1) Δείξτε ότι στο U_{2^e} $(e \geq 3)$ τα μοναδικά στοιχεία με τάξη 2 είναι τα $2^{e-1} \pm 1$ και -1

Λύση: Καταρχήν $2^{e-1} \pm 1 \not\equiv 1 \pmod{2^e}$ και φυσικά $-1 \not\equiv 1 \pmod{2^e}$.

Ακόμα $(2^{e-1} \pm 1)^2 = 2^{2(e-1)} \pm 2 \cdot 2^{e-1} + 1 \equiv 1 \pmod{2^e}$ Άρα έχουν τάξη ίση με 2. Αντίστροφα, εάν το a έχει τάξη ίση με 2 τότε θα πρέπει $a^2 \equiv 1$ οπότε $2^e / (a^2 - 1) \Rightarrow 2^e / (a+1)(a-1)$. Όμως εύκολα βλέπουμε ότι είτε το $a-1$ ή το $a+1$ είναι $\equiv 2 \pmod 4$ οπότε είναι της μορφής $2(1+2k)$ Κατα συνέπεια το 2^{e-1} δίνει τον άλλο παράγοντα δηλ. $2^{e-1} / a+1$ ή $2^{e-1} / a-1$

Οπότε $a = \pm 1 \pmod{2^{e-1}} \Rightarrow a \equiv \pm 1$, ή $a \equiv 2^{e-1} \pm 1 \pmod{2^e}$

2) Να βρεθεί το πλήθος των τετραγωνικών ριζών $\pmod n$ της 1 δηλ. να βρεθεί το πλήθος N των κλάσεων $x \in \mathbb{Z}_n$ που ικανοποιούν την εξίσωση $x^2 \equiv 1 \pmod n$

Λύση:

Έστω $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ η ανάλυση του n σε πρώτους παράγοντες $(p_1 < p_2 < \cdots < p_k)$

Τότε $x^2 \equiv 1 \pmod n \Leftrightarrow x^2 \equiv 1 \pmod{p_i^{e_i}}$

$\vdots$

$x^2 \equiv 1 \pmod{p_k^{e_k}}$

Αν N_i είναι το πλήθος των λύσεων της εξίσωσης $x^2 \equiv 1 \pmod{p_i^{e_i}}$ έχουμε $N = N_1 \cdots N_k$.

Περίπτωση: $p_i > 2$. Τότε τα $x \equiv \pm 1$ ικανοποιούν την $x^2 \equiv 1 \pmod{p_i^{e_i}}$

Αντίστροφα: Εάν $x^2 \equiv 1 \Rightarrow p^e / (x-1)(x+1)$ οπότε επειδή $p > 2$ και $p \nmid x$ θα πρέπει $p^e / (x-1)$ ή $p^e / (x+1)$ δηλαδή $x \equiv \pm 1 \pmod{p^e}$

Οπότε $N_i = 2$ για $p_i > 2$

Εάν $p_i^{e_i} = 2$ ή $p_1^{e_1} = 4$ τότε είναι εύκολο να δούμε ότι $N_1 = 1$ ή $N_1 = 2$ αντίστοιχα.

Εάν $p_1^{e_1} = 2^{e_1} \geq 8$ τότε η $x^2 \equiv 1 \pmod{2^{e_1}}$ έχει λύσεις $\pm 1, 2^{e-1} \pm 1$

όπως είδαμε και στην προηγούμενη άσκηση. Οπότε θ' αναγόμαστε στην περίπτωση $N_1 = 4$

Οπότε από τα παραπάνω προκύπτει ότι:

$$N = \begin{cases} 2^{k+1} & \text{εαν } 8/n \\ 2^k & \text{εαν } n \equiv 4 \pmod 8 \text{ ή εαν } 2 \nmid n \\ 2^{k-1} & \text{εαν } n \equiv 2 \pmod 4 \end{cases}$$

3) Να βρεθεί το πλήθος των τετραγωνικών ριζών (modn) ενός στοιχείου $a \in U_n$:

Λύση: Εαν $a \notin Q_n$ τότε φυσικά το πλήθος τους είναι ίσο με 0.

Εδώ δείχνουμε ότι $a \in Q_n$ δηλαδή υπάρχει μια (συγκεκριμένη) τετραγωνική ρίζα s του a δηλ. $s^2 \equiv a \pmod n$. Τότε εύκολα $(s,n)=1$ δηλ. $s \in U_n$. Ως γνωστό από την θεωρία κάθε αλλο στοιχείο $t \in U_n$ γράφεται ως γινόμενο sx για κάποιο μοναδικό $x \in U_n$ (πράγματι $x = ts^{-1}$) δηλαδή $t = sx$. Οπότε ισχύουν τα παρακάτω:

$$a \equiv t^2 \Leftrightarrow t^2 \equiv a \pmod n \Leftrightarrow t^2 \equiv s^2 \pmod n \Leftrightarrow s^2x^2 \equiv s^2 \pmod n$$

$$\Leftrightarrow x^2 \equiv 1 \pmod n \Leftrightarrow \text{όταν το } x \text{ είναι τετραγ. ρίζα } \pmod n \text{ της μονάδος.}$$

Από την προηγούμενη άσκηση προκύπτει ότι το πλήθος τέτοιων x είναι ίσο με N και άρα το πλήθος των τετραγωνικών ριζών του $a \in Q_n$ είναι αμφιβ. ίσο με N

4) Άσκηση Δείξτε ότι $|Q_n| = \phi(n)/N$

Λύση:

Χωρίζουμε το U_n σε κλάσεις ισοδυναμίας όπου η ισοδυναμία ορίζεται ως εξής: $s \sim s_*$ αν-ν $s^2 \equiv s_*^2 \pmod n$ δηλ. δύο στοιχεία είναι

Ισοδύναμα αν είναι οι τετραγωνικές ρίζες κάποιου αριθμού $a \in Q_n$.

Ομοίως κάθε κλάση ισοδυναμίας αποτελείται από τις τετραγωνικές ρίζες ενός καταλλήλου αριθμού $a \in Q_n$. Κάθε μια κλάση έχει πλήθος στοιχείων ίσο με N όπως είδαμε από την προηγούμενη άσκηση. Το πλήθος των (διαφορετικών) κλάσεων ισοδυναμίας είναι ίσο με το πλήθος των διαφορετικών τετραγωνικών υπολοίπων (mod n) δηλ. ίσο με $|Q_n|$

Από τα προηγούμενα έχουμε $N|Q_n| = |U_n| \Rightarrow N|Q_n| = \phi(n) = |Q(n)| = \frac{\phi(n)}{N}$

5) Άσκηση Έστω a ένας περιττός ακέραιος. Τότε

(α) $a \in Q_2$

(β) $a \in Q_4$ αν-ν $a \equiv 1 \pmod 4$

(γ) $a \in Q_8$ αν-ν $a \equiv 1 \pmod 8$

(δ) $a \in Q_{2^e}$ με $e \geq 3$ αν-ν $a \equiv 1 \pmod 8$

Λύση: Τα (α), (β) είναι εύκολα με μια απλή δοκιμή.

Για το (γ) Έχουμε $U_8 = \{1, 3, 5, 7\}$ και με δοκιμή βλέπουμε ότι

$3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$ δηλαδή το a είναι τετραγωνικό υπόλοιπο $\pmod 8$ αν $a \equiv 1 \pmod 8$

(δ) Έστω $a \in Q_{2^e} \Rightarrow a \equiv s^2 \pmod{2^e}$ για κάποιο $s \in U_{2^e}$

$\Rightarrow a \equiv s^2 \pmod 8 \Rightarrow a \equiv 1 \pmod 8$

Αντίστροφα

Έστω $a \equiv s^2 \pmod 8$ για κάποιο s. Τότε μπορούμε να παρίγουμε από το s μια τετραγωνική ρίζα του $a \pmod{16}$ και μια τετρ. ρίζα του $a \pmod{2^5}$ κοκ μέχρι να βρούμε μια τετρ. ρίζα του $a \pmod{2^e}$ Ας δούμε τις λεπτομέρειες:

Εστω λοιπόν ότι έχαμε βρει μια τετρ. ρίζα (mod 2^i) του α δηλ.

$$s^2 \equiv a \pmod{2^i}$$

Τότε αν $s^2 \equiv a \pmod{2^{i+1}}$ τότε τελειώσαμε για το $(i+1)$ βήμα.

Αν $s^2 \not\equiv a \pmod{2^{i+1}}$ τότε αναγκαστικά το $s(1+2^{i-1})$ είναι μια τετρ. ρίζα $\pmod{2^{i+1}}$ του α όπως πολύ εύκολα μπορούμε να το διαπιστώσουμε υψώνοντας στο τετράγωνο το $s(1+2^{i-1})$ και χρησιμοποιώντας την σχέση $s^2 = a + 2^i k$ όπου κ είναι περιττός. (και α όμοια προφανώς περιττός)

Εφαρμογή

6/ Να βρεθούν οι τετραγωνικές ρίζες του $17 \bmod (2^5)$ αν υπάρχουν

Λύση: Έχουμε $17 \in Q_{2^5} \Leftrightarrow 17 \equiv 1 \pmod 8$ που ισχύει!

Άρα το 17 έχει τετρ. ρίζες $(\bmod 2^5)$. Προχωράμε Βήμα-Βήμα

Βήμα 1ο Λύνουμε την ισοδυναμία $17 \equiv x^2 \pmod 8 \Leftrightarrow 1 \equiv x^2 \pmod 8$

Οπότε μια λύση είναι η $x=1$

Βήμα 2ο Από την προηγούμενη λύση θα βρούμε μια λύση της $17 \equiv x^2 \pmod{16}$

Εύκολα η $x=1$ μας κάνει.

Βήμα 3ο Από την προηγούμενη λύση θα βρούμε μια λύση της $17 \equiv x^2 \pmod{2^5}$

Η λύση $x=1$ δεν μας κάνει! Δοκιμάζουμε την $x(1+2^{i-1}) = x(1+2^3) = 9$ (όπου $i=4$ και $(i+1)=5$). Αυτή δίνουμε μας κάνει (όπως τεκμηριώσαμε από την προηγούμενη άσκηση) Πράγματι: $81 \equiv 17 + 64$ δηλ $9^2 \equiv 17 \pmod{2^5}$

Τέλος αφού βρήκαμε μια τετρ. ρίζα θα μπορούμε να βρούμε και τις $N=4$ τετρ. ρίζες του 17. Δηλ. από την θεωρία οι τετρ. ρίζες είναι οι

$(2^4-1)\cdot 9$, $(2^4+1)\cdot 9$ δηλαδή οι αριθμοί:

$9, -9, 9(16+1) \equiv 25 \pmod{2^5}$, $9(16-1) \equiv 135 \equiv 7 \pmod{2^5}$

δηλαδή έχουμε στις τετρ. ρίζες $\pm 9, \pm 7 \pmod{2^5}$

Μπορούμε βέβαια να χρησιμοποιήσουμε και την θεωρία που μάθαμε στο 17/01/2006 για να λύνουμε εξισώσεις της μορφής $f(x) \equiv 0 \bmod p^e$ αλλά είναι πιο εύκολο να δουλεύουμε με τον τρόπο που αναπτύξαμε ειδικά στην περίπτωση που $f(x) = x^2 - a$ και $p^e = 2^e$ με $e \geq 3$.

7) Άσκηση Να βρεθούν οι τετρ. ρίζες του $41 \pmod{2^6}$. /

Λύση

$41 \pmod 8 \equiv 1 \pmod 8$. Άρα το 41 έχει 4 τετρ. ρίζες $\pmod{2^6}$

Ας τις βρούμε

Βήμα 1ο Λύνουμε την $41 \equiv x^2 \pmod{2^3} \Leftrightarrow 1 \equiv x^2 \pmod 8$

Βρίσκουμε μια προφανή λύση π.χ. την $x=1$

Βήμα 2ο Λύνουμε την $41 \equiv x^2 \pmod{2^4} \Leftrightarrow 9 \equiv x^2 \pmod{2^4}$

$x=1$ φυσικά δεν μας κάνει. Όμως μας κάνει η

$x_* \equiv 1 + 2^{i-1} = 1+4 = 5$

Βήμα 3ο Λύνουμε την $41 \equiv x^2 \pmod{2^5} \Leftrightarrow 9 \equiv x^2 \pmod{2^5}$

Η x_* δεν μας κάνει. Όμως μας κάνει η $x_{**} = 5(1+2^{i-1})$

$= 5(1+8) = 45 \equiv 13 \pmod{2^5}$. Φυσικά θα μπορούσαμε να πάρουμε και την προφανή λύση $x_{**} = 9$

Βήμα 4ο Η $x_{**} = 13$ μας κάνει διότι $x_{**}^2 \equiv 169 \equiv 64 \times 2 + 41 \equiv 41 \pmod{2^6}$

Οπότε οι υπόλοιπες τετραγ. ρίζες του 41 είναι της μορφής

$x_{**}(\pm 1)$ $x_{**}(32 \pm 1)$

8) Άσκηση Έστω p ένας πρώτος >2 και e ≥ 1. Δείξτε ότι $a \in Q_{p^e}$ αν-ν $a \in Q_p$. Ακόμα δείξτε ότι κάθε τετραγωνικό υπόλοιπο a του p^e έχει ακριβώς δύο μόνο τετραγωνικές ρίζες (mod p^e).

Λύση:

Έστω $x^2 \equiv a \pmod{p^e}$ τότε προφανώς $x^2 \equiv a \pmod{p}$ Οπότε $a \in Q_{p^e} \Rightarrow a \in Q_p$.

Αντίστροφα: Έστω $a \in Q_p$ οπότε η εξίσωση $x^2 - a \equiv 0 \pmod{p}$ έχει μία τουλάχιστον ρίζα s_1 Ορίζουμε $f(x) = x^2 - a$. Τότε μπορούμε να πάρουμε από την s_1 μία τετρ. ρίζα s_2 έτσι ώστε $s_2^2 - a \equiv 0 \pmod{p^2}$ και $s_2 \equiv s_1 \pmod{p}$. Από τη s_2 την s_3, κ.ο.κ από την s_i την s_{i+1} με την ιδιότητα

$s_{i+1}^2 - a \equiv 0 \pmod{p^{i+1}}$ και $s_{i+1} \equiv s_i \pmod{p^i}$ έως ότου φτάσουμε στην s_e που ικανοποιεί την $x^2 - a \equiv 0 \pmod{p^e}$ Οπότε $a \in Q_{p^e}$

Λεπτομέρειες της κατασκευής της ακολουθίας $s_2, s_3, \ldots, s_i, s_{i+1}, \ldots$

Έστω λοιπόν ότι $s^2 \equiv a \pmod{p^i}$

Τότε σύμφωνα με το λήμμα της 17/01/2004 οι υπόλοιπες ρίζες της $x^2 - a \equiv 0 \pmod{p^{i+1}}$ είναι οι παρακάτω:

$s_i, s_i + p^i, s_i + 2p^i, \ldots, s_i + (p-1)p^i$ δηλ. της μορφής $s_i + tp^i$ όπου το t ικανοποιεί την εξίσωση:

$$\frac{f(s_i)}{p^i} \equiv -f'(s_i)\, t \pmod{p}$$ Όπως υπάρχει ένα μοναδικό t δίότι: $f'(s_i) = 2s_i \not\equiv 0 \pmod{p}$ διότι $p > 2$ πρώτος

οπότε $(f'(s_i), p)=1$ δηλ το $f'(s_i)$ αντιστρέφεται. πολ/ζουμε λοιπόν και τα δύο μέλη της $\frac{f(s_i)}{p^i} \equiv -(f'(s_i))t \pmod p$

με αυτόν τον αντίστροφο βρίσκουμε το t οπότε ορίζουμε

$s_{i+1} = s_i + tp^i$. Τέλος από την άσκηση βλέπουμε ότι το πλήθος των λύσεων (δηλ. των τετρ. ριζών) είναι ίσο με $N=2$

9) Παράδειγμα Να βρείτε τις τετραγωνικές ρίζες του $6 \pmod{5^2}$

Λύση $6 \in Q_{5^2} \Leftrightarrow 6 \in Q_5$

Όμως $6 \equiv 1 \pmod 5 \Leftrightarrow 6 \equiv 1^2 \pmod 5$. Άρα $6 \in Q_{5^2}$

Υποψήφιες λύσεις για την $6 \equiv x^2 \pmod{5^2}$

$s_2 = 1, 1+5, 1+10, 1+15, 1+20$ δηλ. της μορφής

$s_2 = 1+5t$ όπου t:

$\frac{f(1)}{p} \equiv -f'(1)t \pmod p \Leftrightarrow$

$\frac{1-6}{5} \equiv -2t \pmod 5 \Leftrightarrow$

$-1 \equiv -2t \pmod 5 \Leftrightarrow 1 \equiv 2t \pmod 5$. Οπότε $t=3$

δηλ $s_2 = 1+15 = 16 \pmod{25}$

Οπότε οι ζητούμενες τετραγωνικές ρίζες είναι οι $\pm 16 \pmod{25}$

Από τις παραπάνω ασκήσεις που έχουμε ήδη κάνει προκύπτει η παρακάτω χρήσιμη πρόταση:

10) Έστω $a \in U_n$. Τότε $a \in Q_n$ ανν

(1) $a \in Q_p$ για κάθε περιττό πρώτο p με p/n

(2) εάν $8/n$ τότε θα πρέπει $a \equiv 1 \pmod 8$

(3) Εαν $n \equiv 4 \pmod 8$ τότε θα πρέπει $a \equiv 1 \pmod 4$

Πρόταση:

Εστω $a \in Q_n$ και αρα υπάρχει ενα (πολλαπλάσιου) s ετσι ώστε $a \equiv s^2 \pmod n$. Εστω p/n και $p>2$ πρώτος. Τότε $a \equiv s^2 \pmod p$ δηλαδή $a \in Q_p$.

Εστω $8/n$ τότε απο την $a \equiv s^2 \pmod n$ προκύπτει όμοια $a \equiv s^2 \pmod 8 \Rightarrow a \in Q_8 \Rightarrow$ απο άσκηση 5) εχουμε $a \equiv 1 \pmod 8$

Εστω $n \equiv 4 \pmod 8$ οπότε $a \equiv s^2 \pmod 4 \Rightarrow a \in Q_4 \Rightarrow$ απο άσκηση $a \equiv 1 \pmod 4$

Απόδειξη:

Θα δείξουμε οτι $a \in Q_n$. Εστω $n = p_1^{e_1} \cdots p_k^{e_k}$ με $p_1 < p_2 < \cdots < p_k$ η ανάλυση του n σε πρώτους.

Η εξίσωση $x^2 - a \equiv 0 \pmod n$ γράφεται ισοδύναμα ως σύστημα:

$$\{ x^2 - a \equiv 0 \pmod{p_i^{e_i}} \text{ για } i = 1, 2, \ldots, k \}$$

Θα πρέπει τουλάχιστον κάθε μία απο τις $x^2 - a \equiv 0 \pmod{p_i^{e_i}}$ να έχει λύση!

Για $p_i > 2$ η $x^2 - a \equiv 0 \pmod{p_i^{e_i}}$ έχει λύση όταν έχει λύση η $x^2 - a \equiv 0 \pmod{p_i}$ άρα έχουμε υποθέσει $a \in Q_{p_i}$ (βλέπε και άσκηση 8)

Στην περίπτωση που $p_i = 2$ Τότε εαν $p_i^{e_i} = 2^{e_i} \geq 8$ η εξίσωση $x^2 - a \equiv 0 \pmod{2^{e_i}}$ έχει λύση όταν $a \equiv 1 \pmod 8$ (βλέπε και άσκηση 5)

Εαν ώρα $p_i^{e_i} = 4$ η εξίσωση $x^2 - a \equiv 0 \pmod 4$ έχει λύση όταν $n = 4(2k+1) = 8k+4 \equiv 4 \pmod 8$ οπότε απο υπόθεση έχουμε $a \equiv 1 \pmod 4$ και απο άσκηση προκύπτει $a \in Q_4$.

Τότε εαν $p_i^{e_i}=2$ τότε η εξίσωση $x^2 \equiv a \pmod 2$ έχει μοναδική λύση την $x=1$ διότι επειδή $a \in Q_n$ τότε προκύπτει ότι a δηλ. το a είναι περιττός και άρα $a \equiv 1 \pmod 2$.

Συνοψίζοντας τα παραπάνω βλέπουμε ότι το σύστημα

$\begin{cases} x^2 - a \equiv 0 \pmod{p_i^{e_i}}, & i = 1, \dots, k \end{cases}$ έχει πάντοτε λύση

και άρα και η εξίσωση $x^2 - a \equiv 0 \pmod n \Rightarrow a \in Q_n$

11) Άσκηση Να βρείτε τα στοιχεία του Q_{60} καθώς και τις τετραγωνικές ρίζες των στοιχείων που βρήκατε.

Λύση: Αναλύουμε το 60 σε γινόμενο πρώτων δυνάμεων. Έχουμε

$60 = 2^2 \cdot 3 \cdot 5$.

Όπου $|Q_{60}| = \frac{\phi(60)}{8}$ όπως προκύπτει από άσκηση

Όμως $\phi(60) = \phi(4)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 8 \cdot 2$

Οπότε $|Q_{60}| = 2$ δηλ. υπάρχουν μόνο δύο τετραγωνικά υπόλοιπα και το καθένα έχει 8 τετραγωνικές ρίζες $(\bmod 60)$

Το ένα τετραγωνικό υπόλοιπο είναι σίγουρα το 1

Για να βρούμε το άλλο έστω a θεωρούμε τη διοφαντική εξίσωση χρησιμοποιώντας την προηγούμενη άσκηση:

$a \in Q_{60} \Leftrightarrow a \in Q_4, a \in Q_3, a \in Q_5 \Leftrightarrow$

$\Leftrightarrow a \equiv 1 \pmod 4, a \in Q_3, a \in Q_5$.

Επειδή $a \in Q_3 \Leftrightarrow a \equiv 1 \pmod 3$

$a \in Q_5 \Leftrightarrow a \equiv 1$ ή $4 \pmod 5$

Οπότε τελικά πρέπει να λύσουμε τα γραμμικά συστήματα

$a \equiv 1 \pmod 4$

$a \equiv 1 \pmod 3 \Leftrightarrow a \equiv 1 \pmod{12}$

$a \equiv 1 \text{ ή } 4 \pmod 5 \qquad a \equiv 1 \text{ ή } 4 \pmod 5$

Ξεχνάμε την προηγούμενη διάσπαση $a \equiv 1 \pmod{60}$ και φτιάχνουμε την δική του συνάρτησης

$$\left.\begin{array}{l} a \equiv 1 \pmod{12} \\ a \equiv 4 \pmod 5 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} a \equiv 1, 13, 25, 37, 49 \\ a \equiv 4 \pmod 5 \end{array}\right\}$$

$$\Leftrightarrow a \equiv 49 \bmod 60$$

Από την άσκηση 3) ξέρουμε ότι αν ξέρουμε μια πρ. ρίζα s ενός αριθμού $a \in \mathbb{Q}_n$ τότε οι υπόλοιπες δίνονται από την σχέση $t = sx$ όπου x είναι οι πρ. ρίζες της 1 δηλ. $x^2 \equiv 1 \pmod 4$

Ας επικεντρώσουμε να βρούμε τις 8 πρ. ρίζες της 1:

$x^2 \equiv 1 \pmod{60} \Leftrightarrow x^2 \equiv 1 \bmod 4 \qquad x \equiv \pm 1 \pmod 4$

$x^2 \equiv 1 \bmod 3 \Leftrightarrow x \equiv \pm 1 \pmod 3$

$x^2 \equiv 1 \bmod 5 \qquad x \equiv \pm 1 \pmod 5$

(Βλέπε και άσκηση για τις πρ. ρίζες της 1 σε κάθε περίπτωση)

Οπότε έχουμε τα παρακάτω 8 συστήματα

① $\{x \equiv 1 \bmod 4, x \equiv 1 \bmod 3, x \equiv 1 \bmod 5\} \Leftrightarrow x_1 \equiv 1 \pmod{60}$

② $\{x \equiv -1 \bmod 4, x \equiv 1 \bmod 3, x \equiv 1 \bmod 5\} \Leftrightarrow x_2 \equiv 31 \pmod{60}$

③ $\{x \equiv 1 \bmod 4, x \equiv -1 \bmod 3, x \equiv 1 \bmod 5\} \Leftrightarrow x_3 \equiv 41 \pmod{60}$

⋮ κ.ο.κ

Εάν $a \equiv 49 \equiv 7^2 \pmod{60}$ τότε οι ζητούμενες πρ. ρίζες είναι προφανώς οι:

$$x \equiv 7x_1, 7x_2, \ldots, 7x_8 \pmod{60}$$

Άσκηση Να λυθεί η εξίσωση $x^2-3x+2 \equiv 0 \pmod{15}$

Λύση

Τρόπος 1ος. Επειδή $(4,15)=1$ παίρνουμε και τα δύο μέλη με 4 ώστε να μπορέσουμε να κάνουμε τέλειο τετράγωνο:

$4x^2-12x+8 \equiv 0 \pmod{15}$ ⇔

$(2x)^2-2(2x)3+9 \equiv 1 \pmod{15}$ ⇔

$(2x-3)^2 \equiv 1 \pmod{15}$

Έχουμε τώρα το πρόβλημα της εύρεσης των τετραγωνικών ριζών της 1 (mod 15). Από την άσκηση 2) βλέπουμε ότι το πλήθος τους είναι ίσο με $N=2^k=4$ όπου k το πλήθος των πρώτων διαιρετών του 15. Οπότε υπάρχουν 4 τετρ. ρίζες ακριβώς. Χωρίς ειδικότερο κόπο βρίσκουμε $x_1=1$, $x_2=-1$, $x_3=4$ και $x_4=-4$.

Οπότε το ζητούμενο x ικανοποιεί την εξίσωση:

$2x-3 \equiv x_i \pmod{15}$ ⇔ $2x \equiv 3+x_i \pmod{15}$. Όμως $2^{-1} \equiv 8 \pmod{15}$ οπότε $x \equiv (24+8x_i) \bmod 15$

$\equiv (9+8x_i) \bmod 15$ είναι οι τέσσερις ζητούμενες λύσεις.

Τρόπος 2ος Λύνουμε ξεχωριστά τις εξισώσεις:

$x^2-3x+2 \equiv 0 \pmod 3$

$x^2-3x+2 \equiv 0 \pmod 5$

Από την πρώτη παίρνουμε $x^2 \equiv 3x-2 \equiv -2 \equiv 1 \pmod 3$ με ρίζες $x=1$ ή $2 \pmod 3$ και από την δεύτερη παίρνουμε αυτές δύο λύσεις $x=1$ ή $2 \pmod 5$

Λύνοντας τα 4 γραμμικά συστήματα που προκύπτουν παίρνουμε ξανά τις ίδιες λύσεις $\pmod{15}$

Άσκηση. Δείξτε ότι είναι και αναγκαία συνθήκη για να έχει λύση η εξίσωση $ax^2+bx+c\equiv 0 \pmod{p^e}$ με $p\neq 2$ πρώτος και $(a,p)=1$ είναι να υπάρχει η τετραγωνική ρίζα $\pmod p$ του b^2-4ac. Σ' αυτή την περίπτωση οι λύσεις x δίνονται από τον τύπο

$$x\equiv (2a)^{-1}(-b\pm s)$$

όπου s είναι μια τετρ. ρίζα του $b^2-4ac \pmod{p^e}$

Λύση Έχουμε $(4a,p)=1$ αφού το $4a$ έχει αντίστροφο mod p^e και αφού η $ax^2+bx+c\equiv 0 \pmod{p^e}$ είναι ισοδύναμη με $(4a)(ax^2+bx+c)\equiv 0 \pmod{p^e}$ ή

$$(2ax+b)^2\equiv (b^2-4ac) \pmod{p^e}$$

Επειδή s τ υποθέσεως $b^2-4ac\in Q_p \Rightarrow b^2-4ac\in Q_{p^e}$ αφού το b^2-4ac έχει μόνο δύο διαφορετικές τετραγωνικές ρίζες έστω $\pm s \pmod{p^e}$. Οπότε $2ax+b\equiv \pm s \pmod{p^e}$

$\Rightarrow 2ax\equiv -b\pm s \pmod{p^e} \Rightarrow x\equiv (2a)^{-1}(-b\pm s)$ όπου $(2a)^{-1}$ είναι ο αντίστροφος του $2a \pmod{p^e}$.

14) Να βρείτε τις τετραγωνικές ρίζες του $a=73 \pmod{144}$

Λύση: $144=2^4\cdot 3^2$. Οπότε θα πρέπει $73\in Q_{2^4}$ και $73\in Q_3$ (βλέπε και άσκηση 10). Όμως $73\equiv 1 \bmod 8$ και $73\equiv 1 \pmod 3$. Άρα $73\in Q_{144}$.

Για να βρούμε τις τετρ. ρίζες του 73 πρέπει να λύσουμε τις

$x^2-73\equiv x^2-9\equiv 0 \pmod{24} \Leftrightarrow x\equiv \pm 3, \pm 5 \pmod{2^4}$ και

$x^2-73\equiv x^2-1\equiv 0 \pmod{3^2} \Leftrightarrow x\equiv \pm 1 \pmod{3^2}$ και λύνοντας τα 8 γραμμικά συστήματα βρίσκουμε τις 4 τετραγωνικές ρίζες π.χ. το σύστημα

$x \equiv -3 \pmod{24}$, $x \equiv -1 \pmod{9}$ δίνει $x \equiv 125 \pmod{144}$

δηλ. $x \equiv -19 \pmod{144}$ Οι υπόλοιπες τετραγωνικές ρίζες είναι

οι $x \equiv 19, \pm 35, \pm 37, \pm 53 \pmod{144}$

15) Άσκηση. Να βρεθούν τα τετραγωνικά υπόλοιπα (mod 144)

Λύση $a \in Q_{144} \Leftrightarrow a \in Q_3$ κ' $a \equiv 1 \pmod 8$ (βάσει της

άσκησης 10) $\Leftrightarrow a \equiv 1 \pmod 3$ κ' $a \equiv 1 \pmod 8 \Leftrightarrow$

$a \equiv 1 \pmod{24} \Rightarrow Q_{144} = \{1, 25, 49, 73, 97, 121\}$

Ασκήσεις με χρήση των ιδιοτήτων του συμβόλου του Legendre

16) Να αποδειχθεί ότι η ισοδυναμία $x^2+1 \equiv 0 \pmod p$ με $p>2$ πρώτο

έχει λύση αν ο p είναι της μορφής $4\nu+1$

Λύση: Θα πρέπει $\left(\frac{-1}{p}\right) = 1$ όπως θα δούμε $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

οπότε $(-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow 2 \mid \frac{p-1}{2} \Leftrightarrow p = 4\nu+1$

17) Να αποδειχθεί ότι η ισοδυναμία $x^2+2 \equiv 0 \pmod p$, $p>2$ πρώτος

έχει λύση, αν ο p είναι της μορφής $8\nu+1$ ή $8\nu+3$

Λύση: Θα πρέπει $\left(\frac{2}{p}\right) = 1 \Leftrightarrow \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} (-1)^{\frac{p^2-1}{8}} = 1$

όπου $\frac{p^2-1}{8}$ εάν $4 \mid (p+1)$ δηλ για $p \equiv 7$ ή $3 \pmod 8$ και

$\frac{p-1}{4}$ για $4 \mid (p-1)$ δηλ για $p \equiv 1$ ή $5 \pmod 8$.

οπότε θα πρέπει $\frac{p-1}{2} = \frac{p^2-1}{4}$ που συμβαίνει μόνο για

$p \equiv 1 \bmod 8$ ή $p \equiv 3 \bmod 8$

18) Ν' αποδειχθεί ότι η ισοδυναμία

$x^2+3 \equiv 0 \pmod{p^e}$ όπου $p>3$ πρώτος και $e \geq 1$

είναι ισοδύναμη με $p=6m+1$

Λύση θα πρέπει $-3 \in Q_{p^e} \Leftrightarrow -3 \in Q_p$ δηλ. θα πρέπει

$\left(\frac{3}{p}\right)=1$. Από τον κανόνα της τετραγωνικής αντιστροφής

έχουμε: $\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)$ ενώ, εάν $p \equiv 3 \pmod 4$

Περίπτωση $p \equiv 6m+1$ και περιττός Τότε $p \not\equiv 3 \pmod 4$

και $\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{1}{3}\right)=(-1)^{\frac{p-1}{2}}=1$

$p=6m+1$ και περιττός. Τότε $p \equiv 3 \pmod 4$ οπότε

$\left(\frac{3}{p}\right)=-\left(\frac{p}{3}\right)=-\left(\frac{1}{3}\right)=-1$. και

$\left(\frac{-3}{p}\right)=-\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)=\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=1$

$p=6m+5$ και m άρτιος τότε $p \not\equiv 3 \pmod 4$ και

$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{2}{3}\right)=-(-1)^{\frac{p-1}{2}}=-1$

$p=6m+5$ και m περιττός τότε $p \equiv 3 \pmod 4$ οπότε

$\left(\frac{-3}{p}\right)=-\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)=-(-1)^{\frac{p-1}{2}}\left(\frac{2}{3}\right)=(-1)^{\frac{p-1}{2}}=-1$

19) Ν' αποδειχθεί ότι το πλήθος N των λύσεων της

$x^2 \equiv a \pmod{p^e}$ με $p>2$ πρώτος $e \geq 1$ και $(a,p)=1$ είναι

ίσο με $N=\left(\frac{a}{p}\right)+1$

Λύση: —, — Εάν $a \in Q_{p^e}$ τότε $\left(\frac{a}{p}\right)=1$ και

υπάρχουν κατά τα γνωστά πολύ $N=2$ λύσεις Άρα $N=\left(\frac{a}{p}\right)+1$.

Εάν $a \notin Q_{p^e}$ τότε επειδή $(a,p)=1 \Rightarrow p \nmid a \Rightarrow \left(\frac{a}{p}\right)=-1$

και η εξίσωση έχει $N=0$ λύσεις. Άρα $N=\left(\frac{a}{p}\right)+1$

3) 20) Δείξτε ότι το Q_n είναι μια υποομάδα του U_n. Στην περίπτωση που το n έχει μια αρχική ρίζα g και πτ2 δείξτε ότι το Q_n είναι μια κυκλική υποομάδα με τάξη (πλήθος στοιχείων) ίδιο με $\frac{\phi(n)}{2}$

Λύση: Για να δείξουμε ότι το Q_n είναι υποομάδα της U_n αρκεί να δείξουμε ότι περιέχει το μοναδιαίο στοιχείο του U_n και είναι κλειστή ως προς το γινόμενο και το αντίστροφο.

Καταρχήν $1 \in Q_n$ διότι $1 = 1^2$. Έστω $a, b \in Q_n$ με $a = s^2$ και $b = t^2$ τότε $ab = (st)^2$ οπότε $ab \in U_n$. Τέλος αν $a = s^2$ με $s \in U_n$ τότε $a^{-1} = (s^{-1})^2$ και άρα $a^{-1} \in Q_n$.

Τώρα εάν το n έχει μια αρχική ρίζα g τότε η U_n είναι κυκλική ομάδα με πλήθος στοιχείων ίδιο με $\phi(n)$:

$$U_n = \{g^0, g^1, \dots, g^{\phi(n)-1}\}$$

Είναι εύκολο να δείξουμε ότι $Q_n = \{ g^{2\lambda} / 0 \le 2\lambda < \phi(n)-1 \}$ δηλ. το Q_n αποτελείται μόνο από τις άρτιες δυνάμεις του g. Παρατηρούμε εάν τα $\lambda_1 \neq \lambda_2$ τότε προκύπτει $g^{2\lambda_1} \neq g^{2\lambda_2} \pmod{n}$ οπως εύκολα μπορούμε να αποδείξουμε διότι το $\phi(n)$ είναι άρτιος αριθμός για $n > 2$.

Οπότε $|Q_n| = \frac{\phi(n)}{2}$

21) Να βρεθούν τα στοιχεία του Q_{25}

Λύση: 1ος τρόπος $25 = 5^2$. οπότε $a \in Q_{25} \Leftrightarrow a \in Q_5$ άρα

$a \equiv 1$ ή $4 \pmod 5 \Rightarrow Q_{25} = \{1, 4, 6, 9, 11, 14, 16, 21, 19, 24\}$

<u>2ος τρόπος</u> Το 2 είναι εύκολα αρχική ρίζα του 25. Άρα από τα προηγούμενα έχουμε

$Q_{25} = \{g^0, g^2, g^4, g^6, g^8, g^{10}, g^{12}, g^{14}, g^{16}, g^{18}\} = \{1, 4, 16, \dots\}$

22) Ανήκει το $10 \in Q_{29}$; Λύση: $\left(\frac{10}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{5}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{29}{5}\right) = -\left(\frac{4}{5}\right)$

$= -1$

23) Άσκηση Να βρεθούν τα Q_7 και το Q_{29}

Λύση το $g=2$ είναι αρχική ρίζα του Q_{29} και το $g=3$ του Q_7. Οπότε από Άσκηση 20 έχουμε ότι τα Q_7 και Q_{29} αποτελούνται από τις κάτω δυνάμεις της αρχικής ρίζας δηλαδή:

$$Q_7 = \{3^2, 3^4, 3^6 = 1\} = \{2, 4, 1\}$$

Όμοια $Q_{29} = \{g^0, g^2, \dots g^{26}\} = \{1, 4, \dots\}$

24) Άσκηση Να βρεθούν τα $\left(\frac{a}{7}\right)$ και $\left(\frac{a}{29}\right)$ με την χρήση της προηγούμενης άσκησης

Λύση: Από την προηγούμενη άσκηση είδαμε ότι τα τετραγωνικά υπόλοιπα $(\bmod 7)$ είναι τα $1, 2, 4$ οπότε

$$\left(\frac{a}{7}\right) = \begin{cases} 1 & \text{για } a \equiv 1, 2 \text{ ή } 4 \pmod 7 \\ 0 & \text{για } 7 \mid a \\ -1 & \text{για } a \equiv 3, 5 \text{ ή } 6 \pmod 7 \end{cases}$$

Όμοια $\left(\frac{a}{29}\right) = \begin{cases} 1 & \text{για } a = 1, g^2, \dots, g^{26} \\ 0 & \text{για } 29 \mid a \\ -1 & \text{αλλιώς} \end{cases}$

25) Άσκηση. Δείξτε ότι αν ο $p > 2$ είναι πρώτος και g μία αρχική ρίζα $(\bmod p)$, τότε

$$\left(\frac{g^i}{p}\right) = (-1)^i \quad \text{για κάθε } i.$$

Ισχύει το ίδιο για $p = 2$;

Λύση. Από άσκηση 20 ξέρουμε ότι τα μόνα τετρ. υπόλοιπα είναι οι αρτιές δυνάμεις του g. Επίσης είναι γνωστό ότι

καμμία δύναμη g^i του g δεν διαιρείται με το p όπου $p \nmid g$.

Οπότε

$$\left(\frac{g^i}{p}\right) = \begin{cases} +1 & \text{αν } i \text{ άρτιος} \\ -1 & \text{αν } i \text{ περιττός} \end{cases} = (-1)^i$$

Για $p=2$ έχουμε $g \equiv 1 \bmod 2$ οπότε

$\left(\frac{g^i}{p}\right) = \left(\frac{1}{p}\right) = 1$ που ισχύει πάντα η μοναδική δύναμη του 2 που ανήκει στο $\mathbb{Q}_2$ είναι η μηδενική ($\mathbb{Q}_2 = \{1\}$)

β) Δείξτε ότι για $p \neq 2$ ισχύει $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$

Λύση: Έστω g μία αρχική ρίζα του p. Γνωρίζουμε

$$g^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Οπότε αν $a \equiv g^i \pmod p$ για κάποιο i τότε

$\left(\frac{a}{p}\right) = \left(\frac{g^i}{p}\right) = (-1)^i$ και $a^{\frac{p-1}{2}} \equiv g^{i\left(\frac{p-1}{2}\right)}$

οπότε $a^{\frac{p-1}{2}}$ για i άρτιο $\equiv g^{(2k)\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^k \equiv 1 = (-1)^i$

και $a^{\frac{p-1}{2}}$ για i περιττό $\equiv g^{(2l+1)\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^l g^{\frac{p-1}{2}} \equiv -1 \equiv (-1)^i$

οπότε αποδείξαμε την ισότητα.

γ) Άσκηση. Να βρεθεί το $\left(\frac{11}{19}\right)$.

Λύση: Το 11 και το 19 είναι πρώτοι οπότε μπορούμε να χρησιμοποιήσουμε τον νόμο της τετραγωνικής αντιστροφής.

$$\left(\frac{11}{19}\right) = \left(\frac{19}{11}\right)(-1)^{\frac{19-1}{2}\cdot\frac{11-1}{2}} = \left(\frac{19}{11}\right)(-1)^{45} = -\left(\frac{19}{11}\right)$$

Οπότε:

$$-\left(\frac{19}{11}\right) = -\left(\frac{8}{11}\right) = -\left(\frac{2^2\cdot 2}{11}\right) = -\left(\frac{2}{11}\right)^2\cdot\left(\frac{2}{11}\right) = -\left(\frac{2}{11}\right) = (-1)(-1)^{\frac{11^2-1}{8}}$$

$$= 1$$

Άλλος τρόπος με Λήμμα του Gauss:

$\left(\frac{11}{19}\right) = (-1)^M$ όπου M το πλήθος των στοιχείων της τάξης

$$\{11,\ 2\cdot 11 \pmod{19},\ 3\cdot 11 \pmod{19},\ \dots,\ 9\cdot 11 \pmod{19}\} \cap \{10, 11, \dots, 18\}$$

$$= \{11, 14, 17, 12\} \text{ οπότε } \Rightarrow \left(\frac{11}{19}\right) = (-1)^4 = +1$$

Στις ασκήσεις που ακολουθούν αποδεικνύεται η παρακάτω πρόταση: Έστω $n = p_1^{e_1}\cdots p_k^{e_k}$ με $p_1 < p_2 < \cdots < p_k$ πρώτοι.

Τότε $U_n \cong \begin{cases} C_2 \times C_2^{e_1-2} \times C_{\phi(p_2^{e_2})} \times \cdots \times C_{\phi(p_k^{e_k})} & \text{αν } p_1^{e_1} = 2^{e_1} \text{ και } e_1 \geq 2, \text{ και} \\ C_{\phi(p_1^{e_1})} \times \cdots \times C_{\phi(p_k^{e_k})} & \text{αν } p_1^{e_1} = 2 \text{ ή αν } 2 \nmid n \end{cases}$

Ορισμοί • Με C_n συμβολίζουμε μια κυκλική πολλαπλασιαστική ομάδα με n στοιχεία δηλ. $C_n = \{1, g, g^2, \dots, g^{n-1}\}$ όπου g είναι ένας γεννήτορας της C_n

• Δύο ομάδες G_1 και G_2 είναι ισόμορφες και γράφουμε $G_1 \cong G_2$ αν υπάρχει 1-1 και επί $h: G_1 \to G_2$ που "σέβεται" τις πράξεις δηλ. $h(g_1 \cdot g_1^*) = h(g_1)\cdot h(g_1^*)$ (το h λέγεται τότε ομομορφισμός)

Παράδειγμα

Γνωρίζουμε ότι η U_n είναι κυκλική αν $n = 1, 2, 4$ ή p^e ή $2p^e$
όπου $p > 2$ πρώτος

Σ' αυτές τις περιπτώσεις η τάξη της ομάδας (το πλήθος των στοιχείων της) είναι ίση με $\phi(n)$.

Οπότε σ' αυτές τις περιπτώσεις $U_n \cong C_{\phi(n)}$ ή με άλλα λόγια
(υπάρχει μ στο $\mathbb{Z}$ ώστε $U_n \cong (\zeta_n)^\mu$ ($n = 1, 2, 4, p^e$ ή $2p^e$ και $n = \phi(n)$)

- Το ευθύ γινόμενο $G_1 \times G_2$ δύο ομάδων G_1, G_2 αποτελείται απ' όλα τα διατεταγμένα ζεύγη (g_1, g_2) με $g_1 \in G_1$ και $g_2 \in G_2$. Έστω ότι η πράξη του πολλαπλασιασμού στο G_1 με ουδέτερο e και στον G_2 με ουδέτερο e'. Τότε το $G_1 \times G_2$ είναι ομάδα αν ορίσουμε τον πολλαπλασιασμό ως εξής: $(g_1, g_2) \cdot (g_1', g_2') = (g_1 \circ g_1', g_2 \square g_2')$

Το ουδέτερο στοιχείο του $G_1 \times G_2$ είναι το $(1_{G_1}, 1_{G_2})$ όπου 1_{G_1} είναι το ουδέτερο στο G_1 και όμοια για το 1_{G_2}

Εύκολα με επαγωγή μπορούμε να ορίσουμε και ευθύ γινόμενο
$G_1 \times G_2 \times \ldots \times G_k$

Παράδειγμα Δείξτε ότι αν $(n, m) = 1$ τότε $C_m \times C_n \cong C_n \times C_m \cong C_{mn}$
(π.χ. $C_{20} \times C_3 \cong C_{60}$)

Λύση: Τα στοιχεία του C_m είναι της μορφής g^i όπου g είναι ένας γεννήτορας του C_m. Όμοια τα στοιχεία του C_n είναι της μορφής h^j όπου h ένας γεννήτορας του C_n. Οπότε ορίζουμε ένα ισομορφισμό $f: C_m \times C_n \to C_{mn}$ ως εξής
$h((g^i, h^j)) = K^{(m m_1 j + n n_1 i)}$
όπου m_1 και n_1 είναι ακέραιοι για τους οποίους ισχύει
$m m_1 + n n_1 = 1$ (τέτοιοι υπάρχουν διότι $(m, n) = 1$)

και Κινέζικο υπόλοιπο του C_{mn}.

Άσκηση. Δείξτε ότι αν $(m,n)=1$ τότε $U_m \times U_n \cong U_{mn}$

Απόδειξη περίπου όπως στην προηγούμενη άσκηση.

Έστω $U_m=\{x_1, x_2, \dots, x_{\varphi(m)}=1\}$ και $U_n=\{y_1, y_2, \dots, y_{\varphi(n)}=1\}$

Ορίζουμε τον ισομορφισμό ως εξής

$h: U_m \times U_n \to U_{mn}$ με

$h((x,y)) \equiv (m m_1 y + n n_1 x) \pmod{mn}$

όπου m_1, n_1 τέτοιοι ώστε $m m_1 + n n_1 = 1$ (τέτοιοι υπάρχουν διότι $(m,n)=1$)

είναι εύκολο να δείξουμε ότι

$h(x_1 x_2, y_1 y_2] = h(x_1, y_1) \cdot h(x_2, y_2)$ χρησιμοποιώντας την σχέση ότι $m m_1 = 1 - n n_1$ ή την $n n_1 = 1 - m m_1$ όπου χρειάζεται.

Επίσης εύκολα η h είναι 1-1:

$h(x_1, y_1) = h(x_2, y_2) \Rightarrow m m_1 y_1 + n n_1 x_1 \equiv m m_1 y_2 + n n_1 x_2$

$\Leftrightarrow m m_1 (y_1 - y_2) + n n_1 (x_1 - x_2) \equiv 0 \pmod{mn}$

$\Rightarrow \begin{cases} n n_1 (x_1 - x_2) \equiv 0 \pmod{m} \\ m m_1 (y_1 - y_2) \equiv 0 \pmod{n} \end{cases} \iff \begin{cases} (x_1 - x_2) - m m_1 (y_1 - x_2) \equiv 0 \pmod{m} \\ (y_1 - y_2) - n n_1 (y_1 - y_2) \equiv 0 \pmod{n} \end{cases}$

$\Leftrightarrow x_1 \equiv x_2 \bmod m \Leftrightarrow x_1 = x_2$

$y_1 \equiv y_2 \bmod n \quad y_1 = y_2$

(διότι τα $x_i < m$ και τα $y_i < n$)

Οπότε η h είναι ομομορφισμός και 1-1 άρα είναι και επί δηλ. ισομορφισμός.

Από τις προηγούμενες ασκήσεις προκύπτει τέλος ότι

αν $n = p_1^{e_1} \dots p_k^{e_k}$ είναι η ανάλυση του n σε πρώτους τότε

$$U_n \cong C_{\phi(p_1^{e_1})} \times \dots \times C_{\phi(p_k^{e_k})} \quad \text{για } p_1 > 2$$

και για $p_1 = 2$ έχουμε $U_n \cong U_{2^{e_1}} \times C_{\phi(p_2^{e_2})} \times \dots \times C_{\phi(p_k^{e_k})}$

Για να αποδείξουμε την πρόταση που ακολουθεί θα πρέπει να βρούμε το $U_{2^{e_1}}$ για τις διάφορες περιπτώσεις του e_1.

1) Εαν $p_1^{e_1} = 2^1 = 2$ τότε $U_{p_1^{e_1}} = U_2 = \{1\}$ οπότε δεν χρειάζεται στο γινόμενο των υπόλοιπων κυκλικών ομάδων οπότε

$$U_n \cong C_{\phi(2)} \times C_{\phi(p_2^{e_2})} \times \dots \times C_{\phi(p_k^{e_k})} \cong C_{\phi(p_2^{e_2})} \times \dots \times C_{\phi(p_k^{e_k})}$$

2) Εαν $p_1^{e_1} = 4$ τότε $U_4 = \{1, 3\} = C_2$ οπότε έχουμε

$$U_n \cong C_2 \times C_{\phi(p_2^{e_2})} \times \dots \times C_{\phi(p_k^{e_k})}$$

3) Αν το $p_1 > 2$ τότε δεν μας απασχολούν οι δυνάμεις του 2 οπότε $U_n \cong C_{\phi(p_1^{e_1})} \times \dots \times C_{\phi(p_k^{e_k})}$ τέλος αν

4) $p_1^{e_1} = 2^{e_1} \neq 8$ Τότε μπορούμε να αποδείξουμε ότι $U_{2^{e_1}} = \{\pm 5^i \mid 0 \le i < 2^{e_1-2}\} = \{\pm 3^j \mid 0 \le j < 2^{e_1-2}\}$ δηλ

καθε στοιχείο του είναι της μορφής $(-1)^\ell 5^i$ όπου $\ell = 0, 1$ και $0 \le i < e_1 - 2$ και άρα το $U_{2^{e_1}}$ είναι ισόμορφο με το $C_2 \times C_{2^{e_1-2}}$ όπου ο ισομορφισμός ορίζεται ως εξής:

$$h((-1)^\ell 5^i) = ((-1)^\ell, 5^i) \in C_2 \times C_{2^{e_1-2}}$$ δηλαδή

το (-1) είναι τάξη ίση με 2 και το 5 αποδείκνυεται ότι έχει τάξη 2^{e_1-2} δηλ. $5^{2^{e_1-2}} \equiv 1 \bmod 2^{e_1}$.