SOAR Math Course Homework Eight Solutions Spring, 2003

These solutions are written at the request of students. Please let me know if you don't understand these solutions; I'm happy to expand on them if necessary.

3. (c) Show that part (b) allows us to factor $x^d - 1$ into

$$x^d - 1 \equiv x(x-m)(x-m^2)(x-m^3)\cdots(x-m^{d-1}) \bmod p.$$

(Hint: what are the roots of the equation on the left-hand side? On the right-hand side? You may assume that a polynomial of degree d has at most d roots.)

Solution: The solution here is to use the following fact: k is a root of a polynomial if and only if $(x-k)$ is a factor of the polynomial. In this case, we know from (b) that the d roots of $x^d - 1$ are 0, m, m^2, and so on up to m^{d-1}. This means that $(x-0)$, $(x-m)$, $(x-m^2)$, and so on up to $(x-m^{d-1})$ are all factors of $x^d - 1$. Thus we must have

$$x^d - 1 = Cx(x-m)(x-m^2)(x-m^3)\cdots(x-m^{d-1})$$

for some constant C. If you multiply out the right-hand side, the highest power of x is Cx^d. Matching this with the left-hand side's x^d, we get $C = 1$. This gives us the desired factorization.