

GRUPPEARBEID

Generelt ved gruppearbeid:

- (1) Presentasjon av deltakerne, navn, studieprogram, kull.
- (2) Velg en deltaker til å dele "whiteboard".
- (3) Husk å spørre om alle er enige/er med, og husk å si i fra om du ikke skjønner noe eller har en annen måte å tenke på. I forelesningene skal vi lære og ikke prestere.

1. GRUPPEARBEID A I 19F

Husk:

- (i) $a \equiv a' \pmod n \Leftrightarrow a + n\mathbb{Z} = a' + n\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$.
- (ii) Anta at $a \equiv a' \pmod n$ og $b \equiv b' \pmod n$, da er

$$a + b \equiv a' + b' \pmod n.$$

$$ab \equiv a'b' \pmod n.$$

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

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

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

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

Oppgave 4. Vis følgende resultat.

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

$$a^p \equiv a \pmod p.$$

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 $\varphi: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$ være gitt ved at*

$$\varphi(a + n\mathbb{Z}) = \bar{r}_a,$$

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.

2. GRUPPEARBEID B I 19F

Oppgave 1.

- (1) Beregn Eulers phi-funksjon av verdiene: $\{1, 2, 3, 4, 5, 6, 7\}$.
- (2) Beregn $\varphi(110341894140625) = \varphi(5^8 7^{10})$.

Oppgave 2. Hva sier Eulers teorem når n er et primtall?

Oppgave 3 (Gammel eksamensoppgave). Skriv ned definisjonen på Eulers phi-funksjon, og finn det siste sifferet i tallet $7^{1000000}$.

Oppgave 4 (Gammel eksamensoppgave). Gi definisjonen av Eulers phi-funksjon, og finn resten vi får når vi deler 5^{1000} på 18.