

Note 0

I løbet af semesteret vil jeg ind i mellem skrive en lille note, som bliver udleveret ved TØ. Det kan hænde hvis der er en TØ-opgave vi ikke helt når, som kan løses på en anden måde, eller hvis der i øvrigt er noget som det er værd at skrive en note om. På denne note er der blot nogle praktiske oplysninger.

Instruktor	Rasmus Villemoes
Kontor	Intet endnu
Email	<code>burner@imf.au.dk</code>
Hjemmeside	<code>http://home.imf.au.dk/burner/</code>

På min hjemmeside vil man blandt andet kunne finde de udleverede noter.

Hvis man har spørgsmål til hjemmeopgaverne eller andet, er man altid velkommen til at sende mig en mail eller prøve at finde mig (indtil jeg får et kontor er det sandsynligt at finde mig i D03).

0.1 Afleveringer

I løbet af semesteret bliver der, som i andre fag, stillet et antal afleveringsopgaver (ca. en om ugen). Man skal ved semesterets slutning have afleveret og godkendt mindst 8 af disse for at kunne gå til eksamen. Afleveringer skal afleveres senest onsdag kl. 16 i mit postrum (bag Matematisk Informationskontor), hvis man vil være sikker på at få en rettet udgave tilbage ved førstkommende TØ. Hvis man tidligere har fået godkendt tilstrækkeligt mange afleveringer, er der intet krav om igen at aflevere.

Da eksamen er skriftlig vil jeg anbefale at lave alle afleveringerne.

0.2 TØ

De teoretiske øvelser er til for jeres skyld. Hvis I føler tiden kunne bruges bedre eller der er andet I er utilfredse med, så sig til.

0.3 Om noterne

I kurset benyttes noterne “Concrete Abstract Algebra”, version 4.0. Opgavenumre, sidetal, sætningshenvisninger mv. refererer til denne udgave af noterne. Til oktober udkommer noterne som bog på Cambridge University Press.

0.3.1 Trykfejl

Nogle af rettelserne til den endelige udgave nåede ikke med, inden version 4.0 af noterne blev trykt. Her er en liste over de foreløbig kendte fejl:

Side 5 I beviset for Theorem 1.2.1 rettes “ $n = q_2d + r_2$ ” til “ $x = q_2d + r_2$ ”.

Side 7 Linjen over afsnit 1.4: “ $n \geq 0$ ” rettes til “ $n \geq 1$ ”.

Side 18 Fire linjer inde i §1.8: “It easy” rettes til “It is easy”

Side 31 Afsnit 1.10.3, anden linje: “If a is an” rettes til “If a is an”.

Side 31 Samme afsnit, linjen efter: “Of m is a” rettes til “If m is a”.

Side 34 Linje 6: “algorithm” rettes til “algorithms”.

Side 39 Opgave I.5: Betingelsen $a_r \neq 0$ tilføjes definitionen af en τ -adisk repræsentation.

Side 41 Opgave I.16(ii): “Use (a)” rettes til “Use (i)”.

Side 46 Opgave I.47: Ret “ $X_0 = 3$ ” til “ $X_0 = Y_0 = 3$ ”.

Side 46 Opgave I.49(ii): Delspørgsmålet erstattes af (ret hvor nødvendigt):

Suppose that the prime factorizations of a_1, \dots, a_n over the factor basis $P = \{p_1, \dots, p_r\}$ (assume all a 's factor completely using primes from P) are

$$\begin{aligned} a_1 &= p_1^{m_{11}} \cdots p_r^{m_{r1}} \\ a_2 &= p_1^{m_{12}} \cdots p_r^{m_{r2}} \\ &\vdots \\ a_n &= p_1^{m_{1n}} \cdots p_r^{m_{rn}}. \end{aligned}$$

Translate the problem of finding a subset $\{i_1, \dots, i_s\}$ of $\{1, \dots, n\}$ such that $a_{i_1} \cdots a_{i_s}$ is a square into linear algebra over \mathbb{F}_2 .

Ændringerne består i, at “ a 's” er rettet til “ a 's”, der er byttet rundt på rækkefølgen af indices til m 'erne, og “ i_r ” er rettet til “ i_s ”.

Side 51 Fire linjer inde i beviset: “ $b + cx + \mathbb{Z}$ ” rettes til “ $b + cx + c\mathbb{Z}$ ”

Side 116 Fire linjer over Lemma 3.3.5: “(n times)” rettes til “(n times)”

Side 129 Tre linjer nede i §3.5.7: “helps” rettes til “help” og resten af sætningen erstattes af “this statement.”.

Side 133 Opgave III.17(iii): “ $I = Rn$ ” rettes til “ $I = \langle n \rangle$ ”.

Side 167 Tredje linje: “ $\mu(1) = 0$ ” rettes til “ $\mu(1) = 1$ ”.

Side 168 Første linje efter den store matrix: “ $g \in F_p[X]$ ” rettes til “ $g \in \mathbb{F}_p[X]$ ”.

Side 169 Linjen under anden store matrix: “ $f \mid g^p - g$ ” rettes til “ $f \mid g^2 - g$ ”.

Side 173 Opgave IV.23(i): “ s is a natural number” rettes til “ s is a natural number ≥ 1 ”.

Side 187 Efter ligning (5.3): “assignments” rettes til “assignments”

Side 204 Beviset for Theorem 5.8.3: Forekomster af “ f_n ” og “ g_n ” rettes til henholdsvis “ f_m ” og “ g_m ”.

Side 209 Opgave V.1(iv): “ $f(gh) = f(gh)$ ” rettes til “ $f(gh) = (fg)h$ ”.

Side 211 Nederste linje: “the ideal $R(S - X^2) + R(T - XY)$ ” rettes til “the ideal $\langle S - X^2, T - XY \rangle$ ”

Side 218 Nederste linje: “likes this” rettes til “like this”.

Den mest aktuelle rettelsesliste vil være tilgængelig på min hjemmeside. Hvis du skulle falde over en fejl eller unøjagtighed i noterne (hvad enten det måtte være lærebogen eller disse), så tøv ikke med at sende en mail.

0.4 Ordbog

Da lærebogen og opgaverne er på engelsk, forelæsninger og TØ foregår på dansk, og eksamensopgaverne (når den tid kommer) bliver stillet på dansk, er det en god ting at kunne fagtermerne på begge sprog. Hvis det viser sig nyttigt vil jeg ind i mellem tilføje et “ordbogsafsnit” til noten, hvor jeg oversætter de vigtigste begreber for den kommende tid. Her er første version.

Engelsk	Dansk
odd	ulige (om tal)
even	lige (om tal)
remainder	rest (ved division)
congruence	kongruens
greatest common divisor	største fælles divisor
the Euclidean algorithm	Euklids algoritme
relatively prime	indbyrdes primiske
The Chinese Remainder Theorem	Den kinesiske restklassesætning
prime number	primtal
composite number	sammensat tal
least common multiple	mindste fælles multiplum
encryption	kryptering
decryption	dekryptering
digit	ciffer
quadratic (non-)residue	kvadratisk (ikke-)rest