Algebraic Cryptography
Homework 4

Due Friday, 13 October 2017

Problem 1. Recall that a natural number $p > 1$ is said to be *prime* if it has no divisors x between $1 < x < p$. Prove that $p > 1$ is prime if and only if for any $a, b \in \mathbb{Z}$, whenever p divides ab, either p divides a or p divides b.

Exercise 2. Prove that $[\mathbb{R} : \mathbb{Q}] = \infty$ (*bonus:* more precisely, the degree is $2^{\aleph_0} = \mathfrak{c}$). Explain why "most" elements of $\mathbb{R}$ are transcendental over $\mathbb{Q}$ for a suitable interpretation of "most".

Exercise 3. Prove that if a polynomial $f \in \mathbb{R}[x]$ has odd degree $n > 2$, then f is reducible.

Exercise 4. Suppose α is a root of an irreducible polynomial of degree n over $\mathbb{F}$, so that $\mathbb{F}(\alpha)$ has degree n over $\mathbb{F}$. Find an $\mathbb{F}$-basis for $\mathbb{F}(\alpha)$ (you must prove it is a basis).

Problem 5. Prove that there are exactly $\frac{(p^2-p}{2}$ monic irreducible quadratic polynomials over $\mathbb{F}_p$. Then find all of the monic irreducible quadratic polynomials over $\mathbb{F}_3$, of which there should be 6 by the above formula.

Problem 6. Prove that a polynomial in $\mathbb{F}_p[x]$ has derivative identically zero if and only if it is the p-th power of a polynomial in $\mathbb{F}_p[x]$. Give a criterion for this to happen.

Problem 7. Let $\mathbb{K}$ be the splitting field of the polynomial $X^3 - 2$ over $\mathbb{F}$. Find the degree of $\mathbb{K}$ if $\mathbb{F}$ is: (a) $\mathbb{R}$, (b) $\mathbb{F}_5$, (c) $\mathbb{F}_7$, (d) $\mathbb{F}_{31}$. You must provide justification for your answers.