LØSNING EKSAMEN MA1301 H2017, OPPGAVE 7

Vi skal finne ordenen til $p-1$ modulo p^t for ethvert positivt heltall t. Vi vil vise ved induksjon at ordenen til $p-1$ modulo p^t er $2p^{t-1}$ og at

$$(p-1)^{2p^{t-1}} = 1 + np^t, \quad p \not| n. \tag{1}$$

Når $t = 1$, får vi

$$(p-1)^2 = 1 + (p-2)p,$$

som viser både at (1) holder og at ordenen til $p-1$ er 2.

Vi antar så at ordenen til $p-1$ modulo p^j er $2p^{j-1}$ og at (1) holder for $t = j$. Før vi med utgangspunkt i (1) gjør induksjonsskrittet, gjør vi følgende observasjon: Ordenen k til $p-1$ modulo p^t må dele ordenen m til $p-1$ modulo p^{t+1} siden

$$(p-1)^m \equiv 1 \pmod{p^{t+1}} \quad \Rightarrow \quad (p-1)^m \equiv 1 \pmod{p^t}.$$

Dermed kan vi skrive ordenen til $p-1$ modulo p^{j+1} som $d2p^{j-1}$ for et positivt heltall d. Fra (1) med $t = j$ får vi

$$(p-1)^{d2p^{j-1}} = (1+np^j)^d = 1 + dnp^j + \frac{d(d-1)}{2}n^2p^{2j} + mp^{3j},$$

for et heltall m. Det minste positive tallet d slik at høyresiden blir kongruent til 1 modulo p^{j+1} er $d = p$. Med dette valget av d ser vi at vi også får (1) for $t = j+1$ siden $(p-1)/2$ er et heltall.[1] Resultatet følger nå ved induksjon.

[1] Denne lille ekstra finessen trengs bare når $j = 1$, siden p^{2j} ellers er større enn p^{j+1}.