FERMATS LILLE TEOREM, EULERS TEOREM, WILLSONS TEOREM.

41 F.L.T. Anta at p er et primtall, og anta at $\bar{a} \neq 0$ i $\mathbb{Z}_p$.

Da er $\bar{a}^{p-1} = \bar{1}$.

Bevis: Husk at alle elementer i $\mathbb{Z}_p$ har kanseleringsegenskapen og ingen elementer er nulldivisorer

Se på

$$\{\bar{1}, \bar{2}, \bar{3}, \dots, \overline{p-1}\}$$

og

$$\{\bar{a}\cdot\bar{1}, \bar{a}\bar{2}, \dots, \bar{a}(\overline{p-1})\}$$

ingen elementer er null, og alle er forskjellige

De to mengdene er like, så

$$\bar{1}\cdot\bar{2}\cdot\bar{3}\cdots(\overline{p-1}) = \bar{a}\bar{1}\,\bar{a}\bar{2}\cdots\bar{a}\cdot(\overline{p-1})$$
$$= \bar{a}^{p-1}\,\bar{1}\bar{2}\bar{3}\cdots\overline{(p-1)}$$

$$1 = \bar{a}^{p-1}$$

Korollar: For alle $\bar{a}$, $\bar{a}^p = \bar{a}$.

Bevis:
- Sant for $\bar{a} = 0$.
- For $\bar{a} \neq 0$, $\bar{a}^{p-1} = 1 \Rightarrow \bar{a}^p = a$. ∎

$$\left.\begin{aligned}\bar{a}\bar{l} &= \bar{a}\bar{m}\\ \bar{a}(\bar{l}-\bar{m}) &= 0\end{aligned}\right\} \text{motsigelse}$$

44 EKSEMPEL $\overbrace{\quad\quad}^{*_n}$

Vis at $20n^7 + 14n^5 + n$ er delelig med 35 for alle n. Siden $35 = 7 \cdot 5$ holder det a vise at $*_n$ alltid e delelig med bade 5 og 7.

Fermat.

(mod 5) $\quad 20n^7 + 14n^5 + n = 0 \cdot n^7 + 14n + n = 15n = 0$

(mod 7) $\quad 20n + 0 + n = 21n = 0.$

45 DEF. EULERS ϕ-funksjon er gitt ved

$\phi(n) =$ antall naturlige tall $k \leq n$ s.a. $(k,n)=1$

Eulers Teorem.

46 V Anta at $(a,n)=1$.

Da er $\quad \bar{a}^{\phi(n)} = \bar{1} \quad ; \mathbb{Z}_n.$

Bevis: List opp alle elementer $\bar{a}_j$ med $(a,n)=1$.

$\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\phi(n)}$

Sep $\quad \bar{a}\bar{a}_1, \bar{a}\bar{a}_2, \dots, \bar{a}\cdot\bar{a}_{\phi(n)}$

Gjenta skutten pa basert for Fermat

4.7. Willsons Teorem.

For p prim så har vi at

$$\overline{(p-1)!} = \overline{-1} \quad i \ \mathbb{Z}_p.$$

Bevis: For $p=2$: $\overline{(p-1)!} = \overline{1!} = \overline{1} = \overline{-1}$.

For $p>2$ Da har vi at

$$\mathbb{Z}_p = \{\bar{1}\} \cup \{\bar{-1}\} \cup \{p_1, p_1^{-1}\} \cup \{p_2, p_2^{-1}\} \cup \dots \cup \{p_k, p_k^{-1}\}.$$

$$\overline{(p-1)!} = \overline{-1}. \quad \blacksquare$$

4.8. Lemma I $\mathbb{Z}_p$, p prim, så er 1 og -1 de eneste elementene som er sine egne inverser.

Bevis: Anta $\bar{x}^2 = 1$.

Da har vi $\bar{x}^2 - \bar{1} = 0$

$$\| $$

$$(\bar{x}+\bar{1})(\bar{x}-\bar{1})$$

som gir resultatet siden det ikke finns nulldivisorer i $\mathbb{Z}_p$ $\blacksquare$