Algebra 2 (2014)-Aalborg Universitet
Spiseseddel 18

18. gang (A), fredag 25. april, 8:15-12:00 i lokale G5-112

- 8:15-10:00 Forelæsning: Factorisering af $X^{p^n} - X$ i $\mathbb{F}_p$ og ElGamal (sider 160+173–176).

- 10:00-12:00 Opgaveregning og beviser: A, 39, 40, 41, B + exercises from previous lectures.

  Opgave A: Consider ElGamal cryptosystem. Encrypt and decrypt an example in Maple.

  Opgave B: Compute the cyclotomic classes modulo 15. Use Algorithm 2.3.1 in [JH] to factorize $X^{15} - 1$ (Hint: do not look to much in [JH], please).

  Beviser: Thoerem 4.8.8, Lemma 4.8.1, Theorem 4.8.5, Section 4.8.2, Proposition 4.6.7, Proposition 4.4.3.

Med venlig hilsen,

Diego