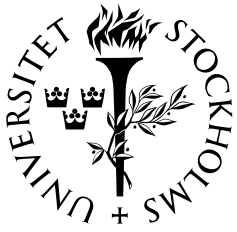

EXAMENSARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

AKS-algoritmen för att bestämma om ett tal är ett primtal eller inte

av

Per Westerlund

2005 - No 14

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 10691 STOCKHOLM

AKS-algoritmen för att bestämma om ett tal är ett primtal eller inte

Per Westerlund

Examensarbete i matematik 10 poäng

Handledare: Torsten Ekedahl

2005

Sammanfattning

AKS-algoritmen undersöker om ett tal är ett primtal eller inte. Den presenterades i augusti 2002 av Agrawal, Kayal och Saxena och är den första algoritmen som är både deterministisk och polynomiell, alltså ger den rätt svar för alla tal inom en tid som är ett polynom av antalet siffror.

Liksom flera andra algoritmer är den baserad på Fermats lilla sats, som inte kan användas direkt eftersom både alla primtal och vissa sammansatta tal uppfyller den. Här testar man några polynom upphöjda till det undersökta talet och de är väl valda så att inga sammansatta tal kan slinka igenom. Både antalet polynom och deras grad är små i förhållande till det undersökta talet.

Först visar jag algoritmen i pseudokod. Inför den senare analysen introducerar jag grundläggande talteori och algebra, bland annat moduloräkning, ringar och kroppar. Därefter beräknar jag algoritmens komplexitet rad för rad. Slutligen bevisar jag att den svarar rätt för både primtal och sammansatta tal.

Innehåll

Kapitel 1

Inledning

Primtal är sådana heltal större än 1 som bara är delbara med sig själva och talet 1. Redan under antiken var de intressanta för matematiker, till exempel för Euklides som visade att det finns oändligt många primtal [Tho91]. Pierre de Fermat formulerade år 1640 sin lilla sats: om p är ett primtal som inte delar a så delar det $a^{p-1} - 1$. Det finns tyvärr sammansatta tal b som delar $a^{p-1} - 1$ för vissa a, så Fermats lilla sats kan inte direkt användas för att bestämma om ett tal är primtal eller inte, utan den måste kombineras med andra satser [Rie94], [Cal].

En av anledningarna till intresset för primtal är att de är relativt lätta att hitta medan det är svårt att faktorisera produkten när man väl har multiplicerat två primtal. Miller är en av många som har studerat primtal de senaste årtiondena. År 1975 hittade han på en algoritm som är polynomiell, dvs tiden under vilken den utförs beror på antalet siffror upphöjt till en konstant. Eftersom den baseras på den utökade Riemanns förmodan så har man inte kunna bevisa att den gör rätt [Mil76]. Från den utvecklades Miller-Rabins algoritm, vars nackdel är att den inte är deterministisk utan slumpmässig. Den baseras på Fermats lilla sats och gör fel med viss sannolikhet för ett visst a. Felsannolikheten kan minskas hur mycket man vill, genom att göra om testet för andra värden på a [Rab80]. Därför användes Miller-Rabins algoritm för att skapa stora primtal för kryptering på 1980-talet och på det tidiga 1990-talet [Smi02]. Den ersattes av Maurers metod som inte avgör om ett tal är primtal utan skapar tal som bevisligen är primtal [Mau94].

År 1983 presenterades en algoritm som tar $\mathcal{O}((\lg n)^{\mathcal{O}(\lg \lg \lg n)})$ beräkningar, vilket är betydligt snabbare än tidigare deterministiska algoritmer [APR83].

Den är dock betydligt långsammare än Miller-Rabins slumpmässiga algoritm. Under de tre senaste årtiondena har flera olika slumpmässiga algoritmer presenterats, såsom Atkin-Morains [AM93].

I augusti 2002 presenterade Manindra Agrawal, Neeraj Kayal och Nitin Saxena vid Indian Institute of Technology Kanpur den numera benämnda AKS-algoritmen som är den snabbaste algoritmen att helt säkert bestämma om ett tal är ett primtal eller inte [AKS02]. Den är bevisat polynomiell, alltså tiden som det tar för algoritmen att avgöra om det är ett primtal är logaritmen av talet upphöjt till en konstant.[1]

Uppsatsens syfte är att beskriva AKS-algoritmen. Först presenteras själva algoritmen och sedan definitioner av olika begrepp inom talteori och algebra. Därefter följer en beräkning av hur snabb algoritmen är och ett bevis på att den svarar rätt.

[1]Diverse material om AKS-algoritmen finns sammanställt på [Sti] och [Car].

Kapitel 2

AKS-algoritmen

Här presenteras Lenstras variant enligt [Ber] och [Gil]. Jag har använt pseudokod med viss inspiration från C. Indragning av en rad betyder att den tidigare instruktionen (`om`, `medan`, `för alla`) gäller det indragna. n är talet som ska testas. Det ska vara ett heltal större än 1.

```
1 om n = a^b där a och b är heltal större än 1 svara SAMMANSATT
2 r ← 3, N ← (n − 1)(n^2 − 1) · · · (n^{4⌈lg n⌉^2−1} − 1)
3 medan r < n
4   om sgd(r, n) ≠ 1 svara SAMMANSATT
5   om r är ett primtal och r inte delar N  gå till rad 7
6   r ← r + 1
7 för alla a från 1 till r
8    om (x − a)^n ≢ (x^n − a) (mod x^r − 1, n) svara SAMMANSATT
9 svara PRIMTAL
```

I slingan, raderna 7–8, är talet r ett primtal och det finns inga primtal mindre än eller lika med r som delar n. Med $\lg n$ menas logaritmen av n med basen 2.

Rad 8 är huvudtestet som för primtal aldrig kan ge svaret SAMMANSATT tack vare Fermats lilla sats, som är grunden för flera primtalstest. Ett primtal uppfyller den alltid liksom vissa sammansatta tal. Så den duger inte. Man skulle ju kunna testa alla a mindre än n. Det är ett uttömmande test som

aldrig ger ett falskt svar för ett sammansatt tal. Det tar dock för lång tid eftersom antalet test blir lika med det testade talet n. Man vill ha ett test vars tidsåtgång är begränsad av ett polynom i antalet siffror i talet n.

Millers algoritm har uppnått detta genom att göra en utvidgning av Fermattestet för alla a från 2 till $2 \lg^2 n$. Den begränsade mängden av testade a gör att denna algoritm är polynomiell i $\lg n$. På grund av att det saknas en länk i beviskedjan kan man inte säga att denna algoritm är uttömmande. Även här går det att göra den uttömmande genom testa alla a ända till n. Det är inte heller någon bra idé.

Sedan räknade Rabin ut "sannolikheten" (i en viss mening) för att ett tal som gick igenom denna utvidgningen av Fermattestet för ett visst a ändå är sammansatt. Sannolikheten är högst $1/4$. Så med t olika värden på a får man att sannolikheten för att ta ett sammansatt tal för ett primtal är $1/4^t$. Så denna algoritm är inte deterministisk utan slumpmässig.

I AKS-algoritmen gör man rad 8-testet $16 \lg^5 n$ gånger. Detta test är baserat på Fermattestet och de enda sammansatta tal som slinker igenom detta test är potenserna av primtal, som kommer att upptäckas allra först i algoritmen, rad 1. För att detta relativt lilla antal utvidgade Fermattest ska vara uttömmande måste hjälpvariabeln r uppfylla vissa villkor. Den första slingan hittar alltid ett sådant r.

Kapitel 3

Relevanta matematiska begrepp

I detta kapitel förklarar jag heltalsaritmetik. Jag börjar med att presentera moduloräkning, som betecknas $a \equiv b \pmod{n}$, och sedan går jag igenom grupper, ringar och kroppar, som är mängder med en eller två operationer, $+$ och $\cdot$. Jag grundar mig på [BB96], [Chr75] och [EG02].

Definition 1 *En delare till eller en faktor i ett heltal a är ett heltal b sådant att det finns ett tal c så att $a = bc$. Det betecknas $b|a$ och man säger att b delar a. Talet a säges också vara en multipel av b*

Exempel: Det gäller att $1|6$, $-2|6$, $6|-6$, $-3|-6$, $5 \not| 6$ och $-4 \not| 6$.

Exempel: Mängden av alla multipler av 6 är $\{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}$ som betecknas $6\mathbb{Z}$.

För alla heltal har vi en divisionsalgoritm formulerad som:

Sats 2 *För alla heltal a och b där $b > 0$ finns det två heltal, en kvot k och en rest r, så att $a = k\,b + r$ där $0 \leq r < b$.*

Bevis: Betrakta $R^+ = \{a - b \cdot k \mid k \in \mathbb{Z}, a - b \cdot k \geq 0\}$, mängden av alla tänkbara icke-negativa rester. R^+ innehåller elementet $a - b\,(-|a|) = a + b \cdot |a|$ eftersom $b > 0$. Så R^+ innehåller minst ett element och alla element är positiva, alltså måste den innehålla ett minsta element r, enligt induktionsprincipen.

Antag att $r \geq b$, då finns det ett s sådant att $s = r - b = a - b\,(q+1) \in R^+$ och $s < r$. Det är en motsägelse eftersom r är det minsta elementet, så $r < b$. Eftersom r ska vara icke-negativt så blir $0 \leq r < b$.

Eftersom $r \in R^+$ så finns det ett tal k så att $a - b\,k = r$. Alltså finns kvoten k och resten r.

Antag att det finns två andra heltal k', r' så att $a - b\,k' = r'$. Välj dem så att $r > r'$. Genom att kombinera detta med $a - b\,k = r$ så fås att $r' + b\,k' = r + b\,k$, vilket ger att $r - r' = b\,(k' - k)$. Alltså $b|(r - r')$ men $r - r'$ måste ligga i intervallet $[1, b-1]$, vilket är en motsägelse. Så då måste $r' - r = 0$ vilket gör att $k = k'$. Alltså är divisionen entydig. □

Exempel: $7 = 1 \cdot 4 + 3$ och $8 = 2 \cdot 4 + 0$.

Definition 3 *Ett primtal är ett positivt heltal $p > 1$ vars enda positiva delare är 1 och p. De andra heltalen större än 1 benämns sammansatta.*

Exempel: 2, 3, 5 och 17 är primtal medan 4, 6 och 21 är sammansatta.

Definition 4 *Den största gemensamma delaren av två tal a och b är ett tal d som delar både a och b och där varje delare till både a och b delar d. Talet d betecknas* $\text{sgd}\,(a, b)$.

Exempel: $\text{sgd}\,(4, 6) = 2$ medan $\text{sgd}\,(4, 21) = 1$ liksom $\text{sgd}\,(5, 6) = 1$ och naturligtvis $\text{sgd}\,(3, 5) = 1$ eftersom bägge talen är primtal.

Definition 5 *Två heltal a och b är relativt prima om* $\text{sgd}\,(a, b) = 1$.

Exempel: 4 och 21 är relativt prima även om inget av dem är primtal, medan 4 och 2 är inte relativt prima eftersom 2 delar både 2 och 4.

3.1 Moduloräkning

I algoritmen räknar man modulo n, alltså med resterna vid division med n. I stället för likhet mellan två tal, har man kongruens mellan tal som skiljer sig med en multipel av n.

Definition 6 *Att a är kongruent med b modulo n, betecknat $a \equiv b \pmod{n}$, betyder att a och b har samma rest vid division med n.*

Det kan formuleras om till ett ofta använt uttryck:

Sats 7 *Om $a \equiv b \pmod{n}$ så $n|(a-b)$*

Bevis: Enligt definition 6 innebär $a \equiv b \pmod{n}$ att $a = q_1 n + r$ och $b = q_2 n + r$ där q_1 och q_2 är heltal och $r \in [0, n-1]$. Då blir $a - b = (q_1 - q_2)n$, vilket är det samma som $n|(a-b)$. □

Exempel: I kongruensen $1 \equiv 5 \pmod{4}$ är resten 1. I $7 \equiv -3 \pmod{5}$ är resten 2, liksom i $2 \equiv 6 \pmod{4}$.

Nästa steg är att undersöka hur räknereglerna fungerar:

Exempel: Utgående från $1 \equiv 5 \pmod{4}$ och $2 \equiv 6 \pmod{4}$ gäller $1 + 2 \equiv 5 + 6 \pmod{4}$ eftersom $3 \equiv 11 \pmod{4}$.
På liknande sätt kan man gå från $2 \equiv 6 \pmod{4}$ till $0 \equiv 4 \pmod{4}$ eftersom $2 - 2 \equiv 6 - 2 \pmod{4}$.

Så additionen och subtraktionen verkar fungera som vanligt.

Exempel: Om vi utgår från $2 \equiv 5 \pmod{4}$ och multiplicerar bägge leden med 2 får vi $1 \cdot 2 \equiv 2 \cdot 5 \pmod{4}$ vilket är $2 \equiv 10 \pmod{4}$, vilket stämmer.
Studera $2 \equiv 6 \pmod{4}$ vilket är $2 \cdot 1 \equiv 2 \cdot 3 \pmod{4}$ men $1 \not\equiv 3 \pmod{4}$.
Däremot fungerar det att gå från $3 \equiv 27 \pmod{4}$ till $1 \equiv 9 \pmod{4}$

Alltså multiplikationen verkar också fungera som vanligt medan divisionen fungerar bara för vissa tal. Så lagarna för moduloräkning kan formuleras som:

Sats 8 **a** *Om $a \equiv c \pmod{n}$ och $b \equiv d \pmod{n}$ så $a \pm b \equiv c \pm d \pmod{n}$.*

b *Om $a + b \equiv a + d \pmod{n}$ så $b \equiv d \pmod{n}$.*

c *Om $a \equiv c \pmod{n}$ och $b \equiv d \pmod{n}$ så $ab \equiv cd \pmod{n}$.*

d *Om $ac \equiv bc \pmod{n}$ och $\text{sgd}(c, n) = 1$ så $a \equiv b \pmod{n}$*

Bevis:

a Eftersom $n|(a-c)$ och $n|(b-d)$ så $n|(a-c) \pm (b-d)$, vilket ger att $n|a \pm b - (c \pm d)$. Detta ger att $a \pm b \equiv c \pm d \pmod{n}$.

b Om $n|(a+b)-(a+d)$ så $n|b-d$.

c De två givna villkoren kan omvandlas till $n|ab-bc$ och $n|bc-cd$ genom multiplikation. Då gäller att $n|ab-bc+bc-cd$ vilket ger $n|ab-cd$.

d Från den givna förutsättningen fås att $ac = bc+qn$ vilket divideras med c. Det ger att $a = b+\frac{qn}{c}$. Då måste $\frac{qn}{c}$ vara ett heltal. Eftersom $\text{sgd}\,(n,c) = 1$ så måste c dela q och då är $\frac{qn}{c}$ en multipel av n. Alltså $a \equiv b \pmod{n}$.

□

För ett positivt heltal n, låt $\mathbb{Z}_n$ vara mängden $\{0, 1, \ldots, n-2, n-1\}$. Om additionen och multiplikationen utförs modulo n, ligger summorna och produkterna i mängden. Operationerna är alltså slutna.

Eftersom $\text{sgd}(2,4) = 2$ medan $\text{sgd}(3,4) = 1$ så går det inte alltid att dividera med 2 men däremot med 3. Skillnaden mellan elementen 2 och 3 i $\mathbb{Z}_4$ uttrycks på följande sätt:

Definition 9 *En nolldelare är ett element a i $\mathbb{Z}_n$ så att $ab \equiv 0 \pmod{n}$ för något nollskilt b i $\mathbb{Z}_n$.*

Definition 10 *Ett inverterbart element är ett element a i $\mathbb{Z}_n$ så att $ab \equiv 1 \pmod{n}$ för något b i $\mathbb{Z}_n$.*

Exempel: I $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ är 1 och 5 inverterbara element med inverserna 1 och 5 medan 2, 3 och 4 är nolldelare.

För att gå från att räkna modulo n till modulo m där m är en faktor i n används följande lemma:

Lemma 11 *Om $a \equiv b \pmod{n}$ och $m|n$ så är $a \equiv b \pmod{m}$.*

Bevis: Det första villkoret ger att $a - b = k \cdot n$ och det andra att $n = m \cdot c$ så $a - b = k \cdot m \cdot c = k' \cdot m$ där $k' = k \cdot c$. □

Definition 12 *Ordningen för ett tal a modulo n, betecknat $o_n(a)$ är vad man måste upphöja a till för att komma tillbaka till 1 modulo n.*

$$o_n(a) = \min_k\{k : k \in \mathbb{Z}_+, a^k \equiv 1 \pmod{n}\}$$

Exempel: Studera $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Där är $o_5(2) = 4$ eftersom $2^2 = 4$, $2^3 = 8 \equiv 3 \pmod 5$ och slutligen $2^4 = 16 \equiv 1 \pmod 5$. På samma sätt blir $o_5(3) = 4$ medan $o_5(4) = 2$ därför att $4^2 = 16 \equiv 1 \pmod 5$.

Lemma 13 $a^b \equiv 1 \pmod{n}$ *om och endast om* $o_n(a)|b$.

Bevis: Antag att $o_n(a) \not| b$ vilket uttrycks som att $b = k \cdot o_n(a) + r$ där $1 \leq r \leq o_n(a)-1$. Då blir $a^b = a^{k\cdot o_n(a)+r} = \left(a^{o_n(a)}\right)^k \cdot a^r \equiv a^r \pmod n$ eftersom $a^{o_n(a)} \equiv 1 \pmod n$. Då måste $a^r \equiv 1 \pmod n$ vilket är en motsägelse eftersom definitionen är $o_n(a)$ det minsta positiva heltalet k så att $a^k \equiv 1 \pmod n$. Alltså måste r vara 0 och $o_n(a)|b$.

Om $o_n(a)|b$ så är $b = k \cdot o_n(a)$. Då är $a^b = a^{k\cdot o_n(a)} = \left(a^{o_n(a)}\right)^k \equiv 1 \pmod{n}$. □

Här är två lemmor som har att göra med faktorer i ett tal och i ett polynom:

Lemma 14 *Om p är ett primtal så är* $p^a - 1|p^b - 1$ *ekvivalent med att* $a|b$.

Bevis: Förutsättningen kan skrivas som $p^b - 1 = k\,(p^a - 1)$ vilket är samma sak som $p^b \equiv 1 \pmod{p^a - 1}$. Enligt lemma 13 är detta ekvivalent med att $o_{p^a-1}(p)|b$. Genom att forma om definition 12 så får man att $o_{p^a-1}(p) = \min_{k\in\mathbb{Z}_+}\{k : p^a - 1|p^k - 1\}$, vilket måste vara a. Alltså $a|b$. □

Lemma 15 $x^r - 1|x^{rk} - 1$

Bevis: $(x^r)^k = \left((x^r)^{k-1} + (x^r)^{k-2} + \cdots + x^r + 1\right) \cdot (x^r - 1) + 1$. □

Eftersom $\text{sgd}\,(p, n) = 1$ för alla n som inte är en multipel av primtalet p så blir det speciella lagar för räkning $\bmod p$ där p är ett primtal.

Sats 16 $(a+b)^p \equiv a^p + b^p \pmod{p}$ *om* p *är ett primtal.*

Bevis: Binomialutveckling ger $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{(p-i)}$ där binomialkoefficienterna är $\binom{p}{i} = \frac{p \cdot \ldots \cdot (i-p+1)}{i!}$ utom för $i = 0$ och $i = p$ då de är 1. Eftersom p är ett primtal så finns det ingen term i nämnaren som eliminerar p ur täljaren. Då är binomialkoefficienten delbar med p. Alltså $\binom{p}{i} \equiv 0 \pmod{p}$ utom för $i = 0$ och $i = p$. Då blir det bara kvar a^p och b^p från binomialutvecklingen. □

Sats 17 *Fermats lilla sats:* $a^p \equiv a \pmod{p}$ *för alla* $a \in \mathbb{Z}$ *om* p *är ett primtal.*

Bevis: Genom induktion från sats 16 fås att $(a+b+c+\ldots)^p \equiv a^p + b^p + c^p + \ldots \pmod{p}$. Det ger att

$$a^p = \underbrace{(1+1+\ldots+1)^p}_{a \text{ stycken}} \equiv \underbrace{1^p + 1^p + \ldots + 1^p}_{a \text{ stycken}} \equiv a \pmod{p} \; . \; \square$$

.

Slutligen fås följande som är viktigt för rad 8 i algoritmen, som testar likhet mellan två polynom i variabeln x, som genomgående kommer att användas som polynomvariabel.

Sats 18 $(x-a)^p \equiv x^p - a \pmod{p}$ *om* p *är ett primtal.*

Bevis: I binomialutvecklingen är enligt sats 16

$$\binom{p}{i} = \frac{p \cdot \ldots \cdot (i-p+1)}{i!} \equiv 0 \pmod{p} \; \forall \; i \in [1, p-1].$$

Därför försvinner alla termer utom den av högst grad och den av lägst grad, där sats 17, Fermats lilla sats, ger $a^p \equiv a \pmod{p}$. □

3.2 Grupper

För att beskriva hur moduloräkningen fungerar med de olika räknesätten + och ·, börjar jag med att definiera en grupp som är en mängd med bara en operation.

Definition 19 *En grupp $(G, \cdot)$ är en icke-tom mängd G tillsammans med en binär operation $\cdot$ på elementen G så att följande villkor uppfylls:*

Slutenhet: *$\forall a, b \in G$ så är $a \cdot b$ ett entydigt definierat element i G.*

Associativitet: *$\forall a, b, c \in G$ så är $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

Identitet: *Det existerar ett $e \in G$ så att $e \cdot a = a$ och $a \cdot e = a$ för alla $a \in G$.*

Invers: *För alla $a \in G$ existerar det ett element i G betecknat a^{-1} så att $a \cdot a^{-1} = e$ och $a^{-1} \cdot a = e$.*

I denna uppsats är alla grupper abelska, vilket innebär:

Definition 20 *En grupp är abelsk om operationen är kommutativ:*
$\forall a, b \in G$ så är $a \cdot b = b \cdot a$.

Exempel: $(\mathbb{Z}, +)$ är en grupp där identiteten är 0 och inversen till 4 är -4. Däremot är inte $(\mathbb{Z}\backslash\{0\}, \cdot)$ en grupp eftersom bara 1 och -1 har inverser. Inför beteckningen $\mathbb{Z}^\times$ för mängden $\{1, -1\}$. Då blir $(\mathbb{Z}^\times, \cdot)$ en grupp.

$(\mathbb{Q}, +)$ är också en grupp. Alla element i $\mathbb{Q}$ utom 0 har multiplikativa inverser. Därför definierar vi $\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$ och bildar den multiplikativa gruppen. $(\mathbb{Q}^\times, \cdot)$. På samma sätt är $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^\times, \cdot)$ och $(\mathbb{C}^\times, \cdot)$ grupper där $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$ och $\mathbb{C}^\times = \mathbb{C}\backslash\{0\}$.

Dessa grupper är oändliga medan följande exempel har ett ändligt antal element.

$(\mathbb{Z}_4, +)$ där $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ och additionen räknas $(\mathrm{mod}\, 4)$. Då gäller likheterna $2 + 3 = 1$ och $3 + 3 = 2$ i gruppen.

$(\mathbb{Z}_4^\times, \cdot)$ där $\mathbb{Z}_4^\times = \{1, 3\}$. Eftersom $3 \cdot 3 = 9 \equiv 1 \pmod 4$ så är $3^{-1} = 3$ i $(\mathbb{Z}_4^\times, \cdot)$.

$(\mathbb{Z}_5, +)$ där $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ och $1 + 4 = 0$ och $2 + 3 = 0$ så $-1 = 4$ och $-2 = 3$ eftersom inverserna betecknas med minustecken i en additiv grupp.

$(\mathbb{Z}_5^\times, \cdot)$ där $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$ $3 \cdot 2 = 1 \equiv 4 \pmod 5$ så $3^{-1} = 2$ i $(\mathbb{Z}_5^\times, \cdot)$. $4 \cdot 4 = 16 \equiv 1 \pmod 5$ så $4^{-1} = 4$ i $(\mathbb{Z}_5^\times, \cdot)$.

Om vi räknar modulo n har heltalen $\ldots, -2\,n+4, -n+4, 4, n+4, 2\,n+4, \ldots$ samma rest och de motsvarar elementet 4 i gruppen $(\mathbb{Z}_n, +)$. På så sätt har vi en koppling mellan moduloräkningen i stycke 3.1 och beskrivningen med en grupp.

Definition 21 *$(H, \cdot)$ är en delgrupp av $(G, \cdot)$ om H är en delmängd av G och operationen $\cdot$ på elementen i H uppfyller villkoren i definition 19.*

Grupper noteras ofta utan att ange operationen. Så $\mathbb{Z}_4^\times$ avser oftast den multiplikativa gruppen och $\mathbb{Z}_5$ den additiva.

Exempel: Den additiva gruppen $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ har delgrupperna $\{0\}$ (den triviala), $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$ och $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ (sig själv). Den additiva gruppen $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ har inga andra delgrupper än den triviala och sig själv.

Vi har en viktig typ av grupper, de cykliska:

Definition 22 *Den cykliska delgruppen av en grupp G genererad av a definieras som mängden $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.*

Om $G = \langle a \rangle$ för något $a \in G$ så är G en cyklisk grupp och a en generator.

Exempel: Gruppen $(\mathbb{Q}, +)$ är inte cyklisk eftersom den genereras av $\{\frac{1}{n!}\}$ för alla positiva heltal n. Däremot om man fixerar n så är en $\{\frac{1}{n!}\}$ en cyklisk delgrupp.

Däremot är $\mathbb{Z} = \langle 1 \rangle = \{\ldots, a^{-2} = -2, a^{-1} = -1, e = 0, a = 1, a^2 = 2, \ldots\}$ en additiv cyklisk grupp. Här används standardnotationen för cykliska grupper med identitetselementet 0 som e, generatorn 1 som a och operationen multiplikationsliknande. Till exempel är $3 = 3 \cdot 1 = a^3$ där det sista ledet använder standardnoteringen.

Den additiva gruppen $\mathbb{Z}_3 = \{0, 1, 2\}$ genereras också av elementet 1. Eftersom den är ändlig medan $\mathbb{Z}$ är oändlig så krävs det en regel att $1 + 1 + 1 = 0$ vilket är $a^3 = e$ med e som 0 och a som 1. Hela gruppen kan skrivas som $\mathbb{Z}_3 = \langle 1 \rangle = \{e = 0, a = 1, a^2 = 2\}$.

Sats 23 *Alla delgrupper av en cyklisk grupp är cykliska.*

Bevis: Låt G vara en cyklisk grupp med generatorn a, alltså $G = \langle a \rangle$, och låt H vara en godtycklig delgrupp av G.

Om $H = e$ då är $H = \langle e \rangle$ som är cyklisk. Annars finns det ett minsta positivt k så att $a^k \in H$. Då är $\langle a^k \rangle \subseteq H$.

Undersök då om H är en delmängd till $\langle a^k \rangle$ genom att ta ett godtyckligt element $x = a^m \in H$. Dividera m med k så blir det $m = qk + r$ där $0 \leq r < k$ enligt sats 2. Då fås $a^m = a^{qk+r} = (a^k)^q \cdot a^r$. $a^r = (a^k)^{-q} \cdot a^m$, där de två faktorerna tillhör H och produkten som blir a^r måste också tillhöra H. r måste vara 0 för annars det finnas ett element a^r med en mindre exponent än a^k, vilket strider mot förutsättningarna.

Då blir $x = (a^k)^q \in \langle a^k \rangle$ vilket ger att $H \subseteq \langle a^k \rangle$. Då är $H = \langle a^k \rangle$ och därmed cyklisk. □

Definition 24 *Ett element a i en grupp har en ordning som är det minsta positiva heltalet så att $a^m = 1$. Det betecknas $o(a)$.*

Exempel: I gruppen $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ har elementen ordningen 1, 4, 2 respektive 4 eftersom $1 \cdot 0 = 0$, $4 \cdot 1 = 4 \equiv 0 \pmod 4$, $2 \cdot 2 = 4 = 0$ och $4 \cdot 3 = 12 \equiv 0 \pmod 4$. Eftersom det är en additiv grupp är ordningen det tal man behöver multiplicera med för att få additionens neutrala element 0 igen.

Sats 25 *Om G är en ändlig abelsk grupp och a är ett element med den största ordningen så delar varje elements ordning elementet a:s ordning.*

Bevis: Låt a vara ett element som har den största ordningen och x ett godtyckligt element. Antag att det inte gäller, alltså att $o(x) \not| o(a)$. Det kan skrivas som att $o(x) = p^\alpha m$ och $o(a) = p^\beta n$ där $\alpha > \beta$ och p är ett primtal

som varken delar m eller n. Genom att upphöja elementen med en faktor så delas ordningen med samma faktor. Då fås $o(x^m) = p^\alpha$ och $o(a^{p^\beta}) = n$. Eftersom $\text{sgd}(p^\alpha, n) = 1$ blir produktens ordning $o(x^m a^{p^\beta}) = p^\alpha n > p^\beta n = o(a)$. a var ju det största elementet så antagandet är fel. Alltså $o(x)|o(a)$. □

Följdsats 26 *Låt G vara en ändlig abelsk cyklisk grupp med n element och H är en delgrupp till G med m element. Då gäller att m delar n.*

Bevis: Låt a vara G:s generator och a^i H:s generator. $o(a_i)|o(a)$ enligt sats 25. Eftersom grupperna är cykliska gäller att $o(a_i) = m$ och att $o(a) = n$ enligt 25 och därav följer satsen.. □

Definition 27 *Sidoklassen aH till delgruppen $H \subseteq G$, där $a \in G$, är mängden $aH = \{ah : h \in H\}$.*

Exempel: Den additiva gruppen $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ har delgruppen $H = \{0, 3\}$, som har sidoklasserna $0 + H = \{0, 3\}$, $1 + H = \{1, 4\}$ och $2 + H = \{2, 5\}$. Det finns inga fler sidoklasser. Det framgår till exempel av $5 + H = \{5 + 0 = 5, 5 + 3 = 2\} = 2 + H$.

Sats 28 *Om H är en delgrupp av en abelsk grupp G och $aH = cH$ och $bH = dH$ för $a, b, c, d \in G$ så är $abH = cdH$.*

Bevis: $aH = cH$ innebär att för alla $h \in H$ så finns det ett $h' : h' = a^{-1}ch$

$bH = dH$ innebär att för alla $h \in H$ så finns det ett $g' : g' = b^{-1}dg$

$abH = \{abf : f \in G\}$

$abf = abca^{-1}f' = abca^{-1}b^{-1}df'' = cdf''$

Den sista likheten kommer av att gruppen är abelsk. □

Sats 29 *Om H är en delgrupp av en abelsk grupp G då är gruppen av sidoklasser av H en grupp med multiplikationen $aHbH = abH$.*

Bevis: Enligt sats 28 är multiplikationen väldefinierad. Uppfyller den alla villkoren?

Slutenhet: OK
Associativitet: OK
Identitet: H är det neutrala elementet, också betecknat eH, i G/H ty $aHeH = eHaH = eH$.
Invers: $a^{-1}H$ är inversen till aH ty $a^{-1}HaH = a^{-1}aH = eH$.
Kommutativitet: OK

Så då uppfylls alla villkor för en abelsk grupp. □

Denna grupp kallas faktorgruppen i G bestämd av H och betecknas G/H.

Exempel: $\mathbb{Z}_n$ konstrueras som $\mathbb{Z}/n\mathbb{Z}$.

Sats 30 *Om H är en delgrupp med m element av en ändlig abelsk grupp G med n element, har faktorgruppen G/H n/m element.*

Bevis: Definiera avbildningen $f : H \to gH$ som $f(h) = gh$ där $g \in G$ och $h \in H$. Om $f(h_1) = f(h_2)$ så är $gh_1 = gh_2$ och där är $h_1 = h_2$ eftersom g har en invers. Alltså är f injektiv. f är också surjektiv utifrån definitionen. Därför är f bijektiv och H och gH har lika många element.

Varje sidoklass gH utgör en ekvivalensklass med relationen $a \sim b$ om $ab^{-1} \in H$. Relationen är reflexiv eftersom $a \sim a$ i och med att $aa\ -1 = e \in H$, symmetrisk eftersom $(ab^{-1})^{-1} = ba^{-1} \in H$ om $a \sim b$ och slutligen transitiv eftersom om $ab^{-1} \in H$ och $bc^{-1} \in H$ så måste $ab^{-1}bc^{-1} = ac^{-1} \in H$ alltså $a \sim c$.

I en ekvivalensrelation tillhör ett element bara en ekvivalensklass. Då finns det n/m ekvivalensklasser i G/H. □

3.3 Ringar

Det tidigare stycket behandlar grupper och där finns det bara en operation. Om man har två operationer, har man ibland en ring. Då utgör den ena operationen en grupp, men inte den andra.

Definition 31 *En kommutativ ring med etta är en mängd R med två binära operationer $+$ och $\cdot$, ibland benämnda addition respektive multiplikation, som uppfyller följande lagar $\forall\, a, b, c \in R$:*

	$+$	$\cdot$
Slutenhet	$a+b \in R$	$a \cdot b \in R$
Associativitet	$a+(b+c)=(a+b)+c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Identitet	$0+a=a+0=a$	$1 \cdot a = a \cdot 1 = a$
Invers	$\exists -a : a+(-a)=0$	—
Kommutativitet	$a+b=b+a$	$a \cdot b = b \cdot a$
Distributivitet	$a \cdot (b+c) = a \cdot b + a \cdot c$	$(a+b) \cdot c = a \cdot c + b \cdot c$

I denna uppsats är alla ringar kommutativa och har en etta.

Exempel: $\mathbb{Z}_4 = \{0,1,2,3\}$ är en kommutativ ring med etta eftersom $(\mathbb{Z},+)$ är en grupp. Multiplikationen är sluten, associativ, kommutativ och har en etta (som är 1). De distributiva lagarna gäller. För att ta reda på vilka som har inverser kan vi titta på $1 \cdot 1 = 1$, $3 \cdot 3 = 1$ så 1 och 3 är sina egna inverser. Däremot har 2 ingen invers ty $2 \cdot 1 = 2$, $2 \cdot 2 = 0$ och $2 \cdot 3 = 2$. Talet 2 sägs då vara en nolldelare. Definitionerna av inverterbart element och nolldelare i ringen R är liknande som i definitionerna 9 och 10.

Studera $\mathbb{Z}_5 = \{0,1,2,3,4\}$ som också är en kommutativ ring med etta. $1 \cdot 1 = 1$, $2 \cdot 3 = 1$ och $4 \cdot 4 = 1$ så alla nollskilda element har en invers.

$\mathbb{Z}[x]$ består av alla polynom med heltalskoefficienter och är också en kommutativ ring med etta, med vanlig polynomaddition och polynommultiplikation. De enda inverterbara elementen är $\mathbb{Z}[x]^\times = \{1,-1\}$. Notationen $R^\times$ är en mängd av de inverterbara elementen i $R^\times$ med avseende på operationen $\cdot$. Ibland används samma beteckning för den muliplikativa gruppen $(R^\times, \cdot)$.

Då samma sätt som delgrupperna infördes genom definition 21, definierar jag delringar.

Definition 32 *S är en delring till ringen R om S är en delmängd av R och operationerna $+$, $\cdot$ på elementen i S uppfyller villkoren i definition 31.*

Om man kan multiplicera ett element i en delring med ett element utanför delringen och få ett element i delring så har man en särskild sorts delring som kallas ideal.

Definition 33 *Ett ideal I är en icke-tom delmängd till en ring R sådan att $a \pm b \in I$ och $ra \in I$ för alla $a, b \in I$ och $r \in R$.*

De ideal jag använder liknar de cykliska delgrupperna från definition 22 i och med att de genereras av ett enda element.

Definition 34 *Ett principalideal i ringen R är idealet $\langle a \rangle = Ra = \{x \in R : x = ra$ för ett givet $r \in R\}$, där a är ett givet element i R.*

Bevis för att mängden $\langle a \rangle = Ra$ är ett ideal: Elementet a tillhör mängden så den har åtminstone ett element. Om $r_1 a$ och $r_2 a$ tillhör mängden Ra så ligger också $r_1 a \pm r_2 a$ i samma mängd eftersom $r_1 a \pm r_2 a = (r_1 \pm r_2)a$ och $r_1 \pm r_2 \in R$. Antag att b tillhör mängden Ra. Då kan b skrivas som ra där $r \in R$. Så då tillhör även bc mängden Ra eftersom $bc = rac = rca \in R$. Det sista kommer från den kommutativa lagen i en ring och från att multiplikationen i en ring är sluten. Då är alla villkor för ett ideal uppfyllda. □

Exempel: I $\mathbb{Z}_4$ finns det triviala idealet $\{0\} = \langle 0 \rangle$, $\{0, 2\} = \langle 2 \rangle$ och ringen själv $\mathbb{Z}_4 = \langle 1 \rangle$. $2 \cdot 1 = 2$, $2 \cdot 2 = 0$ och $2 \cdot 3 = 2$ så oavsett vad man multiplicerar 2 med så är man kvar i delringen $\{0, 2\}$.

Däremot har $\mathbb{Z}_5$ inga andra ideal än $\{0\}$ och sig själv.

Det finns också för ringar en ekvivalensrelation benämnd kongruens som placerar element i samma kongruensklass om skillnaden mellan dem är en multipel av ett givet element.

Definition 35 *Att elementen a och b i ringen R tillhör samma kongruensklass betecknad $[a]$ eller $[a]_I$ innebär att $a - b \in I$, där I är ett ideal. Man kan också skriva $a \equiv b \pmod{I}$. Mängden av kongruensklasserna betecknas R/I.*

Sats 36 *Mängden av kongruensklasser R/I är en ring.*

Bevis: Additionen av kongruensklasser utgör en grupp enligt sats 29. För att undersöka om multiplikationen är väldefinierad, antag att a och b tillhör en kongruensklass och c och d en annan, alltså att $a - b = k_1 g$ och $c - d = k_2 g$ där k_1 och k_2 tillhör R och g genererar I vilket är samma som att $I = \langle g \rangle$. Studera produkten $a \cdot c$ och övergå till b och d:

$$ac = (b + k_1 g) \cdot (d + k_2 g) = bd + g \cdot (dk_1 + bk_2 + k_1 k_2 g) \equiv bd \pmod{I} .$$

Så multiplikationen beror inte på vilket element ur kongruensklassen som väljs. Multiplikationen har en enhet $1 + I$ och den uppfyller den associativa och den kommutativa lagen eftersom den ärver egenskaper från multiplikationen i R. Det kan illustreras med följande bevis för den distributiva lagen, där man går över till att räkna i R och sedan tillbaka till R/I:

$$[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$$

Alltså uppfyller R/I alla villkor för att vara en ring. □

Exempel: I ringen $\mathbb{Z}$ finns det idealet $n\mathbb{Z}$ där n är ett positivt heltal. Då är $\mathbb{Z}/n\mathbb{Z}$ en ring som består av kongruensklasserna $n\mathbb{Z} = \{\dots, -n, 0, n, \dots\}$, $1 + n\mathbb{Z} = \{\dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots\}$ och så vidare till $n - 1 + n\mathbb{Z} = \{\dots, -n - 1, -1, n-, n + 1, 2n - 1, 3n - 1 \dots\}$.

Då betecknar vi $\mathbb{Z}/n\mathbb{Z}$ med $\mathbb{Z}_n$ och skriver dess element som $\{0, 1, 2, \dots, n - 1\}$ fast det är egentligen kongruensklasser $\{[0], [1], \dots, [n - 1]\}$. Jämför ekvivalensrelationen i beviset till sats 30. En ekvivalensklass motsvarar att $ab^{-1} \in H$ i multiplikationsnotation. Med övergång till additionsnotation är det $a - b \in H$ vilket motsvarar kongruensklassen.

$\mathbb{Z}_4$ kan konstrueras som $\mathbb{Z}/\langle 4\rangle$, vilket är samma sak som $\mathbb{Z}/4\mathbb{Z}$.

Genom att använda sig av att $\mathbb{Z}_p$ är en ring där mängden av alla nollskilda element tillsammans med multiplikation är en cyklisk grupp — vilket visas senare — går det att bevisa Fermats lilla sats på ett nytt sätt.

Nytt bevis av Fermats lilla sats: I stället för att räkna (mod p) kan man räkna i den multiplikativa gruppen $\mathbb{Z}_p^\times = \{1, 2, \dots, p - 1\}$, som är cyklisk enligt sats 43 och kan skrivas $\mathbb{Z}_p^\times = \{e, a, \dots, a^{p-2}\}$ med identitetselementet $e = 1$, generatorn a och villkoret $a^{p-1} = e$ för att få en ändlig grupp. Generatorn a måste väljas så att $o(a) = p - 1$.

Till exempel är $\mathbb{Z}_5^\times = \{1, 2, 3, 4\} = \{1, 2, 2^2 = 4, 2^3 = 3\} = \{1, 3, 3^2 = 4, 3^3 = 2\}$. Så både 2 och 3 kan väljas som generator. Eftersom $4^2 = 1$ är inte 4 en generator.

Satsen gäller för 0. Den gäller också för $b \in \mathbb{Z}_p^\times$, där $b = a^i$ för något heltal i eftersom gruppen är cyklisk. Då blir $b^p = (a^i)^p = a^{ip} = a^{i(p-1)+i} = (a^{p-1})^i \cdot a^i = e^i \cdot a^i = a^i = b$.

Här används $1, 2, \ldots, p-1$ för kongruensklasserna $[1], [2], \ldots, [p-1]$, där exempelvis $[1]$ är mängden $\{\ldots, 1-p, 1, 1+p, \ldots\}$. Då gäller satsen för alla heltal. □

Definition 37 *Karakteristiken för en kommutativ ring med ett är det minsta positiva heltalet k så att $k \cdot 1 = \underbrace{1+1+\ldots 1}_{k \text{ stycken}} = 0$, om det existerar. Om det inte finns något är karakteristiken 0.*

Exempel: Karakteristiken för $\mathbb{Z}_4$ är 4 och för $\mathbb{Z}_5$ är 5. Heltalsringen $\mathbb{Z}$ har karakteristiken 0.

Eftersom vi har två operationer på elementen i ring, är det intressant att studera de avbildningar som bevarar operationerna.

Definition 38 *En homomorfi mellan två ringar R och S är en avbildning ϕ som uppfyller att $\phi(a+b) = \phi(a) + \phi(b) = 0$ och att $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ för alla $a, b \in R$.*

Sats 39 *Om ϕ är en homomorfi mellan ringarna R och S, finns det en bijektiv homomorfi mellan $R/\mathrm{Ker}\,\phi$ och $\phi(R)$.*

Bevis: Med $\mathrm{Ker}\,\phi$ avses nollmängden, alltså mängden av alla element i R som avbildas på 0 i S. Om a och b tillhör $\mathrm{Ker}\,\phi$ tillhör också $a \pm b$ nollmängden $\mathrm{Ker}\,\phi$ eftersom $\phi(a \pm b) = \phi(a) \pm \phi(b) = 0$. Likaså om $a \in \mathrm{Ker}\,\phi$ och $b \in R$ tillhör också $a \cdot b$ nollmängden $\mathrm{Ker}\,\phi$ eftersom $\phi(a \cdot b) = \phi(a) \cdot \phi(b) = 0$. Då är $\mathrm{Ker}\,\phi$ ett ideal enligt definition 33. Enligt sats 36 är $R/\mathrm{Ker}\,\phi$ en ring.

Definiera avbildningen $\bar{\phi} : R/\mathrm{Ker}\ \phi \to \phi(R)$ genom $\bar{\phi}([a]) = \phi(a)$ för $a \in R$. Den är då också en homomorfi.

Antag att $\bar{\phi}([a]) = \bar{\phi}([b])$ fast $[a] \neq [b]$. Det kräver att $\phi(a) = \phi(b)$ fast a och b tillhör olika kongruensklasser. Det är en motsägelse så avbildningen är injektiv. Den är också surjektiv eftersom den fyller naturligtvis upp ϕ:s värdemängd $\phi(R)$. Alltså är homomorfin $\bar{\phi}$ bijektiv. □

3.4 Kroppar

Om en ring har multiplikativa inverser till alla element utom 0 är det en kropp. Man kan också säga att en kropp är en ring som inte har några nolldelare. Det kan formuleras så här:

Definition 40 *En kropp är en mängd F med två operationer $+$ och $\cdot$ där bägge utgör en grupp — där elementet 0 inte räknas med för operationen $\cdot$ — och den distributiva lagen gäller. Det innebär att följande lagar gäller för alla a, b, c i mängden F:*

	$+$	$\cdot$
Slutenhet	$a + b \in F$	$a \cdot b \in F$
Associativitet	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Identitet	$0 + a = a + 0 = a$	$1 \cdot a = a \cdot 1 = a$
Invers	$\exists\, -a : a + (-a) = (-a) + a = 0$	$\exists\, a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 0$
Kommutativitet	$a + b = b + a$	$a \cdot b = b \cdot a$
Distributivitet	$a \cdot (b + c) = a \cdot b + a \cdot c$	$(a + b) \cdot c = a \cdot c + b \cdot c$

Exempel: Den minsta kroppen är $\mathbb{Z}_2 = \{0, 1\}$. $\mathbb{Z}_4$ är inte kropp eftersom elementet 2 inte har någon invers. $\mathbb{Z}_3$ och $\mathbb{Z}_5$ är kroppar.

$\mathbb{Z}$ är ingen kropp eftersom de enda elementen med invers är 1 och -1. $\mathbb{Q}$ och $\mathbb{R}$ är dock kroppar eftersom alla nollskilda element har invers.

För att bestämma hur ändliga kroppar ser ut så utnyttjas definition 37 av en rings karakteristik.

Lemma 41 *En kropp har karakteristiken p där p är ett primtal, eller så har den karakteristiken* 0

Bevis: Karakteristik $k > 0$ innebär att $k \cdot 1 = \underbrace{1 + 1 + \ldots 1}_{k \text{ stycken}} = 0$. Antag att k inte är ett primtal och antag att det kan faktoriseras i två tal $k = l \cdot m$. Då är $(l \cdot 1) \cdot (m \cdot 1) = 0$ och eftersom det inte finns nolldelare i en kropp måste något av l och m vara 0, vilket strider mot att k är det minsta positiva heltalet som ger $k \cdot 1 = 0$ Alltså måste k vara ett primtal eller 0. □

Sats 42 *En ändlig kropp F har p^n element, där p är ett primtal och n ett positivt heltal.*

Bevis: Betrakta avbildningen $\phi : \mathbb{Z} \to F$ definierad av $\phi(n) = n \cdot 1_F$, vilket är summan av n ettor i F. Enligt lemma 41 har F karakteristiken ett tal p, som är ett primtal. Talet p tillhör avbildningens nollmängd Ker ϕ. Eftersom avbildningen är en homomorfi är Ker $\phi = \langle p \rangle$. Då finns det en delkropp av F som kan avbildas bijektivt på $\mathbb{Z}_p$ enligt sats 39.

En ändlig kropp har ett ändligt antal element och då måste dess karakteristik vara p som är ett primtal enligt lemma 41. Betrakta avbildningen $\phi : \mathbb{Z} \to K$ definierad av $\phi(n) = n \cdot 1_K$. Eftersom karakteristiken är ändlig så blir bilden av ϕ en kropp $\mathbb{Z}_p$.

Låt b vara ett element i F som inte ligger i $\mathbb{Z}_p$. Bilda potenserna av b så länge de är linjärt oberoende av varandra. Studera linjärkombinationerna baserade på basen $\{1, b, b^2, \ldots, b^{n-1}\}$ och koefficientmängden $\mathbb{Z}_p$. Dessa linjärkombinationer tillsammans med addition och multiplikation utgör en kropp.

På så sätt kan vi skapa en ändlig kropp K som ett ändligdimensionellt vektorrum över $\mathbb{Z}_p$ vars bas har n element. Det blir totalt p^n element i K. □

Det finns tydligen fler ändliga kroppar än $\mathbb{Z}_p$ där p är ett primtal. Deras konstruktion framgår av nästa stycke. I $\mathbb{Z}_p$ är multiplikationen naturligtvis cyklisk. Det är den också i de andra enligt följande sats.

Sats 43 *Den multiplikativa gruppen av de inverterbara elementen i en ändlig kropp F är cyklisk.*

Bevis: De inverterbara elementen i en ändlig kropp $F = GF(p^n)$ utgör en multiplikativ grupp med $p^n - 1$ element eftersom 0 har ingen invers.

Låt a vara ett element i $F^\times$ som har den största ordningen, vilken betecknas med m, som är begränsad av antalet element så $m \leq p^n - 1$.

Eftersom ordningen för ett godtyckligt element b i $F^\times$ delar m enligt sats 25, är $b^m = (b^{o(b)})^{m/o(b)} = 1^{m/o(b)} = 1$. Det innebär att alla $p^n - 1$ element i $F^\times$ är rötter till $x^m - 1$ som har högst m olika rötter eftersom det är ett polynom över en kropp enligt sats 48. Alltså är $p^n - 1 \leq m$.

Dessa två olikheter ger att $m = p^m - 1$ vilket innebär att gruppen är cyklisk. □

3.5 Polynom

På rad 8 i algoritmen jämföres två polynom och deras koefficienter tillhör $\mathbb{Z}_n$ där n är det heltal som ska testas. Genom lemma 11 kan koefficienterna avbildas på kroppen $\mathbb{Z}_p$ där p är en primtalsfaktor i n. Eftersom en kropp inte har några nolldelare så uppfyller polynom över kroppar en del lagar som polynom över ringar inte uppfyller. Det finns till exempel en divisionsalgoritm som ger ett entydigt resultat.

Sats 44 *För två godtyckliga polynom över kroppen F, $f(x)$ och $g(x)$, där $g(x) \neq 0$, finns det två unika polynom, $q(x)$ och $r(x)$ som tillhör $F[x]$ så att $f(x) = q(x) \cdot g(x) + r(x)$ med $\operatorname{grad} r(x) < \operatorname{grad} g(x)$ eller $r(x) = 0$.*

Bevis: Beteckna $f(x) = a_m x^m + \cdots + a_0$ och $g(x) = b_n x^n + \cdots + b_0$.

Polynomen $q(x)$ och $r(x)$ existerar för alla $m < n$ eftersom man sätter då $q(x) = 0$ och $r(x) = f(x)$.

För att kunna använda induktion antag att detta också gäller för $m - 1$. Ta bort den högsta termen i $f(x)$ genom att sätta $f_1(x) = f(x) - a_m {b_n}^{-1} x^{m-n} g(x)$ eftersom ${b_n}^{-1}$ existerar i och med att b_n är ett nollskilt element i en kropp. Enligt induktionsantagandet är $f(x) = q(x) \cdot g(x) + r(x)$ så då fås

$$f(x) = (q_1(x) + a_m {b_n}^{-1} x^{m-n}) g(x) + r(x).$$

Ovanstående tillhör $F[x]$ eftersom alla termerna tillhör $F[x]$. Då bevisar induktionen existensen av $f(x)$ och $g(x)$.

För att visa entydigheten antag att $f(x) = q_1(x) \cdot g(x) + r_1(x)$ och $f(x) = q_2(x) \cdot g(x) + r_2(x)$. Det ger att $(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x)$. Högerledets grad är högst $\operatorname{grad} g(x) - 1$. Vänsterledets grad är minst $\operatorname{grad} g(x)$ om $q_1(x) \neq q_2(x)$ eftersom produkten av de högsta termerna blir aldrig 0 i och med att det inte finns några nolldelare i en kropp. Så då måste $q_1(x) = q_2(x)$ och därför är $r_1(x) = r_2(x)$. Alltså är $q(x)$ och $r(x)$ entydiga. □

Följande sats kallas restsatsen:

Sats 45 *Om $f(x)$ är ett polynom över kroppen F och c tillhör F så existerar ett unikt polynom $q(x)$ så $f(x) = q(x)(x - c) + f(c)$ där $f(c)$ är värdet av $f(x)$ för $x = c$.*

Bevis: Med $f(x) = a_m x^m + \cdots + a_0$ så fås $f(x) - f(c) = a_m(x^m - c^m) + \cdots + a_1(x - c)$.

Eftersom $x^k - c^k = (x - c) \cdot (x^{k-1} + cx^{k-2} + \cdots + c^{k-2}x + c^{k-1})$ för alla positiva heltal k, så delar $x - c$ högerledet och alltså också vänsterledet: $f(x) - f(c) = (x - c)q(x)$.

Därifrån fås att $f(x) = q(x)(x-c)+f(c)$, vilket är en unik uppdelning enligt sats 44. □

Definition 46 *Om $f(x)$ är ett nollskilt polynom över F och c ett element i F så säges c vara en rot till $f(x)$ om $f(c) = 0$.*

Följdsats 47 *Ett element c i kroppen F är en rot till det nollskilda polynomet $f(x)$ över F om och endast om $(x - c)|f(c)$.*

Bevis: Det följer direkt av sats 45. □

Sats 48 *Om $f(x)$ är ett polynom av graden n över kroppen F så har det högst n olika rötter i F.*

Bevis: Satsen gäller för polynom av graden 0, alltså konstanter skilda från noll. Antag att den gäller för alla polynom av graden $n - 1$. Om c är en av $f(x)$:s rötter, är $f(x) = (x - c)q(x)$ enligt följdsats 47. Där har $q(x)$ högst graden $n - 1$ och enligt antagandet högst $n - 1$ rötter. Då kan $f(x)$ ha högst n olika rötter och induktionen är klar. □

Med polynom definieras kongruensklasser på liknande sätt som för heltal, definition 35 och sats 36. Polynom kan vara irreducibla på samma sätt som heltal kan vara primtal.

Definition 49 *Ett polynom av grad 1 eller högre är irreducibelt om det inte kan faktoriseras icke-trivialt.*

På samma sätt som i definition 4 går det att definiera den största gemensamma delaren till två polynom och den uppfyller följande:

Lemma 50 *Varje linjärkombination av två nollskilda polynom $a(x)$ och $b(x)$ över en kropp F är en multipel av* $\text{sgd}(a(x), b(x))$.

Bevis: Beteckna mängden av linjärkombinationer av $a(x)$ och $b(x)$ som $I = \{c(x) \cdot a(x) + d(x) \cdot b(x) : c(x),\, d(x) \in F[x]\}$. I har då ett nollskilt element $e(x)$ som har den lägsta graden. Antag att det nollskilda polynomet $f(x)$ tillhör I. Genom divisionsalgoritmen, sats 44, kan $f(x)$ skrivas som $f(x) = q(x) \cdot e(x) + r(x)$ där $\text{grad}\, r(x) < \text{grad}\, e(x)$ eller $r(x) = 0$. Eftersom $e(x)$ har den lägsta graden av alla nollskilda polynom, måste $r(x)$ vara 0. Alla element i I är multipler av det nollskilda polynomet av lägst grad, $e(x)$.

Ovanstående medför att $e(x)$ är en delare till alla polynom i mängden I och därför en gemensam delare till $a(x)$ och $b(x)$. Studera nu $g(x)$ som också är en gemensam delare till $a(x)$ och $b(x)$. Eftersom $e(x)$ tillhör I så är $e(x) = e_1(x) \cdot a(x) + e_2(x) \cdot b(x)$ där $e_1(x)$ och $e_2(x)$ tillhör $F[x]$. Av detta följer att $g(x)$ delar $e(x)$. Alltså är $e(x)$ den största gemensamma delaren. □

Irreducibla polynom fungerar på liknande sätt som primtal vad gäller kongruensklasser enligt följande sats:

Sats 51 *$F[x]/\langle p(x)\rangle$ är en kropp om $p(x)$ är irreducibel.*

Bevis: $F[x]/\langle p(x)\rangle$ är en kommutativ ring med etta enligt sats 36. Antag att $a(x)$ är ett nollskilt polynom vars grad är mindre än $p(x)$ och låt $a(x)$ vara en representant för restklassen $[a(x)]$ i $F[x]/\langle p(x)\rangle$. Eftersom $p(x)$ är irreducibel är $sgd(a(x), p(x)) = 1$. Det ger enligt lemma 50 ger att det finns två polynom $b(x)$ och $c(x)$ så att $b(x)a(x)+c(x)p(x) = 1$, alltså är $b(x)a(x) \equiv 1 \pmod{p(x)}$ och $[a(x)]$ och $[b(x)]$ är varandras inverser. Då är $F[x]/\langle p(x)\rangle$ en kropp eftersom alla nollskilda element har en invers. □

På det här sättet går det att konstruera ändliga kroppar med p^n element. Om man vill ha 2^3 element så tar man $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ eller $\mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle$.

På rad 8 räknar man modulo $x^r - 1$. För att kunna räkna i en kropp måste detta polynom faktoriseras. Följande sats anger faktorernas grad. Med $o_r(p)$ menas ordningen av p modulo r.

Sats 52 *Polynomet $x^r - 1$ i $\mathbb{Z}_p[x]$, där p och r är primtal, kan faktoriseras som $(x-1) \cdot f_1(x) \cdot \cdots \cdot f_k(x)$ där $k = \frac{r-1}{o_r(p)}$ och polynomen $f_j(x)$ är irreducibla och har graden $o_r(p)$, för $j = 1, \cdots, k$.*

Bevis: Låt $f(x)$ vara en irreducibel faktor i $x^r - 1$ som inte är $x - 1$. Eftersom $f(x)$ är irreducibelt så är ringen $\mathbb{Z}_p[x]/\langle f(x)\rangle$ en kropp enligt sats 51. Beteckna kroppen med F och studera elementet x i F och dess ordning. Eftersom $f(x)|x^r - 1$ så är $x^r \equiv 1 \pmod{f(x)}$, vilket ger att $x^r = 1$ i kroppen F och så därför $o(x)|r$. Eftersom r är ett primtal kan x:s ordning bara vara 1 eller r. Fallet $o(x) = 1$ svarar mot att $x = 1$ i kroppen F vilket är att $x \equiv 1 \pmod{f(x)}$. I så fall måste $f(x) = x - 1$, vilket uteslöts i början. Alltså är $o(x) = r$.

Välj nu det element i $F[x]/\langle p(x)\rangle$ som har den största ordningen och beteckna detta a. Då är $o(a) = p^{\text{grad } f(x)} - 1$ eftersom $(F[x]/\langle p(x)\rangle)^\times$ har $p^{\text{grad } f(x)} - 1$ element och är cyklisk enligt sats 43. Elementet x har ordningen r som relateras till den största ordningen $o(a)$ som $r|p^{\text{grad } f(x)} - 1$ enligt sats 25. Det kan skrivas om som $p^{\text{grad } f(x)} \equiv 1 \pmod{r}$. Lemma 13 ger att $o_r(p)|\text{ grad } f(x)$.

Enligt sats 42 kan a skrivas som:

$$a = \sum_{i=0}^{\text{grad } f(x)-1} a_i\, x^i \quad \text{där } \mathrm{a_i} \in \mathbb{Z}_\mathrm{p}$$

a upphöjt till p blir enligt satserna 16 och 17 i de två sista likheterna:

$$a^p = \left(\sum_{i=0}^{\text{grad } f(x)-1} a_i\, x^i \right)^p = \sum_{i=0}^{\text{grad } f(x)-1} {a_i}^p\, x^{p\,i} = \sum_{i=0}^{\text{grad } f(x)-1} a_i\, x^{p\,i}$$

Genom att fortsätta att upphöja detta till p får man:

$$a^{p^{o_r(p)}} = \sum_{i=0}^{\text{grad } f(x)-1} a_i \left(x^i\right)^{p^{o_r(p)}} = \sum_{i=0}^{\text{grad } f(x)-1} a_i \left(x^{p^{o_r(p)}}\right)^i = \sum_{i=0}^{\text{grad } f(x)-1} a_i\, x^i = a$$

Den näst sista likheten följer av att $p^{o_r(p)} = 1 + K \cdot r$ enligt definitionen av ordning och att $x^r = 1$ enligt det första stycket. Lemma 14 ger att $o(a)|p^{o_r(p)} - 1$, vilket är samma sak som att $p^{\text{grad } f(x)} - 1|p^{o_r(p)} - 1$. Lemma 14 ger då att grad $f(x)|o_r(p)$.

Eftersom graden och ordningen delar varandra gäller att grad $f(x) = o_r(p)$. □

Exempel: I ringen $\mathbb{Z}_2[x]$ är $x^5 - 1 = (x-1) \cdot (x^4 + x^3 + x^2 + x + 1)$. Där finns följden $\{2, 2^2 = 4, 2^3 = 8 \equiv 3 \pmod{5}, 2^4 = 16 \equiv 1 \pmod{5}\}$ i $\mathbb{Z}_5$ så $o_5(2) = 4$. I stället så är $x^7 - 1 = (x-1) \cdot (x^4 + x^3 + x^2 + x + 1) = (x-1) \cdot (x^3 + x^2 + 1) \cdot (x^3 + x + 1)$. Den senare uppdelningen beror på att det finns följden $\{2, 2^2 = 4, 2^3 = 8 \equiv 1 \pmod{7}\}$ i $\mathbb{Z}_7$.

På samma sätt för $\mathbb{Z}_3$ så kan $x^{11} - 1$ delas upp i $x - 1$ och två faktorer av graden 5, liksom $x^{13} - 1$ i $x - 1$ och fyra faktorer av graden 3 eftersom $o_{11}(3) = 5$ och $o_{13}(3) = 3$.

Kapitel 4

Algoritmens komplexitet

I detta kapitel går jag igenom algoritmens komplexitet. Jag använder mig ofta av beteckningen $\mathcal{O}(\lg^a n)$, vilket innebär att antalet räkneoperationer i ett steg är proportionellt mot $\lg^a n$. Med räkneoperationer avser jag multiplikationer eller divisioner, eftersom additioner och subtraktioner går betydligt snabbare. Talen är flyttal eller heltal inom datorns normala storlek. Notationen $\tilde{\mathcal{O}}(\lg^b n)$ är samma sak som $\mathcal{O}(\lg^b n \cdot f(\lg \lg n))$ där f är ett polynom. Jag börjar med att gå igenom detaljer för de olika raderna i algoritmen. Sedan bestämmer jag en gräns för r:s storlek. Slutligen räknar jag samman alla rader.

4.1 Operationers tid

Lemma 53 *Multiplikation och division av två heltal mindre än n kräver $\tilde{\mathcal{O}}(\lg n)$ operationer.*

Förklaring: De två heltalen har $\lg n$ siffror. En direkt multiplikation kräver således $\lg^2 n$ operationer. Schönhage och Strassen har hittat på en snabbare algoritm, som tar bara $\tilde{\mathcal{O}}(\lg n)$ [SS71] [Knu97, s 306–311]. När man har en snabb metod för att multiplicera, kan man också använda den för att dividera. Tiden det tar är då en konstant gånger tiden för motsvarande multiplikation [Knu97, s 313].

Följdsats 54 *Multiplikation av två polynom av graden r tar tiden $\tilde{\mathcal{O}}(r \lg r)$.*

Bevis: Antalet koefficienter r motsvarar antalet siffror i n vilket är $\lg n$. Lemma 53 med $\lg n$ ersatt av r ger $\tilde{\mathcal{O}}(r \lg r)$. □

Lemma 55 *Beräkningen av a^x tar $\mathcal{O}(\lg x)$ multiplikationer.*

Bevis: För att beräkna a^x bestämmer man $a^{2^{\lfloor \lg x \rfloor}}, a^{2^{\lfloor \lg x \rfloor - 1}}, \ldots, a^4, a^2, a$ vilket kräver $\lfloor \lg x \rfloor$ multiplikationer. Det kan visas genom induktion eftersom a^2 kräver 1 multiplikation och om $a^{2^i - 1}$ har krävt $i - 1$ stycken så fås $a^{2^i} = a^{2^{i-1}} \cdot a^{2^{i-1}}$ med i multiplikationer. Då har man $\lfloor \lg x \rfloor$ potenser av a. Om man väljer ut dem enligt x:s binära representation och multiplicerar dem får man x^a. Eftersom nu krävs det högst $\lfloor \lg x \rfloor - 1$ multiplikationer blir det totalt $\mathcal{O}(\lg x)$ multiplikationer. □

Lemma 56 *Beräkningen av $sgd(n, r)$ med Euklides' algoritm tar $\tilde{\mathcal{O}}(\lg^2 n)$.*

Bevis: Den första beräkningen i Euklides' algoritm är att dividera n med r som ger en ny rest r_1. Sedan divideras r med r_1 och det ger en ny rest r_2. Det fortsätter tills resten blir 0. Resultatet är då den sista kvoten.

Antalet steg blir maximalt om n och r är två på varandra följande Fibonaccital. Då kommer algoritmen att gå neråt längs Fibonacciföljden. Det blir $O(\lg n)$ steg eftersom det i:te Fibonaccitalet kan uppskattas trivialt till $\mathcal{O}(2^n)$. I varje steg sker det en division där talen måste representeras som flera minnesceller, $\mathcal{O}(\lg n)$ stycken. Det blir åtminstone en multiplikation i divisionen och den tar då $\tilde{\mathcal{O}}(\lg n)$. Om det blir flera multiplikationer minskas antalet steg med minnescellens storlek. Denna minskning är snabbare än antalet extra multiplikationer.

Så det blir $\tilde{\mathcal{O}}(\lg^2 n)$. □

Lemma 57 *Primtalspotenstestet tar $\tilde{\mathcal{O}}(\lg^3 n)$.*

Bevis: Det gäller att beräkna $n^{1/2}, n^{1/3}, n^{1/4}, \ldots$ med tillräcklig noggrannhet för att kunna kontrollera om de är heltal. Det blir $\mathcal{O}(\lg n)$ tal att dra roten ur. Varje rotutdragning görs exempelvis med Newton-Raphsons metod som kräver lika många steg som antalet siffror, så det blir $\mathcal{O}(\lg n)$ igen. Eftersom varje steg tar $\tilde{\mathcal{O}}(\lg n)$ så blir det totalt $\tilde{\mathcal{O}}(\lg^3 n)$. □

4.2 Storleken på r

Både algoritmens riktighet och komplexitet beror på att den hittar ett r på rad 4 och att det går snabbt. Kraven på r är att det är ett primtal, att n inte har några faktorer mindre än eller lika med r och att r inte delar N. Det kan skrivas om som ett villkor för ordningen av n modulo r.[1]

Lemma 58 $o_r(n) \geq 4\lceil \lg n \rceil^2$

Bevis: På rad 2 beräknas $N = (n-1)(n^2-1)\cdots(n^{4\lceil \lg n \rceil^2 - 1} - 1)$ som r inte ska dela. Eftersom r är ett primtal så får r inte dela någon av faktorerna. Att $r \not| n^i - 1$ innebär att $n^i \not\equiv 1 \pmod r$. Det gäller för $1 \leq i \leq 4\lceil \lg n \rceil^2 - 1$. Enligt definitionen är $o_r(n)$ det minsta i som kan uppfylla att $n^i \equiv 1 \pmod r$ och ordningen måste vara minst $4\lceil \lg n \rceil^2$. □

Man kan göra en överskattning av N.

Lemma 59 $N < 2^{8\lceil \lg n \rceil^4 \lg n}$

Bevis: Omformning av uttrycket för N ger med $x = 4\lceil \lg n \rceil^2$:

$$N = (n-1)(n^2-1)\cdots(n^{x-1}-1) < n \cdots n^{x-1} = n^{x(x-1)/2} < n^{x^2/2} = 2^{x^2 \lg n/2}$$

□

För att ha en produkt att jämföra N med utnyttjar jag ett lemma som kommer från Tjebysjev [HW45, s 345–346].

Lemma 60 *Produkten av alla primtal upp till* $2n$ *är större än eller lika med* 2^n*:*

$$\prod_{p_i \leq 2n} p_i \geq 2^n$$

[1] I originalartikeln [AKS02] används ett annat men likvärdigt sätt att hitta ett r så att $o_r(n)$ överskrider en viss gräns. Denna gräns är dock annorlunda eftersom slingvariabeln a på rad 7 går igenom ett annat intervall.

Bevis:

1. Lemmat gäller för $n \leq 16$ vilket kontrolleras med hjälp av beräkningar ($2 \geq 2^1$, $2 \cdot 3 \geq 2^2$, $2 \cdot 3 \cdot 5 \geq 2^3$, $2 \cdot 3 \cdot 5 \cdot 7 \geq 2^5$ $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \geq 2^6$ och $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \geq 2^8$).

2. Utgå från definitionen av binomialkoefficienten, fördubbla nämnarens termer och kompensera i täljaren:

$$\binom{2n}{n} = \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdots (2n-1) \cdot 2n}{(2 \cdot 4 \cdots 2n)^2} \cdot 2^{2n} = \frac{1 \cdot 3 \cdots (2n-1)}{2 \cdot 4 \cdots 2n} \cdot 2^{2n}$$

   Termerna kan grupperas på följande sätt:

$$\frac{1}{\sqrt{2}} \cdot \frac{3}{\sqrt{2} \cdot \sqrt{4}} \cdot \frac{5}{\sqrt{4} \cdot \sqrt{6}} \cdots \underbrace{\frac{2n-1}{\sqrt{2n-2} \cdot \sqrt{2n}}}_{= \frac{2n-1}{\sqrt{(2n-1)^2-1}} > 1} \cdot \frac{1}{\sqrt{2n}} \cdot 2^{2n}$$

   Genom att alla bråk utom det första och det sista är större än 1 får vi en underskattning av binomialkoefficienten:

$$\binom{2n}{n} > \frac{2^{2n}}{\sqrt{4n}} = 2^{2n - \lg(4n)/2}$$

3. För att överskatta binomialkoefficienten räknar vi antalet gånger som p delar $n!$:

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^m} \right\rfloor$$

   där m är den största potensen av p som finns i n, alltså $m = \left\lfloor \frac{\lg n}{\lg p} \right\rfloor$. Talet $\left\lfloor \frac{n}{p} \right\rfloor$ är antalet multiplar av p som finns bland alla tal upp till n. De multiplar som också är multiplar av p^2 räknas en ytterligare gång genom att lägga till $\left\lfloor \frac{n}{p^2} \right\rfloor$. Då kan vi uttrycka binomialkoefficienten som en produkt av alla primtal till $2n$ upphöjda till antalet gånger som de förekommer.

$$\lg \binom{2n}{n} = \underbrace{\sum_{p_i \le 2n} \lg p_i}_{\text{själva faktorn}} \cdot \sum_{j=1}^{\left\lfloor \frac{\lg 2n}{\lg p_i} \right\rfloor} \underbrace{\left(\left\lfloor \frac{2n}{{p_i}^j} \right\rfloor - 2 \left\lfloor \frac{n}{{p_i}^j} \right\rfloor \right)}_{\text{antalet gånger: 0 eller 1}}$$

Nu delar vi upp den andra summan i fallet $j = 1$ och i resten. I fallet $j = 1$ överskattas summanderna i den inre summan till 1.

$$\lg \binom{2n}{n} \le \sum_{p_i \le 2n} \lg p_i + \sum_{p_i \le \sqrt{2n}} \lg p_i \sum_{j=2}^{\left\lfloor \frac{\lg 2n}{\lg p_i} \right\rfloor} \underbrace{\left(\left\lfloor \frac{2n}{{p_i}^j} \right\rfloor - 2 \left\lfloor \frac{n}{{p_i}^j} \right\rfloor \right)}_{0 \text{ eller } 1}$$

Nu står $\sum_{p_i \le 2n} \lg p_i$ i högerledet, vilket är den summa som vi vill ha. Då försöker vi överskatta den högre termen och där sätter vi den inre summanden till 1.

$$\lg \binom{2n}{n} \le \sum_{p_i \le 2n} \lg p_i + \sum_{p_i \le \sqrt{2n}} \underbrace{\lg p_i \left(\frac{\lg 2n}{\lg p_i} - 1 \right)}_{\le \lg 2n - 1 \le \lg 2n}$$

Genom en ytterligare överskattning av parentesen eftersom $\lg p_i \ge 1$ blir det:

$$\lg \binom{2n}{n} \le \sum_{p_i \le 2n} \lg p_i + \sum_{p_i \le \sqrt{2n}} \lg(2n) - 1$$

Genom att antalet primtal upp till $\sqrt{2n}$ är högst $\sqrt{2n}/2$ stycken får vi en överskattning av binomialkoefficienten:

$$\lg \binom{2n}{n} \le \sum_{p_i \le 2n} \lg p_i + \frac{\sqrt{2n} \lg 2n}{2} - \frac{\sqrt{2n}}{2}$$

4. Sammanställ dessa gränser för binomialkoefficienten:

$$2n - \frac{\lg 4n}{2} < \lg \binom{2n}{n} \le \sum_{p_i \le 2n} \lg p_i + \frac{\sqrt{2n} \lg 2n}{2} - \frac{\sqrt{2n}}{2}$$

Omformning ger:

$$\lg \prod_{p_i \leq 2n} p_i = \sum_{p_i \leq 2n} \lg p_i > 2n - \frac{\lg 4n}{2} - \frac{\sqrt{2n}\lg 2n}{2} + \sqrt{2n}2$$

För $n \geq 16$ är $2n - \frac{\lg 4n}{2} - \frac{\sqrt{2n}\lg 2n}{2} + \sqrt{2n}2 \geq n$ eftersom insättning av $n = 16$ ger att $32 - 3 - \sqrt{2} \cdot 2(5-1) = 29 - 8\sqrt{2} > 16$ och uttryckets derivata är $2 - \frac{1}{2n} - \frac{1}{2\sqrt{2n}}(\lg 2n + 1)$ som är större än 1 för alla $n \geq 16$.

□

Sats 61 *Storleken på det r som bestäms av raderna 3–6 begränsas av $\mathcal{O}(\lg^5 n)$.*

Bevis: Lemmorna 59 och 60 ger tillsammans med $m = 8\lceil \lg n \rceil^4 \lg n$:

$$N < 2^{8\lceil \lg n \rceil^4 \lg n} = 2^m \leq \prod_{p_i \leq 2m} p_i$$

Då finns det ett primtal $r \leq 2m = 16\lceil \lg n \rceil^4 \lg n$ som inte delar N eftersom produkten av alla primtal upp till $2m$ är större än N. Alltså är r begränsad av $\mathcal{O}(\lg^5 n)$. □

4.3 Sammantagen komplexitet

Genom att gå igenom algoritmen rad för rad beräknas dess komplexitet:

1 $\tilde{\mathcal{O}}(\lg^3 n)$ för primtalspotenstest
2 $\tilde{\mathcal{O}}(\lg^5 n)$ för beräkningen av N
3 slinga r gånger
4 $\tilde{\mathcal{O}}(\lg^2 n)$ för Euklides' algoritm
5 $\tilde{\mathcal{O}}(\sqrt{r}\lg r)$ för primtalstest och $\tilde{\mathcal{O}}(\lg^5 n)$ för N-division
6
7 slinga r gånger
8 $\tilde{\mathcal{O}}(r \lg^2 n)$ för upphöjning

9

På rad 1 har lemma 57 använts och på rad 4 lemma 56. För primtalstestet har den grundläggande metoden använts, att testa alla tänkbara faktorer ända till $\sqrt{r}$.

För att beräkna N behöver man ha $n, n^2, n^3, \ldots, n^{4\lceil \lg n \rceil^2 - 1}$. Enligt lemma 55 kan man räkna ut $n, n^2, n^4, \ldots, n^{2^k}$, där $k = \lfloor \lg(4\lceil \lg n \rceil^2 - 1) \rfloor$, med $\mathcal{O}(\lg \lg n)$ multiplikationer. Sedan ska varje potens n^i, där $i \in [1, 4\lceil \lg n \rceil^2 - 1]$ beräknas genom multiplikation av potenserna där exponenten är en 2-potens valda enligt binärrepresentation av exponenten i.

Antalet multiplikationer begränsas därför av antalet ettor i alla binära tal med k siffror. Det är sammanlagt $k \cdot 2^k/2$ stycken, så antalet multiplikationer är $\mathcal{O}(\lg^2 n \lg \lg n)$. Varje multiplikation tar $\tilde{\mathcal{O}}(\lg^3 n)$ så totalt blir det $\tilde{\mathcal{O}}(\lg^5 n)$ för att beräkna faktorerna i N. Det är ingen idé att multiplicera ihop dem eftersom på rad 7 ska man testa om N delas av r. Där är det $4\lceil \lg n \rceil^2 - 1$ faktorer att testa och den största storleken är $\tilde{\mathcal{O}}(\lg^3 n)$. Totalt tar det också $\tilde{\mathcal{O}}(\lg^5 n)$.

På rad 8 sker det en upphöjning, som blir flera multiplikationer av polynom vars högsta grad är r och vars koefficienter är mindre än n. Med hjälp av lemmorna 55, 54 och 53 blir det sammantaget $\mathcal{O}(\lg n) \cdot \mathcal{O}(r \lg r) \cdot \mathcal{O}(\lg n \lg \lg n) = \tilde{\mathcal{O}}(r \lg^2 n)$.

Sats 62 *Algoritmens komplexitet är* $\tilde{\mathcal{O}}(\lg^{12} n)$.

Bevis: Algoritmen består av tre delar, där den första, primtalspotenstestet, tar $\tilde{\mathcal{O}}(\lg^3 n)$. Nästa del är r-slingan, som gås igenom r gånger och som varje gång tar $\tilde{\mathcal{O}}(\sqrt{r} \lg r) + \tilde{\mathcal{O}}(\lg^2 n)$. Då tar den $\tilde{\mathcal{O}}(r^{3/2} \lg r) + \tilde{\mathcal{O}}(r \lg^2 n)$. Sist kommer testslingan som gås igenom r gånger vilket ger $\tilde{\mathcal{O}}(r^2 \lg^2 n)$.

Enligt sats 61 är r begränsad av $\mathcal{O}(\lg^5 n)$. Sätt in det i r- och testslingans komplexitet. Då dominerar testslingan över r-slingan och primtalspotenstestet och för hela algoritmen blir komplexiteten $\tilde{\mathcal{O}}(\lg^{12} n)$. □

Kapitel 5

Algoritmens korrekthet

I detta kapitel visar jag att algoritmen är korrekt, alltså att den ger rätt svar både när talet är ett primtal och när det är sammansatt. I stället för $(\text{mod } n, x^r - 1)$ skriver jag att beräkningarna sker i ringen $\mathbb{Z}_n[x]/\langle x^r - 1\rangle$. Med A avser jag mängden av heltalen $[1, r]$.

Sats 63 *Om n är ett primtal svarar algoritmen PRIMTAL.*

Bevis: Eftersom n är ett primtal kan inte algoritmen avslutas med SAMMANSATT på rad 1.

Om n är ett primtal finns det inget tal r som uppfyller $1 < r < n$ och som delar n. Då är $\text{sgd}\,(r, n) = 1$ och algoritmen ger inte SAMMANSATT på rad 4.

Enligt sats 18 är det vänstra och det högra ledet på rad 8 lika och algoritmen kan inte ge SAMMANSATT.

Det finns bara ett möjligt svar kvar PRIMTAL på rad 9. □

Beviset för att algoritmen svarar rätt för ett sammansatt tal är ett omfattande motsägelsebevis, som består av tre delar. Den första delen är en omformulering av villkoren för att algoritmen ska svara PRIMTAL för ett sammansatt tal.

Antagande 64 *n är ett sammansatt tal men algoritmen ger ändå PRIMTAL vilket innebär att:*

$(x-a)^n = x^n - a \; \forall a \in A \; i \; \mathbb{Z}_n[x]/\langle x^r - 1\rangle$

Enligt sats 61 hittar algoritmen alltid ett r så att `medan`-slingan i algoritmen avslutas. Då uppfylls ovanstående villkor från rad 8 i algoritmen. Dessa likheter ska jag använda för att visa att n måste då vara ett primtal, vilket strider mot antagandet.

Låt p vara en primtalsfaktor i n. Då ger antagande 64 att:

Lemma 65 $(x-a)^n = x^n - a \; \forall a \in A \; i \; \mathbb{Z}_p[x]/\langle x^r - 1\rangle$

Bevis: Eftersom avbildningen från $\mathbb{Z}_n[x]/\langle x^r - 1\rangle$ till $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ är att räkna alla koefficienter $(\mathrm{mod}\, p)$, bevaras likheter. □

Nästa del är att studera en uppställning av $m = p^i n^j$ för $i, j \geq 0$. Om n är en primtalspotens, $n = p^k$, då finns det två olika par, (i_1, j_1) och (i_2, j_2), sådana att $p^{i_1} n^{j_1} = p^{i_2} n^{j_2}$. Resten av beviset handlar om att visa att det finns två sådana par.

Ovanstående lemma 65 är något som undersöks av algoritmen och som gäller för n. Motsvarande gäller alltid för p enligt lemma 18. Jag vill visa att liknande gäller för $p^i n^j$. För att kunna använda induktion studerar jag om likheten gäller för en produkt om den gäller för faktorerna.

Lemma 66 *Om* $(x-a)^{m_1} = x^{m_1} - a$ *och* $(x-a)^{m_2} = x^{m_2} - a$ *gäller* $\forall a \in A$ *i* $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ *så gäller att* $(x-a)^{m_1 m_2} = x^{m_1 m_2} - a \; \forall a \in A$ *i* $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$.

Bevis: Alla likheter gäller för alla $a \in A$ och i ringen $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ om inte annat anges. Den första förutsättningen ger att $(x-a)^{m_1 m_2} = ((x-a)^{m_1})^{m_2} = (x^{m_1} - a)^{m_2}$. Sätt in x^{m_1} i stället för x i den andra förutsättningen och det ger $(x^{m_1} - a)^{m_2} = x^{m_1 m_2} - a$ för alla $a \in A$ och i ringen $\mathbb{Z}_p[x]/\langle x^{rm_1} - 1\rangle$. Det går att gå tillbaka till $\mathbb{Z}_p[x]/\langle x^r - 1\rangle$ eftersom $x^r - 1 | x^{rm_1} - 1$ och då kan det kopplas ihop med den första förutsättningen. □

Då kan jag bevisa genom induktion att:

Sats 67 $(x-a)^m = x^m - a \; \forall \; a \in A \; i \; \mathbb{Z}_p[x]/\langle x^r - 1\rangle$

Bevis: Ett första steg är att det gäller för $m = p^0 n^0 = 1$.

I nästa steg multiplicerar man med p respektive n. Då konstaterar man att om satsen gäller för $m = p^{i-1}n^j$ gäller den också för $m = p^i n^j$ enligt lemma 66 och lemma 18. På samma sätt så om satsen gäller för $m = p^i n^{j-1}$ så gäller den också för $m = p^i n^j$ enligt lemma 66 och antagande 64.

Enligt induktion gäller då satsen för alla $m = p^i n^i$ där i, j är icke-negativa heltal. □

Följdsats 68 $(x^k - a)^m = x^{km} - a \ \forall \ a \in A \ \forall \ k \in \mathbb{Z}_+ \ i \ \mathbb{Z}_p[x]/\langle x^r - 1\rangle$

Bevis: Utgå från sats 66 och ersätt x med x^k där k är ett positivt heltal. Det ger att $(x^k - a)^m = x^{km} - a \ \forall \ a \in A \ \forall \ k \in \mathbb{Z}_+$ i $\mathbb{Z}_p[x]/\langle x^{kr} - 1\rangle$. Satsen följer eftersom $x^r - 1 | x^{kr} - 1$ enligt lemma 15. □

Det är intressant att studera $p^i n^j \pmod r$ eftersom $m = p^i n^j$ är en exponent till polynom i x och dessa polynom räknas modulo $x^r - 1$.

Lemma 69 *Definiera den multiplikativa gruppen $S = \mathbb{Z}_r^\times / \langle p, n\rangle$ och låt d vara antalet element i S. Då kan varje $b \in \mathbb{Z}_r^\times$ skrivas som $sp^i n^j$ där s tillhör S och i, j är icke-negativa heltal. Då är också $o_r(n) \leq \frac{r-1}{d}$.*

Bevis: Definiera $\langle p, n\rangle = \{b \in \mathbb{Z}_r^\times : b \equiv p^i n^j \pmod r\}$, som är en delgrupp av $\mathbb{Z}_r^\times$. Då kan vi skapa faktorgruppen $S = \mathbb{Z}_r^\times / \langle p, n\rangle$ med d element, där $d = \frac{r-1}{|\langle p,n\rangle|}$ enligt sats 30, vilket ger att $|\langle p, n\rangle| = \frac{r-1}{d}$. Faktorgruppen S består ju av sidoklasserna till $\langle p, n\rangle$ så varje element i $\mathbb{Z}_r^\times$ är produkten av ett element i S och ett element i $\langle p, n\rangle$.

Delgruppen $\langle p, n\rangle$ har i sin tur en delgrupp $\langle n\rangle$ med $o_r(n)$ element. Det ger att $o_r(n)$ delar $|\langle p, n\rangle|$ enligt följdsats 26. Därför har vi att $o_r(n) = |\langle n\rangle| \leq |\langle p, n\rangle| = \frac{r-1}{d}$. □

Nu letar jag efter ett $m_1 = p^{i_1} n^{j_1}$ och ett $m_2 = p^{i_2} n^{j_2}$ i uppställningen där $m_2 = m_1 + kr$. De ska vara lika även om exponenterna är olika. Det räcker med att begränsa sig i frågan om storleken på m_1 och m_2.

Sats 70 *Det finns m_1 och m_2 där $m_1 = p^{i_1} n^{j_1}$, $m_2 = p^{i_2} n^{j_2}$, $i_1, i_2, j_1, j_2 \in \left[0, \sqrt{\frac{r-1}{d}}\right]$, $(i_1, j_1) \neq (i_2, j_2)$ och $m_2 = m_1 + kr$ där k är ett heltal.*

Bevis: Antalet tänkbara olika par (i,j) är $\left(1+\left\lfloor\sqrt{\frac{r-1}{d}}\right\rfloor\right)^2$, vilket är större än $\left(1+\sqrt{\frac{r-1}{d}}-1\right)^2=\frac{r-1}{d}$, medan antalet olika möjliga m räknat modulo r är $\frac{r-1}{d}$ som är storleken på $\langle p,n\rangle$ enligt lemma 69. Så det finns fler par än tal modulo r och då enligt Dirichlets lådprincip finns det två tal $m_1=p^{i_1}n^{j_1}$ och $m_2=p^{i_2}n^{j_2}$ där $(i_1,j_1)\neq(i_2,j_2)$ som är lika modulo r alltså $m_2=m_1+kr$ för något heltal k. □

Fixera nu dessa två tal m_1 och m_2 och de uppfyller följande:

Sats 71 $(x^s-a)^{m_1}=(x^s-a)^{m_2}\ \forall\, a\in A,\forall\, s\in S$ *i* $\mathbb{Z}_p[x]/\langle x^r-1\rangle$

Bevis: Utgå från sats 67 för m_2 och sätt in relationen mellan m_1 och m_2 ur sats 70 :

$$(x^s-a)^{m_2}=x^{s\cdot m_2}-a=x^{s(m_1+kr)}-a=x^{s\cdot m}\cdot\left(x^r\right)^{s\cdot k}-a$$

Fortsätt med lemma 15 och sats 67 för m_1 så fås slutligen att:

$(x^s-a)^{m_2}=x^{s\cdot m_1}-a=(x^s-a)^{m_1}\ \forall\, a\in A$ och $\forall\, s\in S$ i $\mathbb{Z}_p[x]/\langle x^r-1\rangle$ □

Nu går jag över från en ring till en kropp.

Sats 72 $(x-a)^{m_1}=(x-a)^{m_2}\ \forall\ a\in A$ *i* $\mathbb{Z}_p[x]/\langle h(x)\rangle$ *med* $\operatorname{grad} h(x)=o_r(p)$

Bevis: Enligt sats 52 har polynomet x^r-1 en irreducibel faktor $h(x)$ med graden $o_r(p)$. Då går det att avbilda ringen $\mathbb{Z}_p[x]/\langle x^r-1\rangle$ på sin delring $\mathbb{Z}_p[x]/\langle h(x)\rangle$ som är en kropp. Då bevaras likheter. □

Nu har jag kommit till den tredje delen av beviset. Ovanstående likhet gäller i en kropp och där är multiplikationen cyklisk så skillnaden mellan m_1 och m_2 är en multipel av storleken på den multiplikativa delgruppen där likheten gäller. Denna delgrupp behöver inte innehålla alla nollskilda element i kroppen $\mathbb{Z}_p[x]/\langle h(x)\rangle$ eftersom likheten inte nödvändigtvis gäller för alla element. Om jag kan visa att delgruppens storlek är större än både m_1 och m_2 måste de vara lika.

Beteckna med G den delgrupp av $\mathbb{Z}_p[x]/\langle h(x)\rangle^\times$ vars element g uppfyller $g^{m_1}=g^{m_2}$. Till G hör alla polynom $x-a$ för alla $a\in A$ liksom produkterna av dessa. För att beräkna en undre gräns för G:s storlek används följande lemma:

Lemma 73 *Definiera en avbildning från* $\mathbb{Z}_p[x]$ *till* $(\mathbb{Z}_p[x]/\langle h(x)\rangle)^d$ *genom* $e(x) \mapsto (e(x^{s_1}), e(x^{s_2}), \ldots, e(x^{s_d}))$ *där* $s_1, s_2, \ldots, s_d$ *är alla element i* $S = \mathbb{Z}_r^\times/\langle p, n\rangle$. *Den är injektiv för elementen* $e(x) = \prod_{a\in A}(x-a)^{e_a}$ *där* e_a *är icke-negativa heltal och* $\sum_{a\in A} e_a \leq r-2$.

Bevis: Antag att $e(x) = \prod_{a\in A}(x-a)^{e_a}$ och att $f(x) = \prod_{a\in A}(x-a)^{f_a}$ eller $f(x) = 0$, där $\sum_{a\in A} e_a \leq r-2$ och $\sum_{a\in A} f_a \leq r-2$ liksom att $e(x) \neq f(x)$ och $e(x^s) = f(x^s)$ i $\mathbb{Z}_p[x]/\langle h(x)\rangle$ för alla $s \in S$.

Då fås att $e(x^s)^{p^i n^j} = \prod_{a\in A}(x-a)^{p^i n^j e_a} = \prod_{a\in A}\left(x^{p^i n^j} - a\right)^{e_a} = e(x^{sp^i n^j})$ enligt följdsats 68 liksom på samma sätt att $f(x^s)^{p^i n^j} = f(x^{sp^i n^j})$. Alltså är $e(x^{sp^i n^j}) = f(x^{sp^i n^j})$. Alla likheter gäller i $\mathbb{Z}_p[x]/\langle h(x)\rangle$ för alla s i S och alla icke-negativa heltal i och j.

Om $e(x)$ och $f(x)$ är konstanta måste de vara lika. Studera annars $g(x) = e(x) - f(x)$. Eftersom $sp^i n^j \pmod r$ genererar hela $\mathbb{Z}_p^\times$ fås att $g(x^u) = 0$ i $\mathbb{Z}_p[x]/\langle h(x)\rangle$ för alla $u \in \mathbb{Z}_p^\times$. Detta är samma sak som att $g(y^u) = 0$ i $(\mathbb{Z}_p[y]/\langle h(y)\rangle)[x]$ eftersom man räknar varje term modulo $h(x)$ i stället för hela polynomet. Rötterna y^u är distinkta eftersom de tillhör en kropp med $1 + k\cdot r$ element där k är ett positivt heltal enligt definitionen av ordning. Så $g(x)$ som polynom över $\mathbb{Z}_p[y]/\langle h(y)\rangle$ har minst $r-1$ rötter eftersom varken 0 eller 1 räknas med. Enligt definitionen har $g(x)$ högst graden $r-2$. Det motsäger sats 48, så antagandet stämmer inte utan $f(x) = g(x)$ och avbildningen är injektiv. □

Sats 74 $m_1 = m_2 + k\cdot N$ *där* $k \in \mathbb{Z}$ *och* $N \geq 2^\ell$.

Bevis: Börja med att undersöka hur många element i $(\mathbb{Z}_p[x]/\langle h(x)\rangle)^d$ som uppfyller ekvationen i sats 72. Enligt lemma 73 är alla produkter av formen $e = \prod_{a\in A}(x-a)^{e_a}$ där $e_a \leq 0$ och $\sum_{a\in A} e_a \leq r-2$ distinkta. Deras antal är antalet r-tupler av icke-negativa heltal vars summa är högst $r-2$. Lägg då till ett ytterligare tal så att summan blir $r-2$.

Antalet $r+1$-tupler av icke-negativa heltal vars summa är $r-2$ är antalet sätt att placera $r-2$ likadana bollar (motsvarar ettor) $r+1$ olika lådor (motsvarar de olika elementen a i mängden och slasken, det som saknas till graden $r-2$). Det är samma sak som antalet permutationer av $r-2$ likadana element av en sort och r likadana element av en annan sort. De r elementen är då avskiljningar mellan de $r+1$ lådorna. Dessutom tillkommer nollvektorn.

$$|\,(\mathbb{Z}_p[x]/\langle h(x)\rangle)^d\,| > \frac{(2r-2)!}{(r-2)!\,r!} = \frac{2r-2}{r}\cdot\frac{2r-3}{r-1}\cdot\frac{2r-4}{r-2}\cdot\cdots\cdot\frac{r}{2}\cdot\frac{r-1}{1} > 2^{r-1}$$

Om man tar ut en term 2 ur de första $r-1$ faktorerna så får man $2-\frac{2}{r}$, $2-\frac{1}{r-1}$, 2, $2+\frac{1}{r-3}$, $\ldots$, $2+\frac{r-4}{2}$. För $r \geq 3$ så kompenserar den sista faktorn för de två första faktorerna som är mindre än 2. Delgruppens storlek N är då:

$$N \geq |\mathbb{Z}_p[x]/\langle h(x)\rangle| > 2^{\frac{r-1}{d}}$$

□

Nästa steg är att studera hur stora m_1 och m_2 är jämfört med delgruppens storlek.

Sats 75 $m_1 = m_2$.

Bevis: Studera storleken på m_1 och m_2 och jämför den med N:

$$m_i \leq p^{\lfloor\sqrt{\frac{r-1}{d}}\rfloor} n^{\lfloor\sqrt{\frac{r-1}{d}}\rfloor} \leq n^{2\sqrt{\frac{r-1}{d}}} = 2^{2\sqrt{\frac{r-1}{d}}\lg n}$$

Eftersom $2\lg n \leq 2\lceil\lg n\rceil < \sqrt{o_r(n)}$ enligt lemma 58 och $o_r(n) \leq \frac{r-1}{d}$ så fås att:

$$m_i < 2^{\sqrt{\frac{r-1}{d}\cdot o_r(n)}} < 2^{\frac{r-1}{d}}$$

Detta är mindre än delgruppens storlek N, alltså måste m_1 vara lika med m_2. □

Sats 76 *Om n är ett sammansatt tal svarar algoritmen SAMMANSATT.*

Bevis: Antagande 64, att den ändå svarar PRIMTAL leder fram till att $m_1 = m_2$ enligt sats 75. Det kan skrivas om som att $n = p^k$, där k måste vara 1, n måste vara ett primtal, eftersom en primtalspotens skulle ha upptäckts

på rad 1. Det ger en motsägelse mot antagande 64 så algoritmen svarar SAMMANSATT. □

Då har jag gått igenom de två fallen: primtal och sammansatt tal och kan komma till en slutsats.

Sats 77 *Om n är ett primtal, svarar algoritmen PRIMTAL annars svarar den SAMMANSATT.*

Bevis: Enligt sats 63 gör algoritmen rätt om det är ett primtal och enligt sats 76 om det är ett sammansatt tal. □

Litteraturförteckning

[AKS02] Manindra Agrawal, Neeraj Kayal och Nitin Saxena. PRIMES in P. http://www.cse.iitk.ac.in/users/manindra/primality_original.pdf eller http://www.cse.iitk.ac.in/users/manindra/primality_v6.pdf i omarbetad version, augusti 2002.

[AM93] A. O. L. Atkin och F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, juli 1993.

[APR83] L.M. Adleman, C. Pomerance och R. S. Rumely. On distinguishing prime numbers from composite numbers. *Annals of Mathematics*, 117, 1983.

[BB96] John A. Beachy och William D. Blair. *Abstract algebra*. Waveland Press, 1996.

[Ber] Daniel J. Bernstein. Proving primality after Agrawal-Kayal-Saxena. http://cr.yp.to/papers/aks.pdf.

[Cal] Chris Caldwell. The prime pages. http://primes.utm.edu/.

[Car] Phil Carmody. The AKS "PRIMES in P" algorithm resource. http://fatphil.org/maths/AKS/.

[Chr75] Stig Christofferson. *Grupper, ringar, kroppar*. LiberLäromedel/ Gleerup, 1975.

[EG02] Kimmo Eriksson och Hillevi Gavel. *Diskret matematik och diskreta modeller*. Studentlitteratur, 2002.

[Gil] George Gilbert. The polynomial time algorithm for testing primality. http://faculty.tcu.edu/ggilbert/primality/AKSTalk.pdf.

[HW45] Godfrey H. Hardy och Edward M. Wright. *An introduction to the theory of numbers*. Clarendon press, 1945.

[Knu97] Donald Knuth. *The Art of Computer Programming*, band 2, Seminumerical algorithms. Addison-Wesley, 1997.

[Mau94] U. E. Maurer. Fast generation of prime numbers and secure public-key cryptographic parameters. *Journal of Cryptololgy*, 3, 1994.

[Mil76] G. L. Miller. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13:300–317, 1976.

[Rab80] M. O. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12:128–138, 1980.

[Rie94] Hans Riesel. *Prime numbers and computer methods for factorization*. Birkhäuser, 1994.

[Smi02] Peter Smith. Prime numbers. *Dr. Dobb's Journal*, ss 93–95, juli 2002.

[SS71] Arnold Schönhage och Volker Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7:281–292, 1971.

[Sti] Anton Stiglic. The PRIMES is in P little FAQ. http://crypto.cs.mcgill.ca/~stiglic/PRIMES_P_FAQ.html.

[Tho91] Jan Thompson. *Wahlström & Widstrands matematiklexikon*. Wahlström & Widstrand, 1991.

Internet-referenserna besöktes senast den 11 maj 2006.