I am slow to learn and slow to forget that which I have learned. My mind is like a piece of steel; very hard to scratch anything on it and almost impossible after you get it there to rub it out. Abraham Lincoln

1. Let \( p \) be a prime of the form \( p = 3k + 1 \). Let \( g \) be a generator, so that the elements of \( \mathbb{Z}_p^* \) can be written \( 1, g, g^2, \ldots, g^{3k-1} \) with \( g^{3k} = 1 \).
   
   (a) Using this generator show that there is an element (actually, two elements) \( \omega \in \mathbb{Z}_p^* \) with \( \omega \neq 1 \) and \( \omega^3 = 1 \).
   
   (b) (*) Show that there exists \( \eta \in \mathbb{Z}_p^* \) with \( \eta^2 = -3 \). [One idea: In \( \mathbb{C} \) write \( \sqrt{-3} \) in terms of \( \omega = e^{2\pi i/3} \). Use this to make an “inspired guess” for \( \eta \) in terms of \( \omega \). Second idea: Find a simple quadratic satisfied by \( \omega \) and “complete the square” to get \( \eta \).]

2. Now suppose \( p \) be a prime of the form \( p = 3k + 2 \).
   
   (a) Again using a generator \( g \) show that there is no element \( \omega \in \mathbb{Z}_p^* \) with \( \omega \neq 1 \) and \( \omega^3 = 1 \).
   
   (b) (*) Show that there does not exist \( \eta \in \mathbb{Z}_p \) with \( \eta^2 = -3 \). [Idea: Reversing Problem 1b find \( \omega \) in terms of \( \eta \).]

Note: Together we get a necessary and sufficient condition for when \(-3\) is a square in \( \mathbb{Z}_p \). There is a result in Number Theory called The Law of Quadratic Reciprocity, which we do not cover in this course, which tells you when \( a \) is a square in \( \mathbb{Z}_p \).

3. Let \( F \) be a finite field with \( q = p^n \) elements. Define \( \sigma : F \to F \) by \( \sigma(\alpha) = \alpha^p \).
   
   (a) Show that \( \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) \) for all \( \alpha, \beta \in F \).
   
   (b) Show that \( \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) \) for all \( \alpha, \beta \in F \).
   
   (c) Show that \( \sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} \) for all nonzero \( \alpha \in F \).
   
   (d) (*) Show that \( \sigma \) is injective. That is, show that if \( \sigma(\alpha) = \sigma(\beta) \) then \( \alpha = \beta \).
   
   (e) Deduce that \( \sigma \) is surjective.

Note: Together this gives that \( \sigma \) is an automorphism, an isomorphism from \( F \) to itself. \( \sigma \) is called the Frobenius automorphism.]
4. Let $F = Z_3[x]/(x^2 + 1)$.

(a) List the elements of $F$.
(b) Find a generator $g$ of $F^*$. (Some grunt work here.)
(c) For each $\alpha \in F$ find the minimal polynomial $p_\alpha(y)$ of $\alpha$ in $Z_3[y]$.
   (E.g., for $\alpha = x$ take $p(y) = y^2 + 1$ as then $p(x) = x^2 + 1 = 0$.)
(d) Factor $y^9 - y$ in $F[y]$.
(e) Factor $y^9 - y$ in $Z_3[y]$. Show how the factors in $F[y]$ join to form factors in $Z_3[y]$.

5. Assume the following theorem: Let $q = p^n$ and set $f(x) = x^q - x$.
Then, in $Z_p[x]$, $f(x)$ factors into the product of all monic irreducible
(over $Z_p[x]$) polynomials of all degrees $d$, where $d$ is a divisor (including
1 and $n$) of $n$.

(a) How many irreducible quadratic polynomials are there over $Z_5[x]$?
   (Count degrees in the factorization of $x^{25} - x$.)
(b) How many irreducible cubic polynomials are there over $Z_5[x]$?
   (Count degrees in the factorization of $x^{125} - x$.)
(c) (*) How many irreducible polynomials of degree six are there over $Z_5[x]$?
   (Count degrees in the factorization of $x^{15625} - x$, noting
   $15625 = 5^6$.)

I have never let my schooling interfere with my education.
– Mark Twain