Elementær Talteori - 3. aflevering

Opgave 1

Vi starter med at omskrive ligningen (alle udregninger er mod 263.

$$\begin{aligned} x^2 + 20x + 211 &\equiv 0 \\ (x+10)^2 + 111 &\equiv 0 \\ (x+10)^2 &\equiv -111 \\ (x+10)^2 &\equiv 152 \end{aligned}$$

Vi finder så om der er en løsning ved brug af legendre symbolet. Vi ser, at 152 har primtals faktoriseringen $152 = 2^3 * 19$.

$$(\frac{152}{263}) = (\frac{2}{263})(\frac{2}{263})(\frac{2}{263})(\frac{19}{263}) = 1 * 1 * 1 * (-1) = -1 \tag{1}$$

Her ser vi, at $263 \equiv -1 \pmod 8$, og derved får vi fra theorem 4.1.7 **[St]** at $(\frac{2}{263}) = 1$. Yderligere fra samme theorem, får vi at

$$(\frac{19}{263}) = (-1)^{\frac{19-1}{2}\frac{263-1}{2}}(\frac{263}{19}) = (-1)^{1179}(\frac{263}{19}) = (-1)(\frac{263}{19}) = -(\frac{16}{19}) \tag{2}$$

Hvor $16 = 2^4$ og $(\frac{2}{19}) = -1$ da $19 \equiv 3 \pmod 8$ igen fra theorem 4.1.7. Altså hvis vi regner videre på (2) får vi

$$-(\frac{16}{19}) = -(\frac{2}{19})(\frac{2}{19})(\frac{2}{19})(\frac{2}{19}) = -(-1)^4 = -1$$

Og dette konkluderer det næstsidste lighedstegn i (1). Da dette giver -1 har ligningen altså ingen heltals løsninger.

Opgave 2

(a)

At den har orden 5, betyder at elementet c skal opløftes i femte potens for at give identitetselementet, 1, for den multiplikative gruppe.
Eftersom gruppen Z_p^* har orden $p-1$ og vi ved at $5|p-1$ siger Cauchy's theorem, at når gruppen er endelig, og 5 er et primtal der dividerer gruppens orden, at der må være et element, c, i gruppen med orden 5.

(b)
Hvis vi skriver ligningen ud og laver nogle omskrivninger, får vi

$$\begin{aligned}(2c+2c^{-2}+1)^2 &\equiv 5 \, mod \, p \\ 4(c^2+c^{-2})+4(c+c^{-1})+4 &\equiv 0 \, mod \, p \\ 4(c^2+c^{-2}+c+c^{-1}+1) &\equiv 0 \, mod \, p\end{aligned}$$

som er ækvivalent med

$$c^2+c^{-2}+c+c^{-1}+1 \equiv 0 \, mod \, p \tag{3}$$
$$c^2+c^3+c+c^4+1 \equiv 0 \, mod \, p \tag{4}$$
$$c^4+c^3+c^2+c^1+1 \equiv 0 \, mod \, p \tag{5}$$

Eftersom c har orden 5, betyder det at $c^5-1 \equiv 0 \mod p$.
Dette kan også skrives som $(c-1)(c^4+c^3+c^2+c^1+1) \equiv 0 \mod p$. Da $c \neq 1$, må ligningen $c^4+c^3+c^2+c^1+1 \equiv 0 \, mod \, p$ altså være sand og derved gælder det at $g^2 \equiv 5 \mod p$.

c
Da vi kan se, at der altid vil være et element af orden 5 samt at der er en løsning til $g^2 \equiv 5 \mod p$, må legendre symbolet $(\frac{5}{p})$ altså være 1.
Alternativt kan vi bruge theorem 4.1.7 [**St**], som kan bruges idet begge tal er primtal, og få

$$(\frac{5}{p}) = -1^{\frac{5-1}{2}\frac{p-1}{2}}(\frac{p}{5}) = (\frac{p}{5})$$

Sidste lighedstegn er da -1 altid vil være opløftet i et lige tal. Det vides desuden, at $p \equiv 1 \mod 5$, altså kan vi reducere det til

$$(\frac{1}{5}) = 1$$

Og derved er det vist for primtal p på denne form $(5q+1)$.

Opgave 3

Ikke lavet.

Opgave 4

Vi kan bruge Dirichlet foldning af $|\mu| * \mu$, da begge er aritmetiske funktioner, til at skrive den nye aritmetiske funktion givet ved

$$(|\mu| * \mu)(n) = \sum_{d/n} |\mu|(d)\mu(\frac{n}{d})$$

ved at sætte $\frac{n}{d} = e$ kan vi omskrive til

$$(|\mu| * \mu)(n) = \sum_{de=n} |\mu|(d)\mu(e)$$

Ikke løst.

Opgave 5

I theorem 5.8 [**JJ**] er det netop bevist, at

$$\sum_{d|n} \phi(d) = n$$

Andel del af opgaven, hvor vi vil vise

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

trækker vi på korollar 8.7 [**JJ**] som siger, at

$$\phi(n) = \sum_{d|n} \frac{\mu(d)n}{d}$$

Her kan vi trække n ud af summen da denne kun antager en værdi.

$$\phi(n) = n\sum_{d|n} \frac{\mu(d)}{d}$$

Og herefter dividere på begge sider med n

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

Og derved er det vist ved simple omskrivninger fra dette korollar.