Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall 2017

Extra Credit Problem Set # 11 (due on Wednesday 13 December)

Reading: DF 7.4–7.6, 8.1–8.3, 9.1–9.2.

Problems:

1. DF 7.4 Exercises 37, 38.

2. DF 7.5 Exercises 3, 5.

3. DF 8.1 Exercises 3, 6, 8, 12.

4. DF 8.2 Exercises 3, 5.

5. DF 8.3 Exercise 8.

6. DF 9.1 Exercises 13 (**Hint.** For any commutative ring R with 1 and any $g \in R$, prove that $R[x]/(x-g) \cong R$, then use this to prove that $y^2 - x$ is prime in $F[x,y]$).

7. DF 9.2 Exercises 2, 3 (this provides a way to build more finite fields).

8. *Finite field with p^2 elements.* Before, we constructed $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$. In an analogous way, construct $\mathbb{F}_9$, $\mathbb{F}_{25}$, and $\mathbb{F}_{49}$.

9. *Subgroups of fields.* Let F be a field.

(a) Prove that any nonzero polynomial of degree n with coefficients in F has at most n roots in F. Hint. Induction on the degree of the polynomial.

(b) Prove that every finite subgroup of the multiplicative group $F^\times = F \smallsetminus \{0\}$ is cyclic. Hint. Fix a prime p dividing the order n of the subgroup, let q be the highest power of p dividing n. Consider the map $F^\times \to F^\times$ defined by raising to the n/q power. By considering the orders of the kernel and image of this map, conclude that there is an element of this subgroup of order q (at some point, you'll need the previous part). Do this for each prime dividing n and then find a generator for the group.

(c) Prove that if F is a finite field then $F^\times$ is cyclic. For each field F having at most 7 elements, find an explicit generator of $F^\times$.

10. Call a positive integer n *special* if there exists an integer m with $1 < m < n$ so that

$$1 + 2 + \cdots + (m-1) = (m+1) + \cdots + n.$$

For example, $n = 8$ is special with $m = 6$, while $n = 7$ is not special. Find all positive integers that are special.

11. *RSA Public Key Yale Example, cf. DF 8.1 Exercise 12.* You intercept a message from President Salovey to the Yale Corporation encrypted using the public key $N = 3610003458000828019$ and $d = 3123534573$. The encrypted message is $M_1 = 2651355372442353120$. Decrypt the message and try various ciphers to figure out what Salovey is trying to tell them. **Hint.** You might enjoy learning about the Extended Euclidean algorithm.