1. Gruppearbeid A i 19F

Oppgave 1. Hvilken rest får vi når vi deler 18^{31} med 7?

Fasit. Vi har fra Fermats lille teorem at

$$18^{7-1} = 18^6 \equiv 1 \mod 7,$$

siden $\gcd(18, 7) = 1$. Dette gir at

$$18^{30} = (18^6)^5 \equiv 1^5 \mod 7,$$

som impliserer at

$$\begin{aligned} 18^{31} = 18^{30} \cdot 18 &\equiv 1 \cdot 18 \mod 7 \\ &\equiv 4 \mod 7 \end{aligned}$$

Oppgave 2. Hvilken rest får vi når vi deler 24^{38} med 17?

Fasit. Vi har fra Fermats lille teorem at

$$24^{17-1} = 24^{16} \equiv 1 \mod 17,$$

siden $\gcd(24, 17) = 1$. Dette gir at

$$24^{34} = (24^1 7)^2 \equiv 1^2 = 1 \mod 17,$$

som impliserer at

$$\begin{aligned} 24^{38} = 24^{34} \cdot 24^4 &\equiv 1 \cdot 24^4 \mod 17 \\ &\equiv 7^4 \mod 17, \text{ siden } 24 \equiv 7 \mod 17 \\ &\equiv (-2)^2 \mod 17, \text{ siden } 7^2 = 49 \equiv -2 \mod 17 \\ &\equiv 4 \mod 17 \end{aligned}$$

Oppgave 3.

(a) La p være et primtall. Vis at antall elementer i $U(\mathbb{Z}_{p^n})$ for $n \geq 1$ er $p^n - p^{n-1}$.

(b) La p være et primtall i $\mathbb{Z}$, og la $n \geq 1$ være et heltall. Vis at for $a \in \mathbb{Z}$ med $\gcd(a, p) = 1$, så er

$$a^{p^n - p^{n-1}} \equiv 1 \mod p^n.$$

Fasit. (a) Husk at $U(\mathbb{Z}_{p^n}) = \{\overline{z} \in \mathbb{Z}_{p^n} \mid \gcd(z, p^n) = 1\}$. Siden $\gcd(z, p^n) = 1$ hvis og bare hvis $\gcd(z, p) = 1$, har vi at

$$\begin{aligned} U(\mathbb{Z}_{p^n}) &= \{\overline{z} \in \mathbb{Z}_{p^n} \mid \gcd(z, p) = 1\} \\ &= \{\overline{z} \mid 0 \leq z < p^n \text{ og } z \text{ er ikke et multiplum av } p \end{aligned}$$

Det er p^n heltall z slik at $0 \leq z < p^n$, og det er p^{n-1} multiplum z av p med $0 \leq z < p^n$:

$$0, p, 2p, 3p, 4p, \ldots, (p^n - 2)p, (p^n - 1)p.$$

Dette gir at $|U(\mathbb{Z}_{p^n})| = p^n - p^{n-1}$.

(b) La $a \in \mathbb{Z}$ være slik at $\gcd(a, p) = 1$. Dette gir at $\gcd(a, p^n) = 1$ for alle $n \geq 1$. Da er $\overline{a}$ en enhet i $U(\mathbb{Z}_{p^n})$, som er en gruppe med orden $p^n - p^{n-1}$. Dette gir at

$$\overline{a}^{p^n - p^{n-1}} = \overline{1}$$

i $\mathbb{Z}_{p^n}$. Dette er ekvivalent med at $a^{p^n - p^{n-1}} \equiv 1 \mod p^n$.

Oppgave 4. Vis følgende resultat.

Korollar 66. *La p være et primtall. Hvis $a \in \mathbb{Z}$, da er*

$$a^p \equiv a \mod p.$$

Fasit. Vi har to tilfeller: $p \mid a$ og $p \nmid a$.

1) Hvis $p \nmid a$, dvs. $\gcd(a, p) = 1$, så er $a^{p-1} - 1 \in p\mathbb{Z}$ (Setning 65). Multipliserer vi med a får vi at $a(a^{p-1} - 1) = a^p - a \in p\mathbb{Z}$, som er equivalent med at

$$a^p \equiv a \mod p.$$

2) Hvis $p \mid a$, da vil $p \mid am$ for alle $m \in \mathbb{Z}$. Spesilet for $m = a^{p-1} - 1$, og vi får at

$$p \mid a(a^{p-1} - 1) = a^p - a,$$

dvs. $a^p \equiv a \mod p$.

Oppgave 5. Fullfør beviset for følgende setning, som vi bare har gjort delvis i videoen for 19F, i det vi har vist at $\mathbb{Z}/n\mathbb{Z}$ er en ring.

Setning 64. *La $\varphi \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ være gitt ved at*

$$\varphi(a + n\mathbb{Z}) = \overline{r_a},$$

der $a = nq_a + r_a$ for q_a, r_a i $\mathbb{Z}$ med $0 \leq r_a < n$. Vis at φ er en isomorfi av ringer med 1.

Fasit. Vi vet at φ er en isomorfi av grupper. Vi trenger å vise at

(i) $\varphi((a+n\mathbb{Z})(b+n\mathbb{Z}) = \varphi((a+n\mathbb{Z}))\varphi((b+n\mathbb{Z}))$.

(ii) $\varphi((1+n\mathbb{Z})) = 1_{\mathbb{Z}_n}$.

(i) Vi har at

$$\varphi((a+n\mathbb{Z})(b+n\mathbb{Z})) = \varphi((ab+n\mathbb{Z})) = \overline{r}_{ab}$$

og

$$\varphi((a+n\mathbb{Z}))\varphi((b+\mathbb{Z})) = \overline{r_a} \cdot \overline{r_b}.$$

Følgende likheter holder

$$\begin{aligned} ab &= (nq_a + r_a)(nq_b + r_b) \\ &= n(nq_aq_b + r_aq_b + q_ar_b) + r_ar_b \\ &= nq + r \text{ for en } r \text{ med } 0 \leq r < n \end{aligned}$$

og

$$ab = nq_{ab} + r_{ab}$$

Siden differansene $r_{ab} - r_ar_b$ og $r_{ab} - r$ er i $n\mathbb{Z}$. Dette gir at $\overline{r}_{ab} = \overline{r_a} \cdot \overline{r_b}$, og φ tilfredsstiller (i).

(ii) Vi har at $\varphi((1+n\mathbb{Z})) = \overline{1}$ per definisjon, slik at φ er en homomorfi av ringer med 1. Siden φ er en isomorfi av grupper, så er φ en-til-en og på. Dette medfører at φ er en isomorfi av ringer.