Problem List 5: Computer Algebra Manuel Ledo

Exercise 14 : Prove or disprove

a) $x^{1000}+2 \in \mathbb{F}_5[X]$ is squarefree

$f = x^{1000}+2 \in \mathbb{F}_5[X] \Rightarrow f' = 0 \Rightarrow$

$\gcd(f, f') = f \Rightarrow f$ is not squarefree. Disproved

b) Let F be a field and $f, g \in F[X]$. Then the squarefree part of fg is the product of square free parts of f and of g

$\underset{f}{x} \cdot \underset{g}{x} = \underset{f \cdot g}{x^2} \rightarrow$ squarefree part is x Disproved

Exercise 1: p prime, $f \in \mathbb{F}_p[X]$ has degree 4, and

$\gcd(x^p - x, f) = \gcd(x^{p^2} - x, f) = 1$

What can you say about the factorization of f in $\mathbb{F}_p[X]$?

By the theory seen in class, it is not going to have any proper divisor of degree at most 2, and hence, it is going to be an irreducible polynomial $\blacksquare$

Exercise 4: Let $p \in \mathbb{N}$ be a prime and some $f \in \mathbb{Z}[X]$ monic of degree n. Prove that $f(a) \equiv 0 \bmod p$ has n solutions $a \in \mathbb{Z}_p$ iff $f \bmod p$ is a factor of $x^p - x$.

$\Rightarrow$) $S = \{a_1, \dots, a_n\}$ set of solutions a_i's $\in \mathbb{Z}_p \Rightarrow$

$f(a_i) \equiv 0 \bmod p$. Moreover, since f is monic, $\deg(f \bmod p) = n$.

$\Rightarrow$ in $\mathbb{Z}_p$ $f = \prod_{i=1}^{n} (x - a_i)$

We know that $x^p - x$ by LFT $x^p - x = \prod_{a \in \mathbb{Z}_p} (x-a) \Rightarrow f \mid x^p - x$.

$\Leftarrow$) $f \bmod p$ has degree n since it is monic.

$f \bmod p$ factor of $x^p - x = \prod_{a \in \mathbb{Z}_p} (x-a) \Rightarrow f = \prod_{\substack{a_i \in \mathbb{Z}_p \\ 1 \le i \le n}} (x - a_i) \Rightarrow f(a_i) \equiv 0 \bmod p$.

Extra solutions to $f(a) \equiv 0 \bmod p$ would imply higher degree.