Coding and Cryptography Fall 2016
Worksheet on finite fields – Part II

Katherine E. Stange

October 26, 2016

1. Recall last class how we built $\mathbb{F}_4$, the field of four elements, as polynomials in X with coefficients modulo 2, and considered modulo $X^2 + X + 1$. If anyone was missing, give them a quick rundown.
2. Now try to do the same, but using polynomials in Y with coefficients modulo 2, considered modulo $Y^2 + Y$. (I've used Y just so as to distinguish from the last case). In particular, determine the addition, multiplication and division tables. Use the smallest names for the elements, i.e. smallest coefficients and lowest degree.
3. Is this new thing a field? Which, if any, of the field axioms fail? Here they are again, for reference.
   (a) There is an element e_A which satisfies $a + e_A = a$ for all a.
   (b) There is an element e_M which satsifies $ae_M = a$ for all a.
   (c) The elements e_A and e_M are distinct.
   (d) For each a, there is an element a'_A satisfying $a + a'_A = e_A$.
   (e) For each non-zero a, there is an element a'_M satisfying $aa'_M = e_M$.
   (f) Addition is associative.
   (g) Multiplication is associative.
   (h) Addition is commutative.
   (i) Multiplication is commutative.
   (j) Multiplication distributes over addition.
4. Verify: only one field axiom fails. That means we got a *ring*, but not a field.

5. Suppose we consider polynomials in X with coefficients modulo n and considered modulo a polynomial $f(X)$. How many elements does the resulting ring, denoted $(\mathbb{Z}/n\mathbb{Z})[X]/(f(X))$, have? Justify.

6. In order for the ring to be a field, what must be true about n and $f(X)$? Justify.

7. Use the Euclidean algorithm to find the gcd of $X^3 + X - 1$ and $X^3 - X + 1$ in the ring of polynomials with coefficients modulo 3.

8. Remember how to do Euclidean algorithm to find an inverse modulo p, by finding 7^{-1} modulo 13. (If there's one thing you will be able to do at the end of this course, it's that!)

9. By analogy to this case, replace $\mathbb{Z}/13\mathbb{Z}$ with $\mathbb{F}_9 = (\mathbb{Z}/3\mathbb{Z})[X]/(X^3 - X - 1)$ and find the inverse of $X + 1$ using the Euclidean algorithm. Verify your answer is correct by multiplying to check.