MA1301 Tallteori — Høsten 2014 — Oversikt over pensumet

Richard Williamson

3. desember 2014

Innhold

Pensumet

Pensumet for eksamen er forelesningsnotatene: Kapittel 1 – Kapittel 6. Alle øvingene er relevante for eksamen.

Generelle råd

Hvordan bør jeg forberede meg?

Det viktigste er å kunne løse alle oppgavene i øvingene listet nedenfor i de delene av dette dokumentet som handler om de individuelle kapitlene i forelesningsnotatene, og å

kunne løse alle repetisjonsoppgavene som blir lagt ut. Benytt løsningene som har blitt lagt ut for å se hvordan besvarelene dine kan forbedres.

Du kan også øve deg på oppgaver fra tidligere eksamener. Ikke alle av disse oppgavene er relevante: mer spesifikk informasjon er igjen gitt i de delene av dette dokumentet som handler om de individuelle kapitlene av forelesningsnotatene.

Oppgavene i øvingene og repetisjonsoppgavene bør prioriteres over oppgavene fra tidligere eksamener. Jeg vil understreke at det ikke er nok er fokusere på kun å løse for eksempel oppgavene på eksamen fra i fjor.

Legg ikke for mye vekt på Øving 1 – Øving 3. Vanligvis er det ikke flere enn én oppgave på eksamen som ligner på oppgavene i disse øvingene: resten av oppgavene på eksamen blir basert på oppgaver i Øving 4 - Øving 11.

Hvis du ikke er fortrolig med en god del av kurset, anbefaler jeg at du følger rådet mitt i delen «Hva kan jeg gjøre for å bestå?» nedenfor.

Hva slags oppgaver blir det på eksamen?

Oppgavene på eksamen kommer til å ligne på oppgavene i øvingene listet nedenfor i de delene som handler om de individuelle kapitlene i forelesningsnotatene.

Bør vi pugge forelesningsnotatene?

Det er ikke nødvendig å pugge proposisjonene, teoremene, osv, i forelesningsnotatene. Målet med eksamen er å eksaminere forståelsen din, ikke hukommelsen din.

Derimot må de viktigste definisjonene og resultatene huskes. Hvis du imidlertid har gjort en god innsats for å forstå forelesningsnotatene og å prøve å løse oppgavene i øvingene, blir dette ikke noe problem.

Mer spesifikk informasjon om definisjonene og resultatene som behøves er gitt i de delene av dette dokumentet som handler om de individuelle kapitlene av forelesningsnotatene. Symbolet ✓ betyr at noe må huskes. Symbolet ✗ betyr at noe er viktig, men må ikke huskes: hvis det dukker opp på eksamen, blir det gitt. Hvis verken symbolet ✓ eller symbolet ✗ brukes, finnes det en forklaring.

Hva kan jeg gjøre for å bestå?

Alle kan bestå kurset, og målet mitt er at alle som har gjort en god innsats (og det er de aller fleste) kommer til å gjøre dette. Jeg anbefaler at du først og fremst fokusere på følgende temaer.

(1) Hvordan løse «vis uten å regne ut at noe er delelig med noe» oppgaver.

(2) Hvordan løse lineære diofantiske ligninger, lineære kongruenser, og kvadratiske kongruenser. Hvordan bestemme om et heltall er en kvadratisk rest modulo et primtall ved å regne ut Legendresymboler.

(3) Hvordan benytte RSA-algoritmen for å kryptere og dekryptere meldinger.

(4) Hvordan benytte det kinesiske restteoremet i praksis.

(5) Hvordan gjennomføre bevis ved induksjon.

Typiske oppgaver om (2) – (4) kan løses ved å benytte metoder som alltid virker. Hvis du gjør en god innsats og øver deg så mye som mulig på å løse disse typiske oppgavene, bør det derfor ikke være et problem å løse en hvilken som helst lignende oppgave på eksamen. Typiske oppgaver om (1) kan også til en stor grad løses ved å benytte metoder som alltid virker, og typiske oppgaver om (5) følger et felles mønster.

Jeg kommer til å legge ut repetisjonsmateriale for å hjelpe med å få en oversikt over disse temaene: hvilke metoder gjelder hvor, og hvordan de gjennomføres. Dette materialet kan være utgangspunktet for å lese ved behov i forelesningsnotatene for å finne flere eksempler, for å se på teorien som fastslår at metodene virker, osv.

Du kan få en C, eventuelt en enda bedre karakter, ved å løse disse fire typene oppgaver. Hvis du har vanskeligheter med å løse disse fire typene oppgaver, ta kontakt med meg. Da kommer jeg til å tilby jeg ekstra hjelp.

Øv deg igjen og igjen på så mye oppgaver om disse temaene som mulig.

Hva kan jeg gjøre for å få en A eller en B?

Først og fremst: bli fortrolig med temaene (1) – (5) listet i den foregående delen. Du må kunne løse oppgaver om disse temaene fort og nesten uten feil. I tillegg er følgende tema svært viktig.

(6) Hvordan gjennomføre bevis at det finnes uendelig mange primtall med bestemte egenskaper: for eksempel som er kongruent til 3 modulo 4.

Vi har sett rundt seks eksempler på slike bevis i løpet av kurset. Det er viktig at du kan gjennomføre disse bevisene selv. Jeg gir aldri en oppgave på eksamen som er akkurat den samme som et resultat eller en oppgave i kurset, men hvis du har en virkelig god forståelse av metoden, bør du kunne tilpasse den til å løse en oppgave som du ikke har sett før.

Er temaene som ble eksaminert på midtsemesterprøven relevante?

Ja! Oppgaver som ligner på de i midtsemesterprøven kan dukke opp.

Dette er kanskje litt annerledes fra tidligere år. Studentene som tar kurset som fjernundervisning hadde ikke en midtsemesterprøve, og jeg synes at det er viktig at de får muligheten til å vise deres kunnskap om de første delene av kurset.

Bruk ord!

En rekke symboler er ikke en gyldig løsning til en oppgave! Forklar hva du gjør *ved å bruke ord*. Du kommer svært sjeldent til å få alle poengene for en løsning om det ikke er noen ord for å knytte argumentet ditt sammen.

Det er spesielt viktig å bruke ord når du gjennomfører et bevis ved induksjon. For mer om dette, se ≪Andre kommentarer≫ i delen ≪Kapittel 1≫ nedenfor.

Kapittel 1

Hovedtemaene

(1) Hvordan gjennomføre et bevis ved induksjon. Dette gjelder alle variantene av induksjon.

(2) Hvordan definere en sekvens av heltall ved rekursjon.

Det viktigste

I dette kapittelet finnes det mange proposisjoner om de naturlige tallene og om Fibonaccitallene. Mange av disse proposisjonene er ikke så veldig viktige i seg selv: det viktigste er at du forstår hvordan induksjon benyttes for å bevise dem.

De proposisjonene og definisjonene som er viktige i seg selv er listet opp i følgende tabell.

Referanse	Handler om	Må huskes?
Definisjon 1.1.1 og Definisjon 1.1.3	Naturlige tall og heltall	✓
Terminologi 1.4.2	Induksjon	Du blir ikke bedt om å gi denne abstrakte fremstillingen av induksjon, men må forstå den. Det vil si at du må fortstå og huske hvordan oppskriften i Terminologi 1.4.2 benyttes i praksis.
Notasjon 1.6.1	Summetegn	Det er ikke nødvendig å huske den abstrakte fremstillingen, men du må forstå og huske hvordan notasjonen benyttes i praksis.
Definisjon 1.8.1	Fakultet	✓
Definisjon1.9.2	Binomialkoeffisient	✗

Referanse	Handler om	Må huskes?
Proposisjon 1.9.18	Pascals formel	✗
Proposisjon 1.9.30	Binomialteoremet	✗
Terminologi 1.10.2	Rekursjon	Du blir ikke bedt om å gi denne abstrakte fremstillingen av rekursjon, men må forstå den. Det vil si at du må fortstå og huske hvordan oppskriften i Terminologi 1.10.2 benyttes i praksis.
Definisjon 1.11.1	Fibonaccitall	✗
Proposisjon 1.12.9	Binets formel	✗
Terminologi 1.13.2	Varianter av induksjon	Du blir ikke bedt om å gi denne abstrakte fremstillingen av varianter av induksjon, men må forstå den. Det vil si at du må fortstå og huske hvordan oppskriften i Terminologi 1.13.2 benyttes i praksis.

Relevante oppgaver i øvingene

Alle oppgavene Øving 1 – Øving 3 er relevante, men de viktigste og mest relevante for eksamen er følgende.

(1) Oppgave 2 – 4 i Øving 1.

(2) Oppgave 4 i Øving 2.

(3) Oppgave 1 og Oppgave 3 – 5 i Øving 3.

Relevante repetisjonsoppgaver

Kommer snart!

Relevante oppgaver i tidligere eksamener

(1) Oppgave 6, Høsten 2011.

(2) Oppgave 4, Våren 2005.

Relevante oppgaver i midtsemesterprøver

(1) Oppgave 1, 2014.

(2) Oppgave 1, 2013.

(3) Oppgave 1, 2012.

(4) Oppgave 2, 2008.

(5) Oppgave 2, 2007.

Andre kommentarer

(1) Det er svært viktig å fremstille et bevis ved induksjon på en klar måte. Du må skrive uttrykkelig at:

   (a) du benytter induksjon;

   (b) du sjekker om utsagnet er sant i ett tilfelle (eller flere tilfeller, om du benytter én av de variantene av induksjon hvor $c > 0$);

   (c) du antar at utsagnet er sant for et gitt naturlig tall m (eller flere naturlige tall, eller flere tilfeller, om du benytter én av de variantene av induksjon hvor $c > 0$), og benytter denne antakelsen for å vise at utsagnet er sant for $m + 1$.

   Med andre ord, må ordene «sjekke(r)», «induksjon», og «anta(r)» dukke opp et eller annet sted i besvarelesen din!

(2) Husk at rekursjon og induskjon går hand i hand! For å bevise noe om en sekvens som har blitt definert ved rekursjon, for eksempel sekvensen av Fibonaccitall, er det sannsynlig at induksjon behøves.

   I tillegg behøves nesten alltid, eventuelt flere ganger, regelet i definisjonen av sekvensen ved rekursjon:

$$u_{m+1} = u_m + u_{m-1}$$

   for sekvensen av Fibonaccitall.

Kapittel 2

Hovedtemaene

(1) Divisjonsalgoritmen og hvordan den gir muligheten til å dele i flere tilfeller et bevis for et utsagn om heltall.

(2) Euklids algoritme og hvordan den gir muligheten til å finne heltall u og v slik at

$$d = ul + bn,$$

hvor l og n er gitte heltall og $d = \mathsf{sfd}(l, n)$.

(3) Lineære diofantiske ligninger og hvordan begrepet «største felles divisor» og Euklids algoritme gir muligheten til å få en komplett forståelse for dem.

Det viktigste

Referanse	Handler om	Må huskes?
Definisjon 2.1.1	Absoluttverdien	✓
Lemma 2.2.5, Proposisjon 2.2.6, Korollar 2.2.11, Proposisjon 2.2.15, Korollar 2.2.20, Merknad 2.2.17, Merknad 2.2.21	Divisjonsalgoritme	Utsagnene må huskes, men ikke bevisene.
Proposisjon 2.4.2, Proposisjon 2.4.9, Proposisjon 2.4.16	Hvordan divisjonsalgoritmen benyttes i praksis	Proposisjonene er ikke spesielt viktige i seg selv, og må ikke huskes. Du må imidlertid kunne benytte divisjonsalgoritmen for å gjennomføre lignende argumenter.
Definisjon 2.5.1 og Notasjon 2.5.2	Delbarhet	✓
Alle resultatene i §2.5	Grunnleggende proposisjoner om delbarhet	Utsagnene i disse resultatene må huskes, men de er logiske og du er vant til dem fra før, så dette bør ikke være et problem.

Referanse	Handler om	Må huskes?
Definisjon 2.6.1 og Notasjon 2.6.2	Største felles divisor	✓
Merknad 2.6.3, Proposisjon 2.6.12, Korollar 2.6.15, Korollar 2.6.18, Proposisjon 2.6.21, Korollar 2.6.24	Grunnleggende proposisjoner om største felles divisor	Utsagnene i disse resultatene må huskes, men de er logiske, så dette bør ikke være et problem.
Lemma 2.7.3, Korollar 2.7.7, Merknad 2.7.8, Merknad 2.7.15, Korollar 2.7.20	Euklids algoritme og algoritmen for å finne heltall u og v slik at $$d = ul + vn,$$ hvor l og n er gitte heltall og $d = \mathsf{sfd}(l, n)$	Det er ikke nødvendig utsagnene i disse resultatene og bevisene deres, men det er svært viktig å kunne gjennomføre de to algoritmene.
Terminologi 2.9.2	Lineære diofantiske ligninger	✓
Proposisjon 2.9.4	Hvordan finne en løsning til en lineær diofantisk ligning	Det er svært viktig å kunne finne en løsning til en lineær diofantisk ligning i praksis. Det er ikke nødvendig å huske det formelle utsagnet i proposisjonen eller dets bevis.
Korollar 2.9.12	Når en lineær diofantisk ligning har en løsning	Utsagnet må huskes, men ikke beviset.
Korollar 2.9.22	Hvordan finne alle løsningene til en lineær diofantisk ligning	Det er svært viktig å kunne finne alle løsningene til en lineær diofantisk ligning i praksis. Det er ikke nødvendig å huske det formelle utsagnet i proposisjonen eller dets bevis.
Korollar 2.10.20	Den største felles divisoren til et par Fibonaccitall	✗

Relevante oppgaver i øvingene

De meste relevante og viktigste oppgavene i øvingene er følgende.

(1) Oppgaver 1 – 4 i Øving 4. Imidlertid anbefaler jeg at du bruker modulær aritmetikk istedenfor divisjonsalgoritmen direkte for å svare på disse oppgavene: svaret ditt blir dermed kortere og mer elegant.

(2) Oppgave 2 og Oppgave 4 i Øving 5.

(3) Oppgaver 1 – 2 i Øving 6.

Relevante repetisjonsoppgaver

Oppgave 10 – 11.

Relevante oppgaver i tidligere eksamener

(1) Oppgave 1, Høsten 2013.

(2) Oppgave 5 (a), Våren 2011.

(3) Oppgave 1 (a), Høsten 2005.

(4) Oppgave 1, Våren 2005.

(5) Oppgave 1 (a), Våren 2004.

(6) Oppgave 1, Høsten 2003.

Relevante oppgaver i midtsemesterprøver

(1) Oppgave 2, 2014.

(2) Oppgave 3, 2014.

(3) Oppgave 2, 2013.

(4) Oppgave 2, 2012.

(5) Oppgave 1, 2011.

(6) Oppgave 3, 2010.

(7) Oppgave 1, 2009.

(8) Oppgave 2, 2009.

(9) Oppgave 1, 2007.

(10) Oppgave 1, 2006.

(11) Oppgave 2, 2006. (Vanskeligere).

Andre kommentarer

Når ett av l og n er negativt, vær forsiktig når du finner heltall u og v slik at

$$d = ul + nv,$$

hvor l og n er gitte heltall og $d = \mathsf{sfd}(l, n)$. Benytt først algoritmen i Merknad 2.7.15 for å finne u' og v' for $|l|$ og $|n|$, og så gjør følgende:

(a) hvis l er negativ og n er positiv, la $u = -u'$ og $v = v'$;

(b) hvis l er positiv og n er negativ, la $u = u'$ og $v = -v'$;

(c) hvis både l og n er negative, la $u = -u'$ og $v = -v'$.

Se beviset for Korollar 2.7.20 og eksemplene som følger det.

Det er avgjørende at du kommer fram til de riktige u og v når vi finner en løsning til en lineær diofantisk ligningen hvor minst én av koeffisientene er negativ.

Kapittel 3

Hovedtemaene

(1) Algebraiske manipulasjoner med kongruenser.

(2) Lineære kongruenser og hvordan vi kan løse dem.

Det viktigste

Referanse	Handler om	Må huskes?
Definisjon 3.1.2 og Notasjon 3.1.6	Kongruent modulo n	✓

Referanse	Handler om	Må huskes?
Alle resultatene i §3.2	Grunnleggende proposisjoner om kongruens	Utsagnene må huskes, men vi benytter dem hele tida i modulær aritmetikk, så det bør ikke være et problem. Ikke glem Proposisjon 3.2.54, som vi for eksempel benytter ofte i bevis at det finnes uendelig mange primtall med bestemte egenskaper.
Proposisjon 3.3.2, Proposisjon 3.3.3, Proposisjon 3.3.4, Proposisjon 3.3.5, Proposisjon 3.3.6, Proposisjon 3.3.14	Hvordan de grunnleggende proposisjonene om kongruens kan benyttes i praksis for å for eksempel vise at noe er delelig med noe.	Proposisjonene er ikke spesielt viktige i seg selv, og må ikke huskes. Du må imidlertid kunne benytte modulær aritmetikk for å gjennomføre lignende argumenter.
Terminologi 3.4.2	Lineær kongruens	✓
Proposisjon 3.4.5	Å løse en lineær kongruens er det samme som å løse en lineær diofantisk ligning.	✓
Proposisjon 3.4.9	Når en lineær kongruens har en løsning	✓
Merknad 3.4.49 og proposisjonene den refererer til. Se også Merknad 3.4.52.	Hvordan løse en lineær kongruens, og hvordan finne alle løsningene.	Det er ikke nødvendig å huske merknadene og proposisjonene og deres bevis, men det er svært viktig å kunne løse lineære kongruenser i praksis.

Relevante oppgaver i øvingene

(1) Oppgave 3 – 6 i Øving 6.

(2) Oppgave 1 i Øving 7.

(3) Oppgave 5 i Øving 7.

Relevante repetisjonsoppgaver

Oppgave 3 og Oppgave 12.

Relevante oppgaver i tidligere eksamener

(1) Oppgave 2, Høsten 2012.

(2) Oppgave 4 (a), Høsten 2012.

(3) Oppgave 5, Våren 2011.

(4) Oppgave 5 (a), Våren 2005.

(5) Oppgave 6, Høsten 2004.

(6) Oppgave 4 (a), Høsten 2003.

Relevante oppgaver i midtsemesterprøver

(1) Oppgave 4, 2014.

(2) Oppgave 4, 2012.

(3) Oppgave 1, 2010.

(4) Oppgave 3, 2008.

(5) Oppgave 3, 2006. *Tips*: Benytt aritmetikk modulo 10.

Andre kommentarer

Når du blir bedt om å vise at for eksempel

$$3 \equiv 5 \pmod{2},$$

bør besvarelesen din inkluderer følgende observasjoner:

(a) $3 - 5 = -2$;

(b) $2 \mid -2$.

Det er ikke nødvendig å forklare hvorfor $2 \mid -2$, men du kan gjerne gjøre det, ved å observere at $-2 = (-1) \cdot 2$.

Kapittel 4

Hovedtemaene

(1) Primtallsfaktoriseringer og aritmetikkens fundamentalteorem.

(2) Det finnes uendelig mange primtall og varianter.

(3) Fermats lille teorem

(4) Orden og primitive røtter.

(5) Wilsons teorem.

Det viktigste

Referanse	Handler om	Må huskes?
Definisjon 4.1.1	Primtall	✓
Proposisjon 4.2.12 og Korollar 4.2.19	Dersom et primtall deler et produkt, deler det ett av leddene.	Utsagnene må huskes, men ikke beviset.
Teorem 4.3.3 og Teorem 4.7.2		
	Aritmetikkens fundamentalteorem	Utsagnet i Teorem 4.3.3 må huskes, men ikke utsagnet i Teorem 4.7.2, og ingen av bevisene.
Merknad 4.3.13	Hvordan finne en primtallsfaktorisering	Det er svært viktig å kunne finne en primtallsfaktorisering til et naturlig tall i praksis, men det er ikke nødvendig å følge metoden i Merknad 4.3.13 eksakt for å gjøre dette.
Teorem 4.4.2	Det finnes uendelig mange primtall	Det er svært viktig at du forstår beviset og kan gjennomføre det selv.

Referanse	Handler om	Må huskes?
Proposisjon 4.4.9	Det finnes uendelig mange primtall som er kongruent til 3 modulo 4	Det er svært viktig at du forstår beviset og kan gjennomføre det selv.
Proposisjon 4.5.2 og Proposisjon 4.5.7	Vis at noe er delelig med noe, hvor vi har et utsagn om primtall	Proposisjonene er ikke spesielt viktige i seg selv, og må ikke huskes. Det er imidlertid viktig å kunne gjennomføre lignende argumenter.
Merknad 4.6.2	Hvordan finne den største felles divisoren til et par naturlige tall ved å benytte primtallsfaktoriseringene deres.	Det er svært viktig å kunne gjennomføre metoden i praksis.
Definisjon 4.8.2 og Notasjon 4.8.3	Invers modulo et primtall	✓
Korollar 4.8.15	Det finnes en invers modulo p til et hvilket som helst heltall som ikke er delelig med p	Utsagnet må huskes. Det er svært viktig å kunne finne en invers i praksis, det vil si å løse den relevante lineære kongruensen.
Proposisjon 4.8.28	Kan dele modulo et primtall	Det er ikke så viktig å huske det formelle utsagnet, men det er viktig å kunne benytte proposisjonen i praksis.
Proposisjon 4.9.2 og Proposisjon 4.9.6	Binomialkoeffisienter og binomialteoremet modulo et primtall.	✗
Korollar 4.10.5 og Korollar 4.10.8	Fermats lille teorem	Utsagnene må huskes, men ikke bevisene. Det er oftest Korollar 4.10.8 som benyttes i praksis.

Referanse	Handler om	Må huskes?
Proposisjon 4.11.1 og Proposisjon 4.11.10	Hvordan Fermats lille teorem benyttes i praksis for å vise at noe er delelig med noe	Proposisjonene er ikke spesielt viktige i seg selv, men det er svært viktig å kunne gjennomføre lignende argumenter.
Definisjon 4.12.1	Orden	Definisjonen må huskes. I tillegg er det viktig å kunne finne i praksis ordenen modulo p til et heltall.
Proposisjon 4.12.10	Ordenen modulo p til et heltall x deler et hvilket som helst naturlig tall t slik at $x^t \equiv 1 \pmod{p}$.	✗
Definisjon 4.13.1	Primitiv rot	Definisjonen må huskes. I tillegg er det viktig å bestemme om et heltall er en primitiv rot modulo p.
Proposisjon 4.13.6	Gitt en primitiv rot x modulo p, er et hvilket som helst heltall kongruent modulo p til x opphøyd i noe naturlig tall.	✗
Ingen ennå.	Det finnes en primitiv rot modulo et hvilket som helst primtall.	✗
Proposisjon 4.14.11	Lagranges teorem	✗
Proposisjon 4.15.8	Wilsons teorem	Utsagnet må huskes, men ikke beviset.

Referanse	Handler om	Må huskes?
Proposisjon 4.15.13	Hvordan Wilsons teorem benyttes i praksis for å vise at noe er delelig med noe	Proposisjonen er ikke spesielt viktig i seg selv, men det er svært viktig å kunne gjennomføre lignende argumenter i praksis.

Relevante oppgaver i øvingene

(1) Oppgave 2 – 4 i Øving 7.

(2) Oppgave 1 – 4 i Øving 8.

(3) Oppgave 7 i Øving 8.

(4) Oppgave 1 i Øving 9.

Relevante repetisjonsoppgaver

Oppgave 1 – 2 og Oppgave 5 – 8.

Relevante oppgaver i tidligere eksamener

(1) Oppgave 3 (b), Høsten 2013.

(2) Oppgave 5 (b), Høsten 2012. (Kun delen av oppgaven som sier: finn én primitiv rot modulo 17).

(3) Oppgave 4, Høsten 2011.

(4) Oppgave 1, Våren 2011.

(5) Oppgave 2, Høsten 2010.

(6) Oppgave 3, Høsten 2010.

(7) Oppgave 4, Våren 2010.

(8) Oppgave 1, Høsten 2009.

(9) Oppgave 4, Høsten 2007.

(10) Oppgave 4 (c), Høsten 2005. (Kun delen av oppgaven som sier: hva er ordenen til 8 modulo 19).

(11) Oppgave 3 (b), Våren 2005. (Kun delen av oppgaven som sier: avgjør om 3 er en primitiv rot modulo 14).

(12) Oppgave 4, Høsten 2004.

(13) Oppgave 5 (b), Høsten 2004. (Kun delen av oppgaven som sier: avgjør om 7 er en primitiv rot modulo 11).

Relevante oppgaver i midtsemesterprøver

(1) Oppgave 4, 2013.

(2) Oppgave 1, 2010.

(3) Oppgave 4, 2009.

(4) Oppgave 1, 2008.

(5) Oppgave 4, 2007.

(6) Oppgave 4, 2006.

Kapittel 5

Hovedtemaene

(1) Hvordan bestemme om et heltall er en kvadratisk rest modulo et primtall p slik at $p > 2$, ved å benytte Legendresymboler og kvadratisk gjensidighet.

(2) Hvordan benytte dette for å bestemme hvor mange løsninger en kvadratisk kongruens har.

(3) Hvordan finne løsningene til en kvadratisk kongruens

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

gitt en løsning til kongruensen

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

(4) Det finnes uendelig mange primtall kongruent til 1 modulo 4, og kongruent til 7 modulo 8.

(5) Mersenne-primtall.

Det viktigste

Referanse	Handler om	Må huskes?
Terminologi 5.1.3	Kvadratisk kongruens	✓
Proposisjon 5.1.9	Hvordan finne en løsning til en kvadratisk kongruens	Det er ikke nødvendig å huske det formelle utsagnet eller beviset, men det er svært viktig å kunne finne en løsning til en kvadratisk kongruens i praksis, gitt et heltall y slik at y^2 er kongruent modulo p til diskriminanten.
Definisjon 5.2.1	Kvadratisk rest	Definisjonen må huskes. I tillegg er det viktig å kunne finne alle kvadratiske restene modulo et lite primtall.
Korollar 5.2.30. Se også Merknad 5.2.34.	Hvor mange løsninger en kvadratisk kongruens har	✓
Proposisjon 5.3.2	Eulers kriterium	✗
Proposisjon 5.3.18	Det finnes uendelig mange primtall som er kongruent til 1 modulo 4	Det er viktig at du forstår beviset og kan gjennomføre det selv.
Definisjon 5.4.1 og Notasjon 5.4.2	Legendresymbolet	✓
Alle resultatene i §5.5	Grunnleggende proposisjoner om Legendresymbolet	Alle utsagnene bortsett fra utsagnet i Proposisjon 5.5.9 må huskes, men ikke bevisene.
Proposisjon 5.7.2	Det kinesiske restteoremet	✗

Referanse	Handler om	Må huskes?
Proposisjon 5.7.5, Proposisjon 5.7.13, Proposisjon 5.7.20	Hvordan det kinesiske restteoremet benyttes i praksis	Proposisjonene er ikke spesielt viktige i seg selv, men det er svært viktig å kunne benytte det kinesiske restteoremet for å gjennomføre lignende argumenter.
Teorem 5.8.30	Kvadratisk gjensidighet	✗
Korollar 5.9.2 og Korollar 5.9.21	Korollarer til kvadratisk gjensidighet	Det er ikke nødvendig å huske disse korollarene: du blir gitt dem ved behøv på eksamen.
Alle eksemplene og proposisjonene i §5.10	Hvordan regne ut Legendresymboler, hvordan dermed bestemme om et heltall er et kvadratisk rest modulo et primtall, hvordan dermed bestemme hvor mange løsninger en kvadratisk kongruens har.	Eksemplene og proposisjonene er ikke spesielt viktige i seg selv, men det er svært viktig å kunne gjennomføre lignende argumenter.
Proposisjon 5.11.2	Det finnes uendelig mange primtall som er kongruent til 7 modulo 8	Det er viktig at du forstår beviset og kan gjennomføre det selv.
Terminologi 5.12.2	Mersenne-tall og Mersenne-primtall	✗
Proposisjon 5.12.5, Korollar 5.12.18, Proposisjon 5.12.21, Korollar 5.12.31	Hvordan bestemme om et Mersenne-tall er et primtall	Det er ikke nødvendig å huske resultatene, men det er viktig å kunne benytte dem for å bestemme om et Mersenne-tall er et primtall.

Relevante oppgaver i øvingene

Oppgave 1 – 7 i Øving 10.

Relevante repetisjonsoppgaver

Oppgave 13 – 16 og Oppgave 20 – 22.

Relevante oppgaver i tidligere eksamener

(1) Oppgave 2, Høsten 2013.

(2) Oppgave 4 (d), Høsten 2013.

(3) Oppgave 1, Høsten 2012.

(4) Oppgave 7, Høsten 2012.

(5) Oppgave 2, Høsten 2011.

(6) Oppgave 7, Våren 2011.

(7) Oppgave 1, Høsten 2010.

(8) Oppgave 2, Høsten 2009.

(9) Oppgave 6, Høsten 2008.

(10) Oppgave 2, Høsten 2007.

(11) Oppgave 3, Høsten 2006.

(12) Oppgave 2, Høsten 2005.

(13) Oppgave 6, Våren 2005.

(14) Oppgave 3, Høsten 2004.

(15) Oppgave 4, Våren 2004.

(16) Oppgave 2, Høsten 2003.

Kapittel 6

Hovedtemaene

(1) Eulers teorem.

(2) Kryptografi.

Det viktigste

Referanse	Handler om	Må huskes?
Definisjon 6.1.2 og Notasjon 6.1.3	Totienten	✓
Proposisjon 6.1.18 og Proposisjon 6.2.2	Dersom $\mathsf{sfd}(m,n) = 1$, er $\phi(mn) = \phi(m)\phi(n)$. I tillegg: $\phi\left(p^k\right) = p^k - p^{k-1}$ dersom p er et primtall.	Utsagnene må huskes, men ikke bevisene. Det er svært viktig å kunne benytte disse to proposisjonene for å regne ut totienter i praksis.
Proposisjon 6.2.10	Eulers teorem	Utsagnet må huskes, men ikke beviset.
Proposisjon 6.3.2	Hvordan Eulers teorem benyttes i praksis for å vise at noe er delelig med noe	Proposisjonen er ikke spesielt viktig i seg selv, men det er svært viktig å kunne gjennomføre lignende argumenter.
Terminologi 6.4.3	Offentlig nøkkel og privat nøkkel i forbinelse med RSA-algoritmen.	✓
Alle eksemplene i §6.4	Hvordan kryptere og dekryptere en melding ved å benytte RSA-algoritmen	Eksemplene er ikke spesielt viktige i seg selv, men det er svært viktig å kunne kryptere og dekryptere meldinger ved å benytte RSA-algoritmen i praksis.

Relevante oppgaver i øvingene

Oppgave 1 – 5 i Øving 11.

Relevante repetisjonsoppgaver

Oppgave 4, Oppgave 9, og Oppgave 17 – 18.

Relevante oppgaver i tidligere eksamener

Oppgavene om kryptografi på tidligere eksamener er litt annerledes fra oppgavene i øvingene og repetisjonsoppgavene dette året. I tillegg er notasjonen jeg har benyttet dette året litt annerledes. Derfor er oppgavene om kryptografi fra tidligere eksamener ikke så relevante, og jeg anbefaler ikke at du se på dem.

Følgende oppgaver handler om Eulers teorem og totienter, og er relevante.

(1) Oppgave 5 (c), Høsten 2013.

(2) Oppgave 1, Høsten 2011.

(3) Oppgave 4, Våren 2011.

(4) Oppgave 7, Høsten 2010.

(5) Oppgave 2, Høsten 2006. *Tips*: Jobb modulo 10, modulo 100, og modulo 1000.

(6) Oppgave 4 (b), Høsten 2005. Vanskeligere.

(7) Oppgave 2, Høsten 2004. *Tips*: Jobb modulo 10 og modulo 100.

(8) Oppgave 3 (b), Våren 2004.

(9) Oppgave 3 (b), Høsten 2003. *Tips*: Jobb modulo 10.

Andre kommentarer

(1) Tabellen for å oversette mellom symboler og tall blir gitt ved behov på eksamen.

(2) Når vi benytter RSA-algoritmen for å kryptere og dekryptere, må vi jobbe med heltall som er for store for en enkel kalkulator. Likevel kan du alltid sjonglere potenser. Hvis for eksempel du ønsker å regne ut 2^{37} modulo 55, kan du først observere at $2^6 = 64 \equiv 9 \pmod{55}$. Da er

$$2^{12} = \left(2^6\right)^2 = 9^2 = 81 \equiv 26 \pmod{55}.$$

Da er

$$2^{36} = \left(2^{12}\right)^3 \equiv 26^3 \pmod{55}.$$

Poenget er: 26^3 er lite nok å kunne regne ut ved hjelp av en enkel kalkulator. Faktisk er

$$26^3 \equiv 31 \pmod{55}.$$

Vi konkluderer at

$$2^{37} = 2^{36} \cdot 2 \equiv 31 \cdot 2 = 62 \equiv 7 \pmod{55}.$$