Last name _____

First name _____

LARSON—MATH 401—CLASSROOM WORKSHEET 38
Finite Fields.

F is a field (any field). $F[x]$ is the ring of polynomials over F.

If F is a finite field and $f(x)$ is an irreducible polynomial over F then $F[x]/\langle f(x)\rangle$ is a finite field.

We showed that x^2+1 is irreducible in $\mathbb{Z}_3[x]$. So $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field.

We noted that the elements of $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ can be thought of as the possible remainders of dividing polynomials in $\mathbb{Z}_3[x]$ by x^2+1. These are the 9 polynomials of the form a_0+a_1x, with $a_i \in \mathbb{Z}_3$.

That is, $|\mathbb{Z}_3[x]/\langle x^2+1\rangle| = 9$. This 9-element field is variously called F_9 or $GF(9)$.

1. So what are the elements of $\mathbb{Z}_3[x]/\langle x^2+1\rangle$?

2. Make an addition table for $\mathbb{Z}_3[x]/\langle x^2+1\rangle$.

3. Check that $(\mathbb{Z}_3[x]/\langle x^2+1\rangle, +)$ is an abelian group.

4. Make a multiplication table for $\mathbb{Z}_3[x]/\langle x^2+1\rangle$.

5. Check that $(\mathbb{Z}_3[x]/\langle x^2+1\rangle, \cdot)$ is an abelian group with respect to multiplication.

Let's construct a finite field with p^n elements. We cam simply imitate the steps we did in constructing a finite field with 3^2 elements. The idea was: start with the field $\mathbb{Z}_p$. Find a degree n irreducible polynomial $f(x)$ in $\mathbb{Z}_p[x]$. Then $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field with p^n elements (the number of possible remainders when dividing polynomials in $\mathbb{Z}_p[x]$ by $f(x)$).

6. Let's construct a finite field with $4 = 2^2$ elements. Here $p = 2$ and $n = 2$. So start with the field $\mathbb{Z}_2$ and find a degree-2 irreducible polynomial $f(x)$ in $\mathbb{Z}_2[x]$.

7. Find $\mathbb{Z}_p[x]/\langle f(x)\rangle$, that is, find the possible remainders when dividing by $f(x)$. How many are there?

8. Make addition and multiplication tables for $\mathbb{Z}_p[x]/\langle f(x)\rangle$.

9. Check that its a field. Shazaam!