Algebraic Cryptography
Homework 5

Due Wednesday, 25 October 2017

We begin with a bit more number theory, because it came up in our algebra material.

Exercise 1. Prove that $\operatorname{lcm}(j, n) \gcd(j, n) = nj$. If you choose to use the Fundamental Theorem of Arithmetic, you should first prove that; but there is an easier way.

Problem 2. Let $\varphi : \mathbb{N} \to \mathbb{N}$ denote Euler's totient function. That is, $\varphi(n)$ denotes the number of positive integers less than or equal to n which are relatively prime to n. We encountered this function before when reducing the RSA problem to the Integer Factorization Search problem in polynomial time. Since you were unfamiliar with it, I thought it would be good for you to review the basic properties.

(a) Prove that $\varphi(p^k) = p^k - p^{k-1}$ for any prime p.

(b) Prove that
$$\sum_{d|N} \varphi(d) = N.$$

(c) Prove that φ is *multiplicative*. That is, prove that if $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Now for the algebra.

Exercise 3. 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.

Problem 4. Prove that the number of k-th roots of unity in $\mathbb{F}_{p^f}$ is equal to $\gcd(k, p^f - 1)$.

Problem 5. Suppose that $\alpha \in \mathbb{F}_{p^2}$ is a root of the polynomial $x^2+ax+b \in \mathbb{F}_p[x]$.

(a) Prove that α^p is also a root of this polynomial.

(b) Prove that if $\alpha \notin \mathbb{F}_p$, then $a = -\alpha - \alpha^p$ and $b = \alpha^{p+1}$.

(c) Prove that if $\alpha \notin \mathbb{F}_p$ and $c, d \in \mathbb{F}_p$, then $(c\alpha + d)^{p+1} = d^2 - acd + bc^2$ (which is an element of $\mathbb{F}_p$).

(d) Let i be a square root of -1 in $\mathbb{F}_{19^2}$. Use part (c) to find $(2+3i)^{101}$ (that is, write it in the form $a + bi$ for $a, b \in \mathbb{F}_{19}$.

Problem 6. Consider $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ (i.e., the group of units of this ring; the set of integers relatively prime to p^α with multiplication mod p^α) where p is prime.

(a) Suppose $p > 2$, and let g be an integer that generates $\mathbb{F}_p^*$. Let α be any integer greater than 1. Prove that either g or $(p+1)g$ generates $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. Thus the latter is also a *cyclic group*.

(b) Prove that if $\alpha > 2$, then $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ is *not* cyclic, but that the number 5 generates a *subgroup* consisting of half of its elements, namely those which are $\equiv 1 \pmod 4$.