

Øving 10

Ø.2.1 p odde juntall.

a) Siden $1^2 \equiv 1 \pmod{p}$ og $(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod{p}$ har vi funnet to løsninger (de er forskjellige da p er odde). Ved Teorem 8.2 (Lagrange) har vi funnet alle løsningene til $x^2 \equiv 1 \pmod{p}$.

b) Husk: Fermats lille: $\text{gcd}(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Har at $(x-1)(x^{p-2} + x^{p-3} + \dots + x + 1) = x^{p-1} - 1$

Ved Fermats lille får vi at $x^{p-1} - 1 \equiv 0 \pmod{p}$

har løsninger ~~1, 2, ..., p-1~~ $1, 2, \dots, p-1$. Derom $x \not\equiv 1 \pmod{p}$

får vi at

$$0 \equiv x^{p-1} - 1 \equiv (x-1)(x^{p-2} + \dots + x + 1) \pmod{p}$$

siden $x \not\equiv 1 \pmod{p}$ må $x^{p-2} + \dots + x + 1 \equiv 0 \pmod{p}$

der $x \equiv 2, 3, \dots, p-1 \pmod{p}$ er løsningene da

Teorem 8.2 sier at et $(p-2)$ -grads polynom har høyst $(p-2)$ røtter.

Ø.2.2 $x^2 \equiv 1 \pmod{15}$ har løsninger $x = 1, -1, 4, -4$

$x^2 \equiv -1 \pmod{65}$ $x = 8, -8, 18, -18$

$x^2 \equiv -2 \pmod{33}$ $x = 14, -14, 25, -25$

9.1.2 $p=2$ giv $6x^2+5x+1 \equiv x+1 \equiv 0 \pmod{2}$

som har løsning $x \equiv 1 \pmod{2}$. La p så være et vilkårligt primtal. Har at $6x^2+5x+1 \equiv 0 \pmod{p}$ svarer til at løse

$$y^2 \equiv 1 \pmod{p} \quad (*)$$

der $y = 2x + 5$ og $1 = 5^2 - 4 \cdot 6 \cdot 1$.

(*) har løsning $y = \pm 1$ for alle p , og x er da givet som løsninger av

$$2x \equiv \pm 1 - 5 \pmod{p}$$

Hva skjer dersom $p=5$? og $p=3$?

9.1.4 Vi skal vise at $x^2 \equiv 3 \pmod{23}$ har løsning.

Eulers kriterium: $3^{\frac{23-1}{2}} \equiv 1 \pmod{23} \Leftrightarrow 3$ kvadratisk rest modulo 23.

$$3^{-1} \equiv 8 \pmod{23} \quad (\text{ettersom } 3 \cdot 8 = 24 \equiv 1 \pmod{23})$$

$$3^4 = 81 \equiv -11 \pmod{23}$$

$$3^8 \equiv (-11)^2 = 121 \equiv 6 \pmod{23}$$

$$3^{11} = 3^{8+4-1} \equiv 6 \cdot (-11) \cdot 8 \equiv 2 \cdot (-11) = -22 \equiv 1 \pmod{23}$$

Eulers kriterium: $3^{\frac{31-1}{2}} \equiv 1 \pmod{31} \Leftrightarrow 3$ er kvadratisk rest modulo 31.

$$3^3 = 27 \equiv -4 \pmod{31} \quad 2^5 = 32 \equiv 1 \pmod{31}$$

$$3^{15} = (3^3)^5 \equiv (-4)^5 = -1 \cdot (2^5)^2 \equiv -1 \cdot 1^2 = -1 \pmod{31}$$

9.1.5

b) Antag a kvadratisk rest modulo p , dvs $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Vi ser på $(p-a)^{\frac{p-1}{2}} \pmod{p}$:

$$(p-a)^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} (a)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \pmod{p}$$

$$(-1)^{\frac{p-1}{2}} \equiv \begin{cases} 1 & 2 \nmid \frac{p-1}{2} \Leftrightarrow 4 \nmid p-1 \Leftrightarrow p \equiv 1 \pmod{4} \\ -1 & 2 \mid \frac{p-1}{2} + 1 = \frac{p+1}{2} \Leftrightarrow \dots \Leftrightarrow p \equiv 3 \pmod{4} \end{cases}$$

dvs $(p-a)$ kvadratisk rest dersom $p \equiv 1 \pmod{4}$

$(p-a)$ ikke kvadratisk rest dersom $p \equiv 3 \pmod{4}$.

c) La $p \equiv 3 \pmod{4}$. La $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$

da er

$$x^2 \equiv (\pm a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a^{\frac{2}{2}} \equiv 1 \cdot a = a \pmod{p}$$

siden a er kvadratisk rest p

dvs $\pm a^{\frac{p+1}{4}} \pmod{p}$ er løsning av

$$x^2 \equiv a \pmod{p}.$$

9.1.9

a) Anta $a \cdot b \equiv r \pmod{p}$, der r er en kvadratisk rest modulo p . Hvor er

$$1 \equiv r^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p}$$

Hvor er

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & a \text{ kvadratisk rest} \\ -1 & a \text{ ikke kvadratisk rest.} \end{cases}$$

Hvor følgende muligheder ~~er~~

$$(a^{\frac{p-1}{2}} \pmod{p}, b^{\frac{p-1}{2}} \pmod{p}) = (1, 1), (-1, 1), (1, -1), (-1, -1)$$

Siden $a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ må enten begge være kongruente med 1 eller begge kongruente med -1.

9.1.10 Dette følger direkte av oppgave 9.1.9.

$x^2 \equiv ab \pmod{p}$ er løsbart $\Leftrightarrow \begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv b \pmod{p} \end{cases} \begin{cases} \text{begge} \\ \text{enten} \\ \text{løsbare} \\ \text{eller begge} \\ \text{ikke løsbare.} \end{cases}$

E404.8 Dette kan viis ved induksjon. Her er

et direkte bevis:

Merke at $\sum_{i=1}^{2^k} \frac{1}{2^{k+i}} > \frac{1}{2}$ for $k \geq 1$.

Bevis:

Her at $\frac{1}{2^{k+i}} \geq \frac{1}{2^{k+1}}$ for $1 \leq i \leq 2^k$

Eksempel:

$$\left[\begin{array}{l} \frac{1}{5} > \frac{1}{8}, \frac{1}{6} > \frac{1}{8}, \frac{1}{7} > \frac{1}{8}, \frac{1}{8} \geq \frac{1}{8} \\ \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} > \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = 4 \cdot \frac{1}{8} = \frac{1}{2} \end{array} \right]$$

ders.

$$\frac{1}{2^{k+1}} + \dots + \frac{1}{2^{k+2^k}} > 2^k \cdot \frac{1}{2^{k+1}} = \frac{1}{2}$$

$2 \cdot 2^k = 2^{k+1}$

Her at $S_{2^n} = 1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\frac{1}{2}} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\frac{1}{2}} + \dots + \underbrace{\frac{1}{2^{n-1}} + \dots + \frac{1}{2^n}}_{\frac{1}{2}}$

n ganger

ders $S_{2^n} \geq 1 + \underbrace{\frac{1}{2} + \frac{1}{2} + \dots + \frac{1}{2}}_n = 1 + \frac{n}{2}$ □

Oppgave: Vis at rekken $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$ diverger

ders vis at $\sum_{n=2}^{\infty} \frac{1}{n} = \infty$