ΠΡΩΤΗ ΆΣΚΗΣΗ

ΣΤΗΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ

Όνομα: **Λιβαθινός Νικόλαος** **2291**

Ημερομηνία: 23/5/2003

Άσκηση 1

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

Προκειμένου να δώσουμε τις υποομάδες θα πρέπει αρχικά να ορίσουμε τα σύνολα των ομάδων Z_{11} και Z_{15}^*. Όπως γνωρίζουμε ισχύει ότι:

$$Z_n = \{[a]_n : 0 \le a \le n-1\} \text{ και } Z_n^* = \{[a]_n \in Z_n : \gcd(a,n) = 1\}$$

Εφαρμόζοντας τα παραπάνω έχουμε ότι Z_{11}={0,1,2,3,4,5,6,7,8,9,10} κάνοντας τη γνωστή σύμβαση ότι το 0 αναπαριστά το $[0]_{11}$ κοκ. Επίσης έχουμε ότι Z_{15}={0,1,2,3,4,5,6,7,8,9,10, 11,12,13,14} άρα Z^*_{15}={1,2,4,7,8,11,13,14}.

Στη συνέχεια προκειμένου να βρούμε τις υποομάδες των ομάδων, χρησιμοποιούμε στοιχεία γεννήτορες που προέρχονται από τα σύνολα των ομάδων. Με κάθε στοιχείο a της ομάδας δημιουργούμε και μια υποομάδα σύμφωνα με τη σχέση $< a >= a \oplus a \oplus ... \oplus a$.

Έτσι για την ομάδα Z_{11} οι υποομάδες της έχουν τον τελεστή $+_{11}$ και τα ακόλουθα σύνολα:

<0>={0}

<1>={0,1,2,3,4,5,6,7,8,9,10}

<2>={0,1,2,3,4,5,6,7,8,9,10}

<3>={0,1,2,3,4,5,6,7,8,9,10}

<4>={0,1,2,3,4,5,6,7,8,9,10}

<5>={0,1,2,3,4,5,6,7,8,9,10}

<6>={0,1,2,3,4,5,6,7,8,9,10}

<7>={0,1,2,3,4,5,6,7,8,9,10}

<8>={0,1,2,3,4,5,6,7,8,9,10}

<9>={0,1,2,3,4,5,6,7,8,9,10}

<10>{0,1,2,3,4,5,6,7,8,9,10}

Επίσης για την ομάδα Z^*_{15} έχουμε υποομάδες με τελεστή τον $\cdot_{15}$ και με τα ακόλουθα σύνολα:

<1>={1}

<2>={1,2,4,8}

<4>={1,4}

<7>={1,4,7,13,14}

<8>={1,2,4,8}

<11>={1,11}

<13>={1,4,7,13}

<14>={1,14}

Άσκηση 2

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

Αρχικά αναπαριστούμε τους αριθμούς a και b ως γινόμενο πρώτων παραγόντων. Έστω λοιπόν ότι:

$a = p_1^{e1} p_2^{e2} \dots p_k^{ek} \dots p_l^{el}$ και $b = p_1^{f1} p_2^{f2} \dots p_k^{fk} \dots p_l^{fl}$, όπου ισχύει ότι $\forall p_i : i <= k \Rightarrow p_i <= n_0$ και $\forall p_i : i > k \Rightarrow p_i > n_0$

Επίσης χρησιμοποιούμε μηδενικούς εκθέτες έτσι ώστε να έχουμε κοινούς πρώτους παράγοντες για τους a και b.

Με αυτά υπόψη το γινόμενο ab ορίζεται ως ακολούθως:

$ab = p_1^{e1+f1} p_2^{e2+f2} \dots p_k^{ek+fk} \dots p_l^{el+fl}$ ενώ $\gcd(a,b) = p_1^{\min(e1,f1)} p_2^{\min(e2,f2)} \dots p_k^{\min(ek,fk)} \dots p_l^{\min(el,fl)}$

Εφόσον ισχύει ότι gcd(p^{ab},ab)=p για όλους τους πρώτους που είναι μικρότεροι από το n_0, αυτό σημαίνει όλοι οι πρώτοι που είναι μικρότεροι από το n_0 θα είναι διαιρέτες του γινομένου ab.

Επίσης αποκλείεται η περίπτωση να είναι διαιρέτης του γινομένου ab ένας αριθμός της μορφής p_i^x με I<k και x>1. Αν υπάρχει $p_i^x \mid ab \Rightarrow \exists \mu \in \aleph : \mu p_i^x = ab$ και επομένως έχουμε ότι $p_i^{ab} = p_i^{\mu p_i^x} = \underbrace{p_i^x p_i^x p_i^x \dots p_i^x}_{\mu}$, άρα $p_i^x \mid p_i^{ab}$. Κάτι τέτοιο όμως είναι άτοπο διότι $p_i^x > p_i$ και εμείς γνωρίζουμε ότι ο μέγιστος κοινός διαιρέτης είναι ο p_i.

Με τα προηγούμενα καταλήγουμε στο συμπέρασμα ότι τα αθροίσματα των εκθετών $e_i+f_i=1$ για όλους τους πρώτους που είναι μικρότεροι από n_0. Όμως το ότι το άθροισμα κάνει 1 σημαίνει ότι είτε $e_i=0$ και $f_i=1$ είτε $e_i=1$ και $f_i=0$. Οπότε σε κάθε περίπτωση $\min(e_i,f_i)=0$.

Τέλος μένει να εξετάσουμε τι συμβαίνει στους εκθέτες του γινομένου για τους πρώτους που είναι μεγαλύτεροι του n_0. Εφόσον σε αυτή την περίπτωση γνωρίζουμε πως gcd(p^{ab},ab)=1, σημαίνει ότι κανένας πρώτος μεγαλύτερος από n_0 δεν είναι διαιρέτης του γινομένου. Επομένως τα αθροίσματα $e_i+f_i=0$ και εφόσον οι e_i, f_i είναι θετικοί έχουμε πως $e_i=0$ και $f_i=0$, άρα $\min(e_i,f_i)=0$.

Τελικά έχουμε ότι $\gcd(a,b) = p_1^0 p_2^0 \dots p_l^0 = 1$

Άσκηση 3

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

Προκειμένου να ελέγξουμε αν το σύνολο Z_n μαζί με την πράξη του (modulo) πολλαπλασιασμού είναι ομάδα θα πρέπει να εξετάσουμε κατά πόσο ισχύουν οι ακόλουθες ιδιότητες:

1. Κλειστότητα.
2. Προσεταιριστικότητα

3. Ύπαρξη ταυτοτικού στοιχείου.
4. Ύπαρξη μοναδικού αντίθετου στοιχείου για κάθε στοιχείο του συνόλου.

Αρχικά θα πρέπει να εξηγηθεί τι ακριβώς περιλαμβάνει το σύνολο Z_n. Το Z_n είναι το σύνολο των ακεραίων που όταν διαιρεθούν με n αφήνουν υπόλοιπο από 0 ως n-1.

Με αυτό υπόψη εύκολα βλέπουμε πως ισχύει η κλειστότητα επί του τελεστή $\cdot_n$, εφόσον το γινόμενο δύο ακεραίων είναι και αυτός ακέραιος και το modulo μας βάζει πάλι μέσα στο Z_n.

Επίσης εύκολα βλέπουμε πως ισχύει και η προσεταιριστικότητα:

$([a]_n \cdot_n [b]_n) \cdot_n [c]_n=[ab]_n \cdot_n [c]_n=[(ab)c]_n=[a(bc)]_n=[a]_n \cdot_n ([b]_n \cdot_n [c]_n)$

Όσον αφορά το ταυτοτικό στοιχείο μπορούμε να θέσουμε το $[1]_n$, εφόσον $[a]_n \cdot_n [1]_n=[1]_n \cdot_n [a]_n=[a]_n$

Τέλος μένει να δείξουμε ότι για κάθε στοιχείο του Z_n υπάρχει μοναδικό αντίστροφο στοιχείο. Δηλαδή ότι υπάρχει $[a^{-1}]_n$ ώστε $[a]_n \cdot_n [a^{-1}]_n=[a^{-1}]_n \cdot_n [a]_n=[1]_n$. Ωστόσο σύμφωνα με το πόρισμα 31.26 του βιβλίου, για να έχει (μοναδική) λύση η εξίσωση $ax=1 \pmod n$ πρέπει $\gcd(a,n)=1$. Κάτι που στη γενική περίπτωση δεν ισχύει για το Z_n.

Επομένως εφόσον δεν υπάρχει για κάθε στοιχείο του Z_n αντίθετο, το $(Z_n, \cdot_n)$ δεν αποτελεί ομάδα.

Άσκηση 4

Βρείτε τις λύσεις της εξίσωσης 33x=12 (mod 60).

Προκειμένου να λύσουμε την εξίσωση «τρέχουμε» την ρουτίνα MODULAR-LINEAR-EQUATION-SOLVER(a,b,n) που περιγράφεται στην παράγραφο 31.4 του βιβλίου, με a=33, b=12 και n=60.

Αρχικά θα πρέπει να τρέξουμε τη ρουτίνα EXTENDED-EUCLID(60,33) (προκειμένου να εκτελέσουμε την EXTENDED-EULCID έχουμε αντιστρέψει τα a, n). Οπότε έχουμε:

a	**b**	$\lfloor a/b \rfloor$	**d**	**x**	**y**
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

Στη συνέχεια πρέπει να ελέγξουμε αν d|b δηλαδή αν 3|12 που ισχύει, οπότε προχωρούμε για να βρούμε τις d(=3) λύσεις.

Έχουμε ότι $x_0=-9(12/3) \bmod 60=24$. Οπότε $x_1=24+1(60/3) \bmod 60=44$, $x_2=24+2(60/3) \bmod 60=4$.

Οπότε οι τρεις λύσεις της εξίσωσης είναι:

$X_0=24$

$X_1=44$

$X_2=4$

Άσκηση 5

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

Όπως γνωρίζουμε το μέγεθος του Z_m είναι m. Επίσης γνωρίζουμε πως το Z^*_m είναι ένα υποσύνολο του Z_m στο οποίο κάθε στοιχείο έχει πολλαπλασιαστικό αντίστροφο. Ακόμη από το πόρισμα 31.22 του βιβλίου προκύπτει πως δεν υπάρχει περίπτωση να υπάρχει στοιχείο στο Z_m που να έχει πολλαπλασιαστικό αντίστροφο και να μην ανήκει στο Z^*_m. Τέλος γνωρίζουμε πως το μέγεθος του Z^*_m δίνεται από τη συνάρτηση $\phi(m) = m\prod_{p|m}(1-\frac{1}{p})$.

Επομένως καταλαβαίνουμε πως αρκεί να δείξουμε ότι $m - \phi(m) \geq \sqrt{m}$.

$$m - \phi(m) \geq \sqrt{m}$$

$$m - m\prod_{p|m}(1-\frac{1}{p}) \geq \sqrt{m}$$

$$\sqrt{m} - \sqrt{m}\prod_{p|m}(1-\frac{1}{p}) \geq 1$$

$$\sqrt{m}(1-\prod_{p|m}(1-\frac{1}{p})) \geq 1$$

$$\prod_{p|m}(1-\frac{1}{p}) \leq 1-\frac{1}{\sqrt{m}} \qquad (1)$$

Προκειμένου να αποδείξουμε την τελευταία σχέση διακρίνουμε περιπτώσεις για το $\sqrt{m}$.

- $\sqrt{m}$ είναι πρώτος. Εφόσον $\sqrt{m}$ $\sqrt{m}$ = m καταλήγουμε στο συμπέρασμα πως ο μόνος πρώτος παράγοντας του m είναι ο $\sqrt{m}$ και επομένως η (1) ισχύει με την ισότητα.
- $\sqrt{m}$ είναι σύνθετος. Σε αυτή την περίπτωση μπορούμε να διασπάσουμε τον m σε γινόμενο πρώτων παραγόντων ως $m = p_1^{e1}p_2^{e2}...p_l^{el}$. Έτσι το γινόμενο της (1) γίνεται $(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_l})$. Εφόσον πάντα ισχύει ότι $p_i < \sqrt{m} \forall i$ έχουμε ότι $\frac{1}{p_i} > \frac{1}{\sqrt{m}} \Rightarrow 1-\frac{1}{p_i} < 1-\frac{1}{\sqrt{m}}$. Άρα το γινόμενο φράσσεται από το $\left(1-\frac{1}{\sqrt{m}}\right)^l$. Τέλος παρατηρούμε ότι εφόσον το $\sqrt{m}$ είναι σύνθετος ακέραιος, άρα $\sqrt{m} > 1 \Rightarrow 1-\frac{1}{\sqrt{m}} < 1 \Rightarrow \left(1-\frac{1}{\sqrt{m}}\right)^l < \left(1-\frac{1}{\sqrt{m}}\right)$. Και έτσι αποδείχθηκε ότι η (1) ισχύει και όταν $\sqrt{m}$ είναι σύνθετος.

Επομένως σε κάθε περίπτωση ισχύει η (1) και επομένως πάντα θα υπάρχουν τουλάχιστον $\sqrt{m}$ στοιχεία του Z_m που δεν θα έχουν πολλαπλασιαστικό αντίστροφο.

Άσκηση 6

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

Προκειμένου να δείξουμε ότι μεταξύ δύο συνεχόμενων πρώτων υπάρχουν αυθαίρετα πολλοί σύνθετοι, αρκεί να αποδείξουμε ότι για κάθε θετικό ακέραιο υπάρχει μια ακολουθία διαδοχικών ακεραίων που δεν είναι πρώτοι.

Θέτουμε σαν ακολουθία την: (n+1)!+2, (n+1)!+3,…, (n+1)!+(n+1).

Μπορούμε να αποδείξουμε ότι σε αυτή την ακολουθία κανένας αριθμός δεν είναι πρώτος. Παρατηρούμε ότι κάθε όρος της ακολουθίας έχει τη μορφή (n+1)!+k με 1<k<=n+1. Κάθε όρος μπορεί να διαιρεθεί με το k. Αυτό διότι το k προφανώς διαιρεί τον εαυτό του και εφόσον k<=n+1 θα εμπεριέχεται ως γινόμενο μέσα στο παραγοντικό.

Έτσι κάθε όρο μπορούμε να τον ξαναγράψουμε ως k(1+(1.2.3…k-1)(k+1)(k+2)…(n+1)). Ξεκάθαρα φαίνεται ότι κανείς από τους όρους της ακολουθίας δεν είναι πρώτος.

Άσκηση 7

Δείξτε πώς μπορεί να υπολογιστεί το a^{-1} mod n για κάθε $a \in Z_n^*$, χρησιμοποιώντας την ρουτίνα MODULAR-EXPONENTATION. Υποθέστε ότι γνωρίζετε το φ(n).

Σε αυτή την άσκηση το ζητούμενο είναι να βρούμε έναν τρόπο προκειμένου να υπολογίσουμε τον πολλαπλασιαστικό αντίστροφο εκτελώντας μόνο ύψωση σε θετική δύναμη modulo n. Αυτό δηλαδή που κάνει η ρουτίνα MODULAR-EXPONENTATION.

Το κλειδί για τη λύση είναι το θεώρημα του Euler: $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$. Πολλαπλασιάζοντας και τα δύο μέλη με a^{-1} mod n έχουμε: $a^{\phi(n)} a^{-1} \equiv a^{-1} (\mathrm{mod}\, n) \Rightarrow a^{\phi(n)-1} \equiv a^{-1} (\mathrm{mod}\, n)$.

Επομένως μπορούμε να υπολογίσουμε εύκολα τον πολλαπλασιαστικό αντίστροφο του a καλώντας την MODULAR-EXPONENTATION για το a με εκθέτη το φ(n)-1. Βέβαια αυτό προϋποθέτει ότι θα γνωρίζουμε το φ(n).

Άσκηση 8

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

($\Rightarrow$)

Υποθέτουμε ότι gcd(s,t)=1 και θέλουμε να αποδείξουμε ότι gcd(2^s-1,2^t-1)=1.

Για να αποδείξουμε ότι gcd(2^s-1,2^t-1)=1αρκεί να βρούμε έναν γραμμικό συνδυασμό των 2^s-1 και 2^t-1 που να είναι ίσος με τη μονάδα. Σε αυτή την περίπτωση ο συνδυασμός θα είναι ο ελάχιστος δυνατός θετικός άρα θα είναι και gcd, και προφανώς θα ισχύει ότι gcd(2^s-1,2^t-1)=1.

Εφόσον gcd(s,t)=1 θα υπάρχουν x,y τέτοια ώστε sx+ty=1, κατόπιν μπορούμε να γράψουμε ότι

$$1=2^1-1=2^{sx+ty}-1=>$$

$$1=2^{sx}2^{ty}-2^{ty}+2^{ty}-1=>$$

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

Στη συνέχεια μπορούμε να διασπάσουμε τα $(2^{sx}-1)$, $(2^{ty}-1)$ σύμφωνα με γνωστή ταυτότητα ως ακολούθως:

$$2^{sx}-1=(2^s)^x-1=(2^s-1)(2^{s(x-1)}+2^{s(x-2)}+2^{s(x-3)}+\ldots+2^s) \quad (2)$$

$$2^{ty}-1=(2^t)^y-1=(2^t-1)(2^{t(y-1)}+2^{t(y-2)}+2^{t(y-3)}+\ldots+2^t) \quad (3)$$

Μετά από αυτή τη διάσπαση παρατηρούμε ότι μπορούμε να θέσουμε τις ποσότητες

$$(2^{s(x-1)}+2^{s(x-2)}+2^{s(x-3)}+\ldots+2^s)=\mu \quad (4)$$

$$(2^{t(y-1)}+2^{t(y-2)}+2^{t(y-3)}+\ldots+2^t)=\lambda \quad (5)$$

Όπου τα μ,λ είναι απλώς ακέραιοι.

Έτσι αντικαθιστώντας τις (4), (5) στις (2), (3) και αυτές στην (1) έχουμε:

$$1=\mu 2^{ty}(2^s-1)+\lambda(2^t-1) \quad (6)$$

Από τη σχέση (6) έχουμε αποδείξει το ζητούμενο εφόσον έχουμε φέρει τα (2^s-1), (2^t-1) σε μορφή γραμμικού συνδυασμού που κάνει 1.

$(\Leftarrow)$

Υποθέτουμε ότι $\gcd(2^s-1,2^t-1)=1$ και θέλουμε να αποδείξουμε ότι $\gcd(s,t)=1$. Ωστόσο χρησιμοποιώντας την αρχή της αντιθετοαντιστροφής μπορούμε ισοδύναμα να αποδείξουμε ότι δεδομένου ότι $\gcd(s,t) \neq 1$ ισχύει πως $\gcd(2^s-1,2^t-1) \neq 1$.

Έστω ότι $\gcd(s,t)=d>1$, τότε θα υπάρχουν $w,v \in Z$ ώστε $s=dw$ και $t=dv$.

Επομένως έχουμε ότι:

$$2^s-1=2^{dw}-1=(2^d-1)\mu' \quad (7)$$

$$2^t-1=2^{dv}-1=(2^d-1)\lambda' \quad (8)$$

Από τις σχέσεις (7) και (8) προκύπτει ότι τα (2^s-1), (2^t-1) έχουν ως κοινό τους διαιρέτη το (2^d-1). Εφόσον $d>1$ άρα και $2^d-1>1$ επομένως αποδείχτηκε το ζητούμενο ότι $\gcd(2^s-1,2^t-1) \neq 1$.

Άσκηση 9

Λύστε το σύστημα των εξισώσεων:

X=4 (mod 5)

X=1 (mod 9)

X=2 (mod 11)

Προκειμένου να επιλύσουμε το σύστημα των εξισώσεων χρησιμοποιούμε το κινέζικο θεώρημα και θέτουμε τις εξισώσεις του συστήματος ως τις συνιστώσες a_i του a. Θεωρούμε δηλαδή ότι το x είναι το άγνωστο για εμάς ενώ έχουμε ήδη τις συνιστώσες του (4, 1, 2). Αυτό που πρέπει να κάνουμε είναι να ανακατασκευάσουμε το x από τις συνιστώσες.

Το πρόβλημα είναι καλώς ορισμένο εφόσον τα n_i (5, 9, 11) είναι πρώτοι μεταξύ τους και επομένως μπορούμε να προχωρήσουμε. Για να βρούμε το x πρέπει να υπολογίσουμε τα c_i και να χρησιμοποιήσουμε την σχέση (31.28) του βιβλίου.

Υπενθυμίζουμε ότι αυτά ορίζονται ως εξής:

$$n=n_1n_2\ldots n_k.$$

$$m_i=n/n_i$$

$$c_i=m_i(m_i^{-1} \bmod n_i)$$

$$x=\sum c_i m_i \pmod n$$

Στην περίπτωση μας έχουμε ότι n=5*9*11=495.

Επίσης έχουμε ότι $m_1=99$, $m_2=55$, $m_3=45$. Στη συνέχεια πρέπει να βρούμε τους πολλαπλασιαστικούς αντιστρόφους των m_i. Για να βρεθεί αυτό πρέπει να λυθούν οι εξισώσεις $m_i\, m_i^{-1}=1 \bmod n_i$[1]. Τελικά βρίσκουμε ότι

$$99^{-1}=4 \bmod 5$$

$$55^{-1}=1 \bmod 9$$

$$45^{-1}=1 \bmod 11.$$

Κατόπιν βρίσκουμε τα c_i

$$C_1=99(4 \bmod 5)=396$$

$$C_2=55(1 \bmod 9)=55$$

$$C_3=45(1 \bmod 11)=45$$

Οπότε τελικά έχουμε ότι x=396*4+55*1+45*2=1729 mod 495

Άσκηση 10

Δείξτε ότι

Αν α και β άρτιοι τότε gcd(a,b)=2gcd(a/2,b/2).

Αν α είναι περιττός και β είναι άρτιος, τότε gcd(a,b)=gcd(a,b/2).

Αν α και β είναι περιττοί τότε gcd(a,b)=gcd((a-b)/2,b).

1. Για το πρώτο μέρος του ερωτήματος μπορούμε να κάνουμε άμεσα εφαρμογή του πορίσματος 31.4. Υπενθυμίζω ότι το πόρισμα αυτό ορίζει την αλήθεια της ακόλουθης σχέσης:

$$gcd(an,bn)=ngcd(a,b)$$

Εφόσον οι α, β είναι άρτιοι μπορούμε να τους γράψουμε στην μορφή a=2κ, b=2λ για κάποιους ακέραιους κ, λ. Επομένως έχουμε:

$$Gcd(a,b)=gcd(2\kappa,2\lambda)=2gcd(\kappa,\lambda)=2gcd(a/2,b/2)$$

2. Για να λύσουμε το δεύτερο μέρος του ερωτήματος διασπούμε τους α,β σε γινόμενο πρώτων παραγόντων λαμβάνοντας υπόψη ότι α είναι περιττός και β άρτιος. Έτσι έχουμε:

[1] Εναλλακτικά μπορούμε να χρησιμοποιήσουμε τα αποτελέσματα της άσκησης 7.

$$a = 2^0 p_1^{e1} p_2^{e2} \ldots p_l^{el}$$

$$b = 2^k p_1^{f1} p_2^{f2} \ldots p_l^{fl}$$

Οπότε έχω $\gcd(a,b) = 2^{\min(0,k)} p_1^{\min(e1,f1)} p_2^{\min(e2,f2)} \ldots p_l^{\min(el,fl)} =>$

$\gcd(a,b) = p_1^{\min(e1,f1)} p_2^{\min(e2,f2)} \ldots p_l^{\min(el,fl)}$

Επίσης $b/2 = 2^{k-1} p_1^{f1} p_2^{f2} \ldots p_l^{fl}$, οπότε

$$\gcd(a,b/2) = 2^{\min(0,k-1)} p_1^{\min(e1,f1)} p_2^{\min(e2,f2)} \ldots p_l^{\min(el,fl)} =>$$

$$\gcd(a,b/2) = p_1^{\min(e1,f1)} p_2^{\min(e2,f2)} \ldots p_l^{\min(el,fl)} = \gcd(a,b)$$

Οπότε δείξαμε το ζητούμενο.

3. Προκειμένου να αποδείξουμε και το τρίτο μέρος της άσκησης αρχίζουμε κάνοντας πράξεις με τους gcd.

Έτσι έχουμε:

gcd(a,b)=ax1+by1 για κάποιους ακέραιους x1, y1 (1)

gcd(a-b,b)=(a-b)x2+by2 για κάποιους ακέραιους x2, y2 (2)

Από την (1) έχω: gcd(a,b)=ax1+by1+bx1-bx1=(a-b)x1+(y1+x1)b, ωστόσο από τη (2) έχουμε ότι ο gcd(a-b,b)|(α-β) και gcd(a-b,b)|b, άρα gcd(a-b,b)|gcd(a,b) (3)

Επίσης από την (2) έχω: gcd(a-b,b)=ax2+(y2-x1)b, ωστόσο από την (1) έχω ότι gcd(a,b)|a και gcd(a,b)|b άρα gcd(a,b)|gcd(a-b,b) (4).

Επομένως από (3) και (4) έχω ότι gcd(a,b)=gcd(a-b,b).

Επίσης εφόσον α,β είναι περιττοί η διαφορά τους θα είναι άρτια και επομένως σύμφωνα με το δεύτερο μέρος της άσκησης μπορούμε να γράψουμε την ακόλουθη ζητούμενη σχέση:

gcd(a,b)=gcd((a-b)/2,b)