Coding Theory

Sheet 3

Spring 2014

1. Write out addition and multiplication tables for $\mathbf{F}_4$.

2. Which elements are primitive in each of the four fields $\mathbf{F}_5$, $\mathbf{F}_7$, $\mathbf{F}_{13}$, $\mathbf{F}_{17}$ in Question 10 on Sheet 2?

3. In $\mathbf{F}_q$, $q = p^h$, with p prime, show that
$$(x + y)^p = x^p + y^p.$$

4. Find all monic irreducible quadratics in $\mathbf{F}_3[X]$. Which ones are primitive?

   (i) Use a primitive quadratic with root σ to write the non-zero elements of $\mathbf{F}_9$ both in the form $a_0 + a_1\sigma$, with $a_0, a_1 \in \mathbf{F}_3$, and in the form σ^i, with $0 \leq i \leq 7$; find the order of each element.

   (ii) Use a non-primitive quadratic with root τ to write the non-zero elements of $\mathbf{F}_9$ in the form $a_0 + a_1\tau$; find the order of each element.

   (iii) Find an isomorphism between these two $\mathbf{F}_9$'s.

5. Find all irreducible cubics in $\mathbf{F}_2[X]$. Which ones are primitive?

6. Is $X^4 + 1$ irreducible over $\mathbf{F}_3$?

7. Find a primitive quartic F in $\mathbf{F}_2[X]$. If $F(\alpha) = 0$, express the powers α^i, for $i = 0, \ldots, 15$, as polynomials in α of degree at most 3.

8. If $N(m, q)$ is the number of monic irreducible polynomials of degree m in $\mathbf{F}_q[X]$, show, without using the formula in the lectures, that

   (i) $N(2, q) = (q^2 - q)/2$;   (ii) $N(3, q) = (q^3 - q)/3$.

9. Are the following valid ISBN-10s: (i) 3 411 02175 6;   (ii) 2 85036 008 X ?

10. In the following ISBN-10, calculate the digit that has been replace by an asterisk: 0 521 283 $*$ 87.

11. What is the minimum distance of the ISBN-10 code?

12. Is the following a valid ISBN-13:
$$978\,0\,521\,771194\,8\,?$$

13. In the following codabar numbers, calculate the digit x:

    (i) 4539 2786 4132 127x;   (ii) 4929 x462 7341 3478.