ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

# ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΩΜΑΤΩΝ ΣΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ MASSEY-OMURA

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ : ΑΘΑΝΑΣΙΟΣ ΣΠΥΡΟΠΟΥΛΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:ΑΛΕΞΑΝΔΡΟΣ ΠΑΠΑΙΩΑΝΝΟΥ

ΑΘΗΝΑ 2011

# Περιεχομενα

Αφιερωνεται

Στους γονεις μου  Μιχαηλ-Κωνσταντια.
Στο προπαππου μου Κωσταντινο Σπυροπουλο  ο οποιος εκτελεστηκε από ταγματασφαλιτες στην περιοδο της χιτλερικης κατοχης.

# ΕΙΣΑΓΩΓΗ

Σκοπος αυτης της διπλωματικης είναι η αναλυτικη παρουσιαση της αποδειξης του Witt στο θεωρημα του Wedderburn για τους πεπερασμενους δακτυλιους διαιρεσης .Στο πρωτο κεφαλαιο αναφερομαστε στις βασικες αλγεβρικες δομες και στις ιδιοτητες τους.
Στο δευτερο κεφαλαιο προχωραμε στην αποδειξη του θεωρηματος του Weddeburn,δηλαδη οτι κάθε πεπερασμενος δακτυλιος διαιρεσης είναι σωμα.
Στο τελευταιο κεφαλαιο αναφερουμε εφαρμογες των σωματων στην κρυπτογραφια με τη βοηθεια του κρυπτοσυστηματος Massey Omura. Επισης γινεται αναφορα σε θεωρηματα γραμμικων ισοδυναμιων και στη χρηση ελλειπτικων καμπυλων στην κρυπτογραφια .Ετσι ο συγγραφεας θα προσπαθησει να φτιαξει μια γεφυρα μεταξυ του θεωρητικου και του εφαρμοσμενου τμηματος της αλγεβρας και της κρυπτολογιας

Κεφαλαιο 1 Αλγεβρικες Δομες

## 1.1 Συνολα-Εσωτερικη πραξη

Στο Κεφαλαιο αυτό αρχικα θα ασχοληθουμε με βασικες αλγεβρικες δομες και εννοιες οι οποιες εμφανιζονται στο θεωρημα του Wedderburn .Αυτο θα το κανουμε κλιμακωτα ξεκινωντας από την εννοια του συνολου και καταληγοντας σε αυτην του διανυσματικου χωρου.Η εννοια του συνολου είναι <αρχικη> και την δεχομαστε αξιωματικα χωρις αποδειξη.

**Ορισμος:**Συνολο είναι κάθε συλλογη σαφως διακριτων και καλως καθορισμενων αντικειμενων.

Τα αντικειμενα τα οποια απαρτιζουν ένα συνολο καλουνται στοιχεια του συνολου. Με τον ορο καλως καθορισμενα εννοουμε ότι αν Α είναι ένα συνολο και α έιναι καποιο αντικειμενο , τοτε ειτε το α ανηκει στο συνολο ειτε δεν ανηκει.
Αν ένα συνολο Α αποτελειται από στοιχεια και αν α είναι ένα από αυτά τα στοιχεια ,θα συμβολιζουμε αυτό το δεδομενο γραφοντας $a \in A$.Υπαρχει ένα ακριβως συνολο το οποιο δεν εχει στοιχεια και ονομαζεται το κενο συνολο,συμβολίζεται με $\varnothing$ .
Ενα συνολο Γ λεγεται υποσυνολο του συνολου Α αν κάθε στοιχειο του Γ ανηκει και στο Α και γραφουμε ότι $\Gamma \subseteq A$.Ενα απλο παραδειγμα συνολου είναι οι πραγματικοι αριθμοι $\mathbb{R}$ και ένα υποσυνολο τους είναι το συνολο των ακεραιων $\mathbb{Z}$ το οποιο είναι γνησιο υποσυνολο των πραγματικων αριθμων, $\mathbb{R} \supset \mathbb{Z}$ Εχοντας ορισει την εννοια του συνολου και του υποσυνολου ,τωρα θα

ορισουμε τις εννοιες της διαμερισης και της ισοδυναμιας και του καρτεσιανου γινομενου δυο συνολων.

**Ορισμος**:Διαμεριση ενός συνολου Α καλειται μια αναλυση του Α σε υποσυνολα τετοια ώστε κάθε στοιχειο του συνολου να ανηκει σε ένα και μονο ένα από τα υποσυνολα.Αυτα είναι τα υποσυνολα της διαμερισης

Συνεπως τα υποσυνολα μιας διαμερισης δεν εχουν κανενα κοινο στοιχειο οποτε είναι μεταξυ τους ξενα.
Για να οριστει η εννοια της σχεσης ισοδυναμιας που θα παιξει σημαντικο ρολο στην αποδειξη πρεπει πρωτα να ορισουμε τη εννοια σχεση μεταξυ δυο συνολων Α,Β.

**Ορισμος**:Σχεση S από το συνολο Α στο συνολο Β είναι ένα υποσυνολο του Καρτεσιανου γινομενου $A \times B$.

Αν $A = B$ τοτε η σχεση S λεγεται σχεση στο συνολο Α.Η σχεση $a \sim b$ δηλωνει ότι τα $a,b$ ανηκουν στο ιδιο υποσυνολο για δεδομενη διαμεριση ενός συνολου Α που περιεχει τα $a,b$.

Μια σχεση S στο συνολο Α καλειται σχεση ισοδυναμιας στο συνολο Α αν ικανοποιουνται οι ακολουθες τρεις ιδιοτητες

1. $(a,a) \in S$, για κάθε $a \in A$, (ανακλαστικη ιδιοτητα)

2.αν $(a,b) \in S$, τοτε και $(b,a) \in S$ (συμμετρικη ιδιοτητα)

3.αν $(a,b) \in S$ και $(b,c) \in S$, τοτε $(a,c) \in S$ (μεταβατικη ιδιοτητα)

Ο πιο συνηθισμενος τροπος συμβολισμου μιας σχεσης ισοδυναμιας στο συνολο Α είναι με το συμβολο $\sim$ και διαβαζεται ισοδυναμο.Για κάθε ζευγος $(a,b) \in S$ που ανηκει στη σχεση γραφουμε $a \sim b$.
Αν $S$ είναι μια σχεση ισοδυναμιας στο συνολο Α και $a \in A$,το συνολο των στοιχειων x του Α που είναι ισοδυναμα με το $a$ ,λεγεται κλαση ισοδυναμιας του $a$ και συμβολιζεται με $a$ ,δηλαδη

$$a = x : x \in A \, \mu\varepsilon \, (x,a) \in S$$

Το συνολο ολων των κλασεων ισοδυναμιας συμβολιζεται με $A/S$ και αποτελει μια διαμεριση του συνολου Α,αφου οι κλασεις ισοδυναμιας είναι μη κενα συνολα ,ανα δυο ξενα μεταξυ τους και η ενωση τους είναι το συνολο Α.Το συνολο $A/S$ λεγεται συνολο πηλικο του Α ως προς τη σχεση ισοδυναμιας $S$.
Μια πολύ ενδιαφερουσα σχεση ισοδυναμιας είναι η ισοδυναμια modulo n, $n \in \mathbb{Z}$( $\equiv$ (modn)).

**Ορισμος(Ισοτιμια modulo n):** Εστω h,k δυο ακεραιοι στο $\mathbb{Z}$ και n οποιοσδηποτε θετικος ακεραιος.Οριζουμε ότι ο h είναι ισοτιμος με τον k modulo n , και γραφουμε $h \equiv k(\mathrm{mod}\, n)$ ,αν ο h-k διαιρειται με το n ,δηλαδη αν $h-k=n\cdot s$ για καποιο $s \in \mathbb{Z}$.

Οι κλασεις ισοδυναμιας της ισοτιμιας modulo n λεγονται κλασεις υπολοιπων modulo n.Κάθε κλαση υπολοιπων modulo $n \in \mathbb{Z}^+$ περιεχει απειρο πληθος στοιχειων.Αν π.χ $n=3$ οι κλασεις ισοδυναμιας θα ηταν τρια απειρα συνολα τα [0],[1],[2] οπου $[0]=3\cdot z, z \in \mathbb{Z}$, $[1]=3\cdot z+1, z \in \mathbb{Z}$, $[2]=3\cdot z+2, z \in \mathbb{Z}$

Εχοντας αναφερει την εννοια του συνολου ,εφοδιαζουμε ένα με κενο συνολο(ώστε να υπαρχει νοημα) με μια εσωτερικη πραξη(η διμελη πραξη) μεταξυ στοιχειων του συνολου.

**Ορισμος:**Εσωτερικη πραξη σε ένα μη κενο συνολο Α είναι μια απεικονιση Φ της μορφης $\Phi: A \times A \to A$.
Αν $(a,b) \in A \times A$ ,τοτε το στοιχειο $\Phi((a,b))$ ονομαζεται αποτελεσμα της πραξης Φ μεταξυ των δυο στοιχειων του συνολου.

Επειδη το διατεταγμενο ζευγος στοιχειων του Α απεικονιζεται παλι σε ένα στοιχειο του Α λεμε συχνα ότι το συνολο Α είναι κλειστο ως προς την εσωτερικη πραξη στο Α.Για τον συμβολισμο μιας εσωτερικης πραξης χρησιμοποιουμε συνηθως ένα από τα συμβολα $\circ, \bullet, +, .$Οι γνωστες μας πραξεις ,προσθεση και πολλαπλασιασμος ακεραιων η πραγματικων αριθμων είναι εσωτερικες πραξεις στο συνολο των ακεραιων $\mathbb{Z}$ ,η στο συνολο $\mathbb{R}$ των πραγματικων.
Οι πιο βασικες ιδιοτητες που ικανοποιουν οι διαφορες εσωτερικες πραξεις είναι η αντιμεταθετικη,η προσεταιριστικη και η επιμεριστικη ιδιοτητα από αριστερα και δεξια.

**Ορισμος**: Εστω ένα μη κενο συνολο Α και οι εσωτερικες πραξεις $\circ, \bullet$

1.Μια εσωτερικη πραξη $\circ$ στο συνολο Α ονομαζεται αντιμεταθετικη αν και μονο αν για κάθε

$$a \circ b = b \circ a, \forall a, b \in A$$

2.Μια εσωτερικη πραξη $\circ$ στο συνολο Α ονομαζεται προσεταιριστικη αν και μονο αν

$$(a \circ b) \circ c = a \circ (b \circ c), \forall a, b, c \in A$$

3. Μια εσωτερικη πραξη $\circ$ στο συνολο Α ονομαζεται επιμεριστικη ως προς την πραξη $\bullet$ αν για κάθε $a, b, c \in A$ ισχυει ότι:

$$a \circ (b \bullet c) = (a \circ b) \bullet (a \circ c) \text{ και } (b \bullet c) \circ a = (b \circ a) \bullet (c \circ a)$$

Ο πολλαπλασιασμος και η προσθεση ως εσωτερικες πραξεις στο συνολο των πραγματικων αριθμων ($\mathbb{R}$) είναι αντιμεταθετικες και προσεταιριστικες.Επισης στο ιδιο συνολο των πραγματικων αριθμων ο πολλαπλασιασμος επιμεριζει την εσωτερικη πραξη της προσθεσης.Επομενως σε ένα μη κενο συνολο Α είναι δυνατον να ορισθουν διαφορες εσωτερικες πραξεις.Το συνολο Α εφοδιασμενο με μια η περισσοτερες από τις πραξεις αυτές λεμε ότι εχει μια Αλγεβρικη Δομη,η οποια χαρακτηριζεται από τις ιδιοτητες που ικανοποιουν οι πραξεις με τις οποιες είναι εφοδιασμενο. Από τις πιο θεμελιωδης δομες είναι η δομη της Ομαδας.

**Ορισμος**:Θεωρουμε δυο μη κενα συνολα Α,Β.Μια απεικονιση φ της μορφης

$$\varphi : A \times B \to B$$

Ονομαζεται εξωτερικη πραξη στο Β με συνολο τελεστων το Α.Αν

$(\lambda,\beta)\in A\times B$,το στοιχειο $\varphi((\lambda,\beta))$ ονομαζεται αποτελεσμα της εξωτερικης πραξης $\varphi$ μεταξυ των $\lambda\in A$ και $\beta\in B$.

Ο πολλαπλασιασμος πραγματικου αριθμου με διανυσμα είναι μια εξωτερικη πραξηστο συνολοτων διανυσματων του χωρου με συνολο τελεστων το $\mathbb{R}$

## 1.2 Ομαδες

**Ορισμος(Ομαδα):** Ένα συνολο G ,οπου G μη κενο συνολο και $\circ$ μια εσωτερικη πραξη στο G ονομαζεται ομαδα αν ικανοποιουνται τα ακολουθα τρια αξιωματα:

1.Η εσωτερικη πραξη $\circ$ είναι προσεταιριστικη.
$\forall a,b,c$ ισχυει ότι $(a\circ b)\circ c=a\circ(b\circ c)$

2.Υπαρχει ουδετερο στοιχειο $e\in G$, τετοιο ώστε $\forall x\in G$ να ισχυει ότι $e\circ x=x\circ e=x$.
(Το ουδετερο η ταυτοτικο στοιχειο είναι μοναδικο)

3.Για κάθε $x\in G$ υπαρχει $x'\in G$ τετοιο ώστε $x\circ x'=x'\circ x=e$,δηλαδη κάθε στοιχειο $x\in G$ εχει ένα συμμετρικο(η αντιστροφο) στοιχειο $x'\in G$ .
(Το συμμετρικο στοιχειο είναι μοναδικο).

Σε κάθε Ομαδα το ταυτοτικο στοιχειο (e) και τα συμμετρικα στοιχεια είναι μοναδικα και ισχυει ο νομος της δεξιας και αριστερας διαγραφης.Οταν ισχυει η αντιμεταθετικη ιδιοτητα στην εσωτερικη πραξη της ομαδας τοτε η ομαδα καλειται Αβελιανη.Μια Ομαδα μπορει να εχει απειρου πληθους στοιχεια αλλα και πεπερασμενου πληθους.Το συνολο των ακεραιων $\mathbb{Z}$ με εσωτερικη πραξη την προσθεση είναι και ταυτοτικο στοιχειο το 0 είναι ομαδα με απειρου πληθους στοιχεια.Το πληθος των στοιχειων συμβολιζεται με $|A|$.

Για κάθε $n \in \mathbb{Z}^+$,οι $n$ λυσεις στο $\mathbb{C}$ της εξισωσης $x^n = 1$ σχηματιζουν μια πολλαπλασιαστικη ομαδα $U_n$.Ετσι οι

$$U_1 = \{1\} \quad , \quad U_2 = \{-1,1\} \quad , \quad U_3 = \{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\}$$

και

$$U_4 = \{1, i. -1, -i\}$$

είναι αβελιανες ομαδες με εσωτερικη πραξη τον μιγαδικο πολλαπλασιασμο.Η ομαδα $U_n$ λεγεται η πολλαπλασιαστικη ομαδα των n-στων ριζων της μοναδας.

## 1.3 Υποομαδες

Υπαρχουν πολλες ομαδες που περιεχονται σε μεγαλυτερες ομαδες όπως συμβαινει με τις ομαδες των πραγματικων και των ακεραιων αριθμων με πραξη την προσθεση.Οταν ισχυριζομαστε ότι η ομαδα $<\mathbb{Z},+>$ περιεχεται στην ομαδα $<\mathbb{R},+>$ είναι σημαντικο να κατανοησουμε ότι η πραξη + εφαρμοζομενη σε δυο τυχαιους ακεραιους παραγει το ιδιο στοιχειο που θα προεκυπτε αν σκεφτομασταν αυτους τους δυο ως στοιχεια των πραγματικων αριθμων.

**Ορισμος**(Επαγομενη πραξη):Εστω G μια ομαδα και S ένα υποσυνολο της G.Αν για κάθε στοιχειο $a, b \in S$ ισχυει ότι και το γινομενο $ab$ υπολογισμενο στην ομαδα G ανηκει και στο S,τοτε λεμε ότι το υποσυνολο S είναι κλειστο ως προς την πραξη της ομαδας G.Η διμελης πραξη που οριζεται με αυτόν τον τροπο στο S ,λεγεται η επαγομενη πραξη στο S από την G.

**Ορισμος(Υποομαδα)** : Αν ενα υποσυνολο Η μιας ομαδας G είναι κλειστο ως προς την εσωτερικη πραξη της G και αν το Η ικανοποιει και τις ιδιοτητες της ομαδας,δηλαδη είναι και αυτό ομαδα, τοτε το Η καλειται υποομαδα της G.

Δηλαδη το ταυτοτικο στοιχειο $e$ της ομαδας G ανηκει στην Η και για κάθε στοιχειο το οποιο ανηκει στην Η θα ανηκει και το αντιστροφο του.Επισης θα πρεπει παντα να ισχυει και η προσεταιριστικη ιδιοτητα.Οι ρητοι με εσωτερικη πραξη την προσθεση αποτελουν υποομαδα των

πραγματικων αριθμων με την ιδια εσωτερικη πραξη.Επισης ,οι n-στες ριζες της μοναδας στο $\mathbb{C}$ αποτελουν μια υποομαδα,την $U_n$,της ομαδας $\mathbb{C}^*$ των μη μηδενικων μιγαδικων αριθμων με πραξη τον πολλαπλασιασμο.

## 1.4 Κυκλικες Υποομαδες

Εστω G μια ομαδα και εστω $a \in G$.Καθε υποομαδα της G που περιεχει το στοιχειο α πρεπει να περιεχει το $a \cdot a$ το οποιο συμβολιζουμε με $a^2$.Τοτε πρεπει να περιεχει και το $a^2 \cdot a$ το οποιο συμβολιζουμε με $a^3$.Γενικα πρεπει να περιεχει και το $a^n$ για κάθε $n \in \mathbb{Z}^+$ ,δηλαδη το αποτελεσμα του υπολογισμου γινομενων του $a$ με τον εαυτο του ,με n παραγοντες ,για κάθε θετικο ακεραιο (η τα στοιχεια της μορφης $n \cdot a$ με τον προσθετικο συμβολισμο).Ειναι πιθανο το αντιστροφο του a να μην ανηκει σε αυτό τος συνολο.Μια υποομαδα που περιεχει το α πρεπει να περιεχει και το $a^{-1}$,και κατοπιν το $a^{-1}a^{-1}$ ,το οποιο συμβολιζουμε με $a^{-2}$ και γενικα πρεπει να περιεχει το $a^{-m}$ για κάθε $m \in \mathbb{Z}^+$.Τελος πρεπει να περιεχει και το ταυτοτικο $e = aa^{-1}$.Για λογους συμβολισμου γραφουμε $a^0$ για το $e$.Εχουμε δειξει ότι μια υποομαδα της G που περιεχει το α πρεπει να περιεχει όλα τα στοιχεια $a^n$ για κάθε $n \in \mathbb{Z}$.

**Θεωρημα**.Εστω G μια ομαδα και εστω $a \in G$.Τοτε το συνολο $H = \{a^n | n \in \mathbb{Z}\}$ είναι μια υποομαδα της G και μαλιστα είναι η μικροτερη υποομαδα που περιεχει το α,δηλαδη κάθε υποομαδα που περιεχει το α περιεχει και τη Η.

Αποδειξη:

Ελεγχουμε τρεις συνθηκες για το ποτε ένα υποσυνολο Η μιας ομαδας είναι υποομαδα.
1.Το Η πρεπει να είναι κλειστο ως προς τη διμελη πραξη της G.
2.Το ταυτοτικο στοιχειο $e$ της G ανηκει στο Η.
3.Για κάθε $a \in H$ πρεπει να ισχυει ότι το $a^{-1} \in H$.
Αφου $a^r a^s = a^{r+s}$ για κάθε $r, s \in \mathbb{Z}$,βλεπουμε ότι το γινομενο στην G,δυο στοιχειων της Η ανηκει παλι στην Η.Αρα το Η είναι κλειστο ως προς την πραξη ομαδας της G.Επισης $a^0 = e$,αρα $e \in H$,και αν $a^r \in H$,τοτε $a^{-r} \in H$ και

$a^{-r}a^{r}=e$.Επομενως ολες οι συνθηκες ικανοποιουνται ,και $H\leq G$.Τα επιχειρηματα που προηγηθηκαν της διατυπωσης του θεωρηματος ,εδειξαν ότι κάθε υποομαδα της G που περιεχει το $a$ πρεπει να περιεχει την H ,επομενως η H είναι η μικροτερη υποομαδα της G που περιεχει το $a$.

**Ορισμος(Κυκλικη Υποομαδα):**Η ομαδα H του παραπανω θεωρηματος καλειται η κυκλικη υποομαδα της G που παραγεται από το α,και συμβολιζεται με <α>.

**Ορισμος** (Γεννητορας κυκλικη ομαδα)Ενα στοιχειο a μιας ομαδας G παραγει την G λεγεται γεννητορας της G αν $<a>=G$ .Μια ομαδα G ονομαζεται κυκλικη αν υπαρχει ένα στοιχειο a που παραγει την G .

1.Η ομαδα των ακεραιων $\mathbb{Z}$ με πραξη την προσθεση είναι μια κυκλικη ομαδα με γεννητορες το 1 και το -1.

2 Εστω $U_n$ η πολλαπλαστικη ομαδα των νιοστων ριζων της μοναδας στο $\mathbb{C}$.Αυτα τα στοιχεια της $U_n$ παριστανονται γεωμετρικα από ισοκατανεμημενα στοιχεια πανω στην περιφερεια ακτινας 1 με κεντρο την αρχη των αξονων.

Ο γεννητορας αυτης της κυκλικης ομαδας είναι είναι το σημειο $a=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$.Ετσι η $U_n$ με πραξη τον μιγαδικο πολλαπλασιασμο είναι μια κυκλικη ομαδα και το $a=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ ο γεννητορας της.Η ομαδα $U_n$ είναι η κυκλικη υποομαδα $<a>$ της ομαδας U ολων των μιγαδικων ριζων z,με $|z|=1$, με πραξη τον πολλαπλασιασμο.

## 1.5 Κυκλικες Ομαδες

Κυκλικη ομαδα G είναι μια ομαδα με γεννητορα ένα στοιχειο $<a>=G$.

**Θεωρημα:** Κάθε κυκλικη ομαδα είναι αβελιανη.

Αποδειξη:

Εστω G μια κυκλικη ομαδα και $a$ ενας γεννητορας της G,δηλαδη

$G =< a >= \{a^n \,|\, n \in \mathbb{Z}\}$.

Αν $g_1$ και $g_2$ είναι οποιαδηποτε δυο στοιχεια της G,υπαρχουν ακεραιοι $r, s$ τετοιοι,ώστε $g_1 = a^r$ και $g_2 = a^s$ .Τοτε $g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$ αρα η G είναι αβελιανη.

**Θεωρημα:** Κάθε υποομαδα μιας κυκλικης ομαδας είναι και αυτή κυκλικη .

Αποδειξη:Εστω G μια κυκλικη ομαδα με γεννητορα το $a$ και H μια υποομαδα της G.Αν $H = \{e\}$,τοτε η $H =< e >$ είναι κυκλικη.Αν $H \neq \{e\}$ τοτε $a^n \in H$ για καποιο $n \in \mathbb{Z}^+$.Εστω $m \in \mathbb{Z}^+$ ο μικροτερος φυσικος αριθμος για τον οποιο $a^m \in H$.
Ισχυριζομαστε ότι το $c = a^m$ παραγει την H,δηλαδη $H =< a^m >=< c >$
Πρεπει να δειξουμε ότι κάθε $b \in H$ είναι δυναμη του $c$.
Αφου $b \in H$ και $H \leq G$ εχουμε $b = a^n$ για καποιο $n$.Βρισκουμαι $q, r$ τετοιους ,ώστε $n = mq + r$ και $0 \leq r < m$ συμφωνα με τον αλγοριθμο της διαιρεσης.Τοτε

$$a^n = a^{mq+r} = (a^m)^q a^r$$

Αρα

$$a^r = (a^m)^{-q} a^n$$

Τωρα αφου $a^n \in H$, $a^m \in H$ ,και το H είναι ομαδα,το $(a^m)^{-q}$ και το $a^n$ ανηκουν και τα δυο στην H.Αρα

$(a^m)^{-q} a^n \in H$ ,δηλαδη, $a^r \in H$.

Αφου ο $m$ ηταν ο μικροτερος θετικος ακεραιος για τον οποιο $a^m \in H$ και $0 \leq r < m$,πρεπει να εχουμε $r = 0$.Αρα $n = mq$ και $b = a^n = (a^m)^q = c^q$ ,δηλαδη το $b$ είναι δυναμη του $c$.

Το παραπανω θεωρημα αποδεικνυεται χρησιμοποιωντας τον αλγοριθμο της διαιρεσης για τους ακεραιους $\mathbb{Z}$ (Αν $m$ είναι ενας θετικος ακεραιος και $n$ οποιοσδηποτε ακεραιος,τοτε υπαρχουν μονοσημαντα ορισμενοι ακεραιοι $q, r$ τετοιοι,ώστε $n = m \cdot q + r$ και $0 \leq r \prec m$)

**Πορισμα :** Οι υποομαδες του $\mathbb{Z}$ με πραξη την προσθεση είναι ακριβως οι ομαδες $n\mathbb{Z}$ με πραξη την προσθεση,οπου $n \in \mathbb{Z}$.

Η ομαδα των ακεραιων είναι μια κυκλικη ομαδα και ολες οι υπο-ομαδες της συμφωνα με το θεωρημα θα είναι κυκλικες.Ειναι ευκολο να δουμε ότι η

$H = \{nr + ms | n, m \in \mathbb{Z}\}$ είναι υποομαδα των ακεραιων με πραξη την προσθεση οποτε συμφωνα με το θεωρημα είναι κυκλικη .Ο θετικος γεννητορας $d$ της παραπανω κυκλικης ομαδας με πραξη την προσθεση λεγεται μεγιστος κοινος διαιρετης των $r, s$ .

**Ορισμος:** Αν ο μεγιστος κοινος διαιρετης δυο θετικων ακεραιων είναι 1 αυτοι λεγονται πρωτοι προς αλληλους.

Επομενως αν $r, s$ είναι πρωτοι προς αλληλους τοτε ο γεννητορας τους θα είναι η μοναδα και η υποομαδα θα ταυτιζεται με τους ακεραιους αριθμους.

Υπαρχουν δυο περιπτωσεις κυκλικων ομαδων συμφωνα με το πληθος των στοιχειων τους.Οι απειρες που εχουν απειρα στοιχεια (όπως οι ακεραιοι) και οι πεπερασμενου πληθους στοιχειων κυκλικες ομαδες.Εστω G κυκλικη ομαδα με γεννητορα $a$ .Εξεταζουμε τις δυο περιπτωσεις

**Περιπτωση 1**.Η G εχει απειρα το πληθος στοιχεια.Τοτε δυο διαφορετικοι εκθετες του γεννητορα $a$ δεν μπορουν να δωσουν ποτε το ιδιο στοιχειο,δηλαδη ολες οι δυναμεις του α είναι διαφορετικες ανα δυο.Το $\mathbb{Z}$ με πραξη την προσθεση λειτουργει ως προτυπο κάθε απειρης κυκλικης ομαδας.

**Περιπτωση 2**. Η G εχει πεπερασμενη ταξη.Σε αυτην την περιπτωση ,δεν μπορουν ολες οι θετικες δυναμεις ενός γεννητορα $a$ της G να είναι διαφορετικες ανα δυο επομενως για καποιους εκθετες h,k πρεπει να εχουμε ότι $a^h = a^k$ .Αν m είναι ο μικροτερος ακεραιος για τον οποιο ισχυει ότι $a^m = e$ και καμια μικροτερη θετικη δυναμη του α να μην είναι το e (ουδετερο στοιχειο),τοτε η κυκλικη ομαδα αποτελειται απο τα πεπερασμενα στοιχεια $e, a, a^2, ..., a^{m-1}$ ,και το α εχει ταξη m.

**Ορισμος:**Εστω n δεδομενος θετικος ακεραιος και εστω h,k οποιοιδηποτε ακεραιοι .Το υπολοιπο r της διαιρεσης του $h+k$ με $n$, συμφωνα με τον αλγοριθμο της διαιρεσης ,λεγεται αθροισμα των h και k modulo n.

**Θεωρημα:**Το συνολο $0,1,2,...,n-1$ είναι μια κυκλικη ομαδα ,η $\mathbb{Z}_n$, με πραξη την προσθεση modulo n.

Για τις απειρες κυκλικες υποομαδες μας καλυπτει πληρως το παραπανω πορισμα.Δινουμε το βασικο θεωρημα για τους γεννητορες των υποομαδων των πεπερασμενων κυκλικων ομαδων.

**Θεωρημα:** Εστω G μια κυκλικη ομαδα με n στοιχεια που παραγεται από το α.Εστω b στοιχειο της G και $b = a^s$.Τοτε το b παραγει μια κυκλικη υποομαδα H της G που περιεχει $\frac{n}{d}$ στοιχεια ,οπου d είναι ο μεγιστος κοινος διαιρετης των n,s.

Αποδειξη:

Το ότι το $b$ παραγει μια κυκλικη υποομαδα H της G είναι γνωστο από παραπανω θεωρημα.Πρεπει να δειξουμε ότι η H εχει $\frac{n}{d}$ στοιχεια.Η H εχει τοσα στοιχεια οση είναι η μικροτερη θετικη δυναμη $m$ του $b$ που δινει το ταυτοτικο στοιχειο.Τωρα $b = a^s$ και $b^m = e$ αν και μονο αν $(a^s)^m = e$,δηλαδη αν και μονο αν ο $n$ διαιρει τον $ms$.Ποιος είναι ο μικροτερος θετικος ακεραιος $m$ για τον οποιο ο $n$ διαιρει το $ms$?Εστω $d$ ο μεγιστος κοινος διαιρετης των $n, s$.Τοτε υπαρχουν $u, v \in \mathbb{Z}$ τετοιοι ώστε

$$d = un + vs$$

Αφου ο $d$ διαιρει τους $n, s$,μπορουμε να γραψουμε

$$1 = u(\frac{n}{d}) + v(\frac{s}{d})$$

Οπου οι $\frac{n}{d}$ και $\frac{s}{d}$ είναι ακεραιοι .Απο την τελευταια ισοτητα φαινεται οι $\frac{n}{d}$ και $\frac{s}{d}$ είναι πρωτοι προς αλληλους ,διοτι κάθε ακεραιος που διαιρει και τους δυο πρεπει να διαιρει και τον 1.Θελουμε να βρουμε τον μικροτερο θετικο $m$ για τον οποιο ο

$$\frac{ms}{n} = \frac{m(\frac{s}{d})}{(\frac{n}{d})} \text{ είναι ακεραιος.}$$

Συμπεραινουμε ότι ο $\frac{n}{d}$ πρεπει να διαιρει τον $m$,επομενως ο μικροτερος τετοιος $m$ είναι ο $\frac{n}{d}$.Αρα η ταξη του H είναι $\frac{n}{d}$.

**Πορισμα:**Αν $a$ είναι ενας γεννητορας μιας πεπερασμενης κυκλικης ομαδας G με ταξη $n$,τοτε οι αλλοι γεννητορες της G είναι τα στοιχεια της μορφης $a^r$,οπου ο $r$ είναι πρωτος προς τον $n$.

1.6 Συμπλοκα

Εστω H μια υποομαδα μιας ομαδας G, η οποια μπορει να ειναι πεπερασμενης η απειρης ταξης .Παρουσιαζουμε δυο διαμερισεις της G ,οριζοντας δυο σχεσεις ισοδυναμιας, $\sim_L$ και $\sim_R$ στην G .

**Θεωρημα:** Εστω H μια υποομαδα της G .Οριζουμε μια σχεση $\sim_L$ στην G με την

$a \sim_L b$ αν και μονο αν $a^{-1}b \in H$.

Οριζουμε την $\sim_R$ με την

$a \sim_R b$ αν και μονο αν $ab^{-1} \in H$

Τοτε οι $\sim_L$ και $\sim_R$ είναι και οι δυο σχεσεις ισοδυναμιας στην G

Αποδειξη: Δειχνουμε ότι η $\sim_L$ είναι σχεση ισοδυναμιας.
1)Ανακλαστικη ιδιοτητα:Εστω $a \in G$.Τοτε $a^{-1}a = e$ και $e \in H$ αφου το H είναι υποομαδα .Αρα $a \sim_L a$.
2)Συμμετρικη ιδιοτητα:Υποθετουμε ότι $a \sim_L b$.Τοτε $a^{-1}b \in H$.Αφου το H είναι υποομαδα ,το $(a^{-1}b)^{-1}$ ανηκει στην H και $(a^{-1}b)^{-1} = b^{-1}a$ ,αρα το $b^{-1}a \in H$ οποτε $b \sim_L a$.
3)Μεταβατικη ιδιοτητα:Εστω $a \sim_L b$ και $b \sim_L c$.Τοτε $a^{-1}b \in H$ και $b^{-1}c \in H$.Αφου το H είναι υποομαδα ,το $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$,αρα $a \sim_L c$.

Οπως γνωριζουμε κάθε σχεση ισοδυναμιας οριζει μια διαμεριση στο συνολο,εν προκειμενω στη ομαδα G.Η σχεση ισοδυναμιας $\sim_L$ οριζει μια διαμεριση στη G .Ας δουμε με τι μοιαζουν αυτά τα υποσυνολα σ'αυτή τη διαμεριση .Ας υποθεσουμε ότι $a \in G$.Το συνολο που περιεχει το α αποτελειται από όλα τα $x \in G$ για τα οποια $a \sim_L x$,δηλαδη όλα τα $x \in G$ για τα οποια $a^{-1}x \in H$.Τωρα $a^{-1}x \in H$ αν και μονο αν $a^{-1}x = h$ για καποιο $h \in H$ η ισοδυναμα αν και μονο αν $x = ah$ για καποιο $h \in H$.Δηλαδη το υποσυνολο που περιεχει το $a$ είναι το $ah \mid h \in H$ ,το οποιο συμβολιζουμε και με $aH$.Αν

ακολουθησουμε τον ιδιο συλλογισμο για τη σχεση ισοδυναμιας $\sim_R$ που οριζεται από την H ,βλεπουμε ότι το υποσυνολο που περιεχει $a \in G$ σ'αυτή τη διαμεριση είναι το $Ha = \{ha | h \in H\}$.Αφου η G μπορει να μην είναι αβελιανη,δεν εχουμε κανενα λογο να περιμενουμε τα $Ha$ και $aH$ να είναι το ιδιο συνολο της G.

**Ορισμος**: Εστω H μια υποομαδα μιας ομαδας G. Το υποσυνολο $aH = ah | h \in H$ της G λεγεται το αριστερο συμπλοκο της H που περιεχει το α ,ενώ το $Ha = ha | h \in H$ της G λεγεται το δεξιο συμπλοκο της H που περιεχει το $a$.

Για μια αβελιανη υποομαδα H της G,η διαμεριση της G σε αριστερα συμπλοκα H και η διαμεριση σε δεξια συμπλοκα ταυτιζονται. Κάθε συμπλοκο μιας υποομαδας H μιας ομαδας G εχει το ιδιο πληθος στοιχειων με την υποομαδα.

## 1.7 Το Θεωρημα Lagrange

Εστω H μια υποομαδα μιας ομαδας G.Ισχυριζομαστε ότι κάθε αριστερο συμπλοκο και κάθε δεξιο συμπλοκο της H εχει το ιδιο πληθος στοιχειων με την H.Θα το δειξουμε οριζοντας μια ένα προς ένα απεικονιση της H επι του αριστερου συμπλοκου $gH$ της H για οποιοδηποτε στοιχειο $g$ της G.Αν η H εχει πεπερασμενη ταξη αυτό δειχνει ότι η $gH$ εχει το ιδιο ακριβως πληθος στοιχειων με την H.Αν η H είναι απειρη ,η υπαρξη μιας τετοιας απεικονισης θεωρειται ως ο ορισμος της ισοτητας του μεγεθους της H και του μεγεθους του $gH$. Η επιλογη της ένα-προς –ένα απεικονισης $\phi : H \to gH$ είναι προφανης .Θετουμε $\phi(h) = gh$ για κάθε $h \in H$.Η απεικονιση αυτή είναι επι του $gH$ επειδη το $gH$ ορισθηκε ως $\{gh | h \in H\}$.Για να δειξουμε ότι είναι ένα προς ένα ας υποθεσουμε ότι $\phi(h_1) = \phi(h_2)$ για καποια $h_1, h_2$ στην H.Τοτε $gh_1 = gh_2$ και από το νομο διαγραφης στην ομαδα G εχουμε $h_1 = h_2$ .Αυτο δειχνει ότι η $\phi$ είναι ένα προς ένα.Οποτε συνοψιζοντας,κάθε συμπλοκο αριστερο η δεξιο μιας υποομαδας H μιας ομαδας G εχει το ιδιο πληθος στοιχειων με την H.

**Θεωρημα** (**Lagrange**):Εστω Η μια υποομαδα μιας πεπερασμενης ομαδας G .Τοτε η ταξη της Η είναι διαιρετης της ταξης της G.

Αποδειξη : Εστω $n$ η ταξη της G και $m$ η ταξη της Η.Απο τον παραπανω ισχυρισμο κάθε συμπλοκο της Η εχει επισης $m$ στοιχεια.Εστω $r$ το πληθος των υποσυνολων στη διαμεριση της G σε αριστερα συμπλοκα της Η.Τοτε $n = rm$ ,αρα ο $m$ είναι οντως διαιρετης του $n$

**Πορισμα**:Κάθε ομαδα με ταξη πρωτο αριθμο είναι κυκλικη.

Αποδειξη :Εστω ότι η G εχει ταξη τον πρωτο αριθμο $p$ ,και εστω $a$ ένα στοιχειο της G διαφορετικο από το ταυτοτικο στοιχειο.Τοτε η κυκλικη υποομαδα $< a >$ της G που παραγεται από το $a$ εχει τουλαχιστον δυο στοιχεια ,το $a$ και το ταυτοτικο.Ομως από το παραπανω θεωρημα η ταξη της κυκλικης υποομαδας θα πρεπει να διαιρει την ταξη της ομαδας δηλαδη τον πρωτο αριθμο $p$ .Πρεπει λοιπον να εχουμε $m = p$ και $< a >= G$ ,αρα η G είναι κυκλικη ομαδα

Οποτε βλεπουμε ότι υπαρχει ουσιαστικα μονο μια δομη ομαδας με ταξη δεδομενο πρωτο αριθμο $p$ .

**Θεωρημα**:Η ταξη ενός στοιχειου μιας πεπερασμενης ομαδας διαιρει την ταξη της ομαδας.

Αποδειξη :Η ταξη ενός στοιχειου ισουται με την ταξη της κυκλικης υποομαδας που παραγεται από αυτό το στοιχειο οποτε εχουμε το ζητουμενο.

**Ορισμος**:Εστω Η μια υποομαδα μιας ομαδας G.Το πληθος των αριστερων συμπλοκων της Η στην G λεγεται δεικτης $(G : H)$ της Η στην G.

## 1.8 Δακτυλιοι

Η πιο γενικη αλγεβρικη δομη με δυο διμελεις πραξεις λεγεται δακτυλιος.

**Ορισμος:** (Δακτυλιος) Ενας δακτυλιος $< R,+,\cdot >$ είναι ένα συνολο R μαζι με δυο διμελεις πραξεις $+$ και $\cdot$ ,τις οποιες αποκαλουμε προσθεση και πολλαπλασιασμο,ορισμενες στο R ετσι ώστε να ικανοποιουνται τα ακολουθα αξιωματα:

1. $< R,+ >$ είναι μια αβελιανη ομαδα.

2. Ο πολ/σμος είναι προσεταιριστικος.

3. Για κάθε $a,b,c \in R$ ,ισχυουν ο αριστερος επιμεριστικος νομος $a(b+c) = ab+ac$ και ο δεξιος επιμεριστικος νομος $(b+c)a = ba+ca$

Τα αξιωματα 1,2,3 ισχυουν σε κάθε υποσυνολο των μιγαδικων αριθμων που είναι ομαδα με την προσθεση και κλειστο ως προς τον πολλαπλασιασμο.Για παραδειγμα τα $< \mathbb{Z},+,\cdot >, < \mathbb{Q},+,\cdot >, < \mathbb{R},+,\cdot >, < \mathbb{C},+,\cdot >$ είναι ολοι δακτυλιοι.

**Θεωρημα:** Αν $R$ είναι ενας δακτυλιος με ταυτοτικο στοιχειο της προσθεσης το 0 ,τοτε για κάθε $a,b \in R$ εχουμε

1. $0a = a0 = 0$

2. $a(-b) = (-a)b = -(ab)$

3. $(-a)(-b) = ab$

Αποδειξη :

1. $a0+a0=a(0+0)=a0$ .Επομενως ,από το νομο της διαγραφης ,για την προσθετικη ομαδα $<R,+>$ εχουμε $a0=0$ .Ομοιως και από αριστερα.

2. $a(-b)+ab=0$ και $(-a)b+ab=0$

3. $(-a)(-b)=-(a(-b))$ και $-(a(-b))=-(-(ab))$ .Αρα το $-(-(ab))$ είναι το στοιχειο που αν προστεθει $-(ab)$ μας δινει το 0.Αυτο είναι το $ab$ λογω του ορισμου του $-ab$ και της μοναδικοτητας του αντιστροφου σε μια ομαδα.

**Ορισμος:** Ενας δακτυλιος ,στον οποιο ο πολ/σμος είναι αντιμεταθετικη πραξη λεγεται αντιμεταθετικος δακτυλιος.Ενας δακτυλιος με πολλαπλασιαστικο ταυτοτικο στοιχειο 1,για το οποιο $1x=x1=x$ για κάθε $x\in\mathbb{R}$,λεγεται δακτυλιος με μοναδιαιο στοιχειο.Καθε ουδετερο στοιχειο του πολλαπλασιασμου λεγεται μοναδιαιο στοιχειο.

**Θεωρημα**:Αν $R$ είναι ενας δακτυλιος με μοναδιαιο στοιχειο,τοτε αυτό το μοναδιαιο στοιχειο 1 είναι το μονο πολλαπλασιαστικο ταυτοτικο στοιχειο του $R$.

Αποδειξη :Υποθετουμε ότι το 1 και το $1'$ είναι δυο ουδετερα στοιχεια για τον πολλαπλασιασμο σε ένα δακτυλιο R.Θεωρωντας το 1 ως ουδετερο στοιχειο εχουμε

$$(1)(1')=1'$$

Θεωρωντας το $1'$ ως ουδετερο στοιχειο ,εχουμε

$(1)(1')=1.$
Αρα , $1'=1$

Σε ένα δακτυλιο R με μοναδιαιο στοιχειο,το συνολο $R^*$ των μη μηδενικων στοιχειων,αν είναι κλειστο ως προς τον πολλαπλασιασμο και υπαρχουν τα αντιστροφα στοιχεια θα είναι μια πολλαπλασιαστικη ομαδα.Οποτε εχοντας ένα δακτυλιο ψαχνουμε για τα πολλαπλασιαστικα αντιστοφα.

**Ορισμος:** (Μοναδα,Σωμα,Στρεβλο Σωμα) .Εστω R ενας δακτυλιος με μοναδιαιο στοιχειο .Ενα στοιχειο u του R λεγεται μοναδα αν εχει πολλαπλαστικο αντιστροφο στο R.Αν κάθε μη μηδενικο στοιχειο του R είναι μοναδα τοτε ο R ονομαζεται δακτυλιος διαιρεσης.Σωμα ονομαζεται

κάθε αντιμεταθετικος δακτυλιος διαιρεσης.Ενας μη αντιμεταθετικος δακτυλιος διαιρεσης λεγεται στρεβλο σωμα.

Το $\mathbb{Z}$ δεν είναι σωμα αφου το 2 δεν εχει πολλαπλασιαστικο αντιστροφο,το 2 δεν είναι μοναδα του $\mathbb{Z}$ .Οι μονες μοναδες του $\mathbb{Z}$ είναι το 1 και το -1.Το $\mathbb{Q}$ και το $\mathbb{R}$ είναι σωματα.

Υπαρχουν φυσιολογικα οι εννοιες του υποδακτυλιου ενός δακτυλιου και του υποσωματος ενός σωματος.Υποδακτυλιος ενός δακτυλιου λεγεται ένα υποσυνολο του δακτυλιου που είναι δακτυλιος με τις πραξεις που του κληρονομει ο μεγαλος δακτυλιος.Ομοιως οριζεται και η εννοια του υποσωματος για ένα υποσυνολο ενός σωματος.Οταν εχουμε ένα συνολο με καποιου ειδους αλγεβρικη δομη πανω του ,και την προκυπτουσα συμπτυξη να είναι δομη (ομαδα,δακτυλιος,σωμα,ακεραια περιοχη,διανυσματικος χωρος κ.ο.κ) τοτε κάθε υποσυνολο αυτου του συνολου,το οποιο δινει μια αλγεβρικη δομη του ιδιου ειδους με τις πραξεις που φυσιολογικα επαγονται σ'αυτό ,θα λεγεται υποδομη.

## 1.9 Ακεραιες Περιοχες

**Ορισμος:** (Διαιρετες του 0) Αν α και b είναι δυο μη μηδενικα στοιχεια ενός δακτυλιου $R$ τετοια ,ώστε $ab=0$ τοτε τα α και b λεγονται διαιρετες του 0.Ειδικοτερα το α λεγεται αριστερος διαιρετης του 0 και το
Β δεξιος διαιρετης του 0.

Σε ένα αντιμεταθετικο δακτυλιο,κάθε αριστερος διαιρετης του 0 είναι και δεξιος διαιρετης του 0 και αντιστροφος,οποτε δεν υπαρχει διακριση μεταξυ των αριστερων και δεξιων διαιρετων.

**Θεωρημα:** Στο δακτυλιο $\mathbb{Z}_n$ ,οι διαιρετες του 0 είναι ακριβως εκεινα τα στοιχεια που δεν είναι πρωτα προς τον $n$ .

Αποδειξη :

Εστω $m \in \mathbb{Z}_n$ ,οπου $m \neq 0$ ,εστω $d \neq 1$ ο μεγιστος κοινος διαιρετης των $m,n$ .
Τοτε $m(\frac{n}{d}) = (\frac{m}{d})n$ και το $(\frac{m}{d})n$ μας δινει 0 αφου είναι πολλαπλασιο του $n$ .Αρα $m(\frac{n}{d})$=0 στον $\mathbb{Z}_n$ ,ενώ κανενας από τους $m$ , $\frac{n}{d}$ δεν είναι μηδεν,δηλαδη ο $m$ είναι διαιρετης του 0.
Από την άλλη πλευρα ,ας υποθεσουμε ότι ο $m \in \mathbb{Z}_n$ ,είναι πρωτος προς τον $n$ .Αν για καποιο $s \in \mathbb{Z}_n$ είναι $ms = 0$ ,τοτε ο $n$ διαιρει το γινομενο $ms$ των $m$ και $s$ .Αφου ο $n$ είναι πρωτος προς τον $m$ επεται ότι ο $n$ διαιρει τον $s$ ,οποτε $s$ =0 στον $\mathbb{Z}_n$ .

**Πορισμα:** Αν ο $p$ είναι πρωτος,τοτε ο $\mathbb{Z}_p$ δεν εχει διαιρετες του μηδενος.

Αποδειξη :Αφου οι διαιρετες του μηδενος του δακτυλιου $\mathbb{Z}_p$ είναι εκεινα τα στοιχεια που δεν είναι πρωτα προς το $p$ ,για $p$ πρωτο όλα τα στοιχεια του δακτυλιου είναι πρωτα(μ.κ.δ=1) προς το $p$ .

**Θεωρημα:** Οι νομοι της διαγραφης ισχυουν σε ένα δακτυλιο $R$ αν και μονο αν ο $R$ δεν εχει ουτε αριστερους ουτε δεξιους διαιρετες του 0.

Αποδειξη :Εστω $R$ ενας δακτυλιος στον οποιο ισχυουν οι νομοι διαγραφης ,και ας υποθεσουμε ότι $ab = 0$ για καποια $a,b \in R$ .Πρεπει να δειξουμε ότι ειτε το $a$ ειτε το $b$ είναι 0.Αν $a \neq 0$ τοτε η $ab = a0$ μας δινει $b = 0$ από τους νομους διαγραφης.Ομοιως αν $b \neq 0$ επεται ότι $a = 0$ ,δηλαδη αν οι νομοι διαγραφης ισχυουν δεν υπαρχουν αριστεροι η δεξιοι διαιρετες του 0.
Αντιστροφως ,ας υποθεσουμε ότι ο $R$ δεν εχει αριστερους ουτε δεξιους διαιρετες του μηδενος και ας υποθεσουμε ότι $ab = ac$ με $a \neq 0$ .Τοτε

$$ab - ac = a(b - c) = 0$$

Αφου $a \neq 0$ ,και αφου ο $R$ δεν εχει αριστερους διαιρετες του 0 πρεπει να εχουμε $b - c = 0$ ,αρα $b = c$ .Αναλογο επιχειρημα δειχνει ότι αν $ba = ca$ και

$a \neq 0$ ,τοτε $b = c$ .

Αν ο δακτυλιος $R$ δεν εχει διαιρετες του μηδενος τοτε κάθε εξισωση της μορφης $ax = b$ , με $a \neq 0$ στο $R$ μπορει να εχει το πολύ μια λυση $x$ στο $R$ .

**Ορισμος**(Ακεραια περιοχη): Ακεραια περιοχη λεγεται ενας αντιμεταθετικος δακτυλιος ,που δεν περιεχει διαιρετες του 0.

**Θεωρημα:** Κάθε σωμα $F$ είναι ακεραια περιοχη

Αποδειξη :Εστω $a, b \in F$ και ας υποθεσουμε ότι $a \neq 0$ .Τοτε αν $ab = 0$ εχουμε $(\frac{1}{a})ab = (\frac{1}{a})0 = 0$ .
Όμως τοτε

$$0 = (\frac{1}{a})(ab) = [(\frac{1}{a})a]b = 1b = b$$

Δειξαμε ότι αν $ab = 0$ και $a \neq 0$ ,τοτε $b = 0$ στο σωμα ,επομενως δεν υπαρχουν διαιρετες του μηδεν στο $F$ .Προφανως το $F$ είναι αντιμεταθετικος δακτυλιος με μοναδιαιο στοιχειο ,αρα το θεωρημα μας εχει αποδειχθει.

**Θεωρημα:** Καθε πεπερασμενη ακεραια περιοχη είναι σωμα.

Αποδειξη :Εστω

$$0, 1, a_1, ..., a_n$$

Όλα τα στοιχεια μιας πεπερασμενης ακεραιας περιοχης $D$ .Θελουμε να δειξουμε ότι αν $a \in D$ και $a \neq 0$ ,υπαρχει $b \in D$ τετοιο ώστε $ab = 1$ .

Θεωρουμε τα

$$a1, aa_1, ..., aa_n$$

Ισχυριζομαστε ότι όλα τα στοιχεια της $D$ είναι διακεκριμενα,διοτι αν $aa_i = aa_j$ εχουμε $a_i = a_j$ ,λογω των νομων διαγραφης που ισχυουν σε κάθε ακεραια περιοχη .Επισης ,αφου η $D$ δεν εχει διαιρετες του 0,κανενα από αυτά τα στοιχεια δεν είναι 0.Επομενως μετρωντας βρισκουμε ότι τα $a1, aa_1, ..., aa_n$ είναι τα στοιχεια $0, 1, a_1, ..., a_n$ με καποια άλλη διαταξη,δηλαδη

$a1=1$ οποτε $a=1$ η $aa_i=1$ για καποιο $i$.Σε κάθε περιπτωση το $a$ εχει πολλαπλασιαστικο αντιστροφο.

**Πορισμα:** Αν $p$ είναι πρωτος,το $\mathbb{Z}_p$ είναι σωμα,
Το πορισμα επεται αμεσως του ότι ο $\mathbb{Z}_p$ είναι ακεραια περιοχη με πεπερασμενα στοιχεια.

**Ορισμος(Χαρακτηριστικη ενός δακτυλιου):** Αν για καποιο δακτυλιο $R$ υπαρχει ενας θετικος ακεραιος $n$ τετοιος ,ώστε $na=0$ για κάθε $a\in R$,τοτε ο μικροτερος τετοιος φυσικος λεγεται χαρακτηριστικη του δακτυλιου $R$.Αν δεν υπαρχει τετοιος φυσικος αριθμος,λεμε ότι ο $R$ είναι χαρακτηριστικης 0.

Ο δακτυλιος $Z_n$ εχει χαρακτηριστικη $n$,ενώ τα $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ εχουν όλα χαρακτηριστικη 0.

**Θεωρημα:** Αν $R$ είναι ενας δακτυλιος με μοναδιαιο στοιχειο το 1,τοτε ο $R$ εχει χαρακτηριστικη $n>0$ αν και μονο αν ο $n$ είναι ο μικροτερος θετικος ακεραιος ,για τον οποιο $n1=0$.

Αποδειξη :Αν ο $R$ εχει χαρακτηριστρικη $n>0$,τοτε $na=0$ για κάθε $a\in R$,οποτε ,ειδικοτερα $n1=0$.
Αντιστροφα ,ας υποθεσουμε ότι $n$ είναι ενας θετικος ακεραιος για τον οποιο $n1=0$.Τοτε για κάθε $a\in R$,εχουμε

$$na=a+a+...+a=a(1+1+..+1)=a(n1)=a0=0.$$

## 1.10 Τα θεωρηματα των Fermat & Euler

Σε κάθε σωμα τα μη μηδενικα στοιχεια σχηματιζουν ομαδα ως προς τον πολλαπλασιασμο σωματος. Ειδικοτερα στο $\mathbb{Z}_p$ τα στοιχεια $1,2,3,...,p-1$ σχηματιζουν μια ομαδα ταξης $p-1$ με τον πολλαπλασιασμο $\mathrm{mod}ulo\ p$.
Αφου η ταξη κάθε στοιχειου μιας ομαδας διαιρει την ταξη της ομαδας ,βλεπουμε ότι αν $b \neq 0$ και $b \in \mathbb{Z}_p$ ,εχουμε ότι $b^{p-1} = 1$ στο $\mathbb{Z}_p$.

**Θεωρημα(Fermat):** Αν $a \in \mathbb{Z}$ και $p$ είναι πρωτος που δεν διαιρει το $a$ ,τοτε ο $p$ διαιρει τον $a^{p-1} - 1$,δηλαδη $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$ , αν $a \neq 0 (\mathrm{mod}\ p)$.

**Πορισμα:** Αν $a \in \mathbb{Z}$ ,τοτε $a^p \equiv a (\mathrm{mod}\ p)$ για κάθε πρωτο $p$.

Αποδειξη :Το πορισμα προκυπτει από το παραπανω θεωρημα αν $a \neq 0 (\mathrm{mod}\ p)$.Αν $a \equiv 0 (\mathrm{mod}\ p)$ ,τοτε και τα δυο μελη είναι ισα με $0\,\mathrm{mod}ulo p$

Ο Euler εδωσε μια γενικευση του θεωρηματος του Fermat.

**Θεωρημα:** Το συνολο $G_n$ των μη μηδενικων στοιχειων του $\mathbb{Z}_n$ ,που δεν είναι διαιρετες του μηδενος ,είναι ομαδα με τον πολλαπλασιασμο $\mathrm{mod}ulo$ n

Αποδειξη :Πρεπει πρωτα να δειξουμε ότι το $G_n$ είναι κλειστο ως προς τον πολλαπλασιασμο $\mathrm{mod}ulo$ n .Εστω $a, b \in G_n$ .Αν $ab \notin G_n$ ,τοτε θα υπηρχε ένα $c \neq 0$ στον $\mathbb{Z}_n$ ,τετοιο ώστε $(ab)c = 0$ .Αλλα από την $(ab)c = 0$ επεται ότι $a(bc) = 0$ .Αφου $b \in G_n$ και $c \neq 0$ εχουμε $bc \neq 0$ από τον ορισμο της $G_n$ .Τοτε όμως ,από την $a(bc) = 0$ επεται ότι $a \notin G_n$ κατι που αντιφασκει στην υποθεση μας .Σημειωστε ότι αυτό που αποδειξαμε είναι ότι σε κάθε δακτυλιο ,το συνολο των στοιχειων που δεν είναι διαιρετες του μηδενος είναι κλειστο ως προς τον πολλαπλασιασμο.
Δειχνουμε ότι το $G_n$ είναι ομαδα.Ειναι φανερο ότι ο πολλαπλασιαμος $\mathrm{mod}ulo$ n είναι προσεταιριστικος ,και ότι $1 \in G_n$ .Δειχνουμε τωρα ότι για κάθε $a \in G_n$ υπαρχει $b \in G_n$ τετοιο ώστε $ab = 1$ .Εστω $1, a_1, ..., a_r$ τα στοιχεια της $G_n$ .
Τα στοιχεια $a1, aa_1, ..., aa_r$ είναι όλα διαφορετικα διοτι αν $aa_i = aa_j$ τοτε

$a(a_i - a_j) = 0$ και αφου το $a \in G_n$ δηλαδη δεν είναι διαιρετης του 0,πρεπει να εχουμε $a_i - a_j = 0$ δηλαδη $a_i = a_j$ .Μετρωντας βλεπουμε ότι $a1 = 1$ η καποιο $aa_i$ είναι ισο με 1,οποτε το $a$ εχει πολλαπλασιαστικο αντιστροφο.

Εστω $n$ ενας θετικος ακεραιος.Οριζουμε $\phi(n)$ το πληθος των θετικων ακεραιων που είναι μικροτεροι η ισοι του $n$ και πρωτοι προς τον $n$ .Ο $\phi(n)$ είναι ισος με το πληθος των στοιχειων του $\mathbb{Z}_n$ που δεν είναι διαιρετες του 0.

**Θεωρημα(**Euler **) :** Αν $a$ είναι ενας ακεραιος πρωτος προς τον $n$ ,τοτε ο $a^{\varphi(n)} - 1$ διαιρειται με τον $n$ ,δηλαδη $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$

Αποδειξη :Αν ο $a$ είναι ακεραιος πρωτος προς τον $n$ ,τοτε το συμπλοκο $a + n\mathbb{Z}$ του $n\mathbb{Z}$ που περιεχει το $a$ ,περιεχει ένα ακεραιο $b < n$ ,πρωτο προς το $n$ .Χρησιμοποιωντας το γεγονος ότι ο πολλαπλασιασμος αυτων των συμπλοκων με πολλαπλασιασμο αντιπροσωπων τους $\mathrm{mod}\, ulo\, \mathrm{n}$ είναι καλα ορισμενος εχουμε

$$a^{\varphi(n)} \equiv b^{\phi(n)} (\mathrm{mod}\, n)$$

Μπορουμε να θεωρησουμε το $b$ ως στοιχειο της πολλαπλασιαστικης ομαδας $G_n$ που εχει ταξη $\phi(n)$ στοιχεια της $\mathbb{Z}_n$ ,που είναι πρωτα προς τον $n$ .Επομενως $b^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$ και η αποδειξη είναι πληρης.

Χρησιμοποιωντας τα παραπανω θεωρηματα μπορουμε να βρουμε ολες τις λυσεις μιας γραμμικης ισοτιμιας $ax \equiv b (\mathrm{mod}\, m)$

**Θεωρημα:** Εστω $m$ ενας θετικος ακεραιος και $a \in \mathbb{Z}_m$ πρωτος προς τον $m$ .Για κάθε $b \in \mathbb{Z}_m$ ,η εξισωση $ax = b$ εχει μοναδικη λυση στο $\mathbb{Z}_m$ .

Αποδειξη :Το $a$ είναι στοιχειο της πολλαπλασιαστικης ομαδας αφου είναι πρωτο προς το $m$ .Αρα θα εχει αντιστροφο.Το $s = a^{-1}b$ είναι προφανης λυση της εξισωσης.Πολλαπλασιαζοντας και τα δυο μελη της $ax = b$ από τα αριστερα με $a^{-1}$,βλεπουμε ότι είναι μοναδικη λυση.

Μεταφεροντας το θεωρημα αυτό στις ισοτιμιες παιρνουμε το ακολουθο πορισμα.

**Πορισμα :** Αν $a$ και $m$ είναι ακεραιοι πρωτοι μεταξυ τους ,τοτε για κάθε ακεραιο $b$ ,η ισοτιμια $ax \equiv b(\mathrm{mod}\, m)$ εχει ως λυσεις ολους τους ακεραιους που ανηκουν σε ακριβως μια κλαση υπολοιπων $\mathrm{mod}ulo\ m$.

**Θεωρημα:** Εστω $m$ ενας θετικος ακεραιος και $a,b \in \mathbb{Z}_m$ .Εστω $d$ ο μεγιστος κοινος διαιρετης των $a,m$ .Η εξισωση $ax = b$ εχει λυση στο $\mathbb{Z}_m$ αν και μονο αν ο $d$ διαιρει το $b$ .Οταν ο $d$ διαιρει το $b$ η εξισωση εχει ακριβως $d$ λυσεις στο $\mathbb{Z}_m$.

Αποδειξη :Δειχνουμε πρωτα ότι δεν υπαρχει λυση της $ax = b$ στο $\mathbb{Z}_m$ εκτος αν ο $d$ διαιρει το $b$ .Ας υποθεσουμε ότι $s \in \mathbb{Z}_m$ ,είναι μια λυση.Τοτε $as - b = qm$ στους ακεραιους,αρα $as - qm = b$ .Αφου ο $d$ διαιρει τους $a,m$ βλεπουμε ότι ο $d$ διαιρει και το αριστερο μερος της εξισωσης,επομενως και τον $b$ .Δηλαδη η λυση $s$ μπορει να υπαρχει μονο αν ο $d$ διαιρει το $b$.

Ας υποθεσουμε ότι ο $d$ διαιρει το $b$ .Θετουμε

$$a = a_1 d\ ,\ b = b_1 d \ \text{ και } \ m = m_1 d$$

Τοτε η εξισωση $as - b = qm$ στους ακεραιους ξαναγραφεται ως $d(a_1 s - b_1) = dqm_1$ .Βλεπουμε ότι ο $as - b$ είναι πολ/σιο του $m$ αν και μονο αν ο $a_1 s - b_1$ είναι πολ/σιο του $m_1$ .Ετσι οι λυσεις $s$ της $ax = b$ στο $\mathbb{Z}_m$ είναι ακριβως τα στοιχεια που ως κλασεις $\mathrm{mod}ulo m_1$ ,δινουν λυσεις της $a_1 x = b_1$ στο $\mathbb{Z}_{m1}$ .Εστω τωρα $s \in \mathbb{Z}_{m1}$ η μοναδικη λυση της $a_1 x = b_1$ στο $\mathbb{Z}_{m1}$ που δινεται από το παραπανω θεωρημα.Τα στοιχεια του $\mathbb{Z}_m$ που ως κλασεις $\mathrm{mod}ulo\ m_1$ συμπιπτουν με τον $s$ ,είναι ακριβως εκεινα που στον $\mathbb{Z}_m$ γραφονται στη μορφη

$$s, s + m_1, s + 2m_1, ..., s + (d-1)m_1$$

Δηλαδη υπαρχουν ακριβως $d$ λυσεις της εξισωσης στον $\mathbb{Z}_m$.

Πορισμα: Εστω $d$ ο μεγιστος κοινος διαιρετης των θετικων ακεραιων $a$ και $m$ .Η ισοτιμια $ax \equiv b(\mathrm{mod}\, m)$ εχει λυση αν και μονο αν ο $d$ διαιρει τον $b$ .Σ'αυτην τη περιπτωση οι λυσεις είναι ολοι οι ακεραιοι που ανηκουν σε ακριβως $d$ διαφορετικες κλασεις υπολοιπων $\mathrm{mod}ulo\ m$.

## 1.11 Το Σωμα πηλικων μιας ακεραιας περιοχης.

Αν μια ακεραια περιοχη εχει την ιδιοτητα κάθε μη μηδενικο στοιχειο της να εχει πολλαπλασιαστικο αντιστροφο,τοτε είναι σωμα.Ομως πολλες ακεραιες περιοχες ,όπως οι $\mathbb{Z}$ ,δεν σχηματιζουν σωμα.Εντουτοις μπορει κανεις να θεωρει καθε ακεραια περιοχη εμβαπτισμενη σε ένα σωμα,ένα σωμα πηλικων της ακεραιας περιοχης.Το σωμα αυτό θα είναι το ελαχιστο σωμα που περιεχει την ακεραια περιοχη .Οι ακεραιοι περιεχονται στο σωμα $\mathbb{Q}$ του οποιου όλα τα στοιχεια εκφραζονται ως πηλικα ακεραιων.

**Θεωρημα:** Μπορουμε να επεκτεινουμε (η να εμβαπτισουμε) οποιαδηποτε ακεραια περιοχη $D$ σε ένα σωμα $F$ με τετοιο τροπο,ώστε κάθε στοιχειο του $F$ να γραφεται ως πηλικο δυο στοιχειων της $D$.(Ένα τετοιο σωμα $F$ λεγεται σωμα πηλικων της $D$)

Η κατασκευη χωριζεται σε 4 βηματα:
1)τον ορισμο των στοιχειων της $F$
2)Τον ορισμο των διμελων πραξεων της προσθεσης και πολλαπλασιασμου στο $F$
3)Ελεγχος των αξιωματων του σωματος για να δειξουμε ότι η $F$ είναι οντος σωμα με αυτές τις πραξεις
4)Δειχνουμε ότι μπορουμε να θεωρησουμε ότι το $F$ περιεχει την $D$ ως ακεραια υποπεριοχη.

Για δοθεισα ακεραια περιοχη $D$ ,σχηματιζουμε το καρτεσιανο γινομενο $D\times D=\{(a,b)\big|a,b\in D\}$.Θεωρουμε ότι ένα διατεταγμενο ζευγος $(a,b)$ παριστανει ένα τυπικο πηλικο $\frac{a}{b}$.Ενα υποσυνολο $S$ του $D\times D$ που οριζεται ως $S=\{(a,b)\big|a,b\in D,b\neq 0\}$.

Στο συνολο $S$ οριζουμε μια σχεση ισοδυναμιας με τη σχεση $(a,b)\sim(c,d)$ αν και μονο αν $ad=bc$.Τελος οριζουμε ως $F$ το συνολο ολων των κλασεων ισοδυναμιας $[(a,b)]$ με $(a,b)\in S$.

Αν $[(a,b)]$ και $[(c,d)]$ είναι στοιχεια του $F$ ,οι ισοτητες

$$[(a,b)]+[(c,d)]=[(ad+bc,bd)]$$

και

$$[(a,b)][(c,d)]=[(ac,bd)]$$

δινουν καλα ορισμενες πραξεις προσθεσης και πολλαπλασιασμου στο $F$ .

## 1.12 Στρεβλα Σωματα

Το πιο χαρακτηριστικο παραδειγμα στρεβλου σωματος είναι οι τετραδες του Hamilton.

Θεωρουμε ένα συνολο $\Im=\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$ .Τωρα η $<\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R},+>$ γινεται ομαδα με πραξη την προσθεση κατά συντεταγμενες,δηλαδη το ευθυ γινομενο του $\mathbb{R}$ με πραξη την προσθεση επι τον εαυτο του τεσσερις φορες.Εχουμε ετσι την πραξη της προσθεσης στο $\Im$ .θα ξεχωρισουμε καποια στοιχεια του $\Im$ ,δινοντας τους νεα ονοματα.θετουμε

$1=(1,0,0,0)$ , $i=(0,1,0,0)$,
$j=(0,0,1,0)$ και $k=(0,0,0,1)$

$a_1=(a_1,o,o,o)$ $a_2i=(0,a_2,o,o)$

$a_3j=(0,0,a_3,0)$ $a_4k=(0,0,0,a_4)$

Συμφωνα με τον ορισμο που εχουμε δωσει για την προσθεση,εχουμε

$$(a_1,a_2,a_3,a_4)=a_1+a_2i+a_3j+a_4k$$

Επομενως

$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3) j + (a_4 + b_4)k$$

Για να ορισουμε τον πολλαπλασιασμο στο $\mathfrak{I}$ οριζουμε

$1a = a1 = a \quad$ για $\ a \in \mathfrak{I}$

$$i^2 = j^2 = k^2 = -1$$

Και

$$ij = k,\ jk = i, ki = j \qquad ji = -k, kj = -i, ik = -j$$

Οριζουμε το γινομενο δυο τετραδων με τροπο ώστε να ισχυουν οι επιμεριστικοι νομοι

$$(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k) = (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4)$$
$$+(a_1 b_2 + a_2 b_1 + a_3 b_4 + a_4 b_3)i \ \ +(a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)\, j \ \ +(a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)k$$

Βλεπουμε ότι ο πολλαπλασιασμος δεν είναι αντιμεταθετικος αφου $ij = -ji$ .Επιπλεον,υπαρχει και πολλαπλασιαστικο αντιστροφο για καθε στοιχειο α στο $\mathfrak{I}$.

Επομενως δειξαμε το παρακατω θεωρημα.

Θεωρημα:Οι τετραδες $\mathfrak{I}$ αποτελουν στρεβλο σωμα με την προσθεση και τον πολλαπλασιασμο.

Η αλγεβρα δεν είναι τοσο πλουσια σε στρεβλα σωματα οσο είναι σε σωματα.Για παραδειγμα δεν υπαρχουν πεπερασμενα στρεβλα σωματα.Αυτο είναι το περιεχομενο του θεωρηματος του Weddeburn το οποιο διατυπωνουμε παρακατω.

Θεωρημα:Κάθε πεπερασμενος δακτυλιος διαιρεσης είναι σωμα.

Η αποδειξη του θα γινει στο επομενο κεφαλαιο.

## 1.13 Διανυσματικοι Χωροι

Ορισμος:Εστω $F$ ένα σωμα .Ενας διανυσματικος χωρος πανω από το $F$ απότελειται από μια αβελιανη ομαδα $V$ με την προσθεση,μαζι με μια πραξη βαθμωτου πολλαπλασιασμου των στοιχειων του $V$ με τα στοιχεια του $F$ από τα αριστερα τετοια ώστε για κάθε $a,b \in F$ και $\alpha, \beta \in V$ να ικανοποιουνται οι ακολουθες συνθηκες:

1. $a\alpha \in V$
2. $a(b\alpha) = (ab)\alpha$
3. $(a+b)\alpha = (a\alpha) + (b\alpha)$
4. $a(\alpha + \beta) = (a\alpha) + (a\beta)$
5. $1\alpha = \alpha$

Τα στοιχεια του $V$ λεγονται διανυσματα και τα στοιχεια του $F$ βαθμωτα.

Κεφαλαιο 2

## 2.1 Αποδειξη του Θεωρηματος του Weddeburn

.

Ο στοχος αυτου του κεφαλαιου είναι η ενδελεχης αποδειξη του θεωρηματος Weddeburn .Γνωριζουμε ότι ενας δακτυλιος με μοναδιαιο στοιχειο λεγεται δακτυλιος διαιρεσης αν και μονο αν κάθε μη μηδενικο στοιχειο του εχει

πολλαπλασιαστικο αντιστροφο .Αρα για να γινει αυτος ο δακτυλιος σωμα χρειαζομαστε μονο την αντιμεταθετικη ιδιοτητα ως προς τον πολλαπλασιασμο.Ενας μη αντιμεταθετικος δακτυλιος διαιρεσης λεγεται στρεβλο σωμα. Το πιο γνωστο παραδειγμα στρεβλου σωματος είναι οι τετραδες του Hamilton που παραθεσαμε στο προηγουμενο κεφαλαιο.Η αλγεβρα δεν είναι τοσο πλουσια σε στρεβλα σωματα οσο είναι σε σωματα όπως εχουμε αναφερει και συμφωνα με το θεωρημα ολοι οι πεπερασμενοι δακτυλιοι διαιρεσης είναι σωματα.Το ομορφο αυτό θεωρημα αποδιδεται στον MacLagan Weddeburn ,εχει εν-τουτοις αποδιχτει από πολλους μαθηματικους εχοντας χρησιμμοποιησει ποικιλες ιδεες.Μια αποδειξη ξεχωριζει για την απλοτητα και την κομψοτητα της. Η αποδειξη του Witt.Συνδιαζει δυο βασικες ιδεες και ένα μεγαλιωδες τελειωμα.

Θεωρημα(Wedderburn): Κάθε πεπερασμενος δακτυλιος διαιρεσης $R$ είναι σωμα.

Αποδειξη :

Για ένα τυχον στοιχειο $s \in R$, $(R,+,\cdot)$ πεπερασμενος δακτυλιος διαιρεσης ,το $C_s$ είναι το συνολο $x \in R : xs = sx$ των στοιχειων που αντιμετατιθενται με το s.
Το συνολο $C_s$ περιεχει τα στοιχεια $0,1$ αφου
$0s = s0 = 0$ και $1s = s1 = s$ και τα $s, s^{-1}$(ο πολλαπλασιαστικος αντιστροφος του $s$).
1)Δειχνουμε ότι το $C_s$ είναι υποδακτυλιος διαιρεσης

Για κάθε $a,b \in C_s$ ισχυει ότι $(a+b)s = as+bs = s(a+b)$
Αρα το $(a+b) \in C_s$ οποτε η προσθεση είναι κλειστη εσωτερικη πραξη στο συνολο $C_s$ .Λογω του ότι όλα τα στοιχεια του $C_s$ είναι στοιχεια του δακτυλιου $(R,+,\cdot)$ η προσθεση θα είναι αντιμεταθετικη.
Εστω $a \neq 0,1 \in C_s$ οπου $as = sa$ .
Για τυχον στοιχειο $a \in C_s$ δειχνουμε ότι ο προσθετικος και ο πολλαπλασιαστικος αντιστοφος του $a$ ανηκει στο $C_s$ .
1) $-(as) = -(sa) \Rightarrow (-a)\cdot s = s(-a)$ αρα ο $-a$ ο προσθετικος αντιστροφος του $a$ ανηκει στο $C_s$ .Οποτε το $C_s$ με εσωτερικη πραξη την προσθεση είναι αβελιανη ομαδα.
2)Μενει να δειξουμε ότι για κάθε $a \in C_s$ επεται ότι $a^{-1} \in C_s$ δηλαδη $a^{-1}\cdot s = s\cdot a^{-1}$.Εστω ότι ισχυει,πολλαπλασιαζουμε από αριστερα με $a$ και εχουμε $a\cdot(a^{-1}\cdot s) = a\cdot(s\cdot a^{-1})$ .Λογω προσεταιριστικοτητας της πραξης του πολλαπλασιασμου εχουμε $(a\cdot a^{-1})\cdot s = (a\cdot s)\cdot a^{-1}$.Με πραξεις στην πρωτη και δευτερη παρενθεση(πολ/σμο και αντιμεταθετικη ιδιοτητα αντιστοιχα) προκυπτει ότι $s = s\cdot(a\cdot a^{-1})$ ,δηλαδη $s = s$.Οποτε για κάθε $a \in C_s$ το $a^{-1} \in C_s$ .
Οποτε δειξαμε ότι ο $C_s$ είναι υποδακτυλιος διαιρεσης.
.

Το κεντρο Z είναι το συνολο των στοιχειων του δακτυλιου διαιρεσης που αντιμετατιθενται με όλα τα στοιχεια του δακτυλιου, οποτε ισχυει ότι $Z = \bigcap_{s\in R} C_S$ .
Τα 0 και 1 ανηκουν στο Z ,όλα τα όλα στοιχεια του αντιμετατιθενται οποτε το Z είναι ένα πεπερασμενο σωμα.Εστω το πληθος των στοιχειων του Z να είναι ισο με $|Z| = q$ .

Θεωρουμε τους δακτυλιους $R$ και $C_s$ ως διανυσματικους χωρους πανω στο σωμα Z και συμπεραινουμε ότι το πληθος των στοιχειων του $R$ είναι ισο με $|R| = q^n$ οπου n είναι η διασταση του διανυσματικου χωρου $R$ πανω στο Z και ομοια $|C_s| = q^{n_s}$ για ακεραιο $n_s \geq 1$.

Εστω ότι το $R$ δεν είναι σωμα .Αυτό σημαινει ότι για καποια $s \in R$ το $C_s$ είναι γνησιο υποσυνολο του $R$ ,δηλαδη $n_s < n$ .

Στο συνολο $R^* = R - 0$ οριζουμε τη σχεση
$r' \sim r :\Leftrightarrow r' = x^{-1}rx$ για καποιο $x \in R^*$ .

Δειχνουμε ότι η ~ είναι σχεση ισοδυναμιας ,δηλαδη ότι ικανοποιει την ανακλαστικη (α~α),
τη συμμετρικη(α~β τοτε β~α) και
τη μεταβατικη ιδιοτητα(α~β και β~γ τοτε α~γ).

1.Ανακλαστικη Ιδιοτητα
$r \sim r$ : $r = x^{-1} \cdot r \cdot x \Rightarrow$ για $x = 1_\Delta$
εχουμε
$r = 1_\Delta^{-1} r 1_\Delta$ αρα $r \sim r$

2.Συμμετρικη Ιδιοτητα
$r_1 \sim r_2 \Leftrightarrow r_2 \sim r_1$
$r_1 = x^{-1} r_2 x \Rightarrow r_2 = x r_1 x^{-1}$
Για $x = y^{-1}$ εχουμε $r_2 = y^{-1} r_1 y$
Αρα $r_2 \sim r_1$

3.Μεταβατικη Ιδιοτητα
$r_1 \sim r_2$ και $r_2 \sim r_3$
δειχνουμε ότι $r_1 \sim r_3$

$r_1 = x^{-1} r_2 x$ και $r_2 = y^{-1} r_3 y$
Αρα $r_1 = x^{-1} y^{-1} r_3 yx$ ,που ισουται με $r_1 = (yx)^{-1} r_3 yx$

Δειξαμε το ζητουμενο ότι $r_1 \sim r_3$ αρα η $r' \sim r :\Leftrightarrow r' = x^{-1} r x$ είναι σχεση ισοδυναμιας.

Το συνολο $A_s := \{ x^{-1} s x : x \in R^* \}$ είναι η κλαση ισοδυναμιας που περιεχει το s,δηλαδη όλα τα στοιχεια που είναι ισοδυναμα με το $s$ και γραφονται στη μορφη $x^{-1} s x$ .Η κλαση εχει ταξη $|A_s|$=1(περιεχει μονο ένα στοιχειο το $s$ ) ακριβως όταν το s ανηκει στο κεντρο Z,δηλαδη όταν αντιμετατιθεται με κάθε στοιχειο του δακτυλιου διαιρεσης.

Από την υποθεση μας (ότι ο πεπερασμενος δακτυλιος διαιρεσης δεν είναι σωμα) υπαρχουν κλασεις ισοδυναμιας $A_s$ με ταξη μεγαλυτερη του 2(περιεχουν δυο στοιχεια και πανω,δηλαδη $|A_s| \geq 2$ .

Θεωρουμε για $s \in R^*$ την απεικονιση $f_s : x \to x^{-1} s x$ από $R^*$ επι του $A_s$ .

Δηλαδη απεικονιζουμε κάθε στοιχειο του δακτυλιου στην κλαση ισοδυναμιας του $s$.

Για $x, y \in R^*$ βλεπουμε ότι αν

$x^{-1}sx = y^{-1}sy \Leftrightarrow$

$(yx^{-1})s = s(yx^{-1}) \Leftrightarrow$

$\Leftrightarrow yx^{-1} \in C_s^* \Leftrightarrow y \in C_s^* x$

για $C_s^* := C_s - \{0\}$,οπου το $C_s^* x = \{zx : z \in C_s^*\}$ εχει ταξη $\left|C_s^*\right|$.Αφου κάθε στοιχειο της μορφης $x^{-1}sx$ είναι εικονα ακριβως $\left|C_s^*\right| = q^{n_s} - 1$ στοιχειων του $R^*$ μεσω της απεικονισης $f_s$ , συμπεραινουμε ότι $\left|R^*\right| = \left|A_s\right|\left|C_s^*\right|$.

Παρατηρουμε ότι ,η ταξη του $A_s$ ισουται με $\frac{\left|R^*\right|}{\left|C_s^*\right|} = \frac{q^n - 1}{q^{n_s} - 1} = \left|A_s\right|$ και είναι ενας ακεραιος αριθμος για κάθε s.

Γνωριζουμε ότι οι ταξεις ισοδυναμιας σε ένα συνολο διαμεριζουν το συνολο και εν προκυμενω διαμεριζουν τον $R^*$.

Ομαδοποιουμε τα στοιχεια του κεντρου $Z^*$ και οριζουμε ως $A_1, ..., A_n$ τις ταξεις ισοδυναμιας που περιεχουν πανω από ένα στοιχειο.Απο υποθεση γνωριζουμε ότι $t \geq 1$.

Αφου $\left|R^*\right| = \left|Z^*\right| + \sum_{k=1}^{t} \left|A_k\right|$ αποδειξαμε την λεγομενη φορμουλα ταξης

$q^n - 1 = q - 1 + \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1}$ (1) που ισχυει ότι $1 < \frac{q^n - 1}{q^{n_k} - 1} \in N$ για όλα τα κ.

Ισχυριζομαστε ότι $q^{n_k} - 1 \left| q^n - 1 \right.$ σημαινει ότι $n_k \left| n \right.$ .

Γραφουμε τον αλγοριθμο της διαιρεσης για τα $n, n_k$

$n = an_k + r$ με $0 \leq r < n_k$ ,τοτε $q^{n_k} - 1 \left| q^{an_k + r} - 1 \right.$ και προφανως ισχυει ότι $q^{n_k} - 1 \left| (q^{an_k + r} - 1) - (q^{n_k} - 1) \right.$.Επομενως κανοντας τις πραξεις εχουμε ότι $q^{n_k} - 1 \left| q^{n_k}(q^{(a-1)n_k + r} - 1) \right.$ και ότι $q^{n_k} - 1 \left| q^{(a-1)n_k + r} - 1 \right.$ αφου οι $q^{n_k} - 1$ και $q^{n_k}$ είναι σχετικα πρωτοι μεταξυ τους.Συνεχιζοντας με ομοιο τροπο δηλαδη αφαιρωντας το $q^{n_k} - 1$ ,α-1 φορες ακομη, βρισκουμε ότι $q^{n_k} - 1 \left| q^r - 1 \right.$ το οποιο ισχυει μονο στην περιπτωση που το $r = 0$ ,αρα $n_k \left| n \right.$ για όλα τα κ.(2)

Θεωρουμε το πολυωνυμο $x^n-1$.Οι ριζες του στους μιγαδικους C ονομαζονται οι n-οστες ριζες της μοναδος. Αφου $l^n=1$,ολες οι ριζες του εχουν μετρο μοναδα $|l|=1$, και είναι σημεια του μοναδιαιου κυκλου στο μιγαδικο επιπεδο. Επομενως είναι οι αριθμοι της μορφης $l_k=e^{\frac{2k\pi i}{n}}=\cos(\frac{2k\pi i}{n})+i\sin(\frac{2k\pi i}{n}),0\le k\le n-1$.Καποιες από τις ριζες ικανοποιουν τη σχεση $l^d=1$ για $d<n$.Παραδειγματος χαρη η ριζα $l=-1$

ισχυει για $d=2,l^2=1$ .Για μια ριζα l, οριζουμε με d το μικροτερο θετικο εκθετη τετοιο ώστε $l^d=1$ οπου d είναι η ταξη του l της πολλαπλασιαστικης ομαδας των νιοστων ριζων της μοναδας. Οποτε $d|n$ από θεωρημα του Lagrange(Η ταξη κάθε στοιχειου μιας ομαδας διαιρει την ταξη της ομαδας ).

Ομαδοποιουμε ολες τις ριζες ταξεως d και θετουμε

$\Phi_d:=\prod_{l\tau\alpha\xi\eta\varsigma d}(x-l)$ .

Παρατηρουμε ότι ο ορισμος του $\Phi_d$ είναι ανεξαρτητος του n.
Αφου κάθε ριζα εχει καποια ταξη d συμπεραινουμε ότι $x^n-1=\prod_{d|n}\Phi_d(x)$.(3)

Ισχυριζομαστε οτι οι συντελεστες των πολυωνυμων $\Phi_n(x)$ είναι ακεραιοι ( για όλα τα n ισχυει ότι $\Phi_n(x)\in\mathbb{Z}\ x$ ) και ο σταθερος συντελεστης είναι ειτε 1 ειτε -1.

Ας αποδειξουμε προσεκτικα αυτό τον ισχυρισμο .Για $n=1$ η μονη ριζα είναι η μοναδα και ετσι $\Phi_1(x)=x-1$.Χρησιμοποιουμε την μεθοδο της επαγωγης ,και υποθετουμε ότι $\Phi_d(x)\in\mathbb{Z}\ x$ για όλα τα $d<n$ και ότι ο σταθερος συντελεστης είναι ειτε 1 η -1.Απο την σχεση (3) εχουμε

$$x^n-1=p(x)\phi_n(x) \qquad (4)$$

οπου $p(x)=\sum_{j=0}^{l} p_j x^j, \phi_n(x)=\sum_{k=0}^{n-l} a_k x^k$ με $p_0=+1$ η $p_0=-1$ .Απο το γεγονος ότι $-1=p_0 a_0$ εχουμε ότι $a_0 \in -1,1$ .Υποθετουμε ότι $a_0, a_1, ..., a_{k-1} \in \mathbb{Z}$ .Υπολογιζουμε τους συντελεστες του $x^k$ και στις δυο μεριες της εξισωσης $x^n-1=p(x)\phi_n(x)$ βρισκουμε ότι $\sum_{j=0}^{k} p_j a_{k-j}=\sum_{j=1}^{k} p_j a_{k-j}+p_0 a_k \in \mathbb{Z}$ .Απο υποθεση γνωριζουμε ότι $a_0, a_1, ..., a_{k-1} \in \mathbb{Z}$ (και όλα $p_j \in \mathbb{Z}$ ).Επομενως το $p_0 a_k$ και πιο συγκεκριμενα το $a_k$ πρεπει να είναι ακεραιοι αφου το $p_0$ παιρνει τις τιμες 1,-1.

Εστω το $n_k | n$ ότι είναι οι αριθμοι που εμφανιζονται στην εξισωση

$$q^n-1=q-1+\sum_{k=1}^{t}\frac{q^n-1}{q^{n_k}-1} \quad .$$

Τοτε $x^n-1=\prod_{d|n}\Phi_d(x)=(x^{n_k}-1)\Phi_n(x)\prod_{d|n,d\neq n}\Phi_d(x)$ οπου γνωριζουμε ότι το d δεν διαιρει το $n_k$.Συμπαιρενουμε ότι στο $\mathbb{Z}$ ισχυουν οι δυο σχεσεις

1) $\Phi_n(q) | q^n-1$

2) $\Phi_n(q) \left| \frac{q^n-1}{q^{n_k}-1} \right.$ (5)

Αφου η σχεση (5) ισχυει για όλα τα κ, συμπεραινουμε από την(1) ότι

$\Phi_n(q) | q-1$ που είναι ατοπο.

Γνωριζουμε ότι $\Phi_n(x)=\prod(x-l)$ οπου l είναι ολες οι ριζες ταξεως n του $x^n-1$.Εστω ότι $l'=a+ib$ να είναι μια ριζα. Επισης, $|l'|=a^2+b^2=1$ οποτε εχουμε

$$|q-l'|^2=|q-a-ib|^2=(q-a)^2+b^2=q^2-2aq+a^2+b^2=q^2-2aq+1>q^2-2q+1=(q-1)^2$$

Συμπεραινουμε ότι $|q-l'|>(q-1)$ .Η σχεση αυτή ισχυει για ολες τις ριζες ταξεως n. Οποτε $|\Phi_n(q)|=\prod_l |q-l|>q-1$ το οποιο σημαινει ότι το $\Phi_n(q)$ δεν δυναται να είναι διαιρετης του $q-1$,ατοπο τελος της αποδειξης.

Κεφαλαιο 3 Εφαρμογες Σωματων στην κρυπτογραφια

## 3.1 Γραμμικες Ισοδυναμιες πρωτου Βαθμου

Η λυση πρωτοβαθμιων ισοδυναμιων είναι ουσιωδες συστατικο της κρυπτογραφιας.Η επιλυση μιας γραμμικης διοφαντικης εξισωσης της μορφης $ax+by=c$ είναι ουσιαστικα η επιλυση της ισοδυναμιας $ax=c \bmod b$ δηλαδη για ποιες τιμες του $x$ ισχυει η σχεση $ax-c=\pi o\lambda b$ .

Για $a,b,c \in \mathbb{Z}$ μπορουμε να βρουμε ακεραιο $n$ με $an = b \bmod c$ .Αν ο $n$ ικανοποιει την ισοδυναμια τοτε ολοι οι ακεραιοι της μορφης $n+kc$ .Οποτε υπαρχουν απειρες λυσεις της παραπανω ισοδυναμιας.Οι λυσεις αυτές είναι ολες ισοδυναμες $\bmod c$ .
Υπαρχουν όμως και λυσεις της ισοδυναμιας μη ισοδυναμες $\bmod c$ .
Γνωριζουμε ότι η διοφαντικη $ax+by=c$ εχει λυσεις αν και μονο αν ο ΜΚΔ $(a,b)=d$ διαιρει το c.Καθε λυση θα εχει τη μορφη

$x = x_0 + \frac{bt}{d}$ και $y = y_0 - \frac{at}{d}$ οπου $x_0, y_0$ μια συγκεκριμενη λυση και $t$ μια παραμετρος.Βλεπουμε ότι από τις απειρες τιμες του $x$ ,οι $x_0 + \frac{b}{d}, x_0 + \frac{2b}{d}, ..., x_0 + \frac{(d-1)b}{d}$ είναι μη ισοδυναμες $\bmod b$ διοτι το απολυτο της διαφορας δυο οποιονδηποτε από αυτές είναι μικροτερο του $b$ .Αυτη η σκεψη αποτελει την αποδειξη του παρακατω θεωρηματος.

**Θεωρημα:**Αν $d = \text{ΜΚΔ}(a,c)$ τοτε η ισοδυναμια $an = b \bmod c$ δεν εχει λυση αν $d \dagger b$ και εχει $d$ μη ισοδυναμες λυσεις αν $d \mid b$ .

Για $b=1$ η ισοδυναμια γινεται $an = 1 \bmod c$ .Αν $aa' = 1 \bmod c$ λεμε ότι ο $a'$ είναι ο αντιστροφος του $a \bmod c$

Πορισμα:Αν ο $\text{ΜΚΔ}(a,c)=1$ τοτε ο α εχει αντιστροφο( $a'$ τετοιο ώστε $aa' = 1 \bmod c$ ) που είναι μοναδικος $\bmod c$ .

Εχουμε αναφερει το θ.Euler και το πορισμα του ,το λεγομενο μικρο θεωρημα του Fermat.Τα δυο αυτά θεωρηματα εχουν εφαρμογη στην μεθοδο RSA της κρυπτογραφιας με δημοσιο κλειδι. θ.Wilson

**Θεωρημα(**Euler **) :** Αν ο $\text{ΜΚΔ}(a,m)=1$ τοτε $a^{\varphi(m)} \equiv 1 (\bmod m)$
Αποδειξη :Εστω $r_1, r_2, ...., r_{\phi(m)}$ ένα περιορισμενο συνολο υπολοιπων $\bmod m$ .Εφοσον $\text{ΜΚΔ}(a,m)=1$ εχουμε ότι οι αριθμοι $ar_1, ar_2, ...., ar_{\phi(m)}$ θα είναι ολοι πρωτοι προς τον $m$ ..Επισης είναι ολοι μη ισοδυναμοι μεταξυ τους.Αντιστοιχουμε κάθε αριθμο $ar$ με καποιο $r_j$ ώστε $ar_i = r_j \bmod m$ .
Τοτε $r_1 r_2 ... r_{\phi(m)} = ar_1 ar_2 .... ar_{\phi(m)} \bmod m$ με $R = r_1 r_2 ... r_{\phi(m)}$ οποτε η σχεση γινεται $R = a^{\phi(m)} R \bmod m$ .Αλλα ο $\text{ΜΚΔ}(R,m)=1$ διοτι ο $R$ είναι ένα γινομενο $\phi(m)$ το πληθος αριθμων οπου κάθε παραγοντας είναι πρωτος προς τον $m$ .
Αρα $a^{\varphi(m)} \equiv 1 (\bmod m)$ από τον κανονα της απλοποιησης ισοδυναμιων

Μικρο Θεωρημα Fermat: Αν $p$ πρωτος ,τοτε $n^p = n \bmod p$

Αποδειξη :Αν ο $p|n$ τοτε $n^p = 0 = n \bmod p$ .

Αν ο $p \dagger n$ τοτε ΜΚΔ $(p,n) = 1$

Αρα από το Θ. Euler εχουμε $n^{p-1} = 1 \bmod p$ .Πολλαπλασιαζουμε και τα δυο μελη επι $n$ και εχουμε το ζητουμενο.

Θεωρημα Wilson: Η ισοδυναμια $(m-1)! = -1 \bmod m$ ισχυει αν και μονο αν ο $m$ είναι πρωτος.

Θα εξετασουμε την λυση ενός συστηματος πρωτοβαθμιων ισοδυναμιων της μορφης

$a_1 x = b_1 \bmod m_1$
$a_2 x = b_2 \bmod m_2$
…
$a_n x = b_n \bmod m_n$

Είναι πολύ χρησιμο και μας βοηθαει να λυσουμε μια ισοδυναμια με μετρο μεγαλο αριθμο.Εστω $m = p_1^{l_1} p_2^{l_2} .. p_s^{l_s}$ η παραγοντοποιηση του $m$ σε πρωτους παραγοντες.Αλλα από το Θεμελιωδες Θεωρημα της Αριθμητικης $m|n$ αν και μονο αν $p_i^{l_i} | n$ για κάθε $i$ αρα

$A = B \bmod m$ αν και μονο αν ισχυουν οι ισοδυναμιες

$A = B \bmod p_1^{l_1}$
$A = B \bmod p_2^{l_2}$
……..
$A = B \bmod p_s^{l_s}$

Δηλαδη η ισοδυναμια $a\ x = b \bmod m$ εχει το ιδιο συνολο λυσεων με το συστημα

$a\ x = b \bmod p_1^{l_1}$
….
$a\ x = b \bmod p_n^{\ln}$

Αυτό προκυπτει από το γνωστο και ως κινεζικο θεωρημα υπολοιπων το οποιο αποδιδεται επισης και στον Ελληνα Μαθηματικο Νικομαχο τον Γερασηνο.

Θεωρημα(Κινεζικο Θεωρημα Υπολοιπων(ΚΘΥ))
Εστω οι $s$ φυσικοι $m_1 m_2 .. m_s$ οπου ολοι είναι πρωτοι προς αλληλους και $M = m_1 m_2 .. m_s$ .Εστω επιπλεον οι $s$ το πληθος ακεραιοι $a_i$ $1 \le i \le s$ με ΜΚΔ $(a_i, m_i) = 1$ για κάθε $i$.
Τοτε οι $s$ ισοδυναμιες

$a_1 x = b_1 \bmod m_1$
$a_2 x = b_2 \bmod m_2$
..... και
$a_s x = b_s \bmod m_s$

Εχουν μια μοναδικη λυση $\bmod M$

## 3.2 Ισοδυναμιες δευτερου βαθμου

Η απλουστερη μορφη ισοδυναμιας δευτερου βαθμου είναι της μορφης $x^2 = a \bmod p$ με $p$ πρωτο.Η λυση οδηγει στο περιφημο θεωρημα του Gauss το νομο τετραγωνικης αντιστρεπτοτητας .Γνωριζουμε ότι τα στοιχεια ενός περιορισμενου συνολου υπολοιπων αποτελουν μια πολλαπλασιαστικη ομαδα.Αν ο $p$ είναι πρωτος υπαρχει ακεραιος $g$ με την ιδιοτητα οι $g, g^2 .., g^{p-1}$ να αποτελουν ένα περιορισμενο συνολο υπολοιπων ητοι μια κυκλικη ομαδα.

Ορισμος:Αν $h$ είναι ο μικροτερος θετικος ακεραιος τετοιος ώστε $a^h = 1 \bmod m$ τοτε λεμε ότι ο $a$ ανηκει στον εκθετη $h$ $\bmod ulo\ m$

**Θεωρημα:**Μια ικανη και αναγκαια συνθηκη για να ισχυει $a^b = 1 \bmod m$ για καποιον ακεραιο $b$ είναι ο ΜΚΔ $(a, m) = 1$.

Θ **Θεωρημα:**Αν ο $a$ ανηκει στον εκθετη $h \bmod m$ και $a^r = 1 \bmod m$ τοτε $h | r$ .

Ορισμος:Αν ο ακεραιος $g$ ανηκει στον εκθετη $\phi(m) \bmod m$ τοτε ο $g$ ονομαζεται αρχικη η πρωταρχικη ριζα $\bmod m$.

**Θεωρημα:**Αν ο $g$ είναι αρχικη ριζα $\bmod m$ τοτε οι δυναμεις του $g$ ,δηλαδη $g, g^2, ..., g^{\phi(m)}$ είναι ολες μη ισοδυναμες $\bmod m$ και αποτελουν ένα περιορισμενο συνολο υπολοιπων $\bmod m$.

**Θεωρημα:**Αν ο $a$ ανηκει στον εκθετη $h \bmod m$ και $\text{ΜΚΔ}(k,h) = d$ τοτε ο $a^k$ ανηκει στον $h/d \bmod m$

Πορισμα:Αν $g$ είναι πρωταρχικη ριζα $\bmod m$ τοτε η $g^r$ είναι επισης μια πρωταρχικη ριζα $\bmod m$ αν και μονο αν ο $\text{ΜΚΔ}\ (r, \varphi(m)) = 1$

**Θεωρημα:**Αν υπαρχει καποια πρωταρχικη ριζα $\bmod m$ τοτε το πληθος των αμοιβαια μη ισοδυναμων πρωταρχικων ριζων είναι $\varphi(\phi(m))$

**Θεωρημα:**.Για κάθε πρωτο $p$ ,υπαρχουν πρωταρχικες ριζες $\bmod p$.

## 3.3 Τετραγωνικα Υπολοιπα

Ορισμος:Εστω ο πρωτος $p$ και $\text{ΜΚΔ}(a, p) = 1$.Αν $p \dagger a$ και η εξισωση $x^2 = a \bmod p$ εχει λυση λεμε ότι ο $a$ είναι τετραγωνικο υπολοιπο $\bmod p$.

**Θεωρημα:**.(Κριτηριο Euler) :Ο αριθμος $a$ είναι τετραγωνικο υπολοιπο $\bmod p$ αν και μονο αν $a^{\frac{p-1}{2}} = 1 \bmod p$

Πορισμα:Εστω $g$ μια πρωταρχικη ριζα $\bmod p$ και εστω $\text{ΜΚΔ}\ (a, p) = 1$.Εστω $r$ ακεραιος με $g^r = a \bmod p$.Τοτε ο $r$ είναι ζυγος αν και μονο αν το $a$ είναι τετραγωνικο υπολοιπο $\bmod p$

Το συμβολο Legendre $(\frac{b}{p})$ οπου $p$ περιττος πρωτος εχει τις τιμες

1 αν ο $b$ είναι τετραγωνικο υπολοιπο
0 αν ο $b$ είναι πολλαπλασιο του $p$
-1 στις άλλες περιπτωσεις

Ισοδυναμα το $(\frac{b}{p})=1$ αν το $b$ είναι τετραγωνικο υπολοιπο στο σωμα $GF(p)$
η αν η ισοδυναμια $x^2 = b \bmod p$

**Θεωρημα:** Αν $p$ μονος πρωτος υπαρχουν $\frac{p-1}{2}$ ακριβως μη ισοδυναμα τετραγωνικα υπολοιπα του $p$ που δινονται από τη σχεση $1^2, 2^2, ...., (\frac{p-1}{2})^2$

Λημμα **:**Αν $p$ μονος πρωτος και $(a, p)=1$ τοτε ειτε
$a^{\frac{p-1}{2}} = 1 \bmod p$ ειτε $a^{\frac{p-1}{2}} = -1 \bmod p$

Θεωρημα( Κριτηριο του Euler) **:** Αν $p$ μονος πρωτος και $(a, p)=1$ τοτε
$(\frac{a}{p}) = a^{\frac{p-1}{2}} \bmod p$

Πορισμα **:** Αν $p$ μονος πρωτος και $(a, p)=1$ και $a = b \bmod p$ τοτε $(\frac{a}{p}) = (\frac{b}{p})$

Πορισμα **:** Αν $p$ μονος πρωτος τοτε $(\frac{-1}{p}) = \{ +1, p = 1 \bmod 4$ η $-1, p = 3 \bmod 4$

Πορισμα **:** Αν $p$ μονος πρωτος και $p \dagger ab$ τοτε $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

**Θεωρημα(**Λημμα του Gauss**):** Αν $p$ μονος πρωτος και $(a, p)=1$ τοτε

$(\frac{a}{p}) = (-1)^s$ οπου $s$ το πληθος των στοιχειων του $\{a, 2a, 3a, ..., \frac{(p-1)}{2}a\}$ που είναι μεγαλυτερα του $\frac{p}{2}$.

Πορισμα **:** Αν $p$ μονος πρωτος τοτε $(\frac{2}{p}) = \{1$ αν $p = \pm 1 \bmod 8$, -1 αν $p = \pm 3 \bmod 8\}$

Πορισμα **:** Αν $p$ περιττος πρωτος τοτε $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

Νομος της Τετραγωνικης Αντιστρεπτοτητας (QRL)

Για περιττους $p, q$ εχω $(\frac{p}{q}) = \pm(\frac{q}{p})$

Θεωρημα(Νομος της Τετραγωνικης Αντιστρεπτοτητας του Gauss ) **:**
**Αν** $p \neq q$ μονοι πρωτοι τοτε $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$

## 3.4 Πρωταρχικες Ριζες

Εστω η ισοδυναμια $x^m = a \bmod p$, $p$ μονος πρωτος , $a > 2, (a, p) = 1$.Αν η ισοτιμια επιλυεται το $a$ είναι το $m$ ταξης υπολοιπο του $p$ .Εστω ο φυσικος $n$ με $(a, n) = 1$,και ο ελαχιστος φυσικος $k$ με $x^k = 1 \bmod n$ .Ο $k$ λεγεται ταξη του $a \bmod n$ και συμβολιζεται με $ord_n(a)$ .Απο το Θεωρημα του Euler εχουμε για κάθε φυσικο $n$ με $(a, n) = 1$ $a^{\phi(n)} = 1 \bmod n$ αρα η ταξη είναι καλα ορισμενη συναρτηση.

**Θεωρημα:** Αν $ord_n(a) = k$ τοτε $a^h = 1 \bmod n$ αν και μονο αν $k \mid h$ .

**Θεωρημα:** Αν $ord_n(a)=k$ τοτε $ord_n(a^m)=\frac{k}{\text{ΜΚΔ}(m,k)}$

Ονομαζουμε ένα φυσικο $q$ πρωταρχικη ριζα αν $ord_n(q)=\varphi(n)$

**Θεωρημα:** Αν ο $q$ είναι μια πρωταρχικη ριζα του $n$ τοτε τα $q,q^2,...,q^{\phi(n)}$ αποτελουν ένα περιορισμενο συνολο υπολοιπων $\bmod n$.

**Θεωρημα:** Αν ο $p$ μονος πρωτος , $h$ φυσικος και $q$ πρωτος τετοιος ώστε $q^h \mid p-1$ τοτε υπαρχει φυσικος $b$ με $ord_p(b)=q^h$

**Θεωρημα:** Δεν υπαρχουν πρωταρχικες ριζες του $2^n$ για $n>2$.

**Θεωρημα:** Αν $p$ μονος πρωτος τοτε υπαρχουν $\phi(p-1)$ πρωταρχικες ριζες $\bmod p$
Αν υπαρχει πρωταρχικη ριζα για τον (μη πρωτο) $m$ θα εχουμε $\varphi(\varphi(m))$ μη ισοδυναμες πρωταρχικες ριζες του $m$ .Αν $m=p$ πρωτος $\varphi(\varphi(p))=\phi(p-1)$

**Θεωρημα:** Μια αναγκαια συνθηκη για να επιλυεται η $x^m=a \bmod p$ με $d=\text{ΜΚΔ}(m,p-1)$ είναι $a^{\frac{p-1}{d}}=1 \bmod p$

## 3.5 Κρυπτολογια-Κρυπτογραφια-Κρυπταναλυση

Η επιστημη της κρυπτογραφιας εναι πολύ παλια και σκοπος της είναι η ασφαλης μεταφορα πληροφοριων μεταξυ του αποστολεα και του ληπτη ενός μυνηματος.Η επιθυμια να μεταφερουμε μηνυματα με χρηση μυστικων κωδικων σε μορφη που ο αναγνωστης να μην δυναται να αντιληφθει το νοημα τους εχει τις ριζες της στην αρχαιοτητα. Ο Ιουλιος Καισαρας χρησιμοποιουσε τη μυστικη γραφη με μεγαλη συχνοτητα.Ο Καισαρας χρησιμοποιουσε μια αντικατασταση που μετατοπιζε 3 θεσεις προς τα δεξια τα γραμματα του Λατινικου αλφαβητου οπου τα τρια τελευταια γινοντουσαν $A,B,C$.,
Η αντικατασταση του Καισαρα περιγραφεται με το μετασχηματισμο $C=p+3 \bmod 26$ οπου $p$ η αριθμητικη τιμη του γραμματος του απλου

κειμενου και $C$ η αντιστοιχη τιμη στο κρυπτογραφημενο κειμενο.Ο αντιστροφος μετασχηματισμος είναι ο
$p = C - 3 \bmod 26$ και γενικοτερα ο μετασχηματισμος $C = p + k \bmod 26, 0 \le k \le 25$ και ο αντιστροφος του $p = C - k \bmod 26$ αποτελουν το προσθετικο συστημα η συστημα αντικαταστασης του Καισαρα.Ο αριθμος $k$ που περιγραφει το μεγεθος της μετατοπισης λεγεται κλειδι.Το $k = 0$ δεν παρουσιαζει καποιο ενδιαφερον.

Η κρυπτολογια ασχολειται με την αναπτυξη των μεθοδων για την κρυπτογραφηση και αποκρυπτογραφηση μηνυματων.Μεσα στην κρυπτολογια διακρινονται δυο διαφορετικοι κλαδοι.Ο κλαδος της κρυπτογραφιας και της κρυπταναλυσης.Η κρυπτογραφια είναι η περιοχη της κρυπτολογιας που ενδιαφερεται και ασχολειται με την αναπτυξη και τη μελετη μεθοδων και μεθοδολογιων κρυπτογραφησης.Εδω κυριως καποιος χρησιμοποιει μυστικα κλειδια .Μονο αυτοι που εχουν το μυστικο κλειδι μπορουν να αποκρυπτογραφησουν την κρυπτογραφημενη πληροφορια.Η κρυπταναλυση είναι η περιοχη της κρυπτολογιας που επιδιωκει την αναπτυξη τεχνικων ετσι ώστε να αποκρυπτογραφει κρυπτογραφημενα μηνυματα χωρις την εκ των προτερων γνωση καποιων κλειδιων.

## 3.6 Συστηματα Κρυπτολογιας

### 1.Το προσθετικο συστημα

Ένα απλο παραδειγμα ενός μονοαλφαβητικου συστηματος αντικαταστασης είναι το επιλεγομενο προσθετικο.
Σε αυτό, ένα γραμμα του αρχικου αλφαβητου αντικαθισταται από ένα άλλο του οποιου η θεση στο λατινικο αλφαβητο απεχει καποιες μοναδες $\bmod 26$ από την αρχικη του θεση .Η σταθερη αποσταση ονομαζεται κλειδι.
Ο παραληπτης του μηνυματος γνωριζει το κλειδι οποτε όταν παραλαβει το κρυπτογραφημενο κειμενο θα το αποκρυπτογραφησει προσθετοντας τον προσθετικο αντιστροφο του κλειδιου στο $\mathbb{Z}_{26}$.

Θεωρημα:Εστω $p$ η θεση του γραμματος στο απλο κειμενο που κωδικοποιειται με ένα μονοαλφαβητικο προσθετικο συστημα με κλειδι $k$.Τοτε αν εφαρμοσουμε ένα προσθετικο συστημα με κλειδι $26-k$ στο κρυπτοκειμενο θα προκυψει παλι η θεση.

2.Πολλαπλασιαστικα Συστηματα

Στο συστημα αυτό μονοαλφαβητικης αντικαταστασης αντι να προσθεσουμε έναν αριθμο σε κάθε θεση του απλου κειμενου για να προκυπτει το κρυπτοκειμενο τωρα πολλαπλασιαζουμε την θεση με ένα σταθερο αριθμο(το κλειδι) $\bmod 26$.Η πολλαπλασιαστικη ομαδα $\mathbb{Z}_{26}$ είναι δακτυλιος και όχι σωμα αφου ο 26 δεν είναι πρωτος αρα καποια στοιχεια δεν εχουν πολλαπλασιαστικο αντιστροφο.

Θεωρημα.Εστω το μετρο $n$ (στην περιπτωση μας $n=26$) και το κλειδι $k$ με $\text{ΜΚΔ}(n,k)=1$ ητοι $n,k$ πρωτοι προς αλληλους .Τοτε τα $k \bmod n, 2k \bmod n, ..., nk \bmod n$ είναι όλα διαφορετικα.

Για να αποκρυπτογραφησουμε το κρυπτοκειμενο Μ πρεπει να εφαρμοσουμε το κλειδι $k^{-1}$ δηλαδη το πολλαπλασιαστικο αντιστροφο του $k$.Ο πολλαπλασιαστικος αντιστροφος του $k$ είναι ο ακεραιος $r$ με $rk = 1 \bmod 26$

3.Αφφινικα συστηματα

Προκειται για ένα συνδιασμο του προσθετικου και πολλαπλασιαστικου συστηματος που χρησιμοποιει δυο κλειδια εστω $s$ και $r$.Εστω $p$ η θεση καποιου γραμματος στο απλο κειμενο και $c$ η θεση του στο κρυπτοκειμενο.Το $c$ υπολογιζεται από την εξισωση $c = s(p+r) \bmod 26$.Σε ένα αφφινικο κειμενο πρωτα χρησιμοποιουμε ένα προσθετικο συστημα με κλειδι $r$ σ'ένα μηνυμα $m$ και λαμβανουμε ένα ενδιαμεσο κειμενο εστω $m'$ και ακολουθως εφαρμοζουμε στο $m'$ ένα πολλαπλασιαστικο συστημα με κλειδι $s$ για να παρουμε το κρυπτομηνυμα Μ.Η αντιστροφη διαδικασια προβλεπει να εφαρμοσουμε στο Μ το αντιστροφο κλειδι $s^{-1} \bmod 26$ για να παρουμε το

ενδιαμεσο κειμενο $m'$ και ακολουθως να του εφαρμοσουμε ένα προσθετο συστημα με κλειδι $-r \bmod 26$ ώστε να επιστρεψουμε στο $m$.

## 3.7 Κρυπτογραφηση Με Δημοσιο Κλειδι

Στην κρυπτογραφηση με δημοσιο κλειδι,το κλειδι είναι δημοσιευμενο σε εντυπα κοινης χρησης(τηλεφωνικοι καταλογοι,εφημεριδες) και οποιοσδηποτε μπορει να το δει.Ο αποστολεας του μηνυματος κρυπτογραφει το μηνυμα με το δημοσιο κλειδι.Ο δεκτης ο οποιος εχει κανει τη δημοσιευση του κλειδιου μπορει μονο να αποκωδικοποιησει το μηνυμα διοτι μονο αυτος εχει το καταλληλο αποκωδικοποιητικο κλειδι.
Το κρυπτογραφικο συστημα με δημοσιο κλειδι που θα περιγραψουμε βασιζεται στη γνωση της συναρτησης Euler $\varphi(m)$ του mod*ulom* για να υπολογισουμε το αντιστροφο κλειδι (δηλαδη να αποκρυπτογραφησουμε)
Για να υπολογισουμε την $\varphi(m)$ πρεπει να ξερουμε και τον $m$ και τους πρωτους παραγοντες του διοτι $\varphi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$
Πριν την κρυπτογραφηση το απλο κειμενο μετατρεπεται σ'ένα θετικο αριθμο Μ στο δεκαδικο η στο δυαδικο συστημα.
Εχουμε $1 < M < r$ οπου ΜΚΔ$(M,r)$=1 και $r$ το mod*ulo* της κρυπτογραφησης.Η κρυπτογραφηση εγκειται στο ότι υψωνουμε το μηνυμα Μ σε καποιο εκθετη $s$ και κραταμε μονο το υπολοιπο mod*ulor* οποτε το κρυπτογραφημενο κειμενο αναπαρισταται από τον αριθμο $E = M^s \bmod r$ με $1 < E < r$.Αν επιλεξουμε ένα πρωτο αριθμο για modulo η αποκρυπτογραφηση του Ε είναι απλη,δηλαδη είναι ευκολο να παρουμε το μυνημα Μ.

Επιλεγουμε σαν modulo κρυπτογραφησης $r$ έναν πολύ μεγαλο όχι πρωτο αριθμο αλλα της μορφης $r = pq$ που να εχει μονο δυο πρωτους παραγοντες επισης μεγαλους.Θα χρειαστουμε και έναν εκθετη κωδικοποιησης $s$ τετοιο ώστε
ΜΚΔ $(s, \varphi(r))$=1.Οποιος θελει να λαβει ένα μυστικο μηνυμα επιλεγει μια τριπλετα $p, q, s$ και δημοσιοποιει τον εκθετη κωδικοποιησης $s$ και το modulo κωδικοποιησης $r$.Οποτε οποιος εχει να στειλει ένα μηνυμα κατασκευαζει τον αριθμο που αντιστοιχει το μηνυμα Μ,υψωνει τον αριθμο αυτό στη δυναμη $s$ και παιρνει το αποτελεσμα $\bmod r$.

Ο δεκτης πρεπει να υπολογισει τον εκθετη αποκρυπτογραφησης που δινεται από τη λυση της ισοδυναμιας $ts \equiv 1 \bmod \varphi(r)$.Ομως αφου οι παραγοντες του $r$ είναι γνωστοι και η $\varphi(r)$ είναι γνωστη.

$$r = pq \Rightarrow \phi(r) = r(1-\frac{1}{p})(1-\frac{1}{q}) = (p-1)(q-1)$$

και επεται ότι $t \equiv s^{\varphi(\phi(r))-1} \bmod \varphi(r)$ ,διοτι αν πολλαπλασιασουμε επι $s$ $st \equiv s^{\varphi(\phi(r))} \bmod \varphi(r) \equiv 1 \bmod \varphi(r)$ από το θεωρημα Euler και το ότι ΜΚΔ$(s, \varphi(r)) = 1$.

Αφου υπολογισαμε ότι ο $t$ είναι ο καταλληλος και μοναδικος εκθετης αποκωδικοποιησης θα γινει όπως πριν.Το κρυπτογραφημενο μηνυμα είναι $E \equiv M^s (\bmod r)$ και αποκρυπτογραφοντας το εχουμε
$E^t \equiv M^{st} (\bmod r) = M^{\phi(r)k+1} (\bmod r) = M^{\phi(r)k} M (\bmod r) \equiv M (\bmod r)$
Διοτι από το θεωρημα Euler $M^{\phi(r)} - 1 = kr$ .Αρα $E^t = M (\bmod r)$

## 3.8 Το Προβλημα Διακριτου Λογαριθμου

### 3.8.1Ορισμος Προβληματος

Είναι ευκολο για καποιον να υπολογισει το $b^x$ για καποιο μεγαλο $x$ σε σχετικα μικρο χρονο.Δεν είναι ομως ευκολο αν μας δωσουν έναν αριθμο $y$ ,ο οποιος είναι της μορφης $b^x$ (το b είναι γνωστο) να υπολογισουμε το μοναδικο $x$ τετοιο ώστε $b^x = y$ .Δηλαδη δεν υπαρχει αποδοτικος αλγοριθμος που να υπολογιζει το $x = \log_b^y$ .Η επιλυση της παραπανω εξισωσης στο $\mathbb{Z}_p$ ,για $p$ πρωτο είναι το Προβλημα του Διακριτου Λογαριθμου και αν επιλεξουμε

καταλληλα το σωμα στο οποιο εργαζομαστε ,δηλαδη αν το $p$ εχει τουλαχιστον 150 ψηφια και το $p-1$ εχει τουλαχιστον ένα <<μεγαλο>> πρωτο παραγοντα τοτε η λυση είναι παρα πολύ χρονοβορα.

Ορισμος: Εστω $G$ μια πεπερασμενη κυκλικη ομαδα ταξης $n$, $g$ ενας γεννητορας της $G$ και $\beta \in G$.Ο Διακριτος Λογαριθμος του $\beta$ στη βαση $g$ ,που συμβολιζεται $\log_g^b$ ,είναι ο μοναδικος ακεραιος $x$, $0 \le x \le n-1$ με $\beta = g^x$

Ορισμος: Το Προβλημα Διακριτου Λογαριθμου(DLP) είναι το παρακατω :

Δινονται : Ενας πρωτος αριθμος $p$ ,ενας γεννητορας $g$ του $\mathbb{Z}_p^*$ και ένα στοιχειο $\beta$ του $\mathbb{Z}_p^*$.

Ζητειται : Να βρεθει ακεραιος $x$ , $0 \le x \le p-2$ ,τετοιος ώστε $g^x \equiv \beta \bmod p$.

Η δυσκολια του DLP είναι ανεξαρτητη από την επιλογη γεννητορα $g$ του $\mathbb{Z}_p^*$ και του $\beta$ του $\mathbb{Z}_p^*$.

## 3.9 Αλγοριθμοι Επιλυσης του DLP

Στην παραγραφο αυτή θα αναφερουμε τρεις αλγοριθμους για την ευρεση του Διακριτου Λογαριθμου.Για το σκοπο αυτό ο $p$ θα είναι πρωτος αριθμος και το $g$ πρωταρχικο στοιχειο $\bmod p$ ,δηλαδη $g^{p-1} \equiv 1 \bmod p$.Δουλευουμε στην κυκλικη πολλαπλασιαστικη ομαδα $\mathbb{Z}_p^*$ τοτε ο $g$ θα είναι και γεννητορας της.Επισης θεωρουμε τα $p$ και $g$ σταθερα.

Ετσι το DLP γινεται :

Δινεται : $\beta \in \mathbb{Z}_p^*$

Ζητειται :Να βρεθει $x$, $0 \le x \le p-2$ ,τετοιος ώστε $g^x \equiv \beta \bmod p$

Ενας προφανης αλγοριθμος για την επιλυση του παραπανω προβληματος είναι με την εξαντλιτικη μεθοδο αναζητησης στο $\mathbb{Z}_p^*$ ενός $x$ που να ικανοποιει την $g^x \equiv \beta \bmod p$

Ενας άλλος αλγοριθμος γγια την επιλυση του DLP είναι ο Αλγοριθμος του Shanks.Ο αλγοριθμος αυτος υπολογιζει εκ των προτερων όλα τα πιθανα $g^x$,και ταξινομοντας τα ζευγη $(x, g^x)$ βαση της δευτερης συντεταγμενης επιλυει το DLP.

### 3.9.1 Αλγοριθμος του Shanks

1. $m:[\sqrt{p-1}]$
2.Υπολογισε το $g^{mj} \bmod p$, $0 \le j \le m-1$
3.Ταξινομησε τα $m$ διατεταγμενα ζευγη $(j, g^{mj} \bmod p)$ βασει της δευτερης συντεταγμενης ώστε να προκυψει μια ταξινομημενη λιστα $L_1$.
4.Υπολογισε το $\beta g^{-i} \bmod p$, $0 \le i \le m-1$
5.Ταξινομησε τα $m$ διατεταγμενα ζευγη $(i, \beta g^{-i} \bmod p)$ βασει της δευτερης συντεταγμενης ώστε να προκυψει μια ταξινομημενη λιστα $L_2$.
6.Αναζητησε ζευγος $(j, y) \in L_1$ τετοιο ώστε $(i, y) \in L_2$,δηλαδη δυο ζευγη που να εχουν την ιδια τεταγμενη.
7. $(\log_g^\beta =) x := mj + i \bmod(p-1)$

Πραγματι αν $(j, y) \in L_1$ και $(i, y) \in L_2$ τοτε $g^{mj} = y = \beta g^{-i}$
Επομενως $g^{mj+i} = \beta \Rightarrow g^x = \beta \Rightarrow x = \log_g^\beta$

Ο αλγοριθμος επιλυσης του DLP του Shanks δουλευει για πρωτους μεχρι και λιγο πανω από 20 ψηφια.

### 3.9.2 Ο αλγοριθμος των Pohlig-Hellman

Ο αλγοριθμος των Pohlig-Hellman δουλευει για σημαντικα μεγαλυτερους αριθμους $p$,αν όμως ο $p-1$ εχει μονο μικρους πρωτους παραγοντες .Αυτο είναι σημαντικο μειονεκτημα.Ο αλγοριθμος στηριζεται στην παρακατω ιδεα:

Εστω $g$ μια πρωταρχικη ριζα $\bmod p$ ετσι ώστε ο $p-1$ να είναι ο μικροτερος θετικος $n$ με $g^n = 1 \bmod p$ .Αυτο σημαινει ότι
$g^{m_1} = g^{m_2} \bmod p \Leftrightarrow m_1 = m_2 \bmod p-1$.

Εστω λοιπον $\beta = g^x \quad 0 \le x \le p-1$.Θελουμε να υπολογισουμε τον $x$ δηλαδη να επιλυσουμε το DLP.Πραγματι $g^{p-1} = g^{(\frac{p-1}{2})^2} = 1 \bmod p$ .Αρα $g^{\frac{p-1}{2}} = \pm 1 \bmod p$ και αφου ο $p-1$ είναι ο μικροτερος εκθετης με $g^n = 1 \bmod p \Rightarrow g^{\frac{p-1}{2}} = -1 \bmod p$ .Η σχεση $\beta = g^x$ δινει αν την υψωσω στην δυναμη $\frac{p-1}{2}$

$$\beta^{\frac{p-1}{2}} = g^{x\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^x = (-1)^x \bmod p$$

Αρα $\beta^{\frac{p-1}{2}} = +1$ αν $x$ ζυγος

$\beta^{\frac{p-1}{2}} = -1$ αν $x$ μονος

Εστω λοιπον $p-1 = \prod_i q_i^{r_i}$ και εστω $q^r$ ενας από τους πρωτους παραγοντες .Θα επιλυσουμε το DLP $\bmod q^r$ .Αν αυτό γινεται για όλα τα $q_i^{r_i}$ οι απαντησεις θα συνενωθουν σε μια και θα υπολογισουμε το DLP $\bmod p$ .Γραφω $x = x_0 + x_1 q + x_2 q^2 + \ldots$ με $0 \le x_i \le p-1$ και θα υπολογισω τους συντελεστες $x_i$ οποτε και τον $x$.

Παρατηρουμε ότι $x(\frac{p-1}{q}) = x_0(\frac{p-1}{q}) + (p-1)(x_1 + x_2 q + x_3 q^2 + \ldots)$ ητοι

$x_0(\frac{p-1}{q}) + (p-1)n$ οπου $n$ ακεραιος .

Υψωνουμε την $\beta = g^x$ στον ακεραιο $\frac{p-1}{q}$ οποτε

$$\beta^{\frac{p-1}{q}} = g^{x\frac{p-1}{q}} = g^{x_0\frac{p-1}{q}} (g^{p-1})^n = g^{\frac{x_0(p-1)}{q}} 1 \bmod p$$

Αρα για να βρω το $x_0$ εξεταζω τις δυναμεις $g^{\frac{k(p-1)}{q}}$ , $k = 0,1,\ldots q-1$ ,εως οτου μια από αυτές δωσει τον $\beta^{\frac{(p-1)}{q}}$ .Τοτε $x_0 = k$ .

Επεκτεινουμε την ιδεα και σε μεγαλυτερες δυναμεις .Εστω ότι $q^2 \mid p-1$.Θετουμε $\beta_1 = \beta g^{-x_0} = g^{x-x_0}$ και κανουμε την ιδια διαδικασια με παραπανω.

Επαναλαμβανουμε την διαδικασια για ολους τους πρωτους παραγοντες $q_i^{r_i}$ (για όλα τα $i$)

Αλγοριθμος των Pohlig-Hellman

1. $p-1=\prod_i q_i^{r_i}$

2.Για κάθε $i$ επιλυω την εξισωση $\beta = g^x \bmod q^r$

3.Θεωρω $x = x_0 + x_1 q + x_2 q^2 + ... + x_{r-1} q^{r-1}$

4.Βρισκω $k$ τετοιο ώστε $\beta^{\frac{p-1}{q}} = g^{\frac{k(p-1)}{q}} \bmod p$ και θετω $x_0 = k$

5.Για $j=1$ εως $r-1$

6.Θετω $\beta_j = \beta_{j-1} g^{-x_{j-1} q^{j-1}} \bmod p$ (με $\beta_0 = \beta$)

7.Βρισκω $k$ τετοιο ώστε $\beta_j^{\frac{p-1}{q^{j+1}}} = g^{\frac{k(p-1)}{q}} \bmod p$ και θετω $x_j = k$

8.Ενωνω τις ισοδυναμιες και βρισκω τη λυση $x$.

3.9.3 Αλγοριθμος Index Calculus

Για την πολλαπλασιαστικη ομαδα $\mathbb{Z}_p$ υπαρχουν αρκετα ικανοποιητικοι αλγοριθμοι για το DLP οι αλγοριθμοι Index Calculus.

Εστω πρωτος $p$ ,η πρωταρχικη ριζα $g \bmod p$ και $a \in \{1,2,...,p-1\}$.Θελουμε να λυσουμε το DLP ητοι να υπολογισουμε τον $x$ αν $g^x = a \bmod p$.

Index Calculus

1.Επιλεγουμε ένα φραγμα B και υπολογιζουμε το συνολο $F(B) = \{q \text{ πρωτος,q} \le \text{B}\}$ ,δηλαδη τη βαση πρωτων παραγωντων μας.Ο β κατά τα γνωστα είναι β-λειος αν εχει πρωτους παραγοντες μονο στην $F(B)$.

2.Υπολογιζω τον διακριτο λογαριθμο των στοιχειων της $F(B)$ δηλαδη λυνω την εξισωση $g^{x(q)} = q \bmod p, \forall q \in F(B)$
3.Υπολογιζω έναν εκθετη $y \in \{1,2,...,p-1\}$ τετοιον ώστε $ag^y$ να είναι Β-λειος.Εχουμε λοιπον $ag^y = \prod_{q \in F(B)} q^{e(q)}$ οπου $e(q)$ μη αρνητικοι εκθετες , $q \in F(B)$.

Οποτε $ag^y = \prod_{q \in F(B)} q^{e(q)} = \prod_{q \in F(B)} g^{x(q)e(q)} = g^{\sum_{q \in F(B)} x(q)e(q)} \bmod p$ ητοι

$g^x = a = g^{\sum_{q \in F(B)} x(q)e(q)-y} \bmod p$

Η σχεση $a^{m_1} = a^{m_2} \Leftrightarrow m_1 = m_2 \bmod(p-1)$ μας δινει

$x = (\sum_{q \in F(B)} x(q)e(q) - y) \bmod(p-1)$

Δηλαδη τον διακριτο λογαριθμο που θελαμε.

## 3.10 Το Κρυπτοσυστημα Massey-Omura

Ένα λιγοτερο γνωστο κρυπτοσυστημα που στηριζεται στο DLP εισηχθη από τους J.L.Massey και J.Omura.Στο κρυπτοσυστημα αυτό δεν υπαρχει δημοσιο κλειδι για τις δυο πλευρες που επικοινωνουν,δεν είναι όμως συμμετρικο και η επικοινωνια γινεται δημοσια .Παρακατω περιγραφεται η διαδικασια που πρεπει να ακολουθησουν ο Α και ο Β για να επικοινωνησουν με ασφαλεια,χρησιμοποιωντας το Κρυπτοσυστημα Massey-Omura.

**Επιλογη των κλειδιων για το κρυπτοσυστημα Massey-Omura**

1.Αρχικα επιλεγεται καταλληλα ένα πεπερασμενο σωμα $\mathbb{Z}_q$

2.Στη συνεχεια και οι δυο πλευρες επιλεγουν από ένα κρυφο ακεραιο $e$, $e \in [0, q-1]$,τετοιο ώστε ΜΚΔ $(e, q-1) = 1$και υπολογιζουν τον αντιστροφο του $d = e^{-1} \bmod(q-1)$.Εστω ότι $(e_A, d_A)$ οι επιλογες του Α και $(e_B, d_B)$ οι επιλογες του Β.

Υποθετουμε ότι ο Α θελει να στειλει στον Β το κειμενο $m$ κρυπτογραφημενο με το Massey-Omura.Η διαδικασια που ακολουθει είναι η παρακατω

**Ανταλλαγη Μηνυματος με το κρυπτοσυστημα Massey-Omura**

**1.**Ο Α υπολογιζει το $m_A = m^{e_A}$ και το στελνει στον Β.
2.Ο Β λαμβανει το $m_A$,υπολογιζει το $m_{AB} = (m_A)^{e_B} = m^{e_A e_B}$ και το στελνει στην Α.
3.Ο Α λαμβανει το $m_{AB}$ και αφαιρει από αυτό τον εκθετη $e_A$ υψωνοντας το στη δυναμη $d_A$.Δηλαδη υπολογιζει το $m_B = (m_{AB})^{d_a} = m^{e_B}$ και το στελνει στο Β.
4.Ο Β ανακτα το $m$ από το $m_B$ υπολογιζοντας το $m = (m_B)^{d_B}$.

3.11 Ελλειπτικες Καμπυλες πανω από σωμα

Εστω $\mathbb{F}$ ένα σωμα.Το σωμα αυτό θα είναι ειτε το $\mathbb{R}$,ειτε το πεπερασμενο σωμα $q$ στοιχειων $GF(q)$ ,οπου $q = p^r$ και $p$ πρωτος.

Ορισμος:Έστω το σωμα $\mathbb{F}$ με χαρακτηριστικη διαφορη του 2 και του 3 και εστω $x^3 + ax + b$,με $a, b \in \mathbb{F}$,ένα πολυωνυμο τριτου βαθμου χωρις πολλαπλες

ριζες.Τοτε μια ελλειπτικη καμπυλη πανω από το $\mathbb{F}$ είναι το συνολο των στοιχειων $(x, y)$ με $x, y \in \mathbb{F}$,τα οποια ικανοποιουν την εξισωση $y^2 = x^3 + ax + b$ μαζι με ένα στοιχειο Ο,το οποιο ονομαζουμε <<σημειο στο απειρο>>.

Αν το $\mathbb{F}$ είναι ένα σωμα χαρακτηριστικης 2,τοτε μια ελλειπτικη καμπυλη πανω από το $\mathbb{F}$ είναι το συνολο σημειων ,τα οποια ικανοποιουν ειτε μια εξισωση της μορφης

$$y^2 + cy = x^3 + ax + b \, , a, b, c \in \mathbb{F}$$

Ειτε μια εξισωση της μορφης

$$y^2 + xy = x^3 + ax + b \, , a, b, c \in \mathbb{F}$$

Μαζι με ένα <<σημειο στο απειρο>> Ο.
Αν το $\mathbb{F}$ είναι ένα σωμα χαρακτηριστικης 3,τοτε μια ελλειπτικη καμπυλη πανω από το $\mathbb{F}$ είναι το συνολο σημειων ,τα οποια ικανοποιουν μια εξισωση της μορφης

$$y^2 = x^3 + ax^2 + bx + c \, , a, b, c \in \mathbb{F}$$

## 3.12 Ελλειπτικες Καμπυλες πανω από το $\mathbb{R}$

Η βασικη ιδιοτητα των ελλειπτικων καμπυλων που τις κανει πολυτιμα κρυπτογραφικα εργαλεια είναι πως μας δινουν με φυσικο τροπο αβελιανες ομαδες με δομη τετοια ώστε το DLP να είναι υπολογιστικα δυσκολο.Πιο συγκεκριμενα ,το συνολο των σημειων μιας ελλειπτικης καμπυλης ε εφοδιασμενο με μια πραξη προσθεσης αποτελει αβελιανη ομαδα,την οποια θα συμβολιζουμε $G(\varepsilon)$.

Ορισμος:Εστω ε μια ελλειπτικη καμπυλη πανω από το $\mathbb{R}$ ,και εστω $P, Q$ δυο σημεια πανω στην ε.Τοτε οριζουμε το $-P$ (αντιθετο του $P$ ) και το αθροισμα $P + Q$ ως ακολουθως:

1)Αν $P = 0$ ,τοτε οριζουμε $-P = 0$ και $P + Q = Q$ ,δηλαδη το Ο είναι το ουδετερο στοιχειο της ομαδας των στοιχειων της καμπυλης .Στα παρακατω θεωρουμε $P \neq Q \neq O$

2)Το $-P$ είναι το σημειο με την ιδια τετμημενη και αντιθετη τεταγμενη από το $P$ .Απο τον ορισμο της ελλειπτικης καμπυλης είναι προφανες πως το $(x,-y)$ ανηκει στην καμπυλη αν και μονο αν το $(x,y)$ ανηκει στην καμπυλη.

3)Αν τα $P,Q$ εχουν διαφορετικες τετμημενες,τοτε είναι σχετικα ευκολο να παρατηρησουμε ότι η ευθεια $l=PQ$ τεμνει την καμπυλη ακριβως σε ένα ακομα σημειο $R$.

4)Αν $Q=-P$,τοτε οριζουμε $P+Q=O$
5)Τελος,αν $P=Q$,η εφαπτομενη στο $P$ θα τεμνει την καμπυλη ακριβως σε ένα ακομα σημειο $R$(εκτος εάν το $P$ είναι σημειο καμπης ,οποτε παιρνουμε $R=P$).Οριζουμε τοτε $P+Q=-R$

Εστω $(x_1,y_1),(x_2,y_2)$ οι συντεταγμενες των σημειων $P$ και $Q$ αντιστοιχα ,τα οποια ανηκουν στην ελλειπτικη καμπυλη $\varepsilon : y^2=x^3+ax+b$ και $(x_3,y_3)$ οι συντεταγμενες του $P+Q$.
Εστω $y=\beta x+\gamma$ η εξισωση της ευθειας $l$ που διερχεται από τα $P$ και $Q$.Τοτε $\beta=(y_2-y_1)/(x_2-x_1)$ και $\gamma=y_1-\beta x_1$.
Ενα σημειο της $l$ βρισκεται πανω στην ε αν και μονο αν $(\beta x+\gamma)^2=x^3+ax+b$,υπαρχει δηλαδη ένα σημειο τομης για κάθε ριζα της κυβικης εξισωσης .Με πραξεις βρισκουμαι τις συντεταγμενες $(x_3,y_3)$.

## 3.13 Ελλειπτικες καμπυλες πανω από το $GF(q)$

Πανω στο πεπερασμενο σωμα $GF(q)$,οπου $q=p^r$ και $p$ πρωτος,οριζουμε μια ελλειπτικη καμπυλη ε.Μια ελλειπτικη καμπυλη μπορει να εχει το πολύ $2q+1$ σημεια,το σημειο Ο μαζι με $2q$ ζευγη $(x,y),x,y\in GF(q)$ που ικανοποιουν την $y^2=x^3+ax+b$.Αυτο συμβαινει επειδη για κάθε ένα από τα $q$ πιθανα $x$ υπαρχουν το πολύ δυο $y$ ώστε να ικανοποιειται η εξισωση της καμπυλης.Καθως μονο τα μισα εχουν τετραγωνικη ριζα ,είναι φυσικο να περιμενουμε ότι υπαρχουν περιπου τα μισα από αυτά τα $2q+1$ σημεια στη καμπυλη.

**Θεωρημα:** Εστω $\#\varepsilon$ το πληθος των σημειων της ελλειπτικης καμπυλης $\varepsilon$ ορισμενης πανω από το $GF(q)$.Τοτε ισχυει

$$p+1-2\sqrt{p} \le \#\varepsilon \le p+1+2\sqrt{p}$$

**Ορισμος : Το Προβλημα Διακριτου Λογαριθμου στις Ελλειπτικες Καμπυλες είναι το παρακατω**

**Δινονται :** Μια ελλειπτικη καμπυλη $\varepsilon$ ορισμενη πανω από το $GF(q)$,ένα σημειο της Β(η βαση του διακριτου λογαριθμου) και ένα σημειο της $P$.

**Ζητειται :** Να βρεθει αν υπαρχει ,ακεραιος $x$ τετοιος ώστε $xB = P$

**Κρυπτοσυστημα Massey-Omura**

Ο αποστολεα του μηνυματος και ο δεκτης επιλεγουν δημοσια ένα πεπερασμενο σωμα $GF(q)$(με το $q$ μεγαλο) και μια ελλειπτικη καμπυλη ε ορισμενη πανω στο $GF(q)$ και υπολογιζουν δημοσια το $\#\varepsilon$.Κωδικοποιουμε το συνολο των απλων μηνυματων Μ με σημεια της καμπυλης ,αντιστοιχωντας το μυνημα $m$ στο σημειο $P_m$.
Ο Α επιλεγει ένα ακεραιο $e_A$ μεταξυ του 1 και του $\#\varepsilon$ ,τετοιο ώστε ΜΚΔ$(e_A, \#\varepsilon) = 1$ και χρησιμοποιωντας τον Ευκλειδιο αλγοριθμο υπολογιζει το $d_A \equiv e_A^{-1} \bmod \#\varepsilon$.Το ιδιο κανει και ο Β επιλεγοντας ένα $e_B$ και υπολογιζοντας το $d_B$.Τα $e_A, e_B, d_A, d_B$ κρατιουνται μυστικα.
Για να στειλει ο Α το μηνυμα $P_m$ στο Β του στελνει το $e_A P_m$.Ο Β υπολογιζει το $e_B e_A P_m$ και το στελνει πισω στον Α.Ο Α πολλαπλασιαζοντας με $d_A$ υπολογιζει το $d_A e_B e_A P_m = e_B P_m$ και το στελνει στο Β που πλεον μπορει να διαβασει το μηνυμα $P_m$ πολλαπλασιαζοντας με $d_B$.

3.14 Παραδειγμα

Εστω ότι ο Α.Σ θελει να στειλει στο Α.Π το εξης μηνυμα

**venios is retired(ο βενιος πηρε συνταξη)**

Η κρυπτογραφηση θα γινει με τρεις τροπους
1)RSA
2)Με κρυπτοσυστημα Massey Omura
3)Με χρηση ελλειπτικων καμπυλων

1)Με χρηση RSA

Το κειμενο **venios is retired**

Αρχικα κωδικοποιουμε το αλφαβητο ως εξης

Διαστημα **:** 00
A**:**01
B**:02**
C**:03**
D**:**04
E**:05**
F**:06**
G**:07**
H**:08**
I**:09**
J**:10**
K**:11**
L**:12**
M**:13**
N**:14**
O**:15**

P**:16**
Q**:17**
R**:18**
S**:19**
T**:20**
U**:21**
V**:22**
W**:23**
**X:24**
Y**:25**
Z**:26**

Το μηνυμα κωδικοποιειται και χωριζεται σε τετραδες

2205 1409 1519 0009 1900 1805 2001 1805 0400

Ο Α.Π ο οποιος θελει να λαμβανει συχνα μυστικα μηνυματα εχει ορισει ως δημοσιο κλειδι τον εκθετη s=23 και σαν $\mathrm{mod}ulor$ r =4891 κρυπτογραφησης που εχει μονο δυο πρωτους παραγοντες τους $p = 67$ και $q = 73$ και $\phi(r) = (p-1)(q-1) = 4752$.Ο εκθετης κωδικοποιησης $s$ οριστηκε με τετοιο τροπο ώστε $\mathrm{ΜΚΔ}(s, \varphi(r)) = 1$

Τα μπλοκ του μηνυματος κωδικοποιουνται σαν

$C_1 = 2205^{23} \bmod 4891$
$C_2 = 1409^{23} \bmod 4891$
$C_3 = 1519^{23} \bmod 4891$
$C_4 = 9^{23} \bmod 4891$
$C_5 = 1900^{23} \bmod 4891$
$C_6 = 1805^{23} \bmod 4891$
$C_7 = 2001^{23} \bmod 4891$
$C_8 = 1805^{23} \bmod 4891$
$C_9 = 4^{23} \bmod 4891$

Η αποκωδικοποιηση γινεται ως εξης.Υπολογιζουμε τον εκθετη αποκωδικοποιησης $t$ από τη σχεση $st = 1 \bmod (p-1)(q-1)$

2)Με χρηση του κρυπτοσυστηματος Massey Omura

Επιλεγουμε ένα σωμα, εστω το $\mathbb{Z}_{73}$
Οι δυο πλευρες επιλεγουν από έναν τυχαιο κρυφο ακεραιο $e$.
$e_1 \in [0,72]$ και $e_2 \in [0,72]$ τετοια ωστε $(e_1,72)=1$ και $(e_2,72)=1$.Διαλεγουμε δυο δυδιμους πρωτους τους 11,13 ως $e_1, e_2$ αντιστοιχα και υπολογιζουμε τον αντιστροφο τους $d_1 = e_1^{-1} \bmod 72$ και $d_2 = e_2^{-1} \bmod 72$.Ετσι ο Α.Σ εχει τα. $(e_1, d_1)$ και ο Α.Π τα $(e_2 d_2)$ .Το κειμενο κωδικοποιειται και χωριζεται σε δυαδες .
Ο Α.Σ υπολογιζει το $m_A = m^{e_A}$ και το στελνει στον Α.Π. Ο Α.Π λαμβανει το $m_A$,υπολογιζει το $m_{AB} = (m_A)^{e_B} = m^{e_A e_B}$ και το στελνει στον Α.Σ. Ο Α.Σ λαμβανει το $m_{AB}$ και αφαιρει από αυτό τον εκθετη $e_A$ υψωνοντας το στη δυναμη $d_A$.Δηλαδη υπολογιζει το $m_B = (m_{AB})^{d_a} = m^{e_B}$ και το στελνει στο Α.Π. Ο Α.Π ανακτα το $m$ από το $m_B$ υπολογιζοντας το $m = (m_B)^{d_B}$.

Βιβλιογραφια

1.R.E Johnson,University Algebra
2.S.Lang ,Algebra
3.John B.Fraleigh, Algebra
4.Α.ΦελλουρηςΓραμμικη Αλγεβρα και Αναλυτικη Γεωμετρια
5.Χ.Κουκουβινος-Α.Παπαιωαννου,Κρυπτογραφια