MAT2250 Exercise list
Spring 2024 - Instructor: Kris Shaw

9. Week of April 8th - Modular Arithmetic

Warm ups.

(1) Determine the remainders when 3^{15} and 15^{83} are divided by 13.
(2) Is the polynomial $x^2 + x + 1$ irreducible over $\mathbb{Z}_2$? What about over $\mathbb{Z}_3$?
(3) If $f(x)$ is a degree 5 irreducible polynomial over $\mathbb{Z}_p$ how many equivalence classes are there in $\frac{\mathbb{Z}_p}{\langle f(x) \rangle}$.
(4) Confirm that the polynomial $x^2 + x + 2$ is irreducible over $\mathbb{Z}_3$. What is the product $[x][x^2 + 2]$ in $\frac{\mathbb{Z}_3[x]}{x^2+x+2}$ (i.e. represent the product by a polynomial of degree of at most one)? What is the multiplicative inverse of $x + 1$ in $\frac{\mathbb{Z}_3[x]}{\langle x^2+x+2 \rangle}$?

Problem 9.1. Solve the equations $x + 2y = 4$ and $4x + 3y = 4$ in $\mathbb{Z}_7$ and $\mathbb{Z}_5$. Hint: You'll need the multiplicative inverses of 2 and 3 in both fields.

Problem 9.2. Prove the following generalisation of Fermat's little theorem. Let $\phi(m)$ be the number of integers between 1 and m which are relatively prime to m. Prove that if n is relatively prime to m then $n^{\phi(m)} \equiv 1 \mod m$.

Problem 9.3. Let p be a prime number. Use the binomial theorem to prove that $(a+b)^p \equiv a^p + b^p \mod p$ for all $a, b \in \mathbb{Z}$. Give a second proof using Fermat's little theorem. (This equality is sometimes called "The Freshman's dream").

Problem 9.4. Decompose $x^4 + 1$ into irreducible factors over $\mathbb{Z}_3$.

Problem 9.5. For which prime numbers is the polynomial $x^2 + 1$ irreducible over $\mathbb{Z}_p$?

Problem 9.6. An element $a \in GF(q)$ is a square if $a = b^2$ for some $b \in GF(q)$. Show that every element of $GF(2^m)$ is a square. Hint: show that $\{b^2 \mid b \in GF(2^m)\} = GF(2^m)$.