Solutions to HW2

1. (*20 points*) Let p be prime, and consider the field $F = \mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ of order p (the integers mod p).

   (a) The function $g : F \to F$, $g(a) = a^3 - a$ satisfies $g(0) = g(1) = g(-1) = 0$, so it is not one-to-one.

   (b) Because $|F| < \infty$, a function $F \to F$ is one-to-one iff it is into. By (a), g is not one-to-one; so it is not onto.

   (c) By (b), we may choose $b \in F$ such that for all $a \in F$, $g(a) \neq b$. This means that the polynomial $f(x) = x^3 - x - b \in F[x]$ has no root in F, so it has no linear factor in $F[x]$. Because $f(x)$ has degree 3, this means that $f(x)$ is irreducible in $F[x]$.

   (d) Yes for $K = \mathbb{Q}$; but no for $K \in \{\mathbb{R}, \mathbb{C}\}$. By the Fundamental Theorem of Algebra, every polynomial in $\mathbb{C}[x]$ of degree 3 factors into linear factors in $\mathbb{C}[x]$. The fact that every polynomial of degree 3 in $\mathbb{R}[x]$ has a real root (and hence a linear factor in $\mathbb{R}[x]$) is well-known from elementary Calculus. (It also follows by purely algebraic arguments using the Fundamental Theorem of Algebra, and the fact that complex roots come in conjugate pairs.) The polynomial $x^3 - x + 1 \in \mathbb{Q}[x]$ is irreducible in $\mathbb{Q}[x]$ since it is irreducible in $\mathbb{Z}[x]$. For the latter fact, note that any nontrivial factorization $x^3 - x + 1 = (x - a)(x^2 + bx + c)$ in $\mathbb{Z}[x]$ requires $a \mid 1$, so that $a \in \{\pm 1\}$. However, neither of the values ± 1 is a root of $x^3 - x + 1$, so this is impossible.

2. (*20 points*) Let $k, \ell, m, n \in \mathbb{Z}$, and consider the polynomial $f(x) = x^4 + 2kx^3 + 2\ell x^2 + (2m+1)x + (2n+1) \in \mathbb{Z}[x]$. If there is a nontrivial factorization $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$, then the factors $g(x), h(x) \in \mathbb{Z}[x]$ are monic of degree $1, 3$ or $2, 2$. Then, reduction modulo 2 gives a factorization of $x^4 + x + 1 \in \mathbb{F}_2[x]$ into monic factors of degree $1, 3$ or $2, 2$ in $\mathbb{F}_2[x]$. This cannot happen because $x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, as we showed in class on October 7. This proves the required result by contradiction.

3. (*30 points*) Consider the two fields $E = F[\alpha]$ and $K = F[\beta]$ of order 16, constructed as in the assignment.

   (a) Here we tabulate the coefficients $(a, b, c, d) \in F^4$ such that $\alpha^k = a + b\alpha + c\alpha^2 + d\alpha^3$ for $k = 0, 1, 2, \ldots, 14$:

k	(a,b,c,d)
0	$(1,0,0,0)$
1	$(0,1,0,0)$
2	$(0,0,1,0)$
3	$(0,0,0,1)$
4	$(1,1,0,0)$
5	$(0,1,1,0)$
6	$(0,0,1,1)$
7	$(1,1,0,1)$
8	$(1,0,1,0)$
9	$(0,1,0,1)$
10	$(1,1,1,0)$
11	$(0,1,1,1)$
12	$(1,1,1,1)$
13	$(1,0,1,1)$
14	$(1,0,0,1)$

(a) Using the vector coordinates in F^4 for elements of E (expressing each field element as linear combinations of the basis $1, \alpha, \alpha^2, \alpha^3$), we have

$$\begin{aligned} g(\alpha^3) &= \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + 1 \\ &= (1,1,1,1) + (0,1,0,1) + (0,0,1,1) + (0,0,0,1) + (1,0,0,0) \\ &= (0,0,0,0). \end{aligned}$$

This is the zero element of E.

(c) The roots of $f(x) = x^4+x+1$ are $\alpha, \alpha^2, \alpha^4, \alpha^8$. This is to be expected since the map $u \mapsto u^2$ is an automorphism of E, which therefore permutes the roots of $f(x)$.

(d) The roots of x^4+x^3+1 are $\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$. (These are the other elements of multiplicative order 15 not included in (c).)

4. By listing the value of $2^k \bmod 101$ for $k = 0, 1, \ldots, 99$ and searching for the values 94 and 81, we obtain $a = 59$ and $b = 76$. (The only reason this succeeds is the dangerously small choice of the prime $p = 101$.) Finally, the 'secret' key is 31 since $94^{76} \equiv 81^{59} \equiv 31 \bmod 101$.