Algebraic Cryptography
Exam 2 Review

For the second exam you should know the following theorems:

Theorem 1. *If* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$*, then* $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}]\ [\mathbb{K} : \mathbb{F}]$.

Theorem 2. *A monic polynomial* $f \in \mathbb{Z}[x]$ *is irreducible in* $\mathbb{Z}[x]$ *if and only if it is irreducible in* $\mathbb{Q}[x]$.

Theorem 3 (Fundamental Theorem of Algebra)**.** *The field* $\mathbb{C}$ *of complex numbers is algebraically closed.*

Theorem 4. *The polynomial ring* $R[x]$ *is a PID if and only if* R *is a field.*

Lemma 5. *Suppose* g *is an element of finite order* n *in a group* G*. Then* g^j *has order* $\frac{n}{\gcd(j,n)}$.

Theorem 6. *The group* $\mathbb{F}_q^*$ *is cyclic. Moreover, if* g *is a generator of* $\mathbb{F}_q^*$*, then* g^j *is also a generator if and only if* $\gcd(j, q-1) = 1$.

Lemma 7. $(a+b)^p = a^p + b^p$ *in any field of characteristic* p.

Theorem 8. *If* $\mathbb{F}_q$ *is a field of* q *elements, then every element is a root of the polynomial* $x^q - x$ *and* $\mathbb{F}_q$ *is precisely the set of roots of that equation. Conversely, for every prime power* $q = p^f$*, the splitting field over* $\mathbb{F}_p$ *of the polynomial* $x^q - x$ *is a field of* q *elements.*

Theorem 9. *Let* $\mathbb{F}_q$ *be the field with* $q = p^f$ *elements and* σ *is Frobenius automorphism. Then the fixed field of* σ *is the prime field, i.e.,* $\mathbb{F}_q^\sigma = \mathbb{F}_p$*. Moreover, the order of* σ *(in the group* $\mathrm{Aut}(\mathbb{F}_q)$*) is* f.

Theorem 10. *Suppose* $\alpha \in \mathbb{F}_q$ *and* σ *is the Frobenius automorphism. Then the conjugates of* α *over* $\mathbb{F}_p$ *are the elements* $\sigma^j(\alpha) = \alpha^{p^j}$.

Theorem 11. *The subfields of* $\mathbb{F}_{p^f}$ *are* $\mathbb{F}_{p^d}$ *for* $d \mid f$*. Consequently, adjoining an element of* $\mathbb{F}_{p^f}$ *to* $\mathbb{F}_p$ *results in one of these fields.*

Theorem 12. *For* $q = p^f$*, the polynomial* $x^q - x$ *factors over* $\mathbb{F}_p$ *into the product of all monic irreducible polynomials of degrees* d *dividing* f.

You should be able to do the problems assigned as homework, as well as problems from Chapter 3 §2 and §3. You should also be able to complete the following exercises:

Exercise 1. *Prove that for any ring R, the ring $M_n(R)$ is noncommutative whenever $n \geq 2$.*

Exercise 2. *Prove that for a natural number p, $px = 0$ for* some $0 \neq x \in \mathbb{F}$ *if and only if $py = 0$ for* every $y \in \mathbb{F}$.

Exercise 3. *Prove that any field either has characteristic zero or characteristic p, where p is prime. (it cannot have composite characteristic)*

Exercise 4. *Prove that if $\mathbb{F}$ has characteristic p for some prime, then $\mathbb{F}$ contains a copy of $\mathbb{F}_p$, and similarly, if $\mathbb{F}$ has characteristic zero, then $\mathbb{F}$ contains a copy of $\mathbb{Q}$.*

Exercise 5. *Prove that $[\mathbb{R} : \mathbb{Q}] = \infty$ (*bonus: *more precisely, the degree is $2^{\aleph_0} = \mathfrak{c}$) and $[\mathbb{C} : \mathbb{R}] = 2$.*

Exercise 6. *Suppose R is an integral domain (i.e., has no zero divisors). Note that R is a subring of $R[x]$ (by identifying R with the constant polynomials). Prove $(R[x])^* = R^*$ under this identification.*

Exercise 7. *Prove that if a polynomial $f \in \mathbb{R}[x]$ has odd degree $n > 2$, then f is reducible.*

Exercise 8. *Prove the conditions in the definition of algebraically closed are actually equivalent.*

Exercise 9. *Explain why "most" elements of $\mathbb{R}$ are transcendental over $\mathbb{Q}$.*

Exercise 10. *Suppose $\mathbb{F}$ is a field and α is algebraic over $\mathbb{F}$. Prove that the set $J = \{f \in \mathbb{F}[x] \mid \alpha \text{ is a root of } f\}$ is an ideal of $\mathbb{F}[x]$. Conclude that α has a* minimum polynomial*; that is, a polynomial $m_\alpha \in \mathbb{F}[x]$ so that $m_\alpha(\alpha) = 0$ and whenever $f \in \mathbb{F}[x]$ with $f(\alpha) = 0$, m_α divides f. Note: To make the minimum polynomial unique, we also require that it is* monic, *i.e., the coefficient of the highest degree term is 1.*

Exercise 11. *Prove the equivalence in the previous definition. That is, if α is algebraic over $\mathbb{F}$, prove that $[\mathbb{F}(\alpha) : \mathbb{F}] = \deg m_\alpha$. As a corollary, conclude that $\alpha \in \mathbb{F}$ if and only if $\mathbb{F}(\alpha)$ has degree 1 over $\mathbb{F}$ if and only if $\mathbb{F}(\alpha) = \mathbb{F}$.*

Exercise 12. *Prove that the splitting field of $x^3 - 2$ is $\mathbb{Q}(\omega, \sqrt[3]{2})$ and that $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$.*

Exercise 13. *If $f \in \mathbb{F}[x]$ is irreducible of degree d, what are the minimum and maximum possible degrees of the splitting field of f over $\mathbb{F}$?*

Exercise 14. *If a polynomial $f(x)$ has a root α of multiplicity $m \geq 2$ (ie., has $(x-\alpha)^m$, then α is also a root of its derivative $f'(x)$.*

Exercise 15. *Suppose $\mathbb{F}$ is a finite field with q elements, which we will henceforth denote $\mathbb{F}_q$ (we will prove uniqueness up to isomorphism later). Prove that $q = p^n$ for some $n \in \mathbb{N}$ and some prime p.*

Exercise 16. *Prove that* $\operatorname{lcm}(j, n) = \frac{nj}{\gcd(j,n)}$.

Exercise 17. *Let* $\mathbb{F} \subseteq \mathbb{K}$ *be an extension of fields and* $\tau \in \operatorname{Aut}(\mathbb{K})$ *an automorphism which fixes* $\mathbb{F}$. *If* α *is a root of an irreducible polynomial* $f \in \mathbb{F}[x]$, *then* $\tau(\alpha)$ *is a* conjugate *of* α *over* $\mathbb{F}$. *That is,* $\tau(\alpha)$ *is also a root of* f.

Exercise 18. *If* f *is a prime number, then there are* $\frac{p^f - p}{f}$ *distinct monic irreducible polynomials of degree* f *over* $\mathbb{F}_p$.

Exercise 19. *Provide a formula for the number of distinct monic irreducible polynomials of degree* f *(not necessarily prime) over* $\mathbb{F}_p$ *in terms of the divisors of* f.