.I Kvadratiska karaktären av 2, mod p, med ändliga kroppar.

På föreläsning brukar jag visa

$$(\frac{2}{p}) = (-1)^{(p^2-1)/8}$$

i något specialfall. Jag använder komplexa tal.

För den som läst abstrakt alebra kan en variant med ändliga kroppar, och Frobenius, verka naturligare.

Vi låter k beteckna kroppen $\mathbf{Z}_p$. Vidare får K stå för en spaltningskropp till polynomet X^4+1. θ betecknar någon rot. Det gäller $\theta^4 = -1$, $\theta^8 = 1$

Vi bildar nu

$$\alpha = \theta - \theta^3$$

som uppfyller

$$\alpha^2 = \theta^2 + \theta^6 - 2\theta^4 = \theta^2 - \theta^2 + 2 = 2$$

Ekvationen $X^2 = 2$ har alltså rötterna $X = \pm\alpha$ i K, och *inga andra*.

Så frågan är (för olika p) huruvida α tillhör primkroppen k eller ej. Frågan är alltså huruvida $\alpha^p = \alpha$.

$p \equiv 1 \pmod 8$:

$$\alpha^p = \theta^p - \theta^{3p} = \theta^{8k+1} - \theta^{3(8k+1)} = \theta - \theta^3,$$

eftersom $\theta^8 = 1$. Så $\alpha \in k$ och 2 är kvadratisk rest mod p.

$p \equiv 3 \pmod 8$:

$$\alpha^p = \theta^p - \theta^{3p} = \theta^{8k+3} - \theta^{3(8k+3)} = \theta^3 - \theta^9 = \theta^3 - \theta = -\alpha,$$

så $\alpha \notin k$, 2 ej kvadratisk rest mod p.

$p \equiv 5 \pmod 8$:

$$\alpha^p = \theta^p - \theta^{3p} = \theta^{8k+5} - \theta^{3(8k+5)} = \theta^5 - \theta^{15} = -\theta + \theta^3 = -\alpha,$$

eftersom $\theta^4 = -1$. 2 ej kvadratisk rest mod p.

$p \equiv 7 \pmod 8$:

$$\alpha^p = \theta^p - \theta^{3p} = \theta^{8k+7} - \theta^{3(8k+7)} = \theta^7 - \theta^5 = -\theta^3 + \theta = \alpha,$$

eftersom $\theta^4 = -1$. 2 är kvadratisk rest mod p.