SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Enhetsgrupper modulo m

av

Emil Pagrot

2021 - No K30

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Enhetsgrupper modulo m

Emil Pagrot

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Håkan Granath

2021

Multiplicative groups of integers modulo m

Emil Pagrot

Abstract

The multiplicative group of integers modulo m is the group of units in the ring $\mathbb{Z}_m$ and it is an important group in number theory. This paper uses elementary algebra to study and describe the unit group modulo m. Factorizations and properties of Euler's ϕ-function is used together with group and ring theory to describe an algoritm to reduce unit groups to direct products of cyclic groups. This paper therefore proves a result first presented by Gauss in the 19th century that describes for which integers m the unit group is cyclic. Finally this paper present some applications of unit groups modulo m in cryptology.

Sammanfattning

Enhetsgruppen modulo m är gruppen av enheter i ringen $\mathbb{Z}_m$ och är en viktig grupp inom talteori. Arbetet använder abstrakt algebra för att beskriva enhetsgruppen modulo m. Faktoriseringar av och egenskaper hos Eulers ϕ-funktion används tillsammans med grupp- och ringteori för att beskriva en algoritm som reducerar enhetsgrupper modulo m till en kartesisk produkt av cykliska grupper. Arbetet bevisar därmed ett resultat som först presenterades av Gauss under 1800-talet och som förklarar för vilka heltal m som enhetsgruppen modulo m är cyklisk. Avslutningsvis så presenteras några tillämpningar av enhetsgruppen modulo m i kryptologi.

Innehåll

1 Introduktion

Talteori studerar heltal och är idag ett betydelsefullt matematiskt ämnesområde med många kopplingar till andra matematiska ämnesområden. I arbetet använder vi till exempel kopplingar mellan gruppteori och talteori för att beskriva enhetsgruppen modulo m. Talteori återfinns idag inom bland annat kryptografi, numerisk analys och datavetenskap men delområdet är en gammal matematisk gren med kopplingar till både forntidens Babylonien och antikens Grekland [17]. Till exempel har en lertavla med lösningar till den diofantiska ekvationen $x^2 + y^2 = z^2$ spårats till forntidens Babylonien och daterats till cirka 1800 år f.kr.[17]. Talteorin som matematisk inriktning kan däremot härledas till Euklides från Alexandra och samlingsverket *Elementa* från cirka 300 år f.kr.[9]. *Elementa* av Euklides behandlar flera olika ämnen däribland heltal och talteori. Euklides algoritm som är en av historiens äldsta algoritmer presenteras i *Elementa* och är ett exempel på tidig talteori eftersom algoritmen beskriver en metod för att beräkna den största gemensamma delaren av två tal. Ett annat exempel på tidig talteori är den Kinesiska restsatsen som kan härledas till matematikern Sun Zi och 300-talets Kina [1]. Satsen som formulerades i sin helhet av Qin Jiushao 1247 e.kr. beskriver förutsättningar för heltalslösningar till ett särskilt ekvationssystem och en metod för att hitta lösningar till ekvationssystemet [1]. Euklides algoritm och den Kinesiska restsatsen är centrala resultat inom talteori och två bra exempel på tidig modulär aritmetik.

I Kontinentaleuropa hittar vi exempel på problem med resträkning först under medeltiden [3]. I boken Liber Abaci från 1202 så löser Leonardo Fibonacci flera problem med resträkning [3]. Fibonacci använder till exempel restklasser för att gissa okända tal och flera av Fibonaccis exempel är specialfall av den Kinesiska restsatsen [3]. Liber Abaci är ett bra exempel på tidens modulära aritmetik i Europa eftersom modulär aritmetik innan 1800-tal förekommer som restproblem i olika matematiska delområden. Tidens modulära aritmetik är fragmenterad i matematisk litteratur eftersom restproblem förekommer sporadiskt i litteratur om till exempel aritmetik och algebra [3].

Vi går nu framåt i tiden och ser att Carl Friedrich Gauss med boken *Disquisitiones Arthimeticae* från 1801 markerar en övergång från tidig till modern modulär aritmetik [9]. Gauss använder i *Disquisitiones Arthimeticae* både originella resultat och resultat från matematiker som Fermat, Euler och Lagrange för att behandla talteori och introducera en ny modulär aritmetik [13]. Boken är av stor betydelse för modulär aritmetik eftersom Gauss med boken etablerar och systematiserar forskningsfältet samt introducerar termen kongruenser för att hantera gamla problem av resträkning [3]. Gauss förändrar med definitioner av kongruenser och restklasser förståelsen av rester [10]. I boken så presenterar Gauss också viktiga

resultat om enhetsgruppen modulo m som är intressanta för detta arbete. Vi kommer särskilt att bevisa ett resultat som härleds till Gauss och beskriver för vilka m enhetsgruppen modulo m är cyklisk.

Arbetet fokuserar på enhetsgruppen modulo m. Vi ämnar med arbetet beskriva enhetsgruppen modulo m som är en viktig grupp inom talteori och modulär aritmetik. Gruppen har idag flera tillämpningar och används framförallt inom kryptering. Vi kommer i arbetet beskriva gruppens struktur och användningsområden. Vi definierar nu enhetsgruppen modulo m och återkommer till definitionen i senare kapitel för att beskriva gruppens egenskaper.

Definition 1.1. Enhetsgruppen modulo m är mängden av alla element i $\{0, 1, 2, \ldots, m-1\}$ som är relativt prima med m, under gruppoperationen multiplikation modulo m. Vi skriver $\mathbb{Z}_m^*$ för enhetsgruppen modulo m.

Vi kommer i arbetet använda Eulers ϕ-funktion, elementär algebra och ett resultat från Gauss för att reducera enhetsgruppen modulo m till en produkt av cykliska grupper. Gauss visade att $\mathbb{Z}_m^*$ är cyklisk om och endast om $m = 2, 4, p^n$ och $2p^n$ för något udda primtal p och positivt heltal n. Vi kommer bevisa och använda Gauss resultat för att beskriva strukturen av $\mathbb{Z}_m^*$. Vi kommer i arbetet också komma fram till en användbar algoritm för att entydigt bestämma gruppstrukturen av $\mathbb{Z}_m^*$ för godtyckliga m.

Vi utgår i arbetet från Shanks framställning av enhetsgruppen modulo m i *Solved and Unsolved Problems in Number Theory* från 1978 [10, s. 55–120]. Vi använder framförallt en särskild faktorisering från Shanks för att entydigt reducera $\mathbb{Z}_m^*$ till en produkt av cykliska grupper. Vi använder däremot en annan ansats än Shanks för att bevisa för vilka m gruppen $\mathbb{Z}_m^*$ är cyklisk. Vi använder istället litteratur om elementär algebra tillsammans med egna bevis för att bevisa för vilka m gruppen $\mathbb{Z}_m^*$ är cyklisk. Vi refererar löpande till använd litteratur.

2 Algebraisk bakgrund

Vi går i Kapitel 2 igenom den algebra som vi kommer behöva. Vi börjar kapitlet med att beskriva Eulers ϕ-funktion för att sedan gå vidare till att beskriva valda delar av elementär algebra. Vi behandlar och definierar i Kapitel 2 bland annat grupper, delgrupper, sidoklasser, ordningen av en grupp, ordningen av ett element, ringar, kroppar och isomorfier.

2.1 Eulers ϕ-funktion

Vi börjar med att definiera och beskriva funktionen $\phi(m)$ som vi behöver för att beskriva enhetsgruppen modulo m. Funktionen $\phi(m)$ tillskrivs Leonhard Euler och är en viktig funktion inom talteorin [2].

Definition 2.1. För alla positiva heltal m så definierar vi Eulers ϕ-funktion, $\phi(m)$, som antalet positiva heltal mindre än eller lika med m som är relativt prima med m.

Vi kan använda definitionen direkt för att beräkna $\phi(m)$ för små m och vi ser till exempel att $\phi(7) = 6$ eftersom 7 är relativt prima med $1, 2, 3, 4, 5$ och 6. För att beräkna $\phi(m)$ för en primtalspotens m kan vi använda nedanstående sats.

Sats 2.2. *Om p är ett primtal och a är ett positivt heltal så är*

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a(1-1/p). \tag{2.3}$$

Bevis. Låt b vara ett naturligt tal som är mindre än p^a. Vi räknar nu alla b som inte är relativt prima med p^a. Vi ser att p^a och b inte är relativt prima om och endast om $b = 0, p, 2p, 3p, \ldots, (p^{a-1}-2)p, (p^{a-1}-1)p$. Vi ser att antalet b som inte är relativt prima med p^a är lika med antalet multipler av p som är mindre än p^a. Vi räknar talen och får att det finns p^{a-1} tal b som inte är relativt prima med p^a. Vi ser därför att antalet naturliga tal mindre än p^a som är relativt prima med p^a är lika med $p^a - p^{a-1}$. □

Vi noterar särskilt att $\phi(p) = p-1$ om p är ett primtal. Vi studerar nu en egenskap för $\phi(m)$ som vi kan använda för att beräkna $\phi(m)$ för ett sammansatt tal m.

Sats 2.4. *Om två positiva heltal m och n är relativt prima så är $\phi(mn) = \phi(m)\phi(n)$.*

Bevis. Vi använder ett bevis från en videoföreläsning av Michael Penn för att bevisa funktionens multiplikativa egenskap [8].

För att visa att funktionen $\phi(a)$ är multiplikativ för ett positivt heltal $a = mn$ så skapar vi en tabell av alla positiva heltal mindre eller lika med a. Vi skapar en tabell med m rader och n kolumner så att:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \ldots & (n-1)m+3 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
m & m+m & 2m+m & \ldots & (n-1)m+m
\end{array}$$

Vi ser att alla tal i en rad r tillhör samma restklass modulo m eftersom resten för alla tal i en rad r vid division med m blir r. Vi ser till exempel att resten vid division med m blir 3 för alla tal i rad 3. Vi ser också att resten vid division med m för alla tal i rad m blir 0.

Vi noterar nu att $\text{SGD}(k_1m+r,m) = \text{SGD}(k_2m+r,m) = \text{SGD}(r,m)$ om k_1m+r och k_2m+r motsvarar två tal i en rad r för två heltal k_1 och k_2. Vi får att $\text{SGD}(k_im+r,m) = \text{SGD}(r,m)$ för alla tal k_im+r i en rad r. Vi ser således att $\phi(m)$ motsvarar antalet rader i tabellen som består av tal vilka alla är relativt prima med m.

Vi undersöker nu för vilka k_1 och k_2 som två tal k_1m+r och k_2m+r är kongruenta modulo n. Vi har att $(k_1m+r)-(k_2m+r) = (k_1-k_2)m$ och ser att $n \mid (k_1-k_2)m$ om och endast om $n \mid (k_1-k_2)$ eftersom m och n är relativt prima. Vi har vidare att $n \mid (k_1-k_2)$ om och endast om $k_1 = k_2$ eftersom $0 \leq k_1, k_2 < n$. Vi får att $k_1m+r \equiv k_2m+r \pmod{n}$ om och endast om $k_1 = k_2$. Vi får att varje rad innehåller exakt $\phi(n)$ tal som är relativt prima med n eftersom det finns n tal i varje rad och inga två tal i en rad är kongruenta modulo n.

Vi har att $\phi(m)$ motsvarar antalet rader av tal relativt prima med m och att $\phi(n)$ motsvarar antalet tal relativt prima med n i varje rad. Vi får att $\phi(m)\phi(n)$ motsvarar antalet tal mindre än $m \cdot n$ som är relativt prima med m och n. Vi ser nu att $\phi(mn) = \phi(m)\phi(n)$ eftersom $\phi(mn)$ är antalet tal relativt prima med m och n som är mindre än mn. □

Vi använder nu att $\phi(m)$ är multiplikativ för att utveckla beskrivningen av $\phi(m)$ för något positivt heltal m.

Sats 2.5. *Om ett positivt heltal m primtalsfaktoriseras i r antal primtalspotenser $p_i^{a_i}$ så att $m = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ med alla p_i olika så är*

$$\begin{aligned}\phi(m) &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})\cdots(p_r^{r_1} - p_r^{a_r-1}) \\ &= m(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r).\end{aligned} \tag{2.6}$$

Bevis. Låt m vara ett positivt heltal som kan primtalsfaktoriseras i $m = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ med r antal distinkta primtalsfaktorer $p_i^{a_i}$. Vi har av Sats 2.4 att $\phi(m) = \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_r^{a_r})$ och det följer av Sats 2.2 att varje faktor $\phi(p^{a_i}) = p^{a_i} - p^{a_i-1}$. Vi utvecklar nu $\phi(m)$ så att

$$\begin{aligned}\phi(m) &= \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_r^{a_r}) \\ &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})\cdots(p_r^{r_1} - p_r^{a_r-1}) \\ &= p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r) \\ &= m(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r).\end{aligned} \tag{2.7}$$

□

Vi avslutar kapitlet om Eulers ϕ-funktion med en till användbar egenskap som vi behöver för att bevisa egenskaper av enhetsgruppen modulo m.

Sats 2.8. *Om n är ett positivt heltal så är* $\sum_{d|n} \phi(d) = n$.

Bevis. Vi utgår från ett bevis av Keith Conrad [5, s. 2–3].

Låt n vara ett positivt heltal. Vi betraktar listan av positiva heltal mindre eller lika med n och räknar summan av $\phi(d)$ för alla delare $d \mid n$. Vi delar alla tal i listan $1, 2, 3, \ldots, n-1, n$ med n och reducerar respektive bråk till minsta möjliga nämnare så att täljare och nämnare är relativt prima. Vi ser att alla nämnare i listan är delare till n och räknar nu antalet bråk i reducerad form med nämnare d. Vi får för varje $d \mid n$ att antalet bråk med nämnare d är lika med antalet bråk med täljare som är mindre eller lika med d och relativt prima med d. Vi får således att antalet bråk med nämnare d är lika med $\phi(d)$. Vi räknar nu antalet bråk i reducerad form och får att $\sum_{d|n} \phi(d) = n$. □

Vi ser till exempel att

$$\sum_{d|10} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$$

eftersom talen $1, 2, 4$ och 10 är delarna till 10.

2.2 Elementär gruppteori

Vi fortsätter kapitlet om algebraisk bakgrund med att definiera grupper, abelska grupper och delgrupper. Vi kommer senare använda dessa tre definitioner för att beskriva $\mathbb{Z}_m^*$.

Definition 2.9. En grupp $(G, \cdot)$ är en mängd G med en binär operation $\cdot$ som uppfyller villkoren:
1) Associativitet:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ för alla element } a, b, c \in G. \tag{2.10}$$

2) Existens av identitet:

$$\text{Det finns ett } e \in G \text{ så att } a \cdot e = e \cdot a \text{ för alla element } a \in G. \tag{2.11}$$

3) Existens av inverser:

$$\text{För varje } a \in G \text{ så finns det ett element } b \in G \text{ så att } a \cdot b = b \cdot a = e. \tag{2.12}$$

Vi ser till exempel att mängden av alla heltal med addition är en grupp eftersom $(\mathbb{Z}, +)$ uppfyller associativitet, existens av identitet och existens av inverser.

Definition 2.13. En operation $\cdot$ är kommutativ om $a \cdot b = b \cdot a$ för alla element $a, b \in G$. En grupp $(G, \cdot)$ är abelsk om operationen $\cdot$ är kommutativ.

Vi noterar särskilt att alla inverterbara element modulo m bildar en abelsk grupp under multiplikation eftersom multiplikation modulo m är associativ och kommutativ och gruppen innehåller en identitet och inverser för alla element. Vi går vidare med att definiera en delgrupp.

Definition 2.14. H är en delgrupp till en grupp $(G, \cdot)$ om H är en delmängd av G och H är en grupp under operationen $\cdot$.

2.3 Sidoklasser

Vi går vidare med att definiera sidoklasser och bevisa två resultat om sidoklasser. Vi kommer senare använda resultaten om sidoklasser för att beskriva förhållandet mellan ordningen av en ändlig grupp och ordningen av ett element i gruppen.

Definition 2.15. Om H är en delgrupp till G och $g \in G$ så är $gH = \{gh \mid h \in H\}$ en vänstersidoklass till H och $Hg = \{hg \mid h \in H\}$ en högersidoklass till H.

Vi noterar särskilt att vänstersidoklasser är lika med högersidoklasser för abelska grupper. Vi beskriver med följande två satser två viktiga egenskaper för sidoklasser.

Sats 2.16. *Om H är en delgrupp av en grupp G och $g_i \in G$ så är sidoklasserna g_1H och g_2H till delgruppen H antingen lika eller disjunkta.*

Bevis. Vi visar att $g_1H = g_2H$ om $g_1H \bigcap g_2H \neq \emptyset$. Om $g_1H \bigcap g_2H \neq \emptyset$ så finns det två element $h_1, h_2 \in H$ så att $g_1h_1 = g_2h_2$. Vi ser av likheten $g_1h_1 = g_2h_2$ att $g_1 = g_2h_2h_1^{-1}$ och att $g_2 = g_1h_1h_2^{-1}$. Vi får att $g_1h = g_2h_2h_1^{-1}h$ och $g_2h = g_1h_1h_2h^{-1}$ för alla $h \in H$. Vi har att $h_1h_2^{-1}h$ och $h_2h_1^{-1}h$ är element i H eftersom en delgrupp av definition är sluten under multiplikation. Vi får att $g_1h \in g_2H$ och att $g_2h \in g_1H$ vilket medför att $g_1H \subseteq g_2H$ och att $g_2H \subseteq g_1H$. Vi får alltså att $g_1H = g_2H$. $\square$

Vi ser med ett liknande bevis att samma resultat gäller även för högersidoklasser. Vi får därför att två vänstersidoklasser eller två högersidoklasser antingen är lika eller disjunkta.

Sats 2.17. *Om H är en delgrupp till en grupp G så är $G = \bigcup_{g \in G} gH$.*

Bevis. Låt $g_1, g_2 \in G$. Vi har av Sats 2.16 att de två sidoklasserna g_1H och g_2H antingen är disjunkta eller lika. Vi ser att det finns ett identitetselement $e \in H$ så

att $ge = g$ för ett godtyckligt $g \in G$ eftersom H är en delgrupp till G. Vi får att alla element g finns i en sidoklass. Vi ser att G täcks av unionen av alla sidoklasser eftersom unionen av alla sidoklasser är en delmängd av G och eftersom alla $g \in G$ finns i en sidoklass. □

Vi ser att ovanstående resultat även gäller för högersidoklasser. Vi kommer i nästa avsnitt att använda Sats 2.17 för att bevisa en sats om förhållandet mellan ordningen av en ändlig grupp G och ordningen av ett element $g \in G$.

2.4 Ordning

Vi definierar nu ordningen av en grupp och ordningen av ett element i en grupp. Vi kommer senare använda begreppen och flera resultat om ordningen av en grupp och ordningen av ett element för att beskriva $\mathbb{Z}_m^*$.

Definition 2.18. Ordningen $|G|$ av en ändlig grupp G är lika med antalet element i gruppen.

Vi definierar på samma sätt ordningen $|M|$ av en ändlig mängd M som antalet element i mängden. Vi kan nu med definition av sidoklasser och ordning bevisa ett resultat som vi senare kommer använda för att beskriva förhållandet mellan ordningen av ett element och en grupp.

Sats 2.19. *Om H är en ändlig delgrupp till G så är $|gH| = |Hg| = |H|$ för $g \in G$.*

Bevis. Vi visar satsen för vänstersidoklasser. Låt $H = \{h_1, h_2, \ldots, h_n\}$ och $gH = \{gh_1, gh_2, \ldots, gh_n\}$. Vi ser att alla produkter gh_i är olika eftersom $gh_1 = gh_2$ medför att $h_1 = h_2$. Vi får likheten $h_1 = h_2$ eftersom att $g^{-1}gh_1 = h_1$ och $g^{-1}gh_2 = h_2$. Vi får att $|gH| = |H|$ om H är en ändlig grupp eftersom alla element $gh_1 \in gH$ är olika. Resultatet följer på samma sätt för högersidoklasser. □

Vi kan också definiera ordningen av ett element i en grupp men då behöver vi först definiera en cyklisk grupp.

Definition 2.20. En grupp G är cyklisk om det finns ett $g \in G$ så att alla element $a \in G$ kan skrivas som $a = g^n$ för ett heltal n. Om alla element $a \in G$ kan skrivas som en potens av g så kallas g en generator.

Vi ser till exempel att $\mathbb{Z}_n$ bildar en cyklisk grupp under addition för något positivt heltal n.

Sats 2.21. *Om G och H är två cykliska grupper av ordning n så är $G \cong H$.*

Bevis. Låt $G = \{g, g^2, g^3, \ldots, g^n\}$ och $H = \{h, h^2, h^3, \ldots, h^n\}$. Vi definierar nu en avbildning $f : G \to H$ så att $f(g^a) = h^a$ för alla heltal a. Vi ser att f är väldefinierad eftersom $g^{a_1} = g^{a_2}$ om och endast om $a_1 \equiv a_2 \pmod{n}$. Vi har att f är en isomorfi eftersom att $f(g^a g^b) = f(g^{a+b}) = h^{a+b} = h^a h^b = f(g^a)f(g^b)$ för två heltal $a, b \geq 0$. □

Vi skriver C_n för en cyklisk grupp av ordning n och ser av förgående sats att C_n är en unik grupp. Vi återkommer till cykliska grupper i avsnittet om enhetsgruppen modulo m och använder nu definitionen av cykliska grupper för att definiera ordningen av ett element i en grupp.

Definition 2.22. Ordningen av ett element g i en grupp G är lika med antalet element i den cykliska delgruppen av G som genereras av g.

Vi ser till exempel att ordningen av ett element a i $\mathbb{Z}_m$ är lika med antalet element i den cykliska delgruppen som genereras av a. Om a och m är relativt prima så får vi därför att ordningen av a modulo m är det minsta heltal e så att $a^e \equiv 1 \pmod{m}$. Vi har nu tillräckligt med termer och resultat för att bevisa Lagranges sats.

Sats 2.23. *(Lagranges sats) Om H är en delgrupp till en ändlig grupp G så är ordningen av H en delare till ordningen av G.*

Bevis. Låt H vara en delgrupp till en ändlig grupp G. Vi delar G i alla vänstersidoklasser till H och noterar att sidoklasserna enligt Sats 2.17 motsvarar hela G. Vi får att antalet element i G är lika med antalet element i alla vänstersidoklasser till H så $G = g_1H \cup g_2H \cup \ldots \cup g_nH$ för några element $g_1, g_2 \ldots, g_n \in G$. Vi ser nu att $|G| = |g_1H| + |g_2H| + \cdots + |g_nH| = n|H|$ eftersom vi enligt Sats 2.19 har att $|g_iH| = |H|$. Vi får därmed att ordingen av H är en delare till ordningen av G. □

Vi kan nu formulera en användbar följdsats om ordningen av ett element g i en grupp G.

Följdsats 2.24. *Ordningen av ett element g i en ändlig grupp G är en delare till gruppens ordning.*

Bevis. Vi har av Definition 2.22 att ordningen av g är lika med ordningen av delgruppen till G som genereras av g. Ordningen av delgruppen som g genererar är enligt Sats 2.23 en delare till ordningen av G. □

Följdsats 2.24 är ett betydelsefullt resultat som vi återkommer till i senare kapitel för att beskriva cykliska grupper och enhetsgruppen modulo m.

2.5 Ringar, Kroppar och Isomorfier

Vi fortsätter nu med att definiera ringar och kroppar samt likhet mellan algebraiska strukturer.

Definition 2.25. En ring $(R, +, \cdot)$ är en mängd R med två operationer, addition och multiplikation, som uppfyller villkoren:

1. R med addition är en abelsk grupp, med ett neutralt element 0.
2. R med multiplikation är associativ.
3. Multiplikation distribuerar över addition så att $a \cdot (b + c) = a \cdot b + a \cdot c$ och $(a + b) \cdot c = a \cdot c + b \cdot c$ för alla $a, b, c \in R$.

Vi kallar en ring för kommutativ om $a \cdot b = b \cdot a$ gäller för alla $a, b \in R$. Vi ser att heltalen modulo m är en kommutativ ring eftersom $(\mathbb{Z}_m, +)$ är en abelsk grupp, $(\mathbb{Z}_m, \cdot)$ är associativ, multiplikation distribuerar över addition och multiplikation modulo m är en kommutativ operation.

Definition 2.26. En kropp K är en kommutativ ring med ett neutralt element 1 under multiplikation och med en multiplikativ invers för alla element utom 0.

Vi avslutar kapitlet med att definiera en isomorfi mellan grupper respektive mellan ringar.

Definition 2.27. Om $(G_1, *)$ och $(G_2, \circ)$ är två grupper så är en isomorfi av G_1 på G_2 en bijektiv funktion f från G_1 till G_2 som uppfyller $f(a * b) = f(a) \circ f(b)$ för alla $a, b \in G$. Vi skriver $(G_1, *) \cong (G_2, \circ)$, eller kortare $G_1 \cong G_2$, om det finns en isomorfi mellan G_1 och G_2.

Vidare kan vi definiera en ringisomorfi. Vi kommer senare använda ringisomorfier för att beskriva enhetsgruppen mod m.

Definition 2.28. Låt R_1 och R_2 vara två ringar. En avbildning $f : R_1 \to R_2$ kallas en ringisomorfi om f är en bijektion och uppfyller

$$f(a + b) = f(a) + f(b) \tag{2.29}$$

och

$$f(ab) = f(a)f(b) \tag{2.30}$$

för alla $a, b \in R_1$.

3 Enhetsgruppen modulo m

Vi har hitintills beskrivit Eulers ϕ-funktion och elementär gruppteori och är nu redo för att beskriva enhetsgruppen modulo m. En rings enhetsgrupp är gruppen av inverterbara element i ringen. Vi definierade tidigare $\mathbb{Z}_m^*$ som mängden av element i $\mathbb{Z}_m$ som är relativt prima med m. Vi ser till exempel att $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ eftersom 15 är relativt prima med $1, 2, 4, 7, 8, 11, 13$ och 14. För att förklara varför de två definitionerna av $\mathbb{Z}_m^*$ är ekvivalenta så behöver vi studera relationen mellan inverterbarhet modulo m och relativt prima.

Sats 3.1. *Ett tal a är inverterbart modulo m om och endast om* $\text{SGD}(a, m) = 1$.

Bevis. Vi visar först att om a är inverterbar modulo m så är $\text{SGD}(a, m) = 1$. Om a är inverterbar modulo m så finns det ett tal b i $\mathbb{Z}_m$ så att $ab \equiv 1 \pmod{m}$ vilket medför att $ab - km = 1$ för något heltal k. En gemensam delare till a och m delar också $ab - km$, och därmed 1. Vi får därför att a och m är relativt prima om a är invertbar modulo m.

Vi visar nu omvändningen att a är inverterbar modulo m om $\text{SGD}(a, m) = 1$. Om $\text{SGD}(a, m) = 1$ så finns det enligt Bézouts identitet två tal x och y så att $ax + my = 1$ [4]. Då är $ax \equiv 1 \pmod{m}$, så x är en multiplikativ invers till a modulo m. □

Vi ser av Sats 3.1 att enhetsgruppen modulo m också kan definieras som alla inverterbara element i ringen $\mathbb{Z}_m$. Vi får till exempel att $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ eftersom talen $1, 3, 5, 7, 9, 11, 13$ och 15 är relativt prima med 16 och därmed inverterbara i $\mathbb{Z}_{16}$.

3.1 Ordningen av $\mathbb{Z}_m^*$

Ordningen av $\mathbb{Z}_m^*$ är särskilt intressant. Vi ser av Definition 1.1 och 2.1 att ordningen av $\mathbb{Z}_m^*$ är lika med $\phi(m)$. Vi använder oss nu av resultat om $\phi(m)$ för att studera enhetsgrupper av en given ordning k. Vi visar med två exempel hur vi kan bestämma alla enhetsgrupper av en ordning k.

Sats 3.2. *Det finns precis sex enhetsgrupper modulo m av ordning* 16. *Grupperna $\mathbb{Z}_{60}^*$, $\mathbb{Z}_{48}^*$, $\mathbb{Z}_{40}^*$, $\mathbb{Z}_{34}^*$, $\mathbb{Z}_{32}^*$ och $\mathbb{Z}_{17}^*$ är alla av ordning* 16.

Bevis. Vi söker alla enhetsgrupper av ordning 16. Vi har av Sats 2.5 att $p-1$ delar $\phi(m) = 16$ om p är en primtalsfaktor av m. Delare till 16 är $1, 2, 4, 8, 16$. Vi får då att p måste vara lika med $2, 3, 5$ eller 17 eftersom $p - 1$ är lika med $1, 2, 4, 8$ och 16. Vi har att primtalen $2, 3, 5$ och 17 är enda möjliga primtalsfaktorerna av m.

Vi betraktar först fallet $p = 17$. Vi ser att multipliciteten av 17 är som mest 1 eftersom 17 inte delar $\phi(m) = 16$. Vi har att $\mathbb{Z}_{17}^*$ är en enhetsgrupp av ordning 16 eftersom $\phi(17) = 16$.

Vi undersöker nu om det finns något heltal $a > 1$ så att $\phi(17a) = 16$ om $\text{SGD}(17, a) = 1$. Vi får av Sats 2.4 att $\phi(17a) = \phi(17)\phi(a) = 16\phi(a)$. Vi ser av $\phi(17a) = 16$ att $\phi(a) = 1$. Vi har att $\phi(2) = 1$ och får att $\phi(17)\phi(2) = 16$. Vi får därför att $\mathbb{Z}_{34}^*$ är en grupp av ordning 16.

Vi betraktar nu fallet $p = 5$. Vi ser att multipliciteten av 5 är som mest 1 eftersom 5 inte delar $\phi(m) = 16$. Vi ser att $\phi(5) = 4$ och kollar nu om det finns något heltal b så att $\phi(5b) = 16$ om $\text{SGD}(5, b) = 1$. Vi får av $\phi(5b) = 4\phi(b) = 16$ att $\phi(b) = 4$. Vi söker nu b så att $\phi(b) = 4$. Vi får av Sats 2.5 att primtalen som delar b är $2, 3$ och 5 men $5 \nmid b$ eftersom att $SGD(5, b) = 1$. Vi ser att 3 har multiplicitet 1 eftersom 3 inte delar 4. Vi har att $\phi(3) = 2$ och söker ett heltal c med $SGD(15, c) = 1$ så att $\phi(3c) = 4$. Vi får att $\phi(12) = 4$ eftersom $SGD(3, 4) = 1$ och $\phi(3)\phi(4) = 4$. Vi ser också att 2 kan vara av större multiplicitet än 1 eftersom 2 delar 4. Vi ser av Sats 2.2 att $\phi(8) = 4$. Vi har att $\text{SGD}(5, 8) = 1$ och $\text{SGD}(5, 12) = 1$ och får därför att $\phi(5)\phi(8) = \phi(40) = 16$ och $\phi(5)\phi(12) = \phi(60) = 16$. Vi får alltså att $\mathbb{Z}_{40}^*$ och $\mathbb{Z}_{60}^*$ är av ordning 16.

Vi betraktar nu fallet $p = 3$. Vi ser att multipliciteten av 3 är som högst 1 eftersom 3 inte delar 16. Vi söker ett d relativt prima med 15 så att $\phi(3d) = 16$. Vi får att $\phi(d) = 8$ eftersom $\phi(3) = 2$. Vi får av Sats 2.5 att primtal som delar d är $2, 3$ och 5 men $3 \nmid d$ och $5 \nmid d$ eftersom $SGD(15, d) = 1$. Vi får att $d = 2^r$ för något positivt heltal r. Vi har av Sats 2.4 att $\phi(2^r) = 2^{r-1} = 8$. Vi får att $r = 4$ och att $\phi(16) = 8$. Vi har alltså att $\mathbb{Z}_{48}^*$ är av ordning 16.

Vi betraktar avslutningsvis fallet $p = 2$. Vi får att multiplicitet av 2 kan vara större än 1 eftersom 2 delar 16. Vi ser av Sats 2.2 att $\phi(32) = 16$. Vi får alltså att $\mathbb{Z}_{32}^*$ är av ordning 16. □

Sats 3.3. *Det finns precis fyra enhetsgrupper modulo m av ordning* 18*. Grupperna $\mathbb{Z}_{54}^*$, $\mathbb{Z}_{27}^*$ $\mathbb{Z}_{27}^*$ och $\mathbb{Z}_{19}^*$ är alla av ordning* 18*.*

Bevis. Vi söker alla enhetsgrupper av ordning 18. Vi har av Sats 2.5 att $p-1$ delar $\phi(m) = 18$ om p är en primtalsfaktor av m. Delare till 18 är $1, 2, 3, 6, 9$ och 18. Vi får att primtalen $2, 3, 7$ och 19 är enda möjliga primtalsfaktorer av m.

Vi betraktar först fallen $p = 19$ och $p = 7$. Vi ser att multipliciteten av 19 och 7 är som högst 1 eftersom varken 19 eller 7 delar 18. Vi har av Sats 2.2 att $\phi(19) = 18$ och $\phi(7) = 6$. Vi får att $\mathbb{Z}_{19}^*$ är av ordning 18. Vi söker nu något heltal a så att $\phi(19a) = 18$. Vi ser av Sats 2.4 och $\phi(19) = 18$ att $\phi(a) = 1$. Vi får att $a = 1$

vilket medför att $\mathbb{Z}_{38}^*$ är av ordning 18. Vi söker nu ett heltal b så att $\phi(7b) = 18$. Vi ser av Sats 2.4 och $\phi(7) = 6$ att $\phi(b) = 3$. Vi har att det inte finns något b så att $\phi(b) = 3$ eftersom $\phi(m)$ är jämn för $m > 2$.

Vi betraktar nu fallen $p = 3$ och $p = 2$. Vi ser att multipliciteten av 2 och 3 kan vara större än 1 eftersom 2 och 3 delar 18. Vi söker några heltal c och d så att $\phi(2^c 3^d) = 18$. Vi använder Sats 2.2 och får att $\phi(2^c 3^d) = 2^{c-1}(2-1)3^{d-1}(3-1) = 2^c 3^{d-1}$ om $c, d > 0$. Vi har att $18 = 2^1 3^2$ och får därför att $c = 1$ och $d = 3$ så att $\mathbb{Z}_{54}^*$ är av ordning 18. Vi har att $\phi(2^c 3^d) = \phi(3^d)$ om $c = 0$ och att $\phi(2^c 3^d) = \phi(2^c)$ om $d = 0$. Vi har att $\phi(2^c) = 18$ saknar lösning och att $\phi(3^d) = 18$ om $d = 3$. Vi ser därför att $\mathbb{Z}_{27}^*$ också är av ordning 18. □

3.2 Struktur av $\mathbb{Z}_m^*$

Vi kommer nu att använda beskriven gruppteori för att behandla strukturen av en grupp modulo m och enhetsgruppen modulo m. Vi börjar med att definiera en kartesisk produkt av två grupper. Vi bevisar därefter en sats om ringisomorfier för $\mathbb{Z}_m$ för att sedan använda resultatet för att beskriva isomorfier av $\mathbb{Z}_m^*$.

Definition 3.4. Låt $(G, *_1), (H, *_2)$ vara två grupper. Om $g_i \in G$ och $h_i \in H$ så definierar vi den kartesiska produkten $G \times H$ som mängden av alla ordnade par (g_i, h_i). Vi definierar operationer på $G \times H$ komponentvis så att $(g_1, h_1)(g_2, h_2) = (g_1 *_1 g_2, h_1 *_2 h_2)$.

Vi noterar att den kartesiska produkten av två grupper är en grupp. Vi definierar på motsvarande sätt en kartesisk produkt av två ringar R_1 och R_2 som mängden av alla ordnade par (r_1, r_2) med komponentvisa operationer. Vi beskriver med satsen nedan förutsättningar för en ringisomorfi mellan en ring $\mathbb{Z}_m$ och en kartesisk produkt av ringar $\mathbb{Z}_{m_i}$. Vi ser att resultatet har en historisk kontext eftersom satsen är en version av den Kinesiska restsatsen.

Sats 3.5. *(Kinesiska restsatsen) Om två heltal a och b är relativt prima så är $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ given av $f([x]_{ab}) = ([x]_a, [x]_b)$ en ringisomorfi.*

Bevis. Vi vill visa att f är en bijektion som bevarar addition och multiplikation.

Låt $[x_1]_{ab}$ och $[x_2]_{ab}$ vara två restklasser modulo ab. Vi vill visa att $[x_1]_a = [x_2]_a$ och $[x_1]_b = [x_2]_b$ medför att $[x_1]_{ab} = [x_2]_{ab}$. Vi har att $[x_1]_a = [x_2]_a$ och $[x_1]_b = [x_2]_b$ om och endast om $a \mid (x_1 - x_2)$ och $b \mid (x_1 - x_2)$. Vi får nu eftersom a och b är relativt prima att $ab \mid (x_1 - x_2)$ om och endast om $a \mid (x_1 - x_2)$ och $b \mid (x_1 - x_2)$. Vi får att $[x_1]_{ab} = [x_2]_{ab}$ om och endast om $[x_1]_a = [x_2]_a$ och $[x_1]_a = [x_2]_b$ vilket medför att f är injektiv. Vi noterar nu att $|\mathbb{Z}_{ab}| = |\mathbb{Z}_a \times \mathbb{Z}_b| = ab$. Vi får att avbildningen f är bijektiv eftersom f är injektiv och $|V_f| = |D_f|$.

Vi ser nu att avbildningen f bevarar addition:

$$\begin{aligned} f([x_1]_{ab} + [x_2]_{ab}) &= f([x_1 + x_2]_{ab}) \\ &= ([x_1 + x_2]_a, [x_1 + x_2]_b) \\ &= ([x_1]_a + [x_2]_a, [x_1]_b + [x_2]_b) \\ &= ([x_1]_a, [x_1]_b) + ([x_2]_a, [x_2]_b) \\ &= f([x_1]_{ab}) + f([x_2]_{ab}). \end{aligned} \tag{3.6}$$

Vi ser också att avbildningen f bevarar multiplikation:

$$\begin{aligned} f([x_1]_{ab} \cdot [x_2]_{ab}) &= f([x_1 \cdot x_2]_{ab}) \\ &= ([x_1 \cdot x_2]_a, [x_1 \cdot x_2]_b) \\ &= ([x_1]_a \cdot [x_2]_a, [x_1]_b \cdot [x_2]_b) \\ &= ([x_1]_a, [x_1]_b) \cdot ([x_2]_a, [x_2]_b) \\ &= f([x_1]_{ab}) \cdot f([x_2]_{ab}). \end{aligned} \tag{3.7}$$

Vi får alltså att avbildningen f är en ringisomorfi. □

Vi får till exempel att $\mathbb{Z}_{15} \cong \mathbb{Z}_5 \times \mathbb{Z}_3$ eftersom $15 = 5 \cdot 3$ och 5 och 3 är relativt prima. Sats 3.5 är ett viktigt resultat som vi kan utöka till sammansatta tal av flera faktorer.

Sats 3.8. *Om ett heltal $m = m_1 m_2 \cdots m_k$ och heltalen $m_1, m_2, \ldots, m_k$ är parvis relativt prima så är $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$.*

Bevis. Vi bevisar satsen med induktion. Låt ett heltal $m = m_1 m_2$ för två relativt prima heltal m_1 och m_2. Vi vet av Sats 3.5 att $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.

Låt ett heltal $n = n_1 n_2 \cdots n_s$ för några parvis relativt prima heltal $n_1, n_2, \ldots, n_s$. Vi antar nu att $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$.

Låt $n_1, n_2, \ldots, n_s, n_{s+1}$ vara parvis relativt prima heltal och låt $r = n_1 n_2 \cdots n_s n_{s+1}$. Vi har att $r = n n_{s+1}$ och att heltalen $n = n_1 n_2 \cdots n_s$ och n_{s+1} är relativt prima. Vi får av Sats 3.5 och induktionsantagandet att $\mathbb{Z}_r \cong \mathbb{Z}_n \times \mathbb{Z}_{n_{s+1}} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s} \times \mathbb{Z}_{n_{s+1}}$. □

Vi ser nu att till exempel $\mathbb{Z}_{30} \cong \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_2$ eftersom $30 = 5 \cdot 3 \cdot 2$ och $2, 3$ och 5 är parvis relativt prima. Vi har med Sats 3.8 en användbar metod för att beskriva och förenkla enhetsgrupper modulo m. Vi använder nu tre lemman för att utöka Sats 3.8 till enhetsgruppen modulo m. Lemma 3.9, 3.10 och 3.11 utgår från övningar i lektionsanteckningar av Greenleaf [7, s. 10–11].

Lemma 3.9. *Låt $f : R_1 \to R_2$ vara en ringisomorfi. Om 1_1 är multiplikativt identitetselement i R så är $f(1_1)$ multiplikativt identitetselement i R_2.*

Bevis. En ringisomorfi är en bijektion och därför finns det för varje $r_2 \in R_2$ ett $r_1 \in R_1$ så att $r_2 = f(r_1)$. Vi får av egenskaper hos ringisomorfier att $r_2 f(1_1) = f(r_1)f(1_1) = f(r_1 1_1) = f(r_1) = r_2$. Det följer på samma sätt att $f(1_1)r_2 = r_2$ för alla $r_2 \in R_2$ och vi får att $f(1_1)$ är identitetselementet i R_2. □

Lemma 3.10. *Låt $f : R_1 \to R_2$ vara en ringisomorfi. Om $u_1 \in R_1$ är en enhet så är $f(u_1)$ en enhet i R_2.*

Bevis. Låt 1_1 vara identitetselementet i ringen R_1. Varje enhet $u_1 \in R_1$ har en multiplikativ invers $u_1^{-1} \in R_1$ så att $u_1^{-1}u_1 = u_1 u_1^{-1} = 1_1$. Av definition för ringisomorfi och Lemma 3.9 följer att $f(u_1)f(u_1^{-1}) = f(u_1 u_1^{-1}) = f(1_1) = 1_2$. Vi får på samma sätt att $f(u_1^{-1})f(u_1) = 1_2$. Vi får att $f(u_1)$ är en enhet i R_2 med en multiplikativ invers $f(u_1^{-1})$. □

Lemma 3.11. *Om R_1 och R_2 är kommutativa ringar så är enhetsgruppen $U_{R_1 \times R_2} \cong U_{R_1} \times U_{R_2}$.*

Bevis. Låt $(1_1, 1_2)$ vara multiplikativ identitet i $R_1 \times R_2$. Vi har att ett element $(a_1, a_2) \in R_1 \times R_2$ är inverterbart om och endast om det finns ett $(b_1, b_2) \in R_1 \times R_2$ så att $(a_1, a_2)(b_1, b_2) = (1_1, 1_2)$. Vi får av definition för komponentvisa operationer i $R_1 \times R_2$ att (a_1, a_2) har invers (b_1, b_2) i $R_1 \times R_2$ om och endast om $a_1 b_1 = 1_1$ och $a_2 b_2 = 1_2$. Vi har sammanfattningsvis att (a_1, b_2) är inverterbart i $R_1 \times R_2$ om och endast om a_1 är inverterbart i R_1 och a_2 är inverterbart i R_2 vilket medför att $U_{R_1 \times R_2} \cong U_{R_1} \times U_{R_2}$. □

Vi har med Lemma 3.9, 3.10 och 3.11 tillräckligt med teori för att utöka Sats 3.8 till enhetsgruppen modulo m.

Följdsats 3.12. *Om ett heltal $m = m_1 m_2 \cdots m_k$ och heltalen $m_1, m_2, \ldots, m_k$ är positiva och parvis relativt prima så är $\mathbb{Z}_m^* \cong \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*$.*

Bevis. Låt $m = m_1 m_2 \cdots m_k$ för något heltal k och låt heltalen $m_1, m_2, \ldots, m_k$ vara parvis relativt prima. Då är avbildningen $f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ given av $f([x]_m) = ([x]_{m_1}, [x]_{m_2}, \ldots, [x]_{m_k})$ enligt Sats 3.8 en ringisomorfi. Vi har av Lemma 3.10 att f avbildar en enhet i $\mathbb{Z}_m$ till en enhet i $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$. Vi får av Lemma 3.11 att enhetsgruppen i $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ är isomorf med $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*$. Vi får alltså att $\mathbb{Z}_m^* \cong \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*$. □

Vi har nu en metod för att beskriva enhetsgruppen modulo m. Vi ser till exempel att enhetsgruppen $\mathbb{Z}_{42}^* = [1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41]$ är isomorf med $\mathbb{Z}_7^* \times \mathbb{Z}_3^* \times \mathbb{Z}_2^*$ eftersom $42 = 7 \cdot 3 \cdot 2$ och $7, 3$ och 2 är parvis relativt prima.

3.3 Cykliska grupper

Vi har nu en metod för att reducera $\mathbb{Z}_m^*$ till en produkt av mindre enhetsgrupper och fortsätter därför med att beskriva enhetsgruppen modulo m. Vi ämnar med kommande satser och lemman förklara för vilka m gruppen $\mathbb{Z}_m^*$ är cyklisk. Vi börjar med att definiera primitiv rot modulo m. Vi återkopplar därefter till termen kropp och för vilka m gruppen $\mathbb{Z}_m$ är en kropp för att sedan i steg förklara varför $\mathbb{Z}_m^*$ är cyklisk om och endast om $m = 2, 4, p^k$ eller $2p^k$ för ett primtal p och ett heltal $k \geq 1$.

Definition 3.13. Vi säger att a är en primitiv rot modulo m om heltalen a och m är relativt prima och a är av ordning $\phi(m)$.

Vi har att $|\mathbb{Z}_m^*| = \phi(m)$. Vi ser därför att ett tal a är en primitiv rot modulo m om och endast om a är en generator till $\mathbb{Z}_m^*$.

Vi behandlar nu för vilka m som $\mathbb{Z}_m$ är en kropp.

Lemma 3.14. *Ringen $\mathbb{Z}_m$ är en kropp om och endast om m är ett primtal.*

Bevis. Vi har att $\mathbb{Z}_m$ är en kommutativ ring och vill visa att alla element i $\mathbb{Z}_m$ förutom 0 har en multiplikativ invers om och endast om m är ett primtal.

Om $m = p$ för ett primtal p så får vi att alla element som inte finns i restklassen 0 i $\mathbb{Z}_m$ är relativt prima med p. Vi ser att alla element som inte tillhör restklassen 0 i $\mathbb{Z}_m$ har en multiplikativ invers eftersom ett tal a i $\mathbb{Z}_m$ är inverterbar modulo m om och endast om $\text{SGD}(a, m) = 1$.

Om $m = m_1 m_2$ för två heltal $m_1, m_2 > 1$ så får vi att $\mathbb{Z}_m$ inte är en kropp eftersom en äkta delare till m inte är inverterbar modulo m. □

Vi behandlar nu ett användbart resultat om antalet lösningar för ett nollskilt polynom med koefficienter i en kropp.

Lemma 3.15. *Om K är en kropp och $p(x)$ är ett nollskilt polynom av grad n i $K[x]$ så har $p(x)$ som högst n rötter i K.*

Bevis. Vi bevisar satsen med induktion. Om $p(x)$ är ett nollskilt polynom av grad 0 så är $p(x)$ ett konstant polynom. Ett nollskilt konstant polynom p har noll rötter och därför gäller påståendet för $n = 0$.

Vi antar nu att påståendet gäller för alla polynom av en viss grad $n \geq 0$ och visar att påståendet gäller för alla polynom av grad $n+1$. Låt $p(x)$ vara ett polynom av grad $n+1$ i $K[x]$. Om ett $a \in K$ är en rot till $p(x)$ så kan enligt faktorsatsen $p(x)$ faktoriseras som $p(x) = (x-a)g(x)$ för något polynom $g(x) \in K[x]$ [4]. Låt $b \in K$ vara en rot till $p(x)$ skild från a. Vi får av faktoriseringen $p(x) = (x-a)g(x)$ att $b - a \neq 0$ medför att $g(b) = 0$. Vi ser därmed att rötterna till $p(x)$ i K är a och alla rötter till ett polynom $g(x)$ av grad n. Vi vet av antagandet att $g(x)$ har som högst n rötter i K och får att $p(x)$ har som högst $n+1$ rötter i K. □

Vi återkommer till resultatet om antalet lösningar till ett nollskilt polynom i en kropp och behandlar nu några lemman om cykliska grupper som vi behöver för att beskriva för vilka m enhetsgruppen modulo m är cyklisk.

Lemma 3.16. *Om $G = \langle g \rangle$ är en cyklisk grupp och H är en delgrupp till G så är H cyklisk.*

Bevis. Vi ser att H är en cyklisk grupp med generator e om $H = \{e\}$. Vi antar därför att $H \neq \{e\}$. Vi har av Definition 2.20 att alla element i H är lika med g^n för något heltal n. Låt nu k vara det minsta positiva heltal så att $g^k \in H$. Vi har att $n \geq k$ och får av Divisionsalgoritmen [4] att det finns två heltal q och r så att $n = kq + r$ och $0 \leq r < k$. Vi får därför att $g^n = g^{(kq+r)}$ vilket medför att $g^r = (g^k)^{(-q)}g^n$. Vi ser att $g^r \in H$ eftersom en grupp H är sluten under multiplikation och innehåller en invers $(g^k)^{(-1)}$. Vi har att $r = 0$ eftersom att $0 \leq r < k$ och k är det minsta positiva heltal så att $g^k \in H$. Vi får att $n = kq$ vilket betyder att $g^n = g^{kq} = (g^k)^q$. Vi har således att alla g^n är en potens av g^k och att H är en cyklisk grupp med generator g^k. □

Vi kommer senare att använda resultatet för att bestämma ordningen av en delgrupp till en cyklisk grupp. Vi fortsätter med ett resultat om cykliska delgrupper.

Lemma 3.17. *Låt G vara en grupp och $a \in G$. Om a är av ordning n och k är ett positivt heltal så är $\langle a^k \rangle = \langle a^{\mathrm{SGD}(n,k)} \rangle$.*

Bevis. Låt $d = \mathrm{SGD}(n,k)$. Vi vet att $d = k/m$ för något positivt heltal m. Vi har att $a^d = a^{(k/m)}$ och får att $a^k = (a^d)^m$. Vi får därför att $a^k \in \langle a^d \rangle$ och att $\langle a^k \rangle \subseteq \langle a^d \rangle$.

Vi har med Bézouts identitet [4] att $d = ns + kt$ för två heltal s och t. Vi får således att $a^d = a^{(ns+kt)} = a^{ns}a^{kt} = e^s a^{kt} = (a^k)^t$. Vi får att $a^d \in \langle a^k \rangle$ och att $\langle a^d \rangle \subseteq \langle a^k \rangle$. □

Vi använder nu Lemma 3.17 för att bestämma ordningen av ett element a^k i en grupp G.

Lemma 3.18. *Låt G vara en grupp och $a \in G$. Om a är av ordning n och k är ett positivt heltal så är $|a^k| = n/\operatorname{SGD}(n,k)$.*

Bevis. Låt $d = \operatorname{SGD}(n,k)$. Vi bestämmer först $|a^d|$. Vi ser att $|a^d| \leq n/d$ eftersom att $(a^d)^{n/d} = a^n = e$. Låt $0 < m < n/d$. Vi får nu av Definition 2.22 att $(a^d)^m \neq e$ eftersom $dm < n$ och n är det minsta tal så att $a^n = e$. Vi får därför att $|a^d| = n/d$.

Vi bestämmer nu $|a^k|$. Vi ser av Definition 2.22 och Lemma 3.17 att $|a^k| = |\langle a^k \rangle| = |\langle a^d \rangle| = |a^d|$. Vi får således att $|a^k| = n/d$. □

Vi använder nu Lemma 3.16 och 3.18 för att beskriva ett förhållande mellan ordningen av en delgrupp till en cyklisk grupp och en delare till ordningen.

Lemma 3.19. *Låt $G = \langle a \rangle$ vara en cyklisk grupp. Om G är av ordning n så finns det för varje delare d till n precis en delgrupp av ordning d.*

Bevis. Låt H vara en delgrupp till G. Vi får av Sats 2.23 att ordningen av H är en delare till ordningen av G.

Låt $G = \langle a \rangle$ och $d \mid n$. Vi antar nu att det finns två delgrupper H och K av ordning d. Vi ser av Lemma 3.16 att en delgrupp till en cyklisk grupp är cyklisk. Låt därför $H = \langle a^h \rangle$ där h är det minsta positiva heltal så att $a^h \in H$ och $K = \langle a^k \rangle$ där k är det minsta positiva heltal så att $a^k \in K$. Vi får av Lemma 3.18 att $|H| = n/\operatorname{SGD}(n,h)$ och $|K| = n/\operatorname{SGD}(n,k)$.

Vi får av antagandet att $\operatorname{SGD}(n,h) = \operatorname{SGD}(n,k)$. Vi bestämmer nu $\operatorname{SGD}(n,h)$. Vi har av Divisionsalgoritmen [4] att det finns två heltal q och r så att $n = qh + r$ för något $0 \leq r < h$. Vi får att $a^n = a^{(qh+r)}$ vilket medför att $a^r = a^n a^{(-qh)} = ea^{(-qh)} = a^{(-qh)}$. Vi får att $a^r = (a^h)^{(-q)} \in H$ eftersom $H = \langle a^h \rangle$. Vi ser att $r = 0$ eftersom att $r < h$ och h är det minsta positiva heltalet så att $a^h \in H$. Vi får därför att $n = qh$ vilket medför att $h \mid n$. Vi får således att $\operatorname{SGD}(n,h) = h$.

Vi kan på samma sätt visa att $\operatorname{SGD}(n,k) = k$. Vi får således att $h = k$ eftersom $\operatorname{SGD}(n,h) = \operatorname{SGD}(n,k)$ vilket avslutningsvis medför att $H = K$. □

Vi formulerar nu ett resultat om cykliska grupper som följer av tidigare lemman.

Lemma 3.20. *Om $G = \langle a \rangle$ är en cyklisk grupp av ordning n så är $\langle a \rangle = \langle a^k \rangle$ om och endast om n och k är relativt prima.*

Bevis. Resultatet följer direkt av Lemma 3.17 eftersom $\langle a \rangle = \langle a^{SGD(n,k)} \rangle$ om och endast om $SGD(n,k) = 1$. □

Vi visar nu med Lemma 3.19 och 3.20 ett resultat om antalet element av ordning d för en delare d till gruppens ordning.

Lemma 3.21. *Låt G vara en cyklisk grupp av ordning n. Om ett positivt heltal d delar n så är antalet element av ordning d i G lika med $\phi(d)$.*

Bevis. Vi ser att det enligt Lemma 3.19 finns precis en delgrupp H av ordning d. Vi får att alla element av ordning d i G genererar H. Vi ser av Lemma 3.20 att ett element $a \in G$ av ordning k genererar H om och endast om k och d är relativt prima. Vi får därför att antalet element som kan generera H är lika med $\phi(d)$. □

Vi är med hjälp av Lemma 3.14, 3.15 och 3.21 nu redo för att behandla enhetsgruppen modulo p för ett primtal p.

Sats 3.22. *Om p är ett primtal så är gruppen $\mathbb{Z}_p^*$ cyklisk.*

Bevis. Vi använder idéer från Conrad [5, s. 3] och Yiu [6, s. 125] tillsammans med Följdsats 2.24 och Lemma 3.14, 3.15 och 3.21 för att bevisa satsen.

Vi noterar att ordningen av gruppen $\mathbb{Z}_p^*$ är $\phi(p) = p-1$ och att ordningen av varje element i $\mathbb{Z}_p^*$ enligt Följdsats 2.24 är en delare till $p-1$.

Antag att vi har ett element $a \in \mathbb{Z}_p^*$ av ordning d. Delgruppen är av ordning d och innehåller elementen $1, a^1, a^2, \ldots, a^{d-1}$. Vi får att varje element x i delgruppen uppfyller $x^d = 1$ i $\mathbb{Z}_p$. Vi har av Lemma 3.14 att $\mathbb{Z}_p^*$ är en kropp och därför finns det enligt Lemma 3.15 som högst d lösningar till $x^d - 1 = 0$. Antalet element i delgruppen som uppfyller $x^d - 1 = 0$ är lika med antalet möjliga ekvationslösningar. Elementen $1, a^1, a^2, \ldots, a^{d-1}$ är således alla lösningar till $x^d - 1 = 0$. Vi får av Lemma 3.21 att antalet element av ordning d är lika med antalet tal mindre än d som är relativt prima till d. Så antalet element av ordning d är $\phi(d)$. För varje delare d av $p-1$ så är alltså antalet element av ordning d antingen 0 eller $\phi(d)$. Vi har av Sats 2.8 att

$$\sum_{d|p-1} \phi(d) = p - 1. \tag{3.23}$$

Vi får av (3.23) att antalet element av ordning d är lika med $\phi(d)$ för alla delare d eftersom ordningen av $\mathbb{Z}_p$ är $p-1$. Då det finns $\phi(p-1) > 0$ element av ordning $p-1$ så finns det alltså minst ett element som genererar gruppen. Vi har att $\mathbb{Z}_p^*$ är en cyklisk grupp.

□

Vi har till exempel att $\mathbb{Z}_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$ är en cyklisk grupp av ordning $\phi(17) = 16$ eftersom 17 är ett primtal. Vi ämnar nu utöka resultatet till enhetsgruppen modulo p^n då p är ett udda primtal och n är ett positivt heltal. Vi bevisar därför ett lemma som vi senare kommer använda för att bestämma en generator till $\mathbb{Z}_{p^n}$ från en generator r till $\mathbb{Z}_p$. Vi hämtar Lemma 3.24 från lektionsanteckningar från Yiu [6, s. 126].

Lemma 3.24. *Om p är ett udda primtal och a är ett heltal större eller lika med 2 så är $(1 + bp)^{p^{(a-2)}} \equiv 1 + bp^{(a-1)} \, (mod \, p^a)$.*

Bevis. Vi utgår från ett bevis av Yiu [6, s. 126].

Induktion över a. Uppenbart för $a = 2$ då vänsterledet $(1 + bp)^{p^{(2-2)}} = 1 + bp$ är lika med högerledet $1 + bp^{(2-1)} = 1 + bp$. Vi antar nu att $(1 + bp)^{p^{(a-2)}} \equiv 1 + bp^{(a-1)}$ (mod p^a) för något heltal $a \geq 2$. Så $(1 + bp)^{p^{(a-2)}} = 1 + bp^{(a-1)} + kp^a$ för något heltal k. Vi får för $a + 1$ att

$$\begin{aligned} (1 + bp)^{p^{(a-1)}} &= ((1 + bp)^{p^{(a-2)}})^p \\ &= (1 + bp^{(a-1)} + kp^a)^p. \end{aligned} \tag{3.25}$$

Vi får av multinomialsatsen [15] att

$$(1 + bp^{(a-1)} + kp^a)^p = \sum_{i_1+i_2+i_3=p} \binom{p}{i_1, i_2, i_3} (bp^{(a-1)})^{i_2} (kp^a)^{i_3} \tag{3.26}$$

vilket medför att

$$(1 + bp^{(a-1)} + kp^a)^p = \binom{p}{p, 0, 0} + \binom{p}{p-1, 1, 0} bp^{a-1} + Bp^a \tag{3.27}$$

för ett heltal B. Vi noterar att alla termer i Bp^a innehåller faktorn $p^{(a+1)}$ eftersom $i_2 > 1$ medför att $p^{(a-1)i_2} = p^{(a+1)} Cp^a$ för något heltal C och $i_3 > 0$ medför att $(p^a)^{i_3}$ multipliceras med p. Vi får därför att

$$\begin{aligned} (1 + bp^{(a-1)} + kp^a)^p &= 1 + bp^a + Bp^a \\ &\equiv 1 + bp^a \pmod{p^{a+1}}. \end{aligned} \tag{3.28}$$

□

Vi kan nu utöka för vilka m enhetsgruppen modulo m är cyklisk.

Sats 3.29. *Om p är ett udda primtal och n är ett positivt heltal så är gruppen $\mathbb{Z}_{p^n}^*$ cyklisk.*

Bevis. Vi använder idéer från Yiu [6, s. 126] för att bevisa satsen med Lemma 3.20 och 3.24.

Vi vet av Lemma 3.20 att $\mathbb{Z}_p^*$ är en cyklisk grupp med en generator r av ordning $p-1$. Vi har att ordningen av r modulo p^n är en multipel av $p-1$ som delar $\phi(p^n) = p^{n-1}(p-1)$. Vi får att ordningen av r modulo p^n är av formen $p^a(p-1)$ för något heltal $0 \leq a < n$. Vi får att ordningen av r är $p^{n-1}(p-1)$ om och endast om ordningen av r inte delar $p^{n-2}(p-1)$. Vi får således att $\mathbb{Z}_{p^n}^*$ är en cyklisk grupp med generator r om och endast om $r^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$.

Vi vet att $r^{p-1} = 1 + pk$ för något heltal k. Vi vet av Lemma 3.24 att

$$(r^{p-1})^{p^{n-2}} = (1+pk)^{p^{n-2}} \equiv 1 + kp^{n-1} \pmod{p^n}. \tag{3.30}$$

Om $k \not\equiv 0 \pmod{p}$ så är uppenbart $r^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$. Vi får då att r är ett element av ordning $p^{(n-1)}(p-1)$ vilket medför att $\mathbb{Z}_{p^n}^*$ är en cyklisk grupp med en generator r.

Om $k \equiv 0 \pmod{p}$ så är $r^{p-1} \equiv 1 \pmod{p^n}$. Vi påstår att $r+p$ är en generator av $\mathbb{Z}_{p^n}^*$ och undersöker om $(r+p)^{p^{n-2}(p-1)} \equiv 1 \pmod{p^n}$. Vi får att

$$(r+p)^{p^{n-2}(p-1)} = ((r+p)^{p-1})^{p^{n-2}} \tag{3.31}$$

vilket enligt binomialsatsen [3] är lika med

$$(r^{p-1} + (p-1)r^{p-2}p + Ap^2)^{p^{n-2}} \tag{3.32}$$

för något heltal A. Vi har att $r^{p-1} = 1 + pk$ för något heltal k och får att

$$(r+p)^{p^{n-2}(p-1)} = (1 + pk - pr^{p-2} + p^2r^{p-2} + Ap^2)^{p^{n-2}} \tag{3.33}$$

vilket är lika med

$$(1 + pk - pr^{p-2} + Bp^2)^{p^{n-2}} \tag{3.34}$$

för något heltal B. Vi har att $pk \equiv 0 \pmod{p^2}$ eftersom $k \equiv 0 \pmod{p}$ och att $r^{p-2} \not\equiv 1 \pmod{p}$ eftersom r är av ordning $p-1$ i Z_p^*. Vi får att

$$(r+p)^{p^{n-2}(p-1)} = (1+Cp)^{p^{n-2}} \tag{3.35}$$

för något heltal $C \not\equiv 0 \pmod{p}$. Vi får av Lemma 3.24 att

$$(r+p)^{p^{n-2}(p-1)} = (1+Cp)^{p^{n-2}} \equiv 1 + Cp^{n-1} \pmod{p^n}. \tag{3.36}$$

Då $1 + Cp^{n-1} \not\equiv 1 \pmod{p^n}$ så är elementet $r+p$ av ordning $p^{n-1}(p-1)$ och en generator till $\mathbb{Z}_{p^n}^*$. □

Sats 3.29 visar att $\mathbb{Z}_{p^n}^*$ är en cyklisk grupp om p är ett udda primtal men vi kan också använda Sats 3.29 för att bestämma en generator till $\mathbb{Z}_{p^n}$ från en generator till $\mathbb{Z}_p^*$.

Exempel 3.37. Vi söker en generator till gruppen $\mathbb{Z}_{27}^*$ som enligt Sats 3.29 är cyklisk. Vi ser att $\mathbb{Z}_{27}$ är en cyklisk grupp av ordning $\phi(27) = 18$. Vi ser att 2 är en generator till $\mathbb{Z}_3^*$ eftersom $2^1 = 2$ och $2^2 = 1$. Vi får av beviset till Sats 3.29 att 2 och/eller 5 är en generator till $\mathbb{Z}_{27}$. Vi ser nu att 2 är en generator till $\mathbb{Z}_{27}^*$ eftersom $2^{3^{(3-2)}(3-1)} = 64 \equiv 10 \not\equiv 1 \pmod{27}$. Vi ser att 5 också är en generator till $\mathbb{Z}_{27}^*$ eftersom $5^{3^{(3-2)}(3-1)} = 15625 \equiv 19 \not\equiv 1 \pmod{27}$.

Vi återvänder nu till resultat om strukturen av enhetsgruppen modulo m för att behandla enhetsgruppen $\mathbb{Z}_{2p^n}$.

Sats 3.38. *Om p är ett udda primtal och n ett positivt heltal så är gruppen $\mathbb{Z}_{2p^n}^*$ cyklisk.*

Bevis. Låt p vara ett udda primtal och n ett positivt heltal. Vi har av Följdsats 3.12 att $\mathbb{Z}_{2p^n}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_{p^n}^*$ eftersom 2 och p^n är relativt prima. Vi vet att enhetsgruppen $\mathbb{Z}_2^*$ är trivial och noterar att $|\mathbb{Z}_{p^n}^*| = |\mathbb{Z}_{2p^n}^*|$ eftersom $\phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n)$. Vi får att $\mathbb{Z}_{2p^n}^* \cong \mathbb{Z}_{p^n}^*$. Då $\mathbb{Z}_{2p^n}^* \cong \mathbb{Z}_{p^n}^*$ och $\mathbb{Z}_{p^n}^*$ är cyklisk så är $\mathbb{Z}_{2p^n}^*$ också cyklisk. □

Vi ser till exempel av Sats 3.38 att $\mathbb{Z}_{54}^*$ är en cyklisk grupp av ordning $\phi(54) = 18$. För att bestämma en generator till en allmän enhetsgrupp $\mathbb{Z}_{2p^n}$ och till vårt exempel $\mathbb{Z}_{54}^*$ så behöver vi följande sats.

Sats 3.39. *Om ett heltal r är en generator till $\mathbb{Z}_{p^n}^*$ för något udda primtal p och något positivt heltal n så är r (om r är udda) eller $r + p^n$ (om r är jämn) en generator till $\mathbb{Z}_{2p^n}^*$.*

Bevis. Låt r vara en generator till gruppen $\mathbb{Z}_{p^n}^*$ för något positivt heltal n och något udda primtal p. Om r är jämn så ersätter vi r med $r + p^n$ vilket är kongruent med r modulo p^n. Vi noterar att $r + p^n$ är en generator till $\mathbb{Z}_{p^n}^*$. Vi har nu en udda generator r till $\mathbb{Z}_{p^n}^*$. Vi vet att $\text{SGD}(r, 2p^n) = 1$ eftersom r är udda och relativt prima med p^n.

Låt k vara ordningen av r modulo $2p^n$. Vi vet av Följdsats 2.24 att ordningen av ett element i en ändlig grupp delar ordningen av gruppen. Vi får därför att $k \mid \phi(2p^n) = \phi(p^n)$. Vi har också att $2p^n \mid r^k - 1$ eftersom $r^k \equiv 1 \pmod{2p^n}$. Vi har att $p^n \mid r^k - 1$ eftersom $2p^n \mid r^k - 1$ vilket medför att $r^k \equiv 1 \pmod{p^n}$. Vi får att $\phi(p^n) \mid k$ eftersom att $r^k \equiv 1 \pmod{p^n}$. Vi får sammanfattningsvis att $\mathbb{Z}_{2p^n}^*$ är en cyklisk grupp av ordning $\phi(p^n)$ med generator r om r är udda och generator $r + p^n$ om r är jämn. □

Vi har nu en metod för att bestämma en generator till $\mathbb{Z}_{2p^n}^*$ från en generator till $\mathbb{Z}_{p^n}^*$. Vi fortsätter med vårt exempel och försöker nu bestämma en generator till $\mathbb{Z}_{54}^*$. Vi har tidigare visat att 2 är en generator till $\mathbb{Z}_{27}^*$. Uppenbart är inte 2 en generator till $\mathbb{Z}_{2p^n}^*$ eftersom 2 och 54 inte är relativt prima. Vi har då av Sats 3.39 att 29 är en generator till $\mathbb{Z}_{54}^*$.

Vi behandlar nu resterande fall. Vi börjar med att studera för vilka positiva heltal n enhetsgruppen $\mathbb{Z}_{2^n}^*$ är cyklisk.

Sats 3.40. *Låt n vara ett positivt heltal. Gruppen $\mathbb{Z}_{2^n}^*$ är cyklisk om och endast om $n = 1$ eller $n = 2$.*

Bevis. Vi har att $\mathbb{Z}_{2^n}^*$ är en cyklisk grupp om $n = 1$ eller $n = 2$ eftersom $\mathbb{Z}_2^* = \{1\}$ uppenbart är en cyklisk grupp och $\mathbb{Z}_4^* = \{1, 3\}$ är en cyklisk grupp av ordning 2 med generator 3.

Vi visar med motsägelse att gruppen $\mathbb{Z}_{2^n}^*$ inte är cyklisk för $n \geq 3$. Om $\mathbb{Z}_{2^n}^*$ är cyklisk så får vi av Lemma 3.21 att antalet element av ordning 2 i är $\phi(2) = 1$.

Vi visar nu att det finns två element av ordning 2 i $\mathbb{Z}_{2^n}^*$ för $n \geq 3$. Vi ser att $2^n - 1$ och $2^{n-1} + 1$ är två distinkta element eftersom $0 \leq 2^n - 1, 2^{n-1} + 1 < 2^n$ och $2^n - 1 \neq 2^{n-1} + 1$ för $n \geq 3$. Vi har att $2^n - 1$ är av ordning 2 eftersom $(2^n - 1)^2 = 2^{2n} - 2^{n+1} + 1 \equiv 1 \pmod{2^n}$. Vi får att $2^{n-1} + 1$ också är av ordning 2 eftersom $(2^{n-1} + 1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \pmod{2^n}$ för $n \geq 3$.

Vi har med motsägelse att $\mathbb{Z}_{2^n}^*$ inte är cyklisk för $n \geq 3$ eftersom enhetsgruppen innehåller två element av ordning 2. □

Vi har nu ytterligare två fall för vilka $\mathbb{Z}_m^*$ är cyklisk. Om $m = 2$ eller $m = 4$ så är $\mathbb{Z}_m^*$ cyklisk. Vi går nu vidare med att introducera två lemman om ordningen av en kartesisk produkt av grupper som vi använder för att beskriva en kartesisk produkt av cykliska grupper. Vi använder sedan resultatet om en kartesisk produkt av cykliska grupper för att komplettera tidigare fall.

Lemma 3.41. *Låt $G_1, G_2, \ldots, G_n$ vara ett ändligt antal grupper G_i. Om $a_i \in G_i$ har ordning k_i så har $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$ ordning $MGM(k_1, k_2, \ldots, k_n)$.*

Bevis. Låt k vara ordningen av $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$. Vi har $(a_1, a_2, \ldots, a_n)^k = (a_1^k, a_2^k, \ldots, a_n^k)$. Om e_i är identiteten i G_i så är $(a_1^k, a_2^k, \ldots, a_n^k) = (e_1, e_2, \ldots, e_n)$. Vi har av Följdsats 2.24 att ordningen av varje element a_i delar k. Ordningen av $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$ är det minsta heltal k så att $a_i^k = e_i$ för alla i. Vi får att $k = MGM(k_1, k_2, \ldots, k_n)$ eftersom alla $k_i | k$. □

Lemma 3.42. *Om $G_1, G_2, \ldots, G_k$ är ett ändligt antal grupper så är $|G_1 \times G_2 \times \cdots \times G_k| = |G_1||G_2| \cdots |G_k|$.*

Bevis. Vi har av definition att elementen i $G_1 \times G_2 \times \cdots \times G_k$ är av formen $(g_1, g_2, \ldots, g_k)$ för $g_i \in G_i$. Vi noterar att antalet element $(g_1, g_2, \ldots, g_k)$ enligt multiplikationsprincipen är lika med antalet element $g_1 \in G_1$ multiplicerat med antalet element $g_2 \in G_2$ multiplicerat med antalet element $g_3 \in G_3$ och så vidare. Vi får att $|G_1 \times G_2 \times \cdots \times G_k| = |G_1||G_2| \cdots |G_k|$. □

Vi kan nu använda Lemma 3.41 och 3.42 för att bevisa ett resultat om en kartesisk produkt av cykliska grupper. Vi hämtar Lemma 3.43 från Aryeh Zax [19, s. 4–5].

Lemma 3.43. *Om $C = C_{i_1} \times C_{i_2} \times \cdots \times C_{i_k}$ så är C cyklisk om och endast om alla i_j är parvis relativt prima.*

Bevis. Om i_j är parvis relativt prima så är $MGM(i_1, i_2, \ldots, i_k) = i_1 i_2 \cdots i_k$. Vi har av Lemma 3.41 att ett element $a_i \in C$ är av ordning $MGM(i_1, i_2, \ldots, i_k)$. Vi vet av Lemma 3.42 att $|C| = |C_{i_1}||C_{i_2}| \cdots |C_{i_k}| = i_1 i_2 \cdots i_k$. Vi får att C är cyklisk om i_j är parvis relativt prima eftersom det finns ett element $a_i \in C$ av ordning C.

Om i_j inte är parvis relativt prima så är $MGM(i_1, i_2, \ldots, i_k) < i_1 i_2 \cdots i_k$. Vi får att ordningen av alla element $a_i \in C$ är mindre än ordningen av C vilket medför att C inte är cyklisk. □

Vi ser av Lemma 3.43 att C är cyklisk om och endast om det finns ett element i C av ordning $MGM(i_1, i_2, \ldots, i_k)$. Vi noterar också att C inte är cyklisk om två faktorer C_{i_1} och C_{i_2} är av jämn ordning. Vi kommer senare använda resultatet för att bevisa Gauss resultat om $\mathbb{Z}_m^*$. Vi använder nu Lemma 3.42 för att bestämma strukturen av $\mathbb{Z}_{2^n}$ för något heltal $n \geq 2$. Vi börjar med att bestämma en möjlig ordning av 5 i $\mathbb{Z}_{2^n}^*$.

Lemma 3.44. *Om $n \geq 2$ så är $5^{2^{n-2}} \equiv 1 \pmod{2^n}$.*

Bevis. Vi visar med induktion. Vi har att resultatet gäller för $n = 2$ eftersom att $5 \equiv 1 \pmod 4$. Vi antar att $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ för något heltal $n \geq 2$. Vi får av induktionsantaget att $5^{2^{n-2}} = 1 + k2^n$ för något positivt heltal k. Vi har att

$$\begin{aligned} 5^{2^{(n+1)-2}} &= (5^{2^{n-2}})(5^{2^{n-2}}) \\ &= (1 + k2^n)(1 + k2^n) \\ &= 1 + 2k2^n + k^2 2^{2n} \\ &= 1 + k2^{n+1} + k^2 2^{2n} \\ &\equiv 1 \pmod{2^{n+1}}. \end{aligned} \tag{3.45}$$

Vi har alltså att $5^{2^{(n+1)-2}} \equiv 1 \pmod{2^{n+1}}$. Vi får alltså med induktion att $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ om $n \geq 2$. □

Vi använder nu Lemma 3.44 för att bestämma strukturen av $\mathbb{Z}_{2^n}^*$ för $n \geq 2$.

Sats 3.46. *Om $n \geq 2$ så är $\mathbb{Z}_{2^n}^* \cong C_2 \times C_{2^{n-2}}$.*

Bevis. Vi har av fundamentalsatsen för ändliga abelska grupper att en ändlig abelsk grupp är isomorf med en kartesisk produkt av cykliska grupper med primtalspotenser som ordning [2, s. 100–101]. Vi får därför att $\mathbb{Z}_{2^n}^*$ är isomorf med en kartesisk produkt av cykliska grupper. Vi har av Sats 2.5 att $\phi(2^n) = 2^n(1/2) = 2^{n-1}$. Vi får att varje cyklisk grupp i den kartesiska produkten har ordning 2^k för ett heltal $1 \leq k < n-1$ eftersom att $\mathbb{Z}_{2^n}^*$ inte är cyklisk och eftersom att alla element i $\mathbb{Z}_{2^n}^*$ har en ordning som delar 2^{n-1}.

Vi har av Lemma 3.44 att ordningen av 5 i $\mathbb{Z}_{2^n}^*$ delar 2^{n-2}. För att visa att 5 är av ordning 2^{n-2} i $\mathbb{Z}_{2^n}^*$ så visar vi med induktion att $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ för $n \geq 3$. Vi har $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ om $n = 3$ eftersom $5 \equiv 1 + 4 \pmod 8$. Vi antar att $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$ för något $k \geq 3$. Vi får av antagandet att $5^{2^{k-3}} = 1 + 2^{k-1} + a2^k$ för något positivt heltal a. Vi får att

$$\begin{aligned} 5^{2^{(k+1)-3}} &= (5^{2^{k-3}})(5^{2^{k-3}}) \\ &= (1 + 2^{k-1} + a2^k)(1 + 2^{k-1} + a2^k) \\ &= 1 + 2^{2k-2} + 2^k + a2^{k+1} + a2^{2k} + a^2 2^{2k} \\ &\equiv 1 + 2^{2k-2} + 2^k \pmod{2^{k+1}}. \end{aligned} \tag{3.47}$$

Vi har också att 2^{2k-2} är delbart med 2^{k+1} eftersom $k \geq 3$ och får att $5^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+1}}$. Vi ser därför att 5 är av ordning 2^{n-2} i $\mathbb{Z}_{2^n}^*$ för något heltal $n \geq 2$. Vi får att den direkta produkten av cykliska grupper innehåller $C_{2^{n-2}}$ eftersom det finns ett element av ordning 2^{n-2} i $\mathbb{Z}_{2^n}^*$. Vi får av Lemma 3.42 att $\mathbb{Z}_{2^n}^* \cong C_2 \times C_{2^{n-2}}$ eftersom ordningen av $\mathbb{Z}_{2^n}^*$ är 2^{n-1} och ordningen av $C_{2^{n-2}}$ är 2^{n-2}. □

Vi kompletterar nu tidigare fall med två fall för vilka enhetsgruppen modulo m inte är cyklisk. Vi formulerar tidigare resultat och kompletterande fall som en sats.

Sats 3.48. *Enhetsgruppen modulo m är cyklisk om och endast om $m = 2, 4, p^n$ eller $2p^n$ för något udda primtal p och något positivt heltal n.*

Bevis. Vi har med Sats 3.29, 3.38 och 3.40 visat att $\mathbb{Z}_m^*$ är cyklisk om $m = 2, 4, p^n$ eller $2p^n$ för något udda primtal p och positivt heltal n. Vi har med Sats 3.40 också visat att $\mathbb{Z}_m^*$ inte är cyklisk för $m = 2^n$ om $n \geq 3$. Vi kompletterar nu tidigare

resultat med två fall. Låt p, q vara två distinkta udda primtal. Vi visar att $\mathbb{Z}_m^*$ inte är cyklisk om $pq \mid m$ eller om $4p \mid m$.

Vi behandlar först $pq \mid m$. Vi har att $m = kp^n q^r$ för positiva heltal k, n och r. Vi får av Följdsats 3.12 att $\mathbb{Z}_m^* \cong \mathbb{Z}_k^* \times \mathbb{Z}_{p^n}^* \times \mathbb{Z}_{q^r}^*$ eftersom k, p^n och q^r är parvis relativt prima. Vi har av Sats 3.29 att $\mathbb{Z}_{p^n}^* \cong C_{p^{n-1}(p-1)}$ och att $\mathbb{Z}_{q^r}^* \cong C_{q^{r-1}(q-1)}$. Vi ser att grupperna $C_{p^{n-1}(p-1)}$ och $C_{q^{r-1}(q-1)}$ båda är av jämn ordning. Vi får av Lemma 3.43 att produkten av två jämna cykliska grupper inte är cyklisk och ser därför att $\mathbb{Z}_m^*$ inte är cyklisk om $pq \mid m$.

Vi behandlar nu $4p \mid m$. Vi har att $m = k2^r p^n$ för positiva heltal k och n och ett heltal $r \geq 2$. Vi har av Följdsats 3.12 att $\mathbb{Z}_m^* \cong \mathbb{Z}_k^* \times \mathbb{Z}_{2^r}^* \times \mathbb{Z}_{p^n}^*$ eftersom k, 2^r och p^n är parvis relativt prima. Vi ser att $\phi(p^n) = p^{n-1}(p-1)$ och att $\phi(2^r) = 2^{r-1}$. Vi får återigen att båda grupperna $\mathbb{Z}_{2^r}^*$ och $\mathbb{Z}_{p^n}^*$ är av jämn ordning vilket enligt Lemma 3.43 medför att produkten $\mathbb{Z}_m^*$ inte är cyklisk om $4p \mid m$.

Vi har med $m = 2, 4, 2^n, 2p^n$ och $k2^r p^n$ behandlat alla jämna positiva heltal eftersom att $2, 4$ och 2^n beskriver alla potenser av 2 och eftersom att $2p^n$ och $k2^r p^n$ motsvarar alla produkter av 2 och udda primtal. Vi har med $m = p^n$ och $kp^n q^r$ behandlat alla udda positiva heltal. Vi har sammanfattningsvis visat att $\mathbb{Z}_m^*$ är cyklisk om och endast om $m = 2, 4, p^n$ eller $2p^n$ för något positivt heltal n. □

Vi har nu bestämt för vilka m enhetsgruppen m är cyklisk samt bestämt strukturen av $\mathbb{Z}_{2^n}^*$ för $n \geq 2$.

3.4 Cyklisk struktur

Vi fortsätter med att beskriva enhetsgruppen modulo m och kommer nu med flera exempel visa hur vi kan reducera enhetsgrupper modulo m till produkter av cykliska grupper. Vi börjar avsnittet med att formulera ett användbart resultat om cykliska grupper som följer av tidigare resultat.

Sats 3.49. *Om ett heltal $m = m_1 m_2 \cdots m_k$ och heltalen $m_1, m_2, \ldots, m_k$ är parvis relativt prima så är $C_m \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k}$.*

Bevis. Resultatet följer direkt av Lemma 3.42 och 3.43 eftersom $C = C_{m_1} \times C_{m_2} \times \cdots C_{m_k}$ om $m_1, m_2, \ldots, m_k$ är parvis relativt prima och eftersom $|C_m| = |C_{m_1}||C_{m_2}| \cdots |C_{m_k}|$ om $m = m_1 m_2 \cdots m_k$. □

Vi har nu ett resultat som vi kan använda tillsammans med resultat från tidigare kapitel för att reducera enhetsgrupper modulo m till produkter av cykliska grupper.

Exempel 3.50. Vi betraktar $\mathbb{Z}_{77}^*$. Vi ser att 77 är en produkt av primtalen 7 och 11 och får av Följdsats 3.12 att $\mathbb{Z}_{77}^* \cong \mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$. Vi vet av Sats 3.22 att $\mathbb{Z}_7^* \cong C_6$ och $\mathbb{Z}_{11}^* \cong C_{10}$. Vi får att $\mathbb{Z}_{77}^* \cong C_6 \times C_{10}$ vilket enligt Sats 3.49 medför att $\mathbb{Z}_{77}^* \cong C_2 \times C_3 \times C_5 \times C_2$.

Vi har nu en dekomposition av $\mathbb{Z}_{77}^*$ och noterar att det finns flera. Vi kan till exempel skriva $\mathbb{Z}_{77}^* \cong C_2 \times C_5 \times C_6$ eller $\mathbb{Z}_{77}^* \cong C_2 \times C_2 \times C_{15}$ eftersom $C_5 \times C_6 \cong C_2 \times C_{15}$ enligt Sats 3.49. Vi kan alltså skriva $\mathbb{Z}_m^*$ som en produkt av cykliska grupper på olika sätt. Vi behöver därför en metod för att på ett unikt sätt skriva $\mathbb{Z}_m^*$ som en produkt av cykliska grupper.

Vi kan använda oss av en särskilt faktorisering av $\phi(m)$ för att reducera $\mathbb{Z}_m^*$ till en produkt av minsta möjliga antal cykliska grupper. Vi använder oss av Shanks två faktoriseringar av $\phi(m)$ och framställning av $\mathbb{Z}_m^*$ för att entydigt reducera $\mathbb{Z}_m^*$ till en produkt av cykliska grupper [10, s. 92–94].

Definition 3.51. Vi definierar med reglerna A-C nedan en särskild faktorisering ϕ_m av $\phi(m)$ för $m > 2$.

A) Om p är ett udda primtal och $m = p^a$ för ett heltal $a \geq 1$ så har vi $\phi(p^a) = (p-1)p^{a-1}$. Vi faktoriserar sen $p-1$ i n antal primtalspotenser $q_i^{b_i}$ så att $\phi_m = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n} p^{a-1}$. Vi skriver ut respektive faktor $q_i^{b_i}$ i ϕ_m som ett heltal.

B) Om $p = 2$ och $m = p^a$ för ett heltal $a \geq 2$ så skriver vi $\phi_m = 2$ om $a = 2$ och $\phi_m = 2(2^{a-2})$ om $a \geq 3$. Vi skriver ut faktorn 2^{a-2} som ett heltal om $a \geq 3$.

C) Om $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ där p_i är distinkta primtal och a_i är positiva heltal så behandlar vi respektive primtalspotens $p_i^{a_i}$ för sig. Vi sammanfogar faktoriseringarna som vi får av respektive primtalspotens i m till en faktorisering ϕ_m.

Vi får till exempel att $\phi_{25} = 4 \cdot 5$ enligt regel A i Definition 3.51. Vi går nu igenom två större exempel för att förklara definitionen.

Exempel 3.52. Vi beräknar faktoriseringen ϕ_{116}. Vi faktoriserar först $116 = 2^2 \cdot 29$. Vi får av regel A i Definition 3.51 att $\phi(29) = 28$ och faktoriseras som $28 = 2^2 \cdot 7$. Vi skriver respektive faktor i 28 som ett heltal och får att $\phi_{29} = 4 \cdot 7$. Vi får av steg B i Definition 3.51 att $\phi_{2^2} = 2$. Vi får sammantaget att $\phi_{116} = 2 \cdot 4 \cdot 7$.

Exempel 3.53. Vi beräknar faktoriseringen ϕ_{120}. Vi faktoriserar först $120 = 2^3 \cdot 3 \cdot 5$. Vi får av regel A i Definition 3.51 att $\phi_3 = 2$ och $\phi_5 = 4$ och av steg B i Definition 3.51 att $\phi_{2^3} = 2 \cdot 2$. Vi får sammantaget att $\phi_{120} = \phi_{2^3}\phi_3\phi_5 = 2 \cdot 2 \cdot 2 \cdot 4$.

Vi definierar nu en till faktorisering av $\phi(m)$ som vi kommer använda för att på ett kanoniskt sätt reducera $\mathbb{Z}_m^*$ till en produkt av cykliska grupper.

Definition 3.54. Vi definierar stegvis en faktorisering Φ_m av $\phi(m)$. Vi beräknar

ϕ_m och multiplicerar för varje distinkt primtal som delar $\phi(m)$ största motsvarande primtalspotens i ϕ_m till en produkt. Vi lägger undan faktorn och upprepar processen för alla återstående primtalspotenser i ϕ_m. Vi kallar respektive produkt av distinkta primtalspotenser för en karaktäristisk faktor f_i av $\mathbb{Z}_m$. Vi har avslutningvis att $\Phi_m = f_1 f_2 \cdots f_r$ med r karaktäristiska faktorer f_i för vilka $f_i \mid f_{i+1}$.

Vi ser till exempel att $\Phi_{25} = 20$ eftersom primtalen 2 och 5 delar $\phi(25)$ och största motsvarande primtalspotenser i ϕ_{25} är 4 och 5. Vi får att $f_1 = 4 \cdot 5 = 20$ och att $\Phi_{25} = f_1 = 20$. Vi förklarar faktoriseringen Φ_m med två till exempel.

Exempel 3.55. Vi har sedan tidigare att $\phi_{116} = 2 \cdot 4 \cdot 7$. Vi ser att primtalen 2 och 7 delar ϕ_{116} och multiplicerar största motsvarande primtalspotenser så att $f_2 = 4 \cdot 7$. Vi lägger undan faktorn 28 och ser att $f_1 = 2$. Vi får att $\Phi_{116} = f_1 f_2 = 2 \cdot 28$.

Exempel 3.56. Vi har sedan tidigare att $\phi_{120} = 2 \cdot 2 \cdot 2 \cdot 4$. Vi ser att 2 delar ϕ_{120} och multiplicerar största motsvarande primtalspotenser så att $f_4 = 4$. Vi forsätter sedan med återstående faktorer i ϕ_{120} och ser att $f_1 = 2$, $f_2 = 2$ och $f_3 = 2$. Vi får att $\Phi_{120} = f_1 f_2 f_3 f_4 = 2 \cdot 2 \cdot 2 \cdot 4$.

Vi har med Definition 3.54 en kanonisk faktorisering Φ_m av $\phi(m)$ som vi kan använda för att reducera $\mathbb{Z}_m^*$ till en produkt av cykliska grupper. Vi kan bestämma en cyklisk struktur av enhetsgruppen modulo m med karaktäristiska faktorer och Φ_m [10, s. 55–120][12]. Vi sammanfattar nu resultatet i en struktursats för enhetsgruppen modulo m.

Sats 3.57. *Om m är ett positivt heltal och $\Phi_m = f_1 f_2 \cdots f_r$ så är $\mathbb{Z}_m^* \cong C_{f_1} \times C_{f_2} \times \cdots \times C_{f_r}$.*

Bevis. Vi har sedan tidigare att vi kan skriva $\mathbb{Z}_m^*$ som en kartesisk produkt av cykliska grupper. Vi har också att vi kan reducera en cyklisk grupp till en produkt av cykliska grupper om ordningen är en produkt av relativt prima faktorer. Vi ser därför att $\mathbb{Z}_m^* \cong C_{i_1} \times C_{i_2} \times \cdots \times C_{i_k}$ där $\phi_m = i_1 i_2 \cdots i_k$. Vi multiplicerar nu ihop de största primtalspotenserna i ϕ_m till en karaktäristisk faktor. Produkten av motsvarande cykliska grupper blir en cyklisk grupp av karaktäristiska faktorns ordning. Vi lägger sedan undan faktorn och upprepar processen för alla återstående faktorer i ϕ_m. Vi får med Φ_m en entydig framställning av ϕ_m och noterar att faktorerna i respektive karaktäristisk faktor är parvis relativt prima. Vi får att $\mathbb{Z}_m^* \cong C_{i_1} \times C_{i_2} \times \cdots \times C_{i_r} \cong C_{f_1} \times C_{f_2} \times \cdots \times C_{f_s}$. □

Vi har med Sats 3.57 en struktursats som vi kan använda för att entydigt reducera $\mathbb{Z}_m^*$ till en produkt av cykliska grupper. Vi ser till exempel att $\mathbb{Z}_{25}^* \cong C_{20}$ eftersom Φ_{25} består av en karaktäristisk faktor $f_1 = 20$. Vi visar nu Sats 3.57 med två kortare exempel.

Exempel 3.58. Vi får av Sats 3.57 att $\mathbb{Z}_{116}^* \cong C_2 \times C_{28}$ eftersom $\Phi_{116} = f_1 f_2 = 2 \cdot 28$. Vi kan kontrollera resultatet med teori från tidigare kapitel. Vi har att $\mathbb{Z}_{116}^* \cong \mathbb{Z}_4^* \times \mathbb{Z}_{29}^* \cong C_2 \times C_{28}$.

Exempel 3.59. Vi får att $\mathbb{Z}_{120}^* \cong C_2 \times C_2 \times C_2 \times C_4$ eftersom $\Phi_{120} = 2 \cdot 2 \cdot 2 \cdot 4$. Vi kontrollerar resultatet med tidigare teori. Vi har att $\mathbb{Z}_{120}^* \cong \mathbb{Z}_8^* \times \mathbb{Z}_3^* \times \mathbb{Z}_5^* \cong C_4 \times C_2 \times C_4 \cong C_2 \times C_2 \times C_2 \times C_4$.

Vi ser med Exempel 3.58 och 3.59 att vi kan enkelt kan använda faktoriseringen Φ_m för att reducera $\mathbb{Z}_m^*$ till en entydig produkt av cykliska grupper. Vi går nu vidare med ett mer omfattande exempel som visar metodens effektivitet.

Exempel 3.60. Vi betraktar $\mathbb{Z}_{831600}^*$. Vi har att $831600 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$ vilket medför att $\mathbb{Z}_{831600}^* \cong \mathbb{Z}_{2^4}^* \times \mathbb{Z}_{3^3}^* \times \mathbb{Z}_{5^2}^* \times \mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$. Vi ser att $\mathbb{Z}_{16}^* \cong C_2 \times C_4$, $\mathbb{Z}_{27}^* \cong C_{18}$, $\mathbb{Z}_{25}^* \cong C_{20}$, $\mathbb{Z}_7^* \cong C_6$ och $\mathbb{Z}_{11}^* \cong C_{10}$. Vi får att $\mathbb{Z}_{831600}^* \cong C_2 \times C_4 \times C_{18} \times C_{20} \times C_6 \times C_{10}$. Vi faktoriserar nu produkter av relativt prima faktorer så att $\mathbb{Z}_{831600}^* \cong C_2 \times C_2 \times C_2 \times C_2 \times C_3 \times C_4 \times C_4 \times C_5 \times C_5 \times C_9$. Vi multiplicerar nu den största faktorn av respektive primtal till en produkt $f_6 = 4 \cdot 5 \cdot 9 = 180$. Vi upprepar nu metoden för återstående faktorer och får att $f_5 = 3 \cdot 4 \cdot 5 = 60$, $f_4 = 2$, $f_3 = 2$, $f_2 = 2$ och $f_1 = 2$. Vi får att $\mathbb{Z}_{831600}^* \cong C_{f_1} \times C_{f_2} \times C_{f_3} \times C_{f_4} \times C_{f_5} \times C_{f_6} = C_2 \times C_2 \times C_2 \times C_2 \times C_{60} \times C_{180}$.

Vi har nu alltså bevisat en metod för att beskriva enhetsgruppen modulo m som en entydig produkt av cykliska grupper.

4 Tillämpningar

Vi behandlar i kapitlet olika tillämpningar inom kryptering av enhetsgruppen modulo m. Kapitlet fokuserar på kryptering, men $\mathbb{Z}_m^*$ används också inom primtalstestning och heltalsfaktorisering [16].

4.1 Kryptering

Enhetsgruppen modulo m är viktig inom kryptering. Kryptologi beskriver olika metoder för att både skydda och forcera information och kommunikation och är idag ett stort fält som omfattar bland annat både matematik och datavetenskap [11]. Kryptografi, studiet av säker och skyddad kommunikation, är en viktig försättning för dagens kommunikation. Kryptografi har länge varit en del av det samhället och används idag inom till exempel internetbanker, e-handel, medicinska databaser och digital kommunikation för att säkra identiteter, transaktioner och information [11].

Behovet av att skydda kommunikation och information har funnits i över två tusen år. Flera tidiga civilisationer använde en tidig kryptering för att skydda

information från utomstående. Egypten, Babylonien och Assyrien är exempel på forntida civilisationer som använde en tidig kryptering [11]. Det första skrivna exemplet på tidig kryptering finns i Sparta under 400-talet f.kr. [11]. Militära befäl i Sparta använde ett system av koniska stavar för att skydda hemlig militär information [11]. Papper med hemlig militär information blev bara läsbar om den snurrats kring en konisk stav av rätt proportioner.

Krypteringen och dess användningsområden har utvecklats och utökats sedan forntidens koniska stavar och idag används bland annat enhetsgrupper och primitiva rötter modulo p för att skydda information. En välanvänd metod som använder kongruensräkning och $\mathbb{Z}_p^*$ för att kryptera data på en öppen kanal är Diffie-Hellmans nyckelutbyte. Diffie-Hellmans nyckelutbyte tillåter två personer som tidigare inte kommunicerat att skapa en gemensam hemlig nyckel som kan användas för att kryptera data. Vi presenterar metoden med ett kort exempel.

Exempel 4.1. Två personer Alice och Bob enas offentligt om ett primtal $p = 13$ och en generator $g = 2$. Alice väljer nu ett hemlig heltal $a = 4$ och skickar $A = 2^4 \pmod{13} = 3$ till Bob. Bob väljer också ett hemligt heltal $b = 5$ och skickar $B = 2^5 \pmod{13} = 6$ till Alice. Alice beräknar nu en hemlig nyckel till $n = B^a \pmod{p} = 6^4 \pmod{13} = 9$ och Bob beräknar samma nyckel $n = A^b \pmod{p} = 3^5 \pmod{13} = 9$. Alice och Bob har nu en gemensam hemlig nyckel n som de kan använda för att kryptera information.

Det finns idag flera varianter av Diffie-Hellmans nyckelutbyte men den ursprungliga metoden använder $\mathbb{Z}_p^*$ för att bestämma en gemensam nyckel på en offentliga kanal [14]. Diffie-Hellmans nyckelutbyte fungerar väl eftersom Alice och Bob enkelt kan beräkna $n = A^b \pmod{p} = B^a \pmod{p}$ och eftersom en tredje person Eve får svårt att bestämma nycklarna a och b från ekvationerna $2^a = 3 \pmod{13}$ och $2^b = 5 \pmod{13}$. Vi ser till exempel att $a = 4, 16$ och $4 + 12n$ för något positivt heltal n är lösningar till $2^a = 3 \pmod{13}$.

En annan metod som använder egenskaper av $\mathbb{Z}_p^*$ är RSA-kryptering. RSA använder en asymmetrisk kryptering och är idag en av de mest kända och välanvända metoderna för säker kommunikation [18]. Vi presenterar metoden med ett enkelt exempel.

Exempel 4.2. Vi väljer först två distinkta primtal $p = 11$ och $q = 17$. Vi beräknar sen $n = pq = 11 \cdot 17 = 187$. Vi beräknar nu $MGM(p-1, q-1) = MGM(10, 16) = 80$. Vi väljer nu ett heltal e så att $1 < e < 80$ och $\text{SGD}(80, e) = 1$. Vi väljer $e = 13$. Vi beräknar nu den multiplikativa inversen d av e modulo $MGM(10, 16) = 80$. Vi får att $d = 27$ eftersom $27 \cdot 37 \equiv 1 \pmod{80}$. Vi har nu en privat nyckel $(n = 187, d = 37)$ och en offentlig nyckel $(n = 187, e = 13)$. Vi kan nu kryptera ett meddelande $m = 14$ genom att beräkna $a \equiv 14^{13} \equiv 14 \cdot 9^6 \equiv 14 \cdot 168^2 \equiv$

$14 \cdot (-19) \equiv 14 \cdot 174 \equiv 14 \cdot (-13) \equiv 5 \pmod{187}$. Vi kan sedan dekryptera samma meddelande c genom att beräkna $m = 5^{37} \pmod{187} = 14$.

I praktiken används betydligt mycket större primtal än i Exempel 4.2 för att öka säkerheten. Säkerheten i RSA finns i svårigheten att faktorisera stora heltal och hitta en särskild rot till ett sammansatt tal modulo m [18]. Det finns idag ingen effektiv metod för att dekryptera ett meddelande med endast den offentliga nyckeln [18]. Svårigheten i att dekryptera ett meddelande med bara den offentliga nyckeln beror på att vi behöver faktoriseringen av m för att bestämma $\phi(m)$. Vi vill bestämma $\phi(m)$ eftersom vi kan använda använda ordningen av $\mathbb{Z}_m^*$ för att beräkna den privata nyckeln d. Om vi vet $\phi(m)$ så kan vi beräkna d eftersom d är multiplikativ invers av e modulo $\phi(m)$. Vid originella publikationen av algoritmen RSA användes faktiskt $\phi(m)$ för att beräkna en privat nyckel d. Idag används fortfarande $\phi(m)$ ibland men $MGM(p-1, q-1)$ leder i regel till effektivare räkning [18].

Både Diffie-Hellman och RSA är exempel på vanligt förekommande kryptering som använder egenskaper av $\mathbb{Z}_m^*$ för att kryptera information. Utöver DH och RSA så finns det flera andra metoder som också använder $\mathbb{Z}_m^*$ i olika utsträckning. För vidare studier se särskilt ElGamal och DSA (Digital Signature Algoritm).

Referenser

[1] Britannica, *Chinese remainder theorem*. Hämtad 2021-06-20.

[2] J.R. Durbin, *Modern Algebra - An Introduction*. 6 uppl. Hoboken, New Jersey: John Wiley & Sons Inc.

[3] M. Bullynck (2009). *Modular arithmetic before C.F. Gauss: Systematizations and discussions on remainder problems in 18th-century Germany*. Historia Mathematica, 36(1), 48-72.

[4] R. Bøgvad, Q. Xantcha & H. Granath, *Algebra I*. 10 uppl. Stockholms universitet, Stockholm: Matematiska institutionen (2018).

[5] K. Conrad, *Cyclicity of (Z/(p))×*. Hämtad 2021-06-20.

[6] P. Yiu, *Chapter 2 The ring $\mathbb{Z}/m\mathbb{Z}$*. Florida Atlantic University. Hämtad 2021-06-20.

[7] F.P. Greenleaf, *Algebra I: Section 6. The structure of groups*. Hämtad 2021-06-20.

[8] M. Penn, *Number Theory | The Multiplicativity of Euler's Totient Function*. Hämtad 2021-06-20.

[9] J. Najera, *Number Theory - History & Overview. Part I - What is number theory & why is it relevant today?*. towards data science. Hämtad 2019-06-20.

[10] D. Shanks, *Solved and Unsolved Problems in Number Theory*. 2. uppl. New York: Chelsea Publishing Company (1978).

[11] G.J. Simmons, *Cryptology*. Britannica. Hämtad 2021-06-20.

[12] E.W. Weisstein, *Modulo Multiplication Group*. *MathWorld*-A Wolfram Web Resource. Hämtad 2021-06-20.

[13] Wikipedia, *Disquisitiones Arithmeticae*. Hämtad 2021-06-20.

[14] Wikipedia, *Diffie-Hellman key exhange*. Hämtad 2021-06-20.

[15] Wikipedia, *Multinomial theorem*. Hämtad 2021-06-29.

[16] Wikipedia, *Multiplicative group of integeres modulo n*. Hämtad 2021-06-29.

[17] Wikipedia, *Number Theory*. Hämtad 2021-06-20.

[18] Wikipedia, *RSA(cryptosystem)*. Hämtad 2021-06-20.

[19] A. Zax, *When Is the Multiplicative Group Modulo n Cyclic?*. Hämtad 2021-06-20.