Forelesning 17 — torsdag den 16. oktober

4.12 Orden modulo et primtall

Definisjon 4.12.1. La p være et primtall. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Et naturlig tall t er *ordenen* til a modulo p dersom t er det minste naturlige tallet slik at:

(1) $x^t \equiv 1 \pmod{p}$;

(2) $0 \leq t < p$.

Merknad 4.12.2. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Ut ifra Korollar 4.10.8 er

$$x^{p-1} \equiv 1 \pmod{p}.$$

Derfor har x en orden, og denne ordenen er mindre enn eller likt $p - 1$.

Merknad 4.12.3. For å finne ordenen til et heltall x modulo et primtall p, kan vi gå gjennom heltallene x, x^2, x^3, ..., x^{p-1}. Den første potensen i slik at

$$x^i \equiv 1 \pmod{p}$$

er ordenen til x modulo p.

Notasjon 4.12.4. La p være et primtall. La x være et heltall slik at det ikke er sant at $x \equiv 0 \pmod{p}$. Vi betegner ordenen til x modulo p som $\mathsf{ord}_p(x)$.

Eksempel 4.12.5. Siden $1^1 = 1$, er ordenen til 1 lik 1 for et hvilket som helst primtall p.

Eksempel 4.12.6. For å finne ordenen til 2 modulo 3, gjør vi følgende. Kongruensen i den andre raden er modulo 3.

i	2^i
1	2
2	$4 \equiv 1$

Dermed er ordenen til 2 modulo 3 lik 2.

Således har vi følgende ordener modulo 3.

x	Ordenen til x modulo 3
1	1
2	2

Eksempel 4.12.7. Alle kongruenser i dette eksempelet er modulo 5. For å finne ordenen til 2 modulo 5, gjør vi følgende.

i	2^i
1	2
2	4
3	$8 \equiv 3$
4	$2^4 = 2^2 \cdot 2^2 \equiv 4 \cdot 4 = 16 \equiv 1$

Dermed er ordenen til 2 modulo 5 lik 4.

For å finne ordenen til 3 modulo 5, gjør vi følgende.

i	3^i
1	3
2	$9 \equiv 4$
3	$3^3 = 3^2 \cdot 3^1 \equiv 4 \cdot 3 = 12 \equiv 2$
4	$3^4 = 3^3 \cdot 3^1 \equiv 2 \cdot 3 = 6 \equiv 1$

Dermed er ordenen til 3 modulo 5 lik 4.

For å finne ordenen til 4 modulo 5, gjør vi følgende.

i	4^i
1	4
2	$16 \equiv 1$

Dermed er ordenen til 4 modulo 5 lik 2.

Således har vi følgende ordener modulo 5.

x	Ordenen til x modulo 5
1	1
2	4
3	4
4	2

Merknad 4.12.8. Utregningene i Eksempel 4.12.7 er ikke de eneste mulige. For å vise at

$$2^4 \equiv 1 \pmod 5,$$

kan vi også for eksempel regne som følger:

$$2^4 = 2^3 \cdot 2^1 \equiv 3 \cdot 2 = 6 \equiv 1 \pmod 5.$$

Alternativt følger det fra Korollar 4.10.8.

Det samme gjelder i neste eksempel.

Eksempel 4.12.9. Alle kongruenser i dette eksempelet er modulo 7. For å finne ordenen til 2 modulo 7, gjør vi følgende.

i	2^i
1	2
2	4
3	$8 \equiv 1$

Dermed er ordenen til 2 modulo 7 lik 3.

For å finne ordenen til 3 modulo 7, gjør vi følgende.

i	3^i
1	3
2	$9 \equiv 2$
3	$3^3 = 3^2 \cdot 3^1 \equiv 2 \cdot 3 = 6$
4	$3^4 = 3^2 \cdot 3^2 \equiv 2 \cdot 2 = 4$
5	$3^5 = 3^3 \cdot 3^2 \equiv 6 \cdot 2 = 12 \equiv 5$
6	$3^6 = 3^4 \cdot 3^2 \equiv 4 \cdot 2 = 8 \equiv 1$

Dermed er ordenen til 4 modulo 7 lik 6.

For å finne ordenen til 4 modulo 7, gjør vi følgende.

i	4^i
1	4
2	$16 \equiv 2$
3	$4^3 = 4^2 \cdot 4^1 \equiv 2 \cdot 4 = 8 \equiv 1$

Dermed er ordenen til 4 modulo 7 lik 3.

For å finne ordenen til 5 modulo 7, gjør vi følgende.

i	5^i
1	5
2	$25 \equiv 4$
3	$5^3 = 5^2 \cdot 5^1 \equiv 4 \cdot 5 = 20 \equiv -1$
4	$5^4 = 5^3 \cdot 5^1 \equiv (-1) \cdot 5 = -5 \equiv 2$
5	$5^5 = 5^3 \cdot 5^2 \equiv (-1) \cdot 4 = -4 \equiv 3$
6	$5^6 = 5^3 \cdot 5^3 \equiv (-1) \cdot (-1) = 1$

Dermed er ordenen til 5 modulo 7 lik 6.

For å finne ordenen til 6 modulo 7, gjør vi følgende.

i	6^i
1	6
2	$36 \equiv 1$

Dermed er ordenen til 6 modulo 7 lik 2.

Således har vi følgende ordener modulo 7.

x	Ordenen til x modulo 7
1	1
2	3
3	6
4	3
5	6
6	2

Proposisjon 4.12.10. La p være et primtall. La x være et heltall slik at x det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

La s være ordenen til x. La t være et naturlig tall. Da er

$$x^t \equiv 1 \pmod{p}$$

hvis og bare hvis $s \mid t$.

Bevis. Anta først at $x^t \equiv 1 \pmod{p}$. Ut ifra Proposisjon 1.2.6 finnes det naturlige tall k og r slik at $t = ks + r$. Da er:

$$\begin{aligned} x^t &= x^{ks+r} \\ &= x^{ks} x^r \\ &= (x^s)^k x^r. \end{aligned}$$

Ut ifra definisjonen til s er

$$x^s \equiv 1 \pmod{p}.$$

Dermed er

$$x^t \equiv 1^k \cdot x^r,$$

alts

$$x^t \equiv x^r \pmod{p}.$$

Ut ifra antakelsen at

$$x^t \equiv 1 \pmod{p}$$

og Proposisjon 3.2.24, er da

$$x^r \equiv 1 \pmod{p}.$$

Ut ifra definisjonen til s, er s det minste naturlige tallet slik at $x^s \equiv 1 \pmod{p}$. Siden $0 \leq r < s$ og

$$x^r \equiv 1 \pmod{p},$$

følger det at $r = 0$. Dermed er $t = ks$. Vi konkluderer at $s \mid t$.

Anta istedenfor at $s \mid t$. Da finnes det et naturlig tall k slik at $t = ks$. Ut ifra definisjonen til s, er $x^s \equiv 1 \pmod{p}$. Derfor er

$$(x^s)^k \equiv 1^k \pmod{p},$$

altså er

$$x^{sk} \equiv 1 \pmod{p}.$$

Siden

$$sk = ks = t,$$

konkluderer vi at

$$x^t \equiv 1 \pmod{p}.$$

□

Eksempel 4.12.11. Siden $2^6 = 64$ og

$$64 \equiv 1 \pmod{7},$$

fastslår Proposisjon 4.12.10 at ordenen til 2 modulo 7 deler 6. Ut ifra Eksempel 4.12.9 er ordenen til 2 modulo 7 lik 3. Det er riktignok sant at $3 \mid 6$.

Eksempel 4.12.12. Siden $3^8 = 6561$ og

$$6561 \equiv 1 \pmod{5},$$

fastslår Proposisjon 4.12.10 at ordenen til 3 modulo 4 deler 8. Ut ifra Eksempel 4.12.7 er ordenen til 3 modulo 5 lik 4. Det er riktignok sant at $4 \mid 8$.

4.13 Primitive røtter modulo et primtall

Definisjon 4.13.1. La p være et primtall. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Da er x en *primitiv rot* modulo p dersom ordenen til x modulo p er $p - 1$.

Eksempel 4.13.2. Siden ordenen til 1 er $2 - 1 = 1$, er 1 en primitiv rot modulo 2.

Eksempel 4.13.3. Ut ifra tabellen på slutten av Eksempel 4.12.6 har vi følgende.

x	Primitiv rot modulo 3?
1	✗
2	✓

Eksempel 4.13.4. Ut ifra tabellen på slutten av Eksempel 4.12.7 har vi følgende.

x	Primitiv rot modulo 5?
1	✗
2	✓
3	✓
4	✗

Eksempel 4.13.5. Ut ifra tabellen på slutten av Eksempel 4.12.9 har vi følgende.

x	Primitiv rot modulo 7?
1	✗
2	✗
3	✓
4	✗
5	✓
6	✗

Proposisjon 4.13.6. La p være et primtall. La x være en primitiv rot modulo p. La a være et heltall. Da finnes det et heltall r slik at $0 \leq r < p$ og

$$x^r \equiv a \pmod{p}.$$

Bevis. Kommer snart! □

Merknad 4.13.7. Proposisjon 4.13.6 er grunnen for at primitive røtter er viktige. Å kunne uttrykke et hvilket som helst heltall modulo p som en potens av ett heltall er noe er spesielt med aritmetikk modulo p, og svært viktig fra et teoretisk synspunkt. Det er langt fra tilfellet at det finnes et heltall x slik at hvert naturlig tall er *likt* x opphøyd i noe. Når $x = 2$, får vi for eksempel heltallene $2, 4, 8, 16, \ldots$, men får vi ikke de negative heltallene, og heller ikke de naturlige tallene $1, 3, 5, 6, 7, 9, \ldots$.

Oppgaver

O4.1 Oppgaver i eksamens stil

Oppgave O4.1.10. Skriv ned ordenene modulo 11 til alle de naturlige tallene 1, 2, ..., 10. Hvilke av 1, 2, ..., 10 er primitive røtter modulo 11?