Mathematics 216
Robert Gross
Homework 30
Answers

1. Let p be an odd prime. Show that in $\mathbf{F}_p[x]$, the polynomial $x^{p-1} - 1$ factors as

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\cdots(x-(p-2))(x-(p-1))$$

Answer: Let $f(x) = x^{p-1} - 1$. Fermat's Little Theorem tells us that $f(1) = f(2) = \cdots = f(p-1) = 0$, and therefore we know that $x-1$, $x-2$, $\cdots$, $x-(p-1)$ are all factors of $x^{p-1} - 1$. Because those irreducible factors are all unequal, we know that their product must divide $x^{p-1} - 1$. We can therefore write

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

Now, the left-hand side has degree $p-1$, and the right hand side has degree $p-1+\deg(g)$. That shows that $g(x)$ must be a constant. Now, comparing the coefficients of x^{p-1} says that $g(x) = 1$, and we have the desired result.

2. Substitute $x \equiv 0$ into this factorization to derive a congruence involving $(p-1)!$.
Answer: Substitute $x = 0$, and we have

$$-1 \equiv (-1)(-2)(-3)\cdots(-(p-1)) = (-1)^{p-1}(p-1)!.$$

Because p is an odd prime, $p-1$ is even, so we have

$$(p-1)! \equiv -1 \pmod{p}.$$

This result is called *Wilson's Theorem.*

3. Show that in $\mathbf{Z}/12\mathbf{Z}[x]$, there are two different ways to factor the polynomial $x^2 - x$ into linear factors.
Answer: This is trial and error. One factorization is obviously $x^2 - x = x(x-1)$. A bit of work also gives $x^2 - x \equiv (x-4)(x-9)$.