+20) \bmod 60 = 44 \bmod 60 = 44$ //

για $i=2 \Rightarrow x_3 = 24 + 2.20 = 64 \bmod 60 = 4$ //.

Ερώτημα 5

Ως γνωστόν το σύνολο Z_m^* είναι σταθό και συνεπώς για κάθε στοιχείο του υπάρχει πολλαπλασιαστικός αντίστροφος.

Επίσης το $Z_m^* \subset Z_m$. Άρα το πλήθος των στοιχείων του Z_m που δεν έχουν πολλαπλασιαστικό αντίστροφο υπολογίζεται ως:

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

$\varphi(m)$: Συνάρτηση του Euler, που δίνει το πλήθος των στοιχείων της σταθού Z_m^*.

p: ο συμβολισμός των πρώτων αριθμών που διαιρούν το m

Αφού το m είναι τάξης σύνθετος, από τη θεωρία αριθμών, θα γράφεται σαν γινόμενο πρώτων αριθμών. Από αυτούς για το γινόμενο στην σχέση $\varphi(m)$ υπολογίζεται μόνο του μικρότερου εκείνο του οποίο ισχύει $k \le \sqrt{m}$, αφού αλλιώς θα πολλαπλασιάζαν με κάτι μεγαλύτερο από $\sqrt{m}$ δίνοντας αποτέλεσμα μεγαλύτερο του m.

Επομένως από την $(*)$ έχουμε:

$$A = m - m\prod_{p|m}\left(1-\frac{1}{p}\right) \ge m - m\left(1-\frac{1}{k}\right) = m - m + \frac{m}{k} \ge \sqrt{m}$$

Δηλαδή τα στοιχεία χωρίς πολλαπλασιαστικό αντίστροφο στο Z_m έχουν πλήθος τουλάχιστον $\sqrt{m}$

Ερώτημα 6

Έστω $g(p)$ σύνθετοι αριθμοί μεταξύ δύο πρώτων αριθμών, που χωρίζουν τον p από τον επόμενο πρώτο.
Άρα $p_{n+1} = g(p_n) + p_n$ [$g(p)$ το πλήθος των σύνθετων]
Μας ζητείται να δείξουμε ότι το $g(p)$ είναι αυθαίρετα μεγάλο
Έστω ακέραιος $n > 1$ και έστω n ακολουθία ακεραίων
$(n!) + k$, $k \in [2, n]$ ακέραιοι.
Θα έχουμε:

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

Αν p ο μεγαλύτερος πρώτος πριν το $n!+2$, έως τον επόμενο πρώτο θα υπάρχουν $g(p) > n-1$ σύνθετοι αριθμοί.
Άρα οι σύνθετοι αριθμοί μεταξύ δύο πρώτων είναι αυθαίρετα μεγάλου πλήθους εξαρτώμενοι από το n.

Ερώτημα 7

Αρχικά φέρνουμε το $a^{-1} \bmod n$ σε μαθηματική μορφή, αποδεκτή από την MODULAR-EXPONENTIATION ρουτίνα.

Αφού $a \in Z_n^*$ $\Rightarrow$ $\gcd(a,n)=1$ [μεταξύ τους πρώτοι]

Χρησιμοποιούμε με το θεώρημα του Euler για οποιοδήποτε $n>1$ και για κάθε $a \in Z_n^*$ ισχύει:

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

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

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

Το δεξί μέρος της ισότητας είναι το ζητούμενο.

Βλέπουμε ότι $a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$ *

Έτσι με την Μ-Ε υπολογίζουμε το δεξί μέρος της ⊛ που είναι αποδεκτή από την Μ-Ε και έτσι έχουμε το $a^{-1} \bmod n$, που είναι ίσο με αυτό.

Ερώτημα Β

Θελουμε να δειξουμε από το δεδομένο ότι οι s,t είναι μεταξύ τους πρώτοι.

Θεωρούμε ότι οι s,t, δεν είναι μεταξύ τους πρώτοι και έστω m ο κοινός τους παράγοντας

ώστε $s=am$ και $t=bm$

Τότε: $2^s-1 = 2^{am}-1 = (2^m-1)\cdot(2^{(a-1)m} + \dots +1)$

$2^t-1 = 2^{bm}-1 = (2^m-1)\cdot(2^{(b-1)m} + \dots +1)$

Άρα τα 2^s-1, 2^t-1 έχουν και το ίδιο το (2^m-1) ως παράγοντα και συνεπώς $\gcd(2^s-1, 2^t-1) \neq 1$.

Επομένως η υπόθεση που κάναμε είναι λάθος και συνεπώς ισχύει $\gcd(s,t)=1$

Ερώτημα 9

Ισχύει ότι αν n_1, n_2, n_3 πρώτοι μεταξύ τους και $n = n_1 \cdot n_2 \cdot n_3$ τότε για οποιουδήποτε ακέραιους a_1, a_2, a_3 το σύστημα

$$x \equiv a_i \bmod n_i \quad , i \in [1,2,3]$$

έχει μοναδική λύση.

Στο σύστημα που μας δίνεται έχουμε

$\gcd(n_1, n_2) = \gcd(5,9) = 1$

$\gcd(n_2, n_3) = \gcd(5,11) = 1$

$\gcd(n_3, n_1) = \gcd(11,9) = 1$

και $n_1 \cdot n_2 \cdot n_3 = 495 = n$

Για το σύστημα εξισώσεων έχουμε

$x = 4 \pmod 5$ $\quad \alpha_1 = 4 \quad n_1 = 5 \quad m_1 = n/n_1 = 99$

$x = 1 \pmod 9$ $\quad \alpha_2 = 1 \quad n_2 = 9 \quad m_2 = 55$

$x = 2 \pmod{11}$ $\quad \alpha_3 = 2 \quad n_3 = 11 \quad m_3 = 45$

Υπολογίζουμε τα c_i, $c_i = m_i \cdot (m_i^{-1} \bmod n)$

$c_1 = 99 \cdot (4 \bmod 5) = 396$, γιατί $m_1^{-1} = 99^{-1} = 4 \bmod 5$

$c_2 = 55 \cdot (1 \bmod 9) = 55$, γιατί $m_2^{-1} = 55^{-1} = 1 \bmod 9$

$c_3 = 45 \cdot (1 \bmod 11) = 45$, γιατί $m_3^{-1} = 45^{-1} = 1 \bmod 11$

Τελικά $x = \alpha_1 c_1 + \alpha_2 c_2 + \alpha_3 c_3 \pmod n$

$= 4 \cdot 396 + 1 \cdot 55 + 2 \cdot 45 \pmod{495}$

$= 1584 + 55 + 90 \pmod{495}$

$= 1729 \bmod 495 = 244$

Ερώτημα 10

α'. Για όλους τους ακέραιους α και β και για κάθε αρνητικό ακέραιο n.

$$\gcd(\alpha n, \beta n) = n \cdot \gcd(\alpha, \beta) \quad ①$$

Απόδειξη με βάση τον πιο πάνω ορισμό:

Για $n=0$ έχω $\gcd(0,0)=0$ ισχύει.

Για $n>0$, ο $\gcd(\alpha n, \beta n)$ είναι το μικρότερο θετικό στοιχείο του συνόλου $\{\alpha x+\beta y\}$ άρα ο gcd των (α, β)

Τώρα επειδή οι α, β άρτιοι θέτω $\alpha=2\lambda$ και $\beta=2p$

Έχουμε $\gcd(\alpha,\beta)=\gcd(2\lambda, 2p) = 2 * \gcd(\lambda, p)$ ②

Επειδή $\left.\begin{array}{l}\lambda=\alpha/2\\ p=\beta/2\end{array}\right\} \overset{②}{\Rightarrow} \gcd(\alpha,\beta) = 2\gcd\left(\frac{\alpha}{2}, \frac{\beta}{2}\right)$ που είναι το ζητούμενο

β'. Για δύο θετικούς ακέραιους $\alpha, \beta>0$ ισχύει ότι $\gcd(\alpha,\beta)$ είναι το μικρότερο από τα θετικά στοιχεία του $\{\alpha x+\beta y : x,y\in Z^+\}$ των γραμμικών συνδυασμών του α και β

Έστω $\beta=2c$, $c>0$ (β άρτιος). Για το σύνολο των γραμμικών συνδυασμών α και β έχουμε:

$\{\alpha x+\beta y : x,y\in Z^+\} \Rightarrow \{\alpha x+(2c)y : x,y\in Z^+\} \Rightarrow$
$\Rightarrow \{\alpha x + c(2y) : x,y\in Z^+\}$

Σε αυτό το σύνολο το μικρότερο θετικό στοιχείο είναι ο $\gcd(\alpha, c)$.

Από την ισοδυναμία των συνόλων έχουμε ότι το ελάχιστο είναι ίσο με το μικρότερο θετικό στοιχείο του συνόλου $\{\alpha x+\beta y : x,y\in Z^+\}$. Δηλαδή ίσο με το $\gcd(\alpha,\beta)$. Άρα $\gcd(\alpha,\beta)=\gcd(\alpha,c)$ και αφού

$\beta = 2k \Rightarrow k = \beta/2$.

Άρα $\gcd(\alpha, \beta) = \gcd(\alpha, \beta/2)$

γ' Θα αποδείξουμε $\gcd(\alpha, \beta) = \gcd((\alpha-\beta)/2, \beta)$

Έχουμε ότι $\gcd(\alpha, \beta) \mid \alpha, \beta$ (ο gcd διαιρεί το α και β) και άρα διαιρεί και τη διαφορά τους $(\alpha - \beta)$.

Θα είναι επίσης ο gcd των $(\alpha-\beta)$ και β γιατί αφού το $\gcd(\alpha, \beta)$ είναι το μικρότερο θετικό στοιχείο του $\{\alpha x + \beta y : x, y \in \mathbb{Z}^+\}$ θα είναι και το μικρότερο θετικό στοιχείο στο $\{(\alpha-\beta)x + \beta y : x, y \in \mathbb{Z}^+\} \Rightarrow \{\alpha x + \beta(-x+y) : x, y \in \mathbb{Z}^+\}$

Άρα $\gcd(\alpha, \beta) = \gcd((\alpha-\beta), \beta)$.

Όπως $(\alpha-\beta)$ άρτιος ως διαφορά περιττών. Από το β' για β περιττό και $(\alpha-\beta)$ άρτιο έχουμε

$$\gcd(\beta, (\alpha-\beta)) = \gcd\left(\beta, \frac{\alpha-\beta}{2}\right)$$

και τελικά $\gcd(\alpha, \beta) = \gcd\left(\frac{\alpha-\beta}{2}, \beta\right)$