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.

Proof. Suppose that $p > 1$ is prime and p divides ab, but does not divide a. Then since the only positive divisors of p are $1, p$, the only common divisor of p and a is 1, thus $\gcd(p, a) = 1$. By Bezout's identity, there are integers x, y for which $1 = \gcd(p, a) = px + ay$. Since p divides ab, we have $ab = cp$ for some integer c. Therefore,

$$cpy = aby = b(1 - px) = b - px,$$

and hence $b = p(x + cy)$, so p divides b.

For the other direction, suppose that whenever p divides ab, either p divides a or p divides b. Let $p = ab$ be any factorization of p into positive integers. By hypothesis, either p divides a or p divides b. Without loss of generality, we will assume p divides a, and hence $p \leq a$, but then $b \leq 1$, and since a, b are positive integers, we must have $b = 1$ and hence $a = p$. Since any factorization of p has the form $p \cdot 1$, we must have that p is prime. ■

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".

Proof. There are plenty of ways to show that $[\mathbb{R} : \mathbb{Q}] = \infty$, but I will pick an easy one that also shows that most elements of $\mathbb{R}$ are transcendental over $\mathbb{Q}$. Suppose that $\mathbb{F}$ is any extension of $\mathbb{Q}$ of degree at most $\aleph_0$ (i.e., there is a countable basis). Then we will show the cardinality of $\mathbb{F}$ is $\aleph_0$.

Consider a basis $\mathcal{B}$ for $\mathbb{F}$ over $\mathbb{Q}$ which has cardinality $\aleph_0$. Then let $F(\mathcal{B})$ denote the set of finite subsets of $\mathcal{B}$, which we note also has cardinality $\aleph_0$. Finally,

$$\mathbb{F} = \left\{ \sum_{x \in F} c_x x \;\middle|\; F \in F(\mathcal{B}), c_x \in \mathbb{Q} \right\}$$

has cardinality $\aleph_0$.

Since the cardinality of $\mathbb{R}$ is $\mathfrak{c} = 2^{\aleph_0} > \aleph_0$, we must have that $[\mathbb{R} : \mathbb{Q}] > \aleph_0$ (in fact, the above argument actually shows it must be $\mathfrak{c}$). Finally, to show that "most" elements of $\mathbb{R}$ are transcendental over $\mathbb{Q}$, it suffices to show there are only $\aleph_0$ algebraic elements. Indeed, there are countably many polynomials in $\mathbb{Q}[x]$ (identified with $\bigcup_{n=1}^{\infty} \mathbb{Q}^n$, which is a countable union of countable sets and is therefore countable itself). Each polynomial $p \in \mathbb{Q}[x]$ has finitely many ($\deg p$) roots (not necessarily in p), and the countable union of finite sets is countable. Therefore there are only countably many algebraic elements over $\mathbb{Q}$. Since $\mathbb{R}$ has cardinality $\mathfrak{c}$, most (i.e., all but countably many) of its elements must be transcendental over $\mathbb{Q}$. ■

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

Proof. Let $a_n \neq 0$ denote the coefficient of the x^n term of f. Let $\operatorname{sgn}(a_n)$ be 1 if $a_n > 0$ and -1 if $a_n < 0$. Then

$$\lim_{x \to \pm\infty} \frac{f(x)}{x^n} = a_n$$

and hence

$$\lim_{x \to \pm\infty} f(x) = \operatorname{sgn}(a_n)(\pm\infty).$$

In particular, this entails that there exist $a \neq b \in \mathbb{R}$ so that $f(a) < 0$ and $f(b) > 0$. Therefore, on the interval I joining a, b, by the Intermediate Value Theorem there is some $c \in I$ for which $f(c) = 0$. In other words, c is a root of f, and so we may factor $f(x) = (x - c)g(x)$ for $g \in \mathbb{R}[x]$ of degree strictly less than n. Therefore 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).

Proof. Suppose that α is a root of the irreducible polynomial p of degree n over $\mathbb{F}$. Note that $\mathbb{F}(\alpha)$ is the smallest field containing $\mathbb{F}$ and α. In particular, $\{\alpha^k\}_{k \in \mathbb{Z}}$ is an $\mathbb{F}$-spanning set for $\mathbb{F}(\alpha)$. We claim that $\{\alpha^k \mid 0 \leq k < n\}$ is a basis.

To see that this set is linearly independent, suppose that $\sum_{k=0}^{n-1} c_k \alpha^k = 0$ for some $c_k \in \mathbb{F}$. Then either α is a root of the polynomial $f(x) := \sum_{k=0}^{n-1} c_k x^k \in \mathbb{F}[x]$, or else f is the zero polynomial. Consider the ideal of polynomials for which α is a root. Since $\mathbb{F}[x]$ is a PID, this ideal is principally generated by some polynomial m_α. Therefore, its degree must be less than or equal to the degree of any polynomial for which α is a root, and it must divide any such polynomial. If α were a root of f, then m_α would have degree less than n and would also divide p, contradicting the irreducibility of p. Therefore, f is the zero polynomial, and therefore $\{\alpha^k \mid 0 \leq k < n\}$ is linearly independent. In fact, this shows that $m_\alpha = p$ (at least, up to multiplication by a unit, i.e., a nonzero element of $\mathbb{F}$).

To see that $\{\alpha^k \mid 0 \leq k < n\}$ spans $\mathbb{F}(\alpha)$ it suffices to show that any other power of α can be written as a linear combination of these. For this, it suffices to show that α^{-1} and α^n can be written as a linear combination of these, and that any α^k with $k \geq n$ can be written as a linear combination of powers of α with a smaller nonnegative exponent. To this end, let $p(x) = \sum_{k=0}^n b_k x^k$. Note that $b_0 \neq 0$, for otherwise 0 is a root of p, contradicting irreducibility. Then $0 = \sum_{k=0}^n b_k \alpha^k$, and so multiplying by $\frac{\alpha^{-1}}{b_0}$ and rearranging, we find

$$\alpha^{-1} = -\sum_{k=1}^{n} \frac{b_k}{b_0}\alpha^{k-1} = -\sum_{k=0}^{n-1} \frac{b_{k+1}}{b_0}\alpha^k.$$

Similarly, we can divide $p(\alpha) = 0$ by b_n and rearrange to obtain

$$\alpha^n = -\sum_{k=0}^{n-1} \frac{b_k}{b_n}\alpha^k.$$

Thus $\{\alpha^k \mid 0 \leq k < n\}$ is a spanning set, and therefore a basis, for $\mathbb{F}(\alpha)$. ■

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 3 by the above formula.

Proof. Notice that there are p^2 monic quadratic polynomials over $\mathbb{F}_p$ (because the first coefficient must be 1 and the other coefficients are a free choice). A monic quadratic polynomial over $\mathbb{F}_p$ is reducible if and only if it has a root in $\mathbb{F}_p$ if and only if it factors as $(x-a)(x-b)$ for some $a, b \in \mathbb{F}_p$. Of these there are $\binom{p}{2} = \frac{p(p-1)}{2}$ with distinct roots and $\binom{p}{1} = p$ with a repeated root, for a total of $\frac{p(p+1)}{2}$ monic reducible quadratic polynomials over $\mathbb{F}_p$. Thus there are $p^2 - \frac{p(p+1)}{2} = \frac{p^2-p}{2}$ monic irreducible quadratic polynomials over $\mathbb{F}_p$.

From the previous paragraph, it suffices to find 3 monic quadratic polynomials over $\mathbb{F}_3$ for which none of $0, 1, 2$ are a root. It is easily checked that the polynomials given below satisfy that criterion.

$$\begin{gathered} x^2 + 1, \\ x^2 + x + 2, \\ x^2 + 2x + 2. \end{gathered}$$

■

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.

Proof. Suppose that f is the p-th power of a polynomial $g \in \mathbb{F}_p[x]$. Note that we still have the chain rule, even for formal derivatives. Thus since $f = g^p$, we have that $f' = pg^{p-1}g'$ which is identically zero since it is a multiple of p. Alternatively, if $g(x) = \sum_{k=0}^{n} c_k x^k$, then

$$f(x) = (g(x))^p = \left(\sum_{k=0}^{n} c_k x^k\right)^p = \sum_{k=0}^{n} c_k^p x^{kp},$$

thus

$$f'(x) = \sum_{k=1}^{n} c_k^p kpx^{kp-1} = p\left(\sum_{k=1}^{n} c_k^p kx^{kp-1}\right) = 0.$$

Now suppose that $f \in \mathbb{F}_p[x]$ with $f' \equiv 0$. If $f(x) = \sum_{k=0}^{n} c_k x^k$, then our hypothesis is:

$$f'(x) = \sum_{k=1}^{n} c_k kx^{k-1} \equiv 0.$$

In other words, $c_k k = 0$ for all $1 \leq k \leq n$. Since $\mathbb{F}_p$ is a field, this means that for $1 \leq k \leq n$, $c_k = 0$ if k is not a multiple of p. This shows that

$$f(x) = \sum_{k=0}^{m} c_{kp} x^{kp}$$

where $km = n$. Notice that if we set

$$g(x) := \sum_{k=0}^{m} c_{kp} x^k$$

then

$$(g(x))^p = \left(\sum_{k=0}^{m} c_{kp} x^k\right)^p = \sum_{k=0}^{m} c_{kp}^p x^{kp} = \sum_{k=0}^{m} c_{kp} x^{kp} = f(x),$$

where the second to last equality follows from Fermat's Little Theorem.

The criterion is that coefficients of powers of x which are not multiples of p are zero. ■

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.

Proof. Let $\mathbb{F}$ and $\mathbb{K}$ be as in the question.

(a) $x^3 - 2$ is reducible over $\mathbb{R}$ since $\sqrt[3]{2} \in \mathbb{R}$ is a root. Thus

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2)$$

Moreover, the quadratic factor above is irreducible because it has no roots in $\mathbb{R}$ since the discriminant is negative (in fact, its roots are $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ where ω is a primitive cube root of unity. Once we adjoin either root, this polynomial will factor entirely. Thus $[\mathbb{K} : \mathbb{R}] = [\mathbb{R}(\omega) : \mathbb{R}] = 2$.

(b) $x^3 - 2$ is reducible over $\mathbb{F}_5$ since 3 is a root, but it is not a repeated root since 3 is not a root of the derivative $3x^2$. Moreover, no other elements of $\mathbb{F}_5$ are roots of $x^3 - 2$. So $x^3 - 2 = (x-3)(x^2 + 3x + 4)$, and the quadratic term is irreducible over $\mathbb{F}_5$. Once we adjoin either root of this quadratic, the original polynomial splits. Let α be a root of $x^2 + 3x + 4$. Then $[\mathbb{K} : \mathbb{F}_5] = [\mathbb{F}(\alpha) : \mathbb{F}] = 2$.

(c) $x^3 - 2$ has no roots over $\mathbb{F}_7$ and is therefore irreducible (because it has degree three; any reducible polynomial of degree three must split into linear factors or a linear and a quadratic. Either way, it has a root in the field). Let α be any of the roots of $x^3 - 2$. We claim that $x^3 - 2$ factors completely over $\mathbb{F}_7(\alpha)$. Indeed,

$$x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2) = (x - \alpha)(x - 2\alpha)(x - 4\alpha).$$

Therefore, $\mathbb{K} = \mathbb{F}_7(\alpha)$ and $[\mathbb{F}_7(\alpha) : \mathbb{F}_7] = 3$.

If you are wondering how we obtained the factorization above, we divide $x^3 - 2$ by $x - \alpha$, and then apply the quadratic formula (which we can do since we are not in characteristic 2) to the discriminant $\alpha^2 - 4\alpha^2 = (-3)\alpha^2$ has square root 2α, and the multiplicative inverse of 2 is 4 in $\mathbb{F}_7$, so we obtain

$$\frac{-\alpha \pm \sqrt{\alpha^2 - 4\alpha^2}}{2} = 4(-\alpha \pm \sqrt{-3\alpha^2}) = 4\alpha(-1 \pm 2) = 4\alpha, -12\alpha = 4\alpha, 2\alpha.$$

(d) Note that $4, 7, 20$ are already roots of $x^3 - 2$ since $4^3 - 2 = 62 = 2 \cdot 31$, $7^3 - 2 = 341 = 31 \cdot 11$, and $20^3 - 2 = 7998 = 31 \cdot 258$. Thus $\mathbb{F}_7 = \mathbb{K}$ and hence $[\mathbb{K} : \mathbb{F}_7] = 1$.

■