Organizational Notes

1. A Zoom recording link and class notes will be sent out after each Zoom class.

2. Remember to send your answers to the classroom worksheets. Title your email with enough to help me record your “participation”.

3. Homework #5 is due Mon., Oct. 25.

Review

1. A primitive root in $\mathbb{Z}/n\mathbb{Z}$ is an element $a$ such that the order of $a$ is $\phi(n)$.

2. (Big Question). Does every integer ring $\mathbb{Z}/n\mathbb{Z}$ have a primitive root???

3. (Notation). For a ring $R$, define $R[x]$ to be the polynomials with variable $x$ and coefficients in $R$.

4. (Useful Fact). $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1)$.

5. (Useful Fact). $x^n - \alpha^n = (x - \alpha)(x^{n-1} + \alpha x^{n-2} + \ldots + \alpha^{n-3} x^2 + \alpha^{n-2} x + \alpha^{n-1})$.

Primitive Roots! (Section 2.5)

1. (Root Bound) Let $k$ be a field. Show that a polynomial $f \in k[x]$ of degree $d$ has at most $d$ roots in $k$.

2. Check that 5 is prime, $2|(5 - 1)$ and $x^2 - 1 \in \mathbb{Z}/5\mathbb{Z}[x]$ has exactly 2 roots in $\mathbb{Z}/5\mathbb{Z}$.

3. Show that if $p$ is prime and $d|(p-1)$ then $x^d - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ has exactly $d$ roots in $\mathbb{Z}/p\mathbb{Z}$.

4. (Corollary). If $p - 1 = q_1^{n_1} q_2^{n_2} \ldots q_r^{n_r}$ then $x^{q_i^{n_i}} - 1$ has $q_i^{n_i}$ roots in $\mathbb{Z}/p\mathbb{Z}$ and $x^{q_i^{n_i} - 1} - 1$ has $q_i^{n_i - 1}$ roots.
5. (**Primitive Roots**). There is a primitive root in $\mathbb{Z}/p\mathbb{Z}$, when $p$ is prime.

6. (**Corollary**). $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group (with respect to multiplication).

**Major Theory Plan:**

(a) Existence of units.
(b) Chinese Remainder Theorem.
(c) $\phi$ is multiplicative.
(d) Existence of primitive roots.
(e) Quadratic Residues & Legendre Symbol (Chp.4)
(f) Euler’s Criterion.
(g) Gauss' Lemma
(h) Quadratic Reciprocity.