Last name _____

First name _____

LARSON—MATH 401—CLASSROOM WORKSHEET 37
Finite Fields.

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

Let $f(x) \in F[x]$. $\langle f(x) \rangle$ is a maximal ideal if and only if $f(x)$ is irreducible.

$F[x]/I$ is a field iff I is a maximal ideal iff $I = \langle f(x) \rangle$ and $f(x)$ is irreducible.

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 $\mathbb{Z}_3[x]$.

1. So what can you conclude about $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$?

2. What is $\langle x^2 + 1 \rangle$ (that is, what does this mean formally—according to the definition)?

3. What is $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$ (that is, what does this mean formally—according to the definition)?

4. What can you say about the equivalence classes in $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$, that is, what can you say about them more intuitively (akin to our description of the equivalence classes in $\mathbb{Z}_n/\langle n \rangle = \mathbb{Z}_n/n\mathbb{Z}$)?

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

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

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

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

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

10. We know theoretically that $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field. In checking the details what detail remains to check? Why don't we have to check?