Week 3 Final, Math 102 **Name:** *James Wang*
Sept 20, 2023

(15.6.1)

Since g divides f, we can write $f = gk$ for some $k \in F[x]$.

Taking the derivative of f, we get $f' = g'k + gk'$ by the product rule.

Since g also divides f', g has to divide $g'k$ by observation.

Recall that F is a field, so $F[x]$ must be a UFD. Recall further that every irreducible element in a UFD is prime. Given g is irreducible in $F[x]$, g must also be prime.

This means either g divides g' or g divides k.

Suppose for the sake of a contradiction that g divides g'. Notice that since $deg(g) > deg(g')$, g cannot divide g' unless $g' = 0$.

Furthermore, F is a field of characteristic 0. So if $g' = 0$, then g must be a constant polynomial. Yet our coefficients are in a field, so g must then be a unit, which is not irreducible by definition. And we have reached a contradiction.

Hence it must be that g divides k, and $f = gk = ggh = g^2h$ for some $h \in F[x]$.

We have proved that g^2 divides f.

QED

(15.7.3)

We want to find some $a \in \mathbb{F}_{13}$ such that $a^{13} = 2$.

Since $|\mathbb{F}_{13}| = 13$, we know the elements of $\mathbb{F}_{13}$ are roots of the polynomial $x^{13} - x$.

Now using $x = 2$, we get $2^{13} - 2 = 0$. It follows that $2^{13} = 2$.

Hence a 13th root of 2 in $\mathbb{F}_{13}$ is just 2.

(15.7.4)

We recall an important theorem: Let p be a prime integer, and let p^r be a positive power of p. The irreducible factors of the polynomial $x^{p^r} - x$ over the prime field $\mathbb{F}_p$ are the irreducible polynomials in $\mathbb{F}_p[x]$ whose degrees divide r.

First consider the number of irreducible polynomials of degree 3 over $\mathbb{F}_3$:

Since our field is $\mathbb{F}_3$, let $p = 3$. We claim that letting $r = 3$ will help us proceed, because the irreducible factors of $x^{3^3} - x = x^{27} - x$ over $\mathbb{F}_3$ are exactly the irreducible polynomials of degrees 1 and 3 over $\mathbb{F}_3$.

We know the linear polynomials in $\mathbb{F}_3[x]$: $x, x-1, x-2$ are all irreducible, and their product is degree 3. Thus, we know the product of all irreducible polynomials of degree 3 over $\mathbb{F}_3$ must give us degree $27 - 3 = 24$. And we see $24 \div 3 = 8$.

Hence there are 8 irreducible polynomials of degree 3 over $\mathbb{F}_3$.

We use the same method for the number of irreducible polynomials of degree 3 over $\mathbb{F}_5$:

Since our field is $\mathbb{F}_5$, let $p = 5$. We claim that letting $r = 3$ will help us proceed, because the irreducible factors of $x^{5^3} - x = x^{125} - x$ over $\mathbb{F}_3$ are exactly the irreducible polynomials of degrees 1 and 3 over $\mathbb{F}_5$.

We know the linear polynomials in $\mathbb{F}_5[x]$: $x, x-1, x-2, x-3, x-4$ are all irreducible, and their product is degree 5. Thus, we know the product of all irreducible polynomials of degree 3 over $\mathbb{F}_5$ must give us degree $125 - 5 = 120$. And we see $120 \div 3 = 40$.

Hence there are 40 irreducible polynomials of degree 3 over $\mathbb{F}_5$.

(15.8.1)

We want to show every finite extension K of a finite field F is generated by an element α such that $F(\alpha) = K$.

Since F is finite and K is a finite extension of F, K must also be finite.

So $|K| = p^r$ for some prime integer p and positive integer r.

Recall that the multiplicative group $K^\times$ of nonzero elements of K is a cyclic group of order $p^r - 1$, which means there is a generator α of $K^\times$ such that $F(\alpha) = K$.

Hence α is a primitive element that generates the extension K/F.

$$QED$$