Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall 2016

Extra Credit Problem Set # 11 (due on Wednesday 14 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, 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. *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 $N = 10002200057$ and $d = 2527221139$. The encrypted message is $M_1 = 8403912879$. Decrypt the message and try various ciphers to figure out what Salovey is trying to tell them. **Hint.** Use a computer.