MTH 461 **Spring 2023**
Writing Credit **Drew Armstrong**

This course has an optional writing credit.

Details.

- Write a paper on a topic that is closely related to the course material.
- The style should be similar to a typical math textbook or research paper.
- The paper should be typeset instead of hand written.
- The paper should be approximately 10 pages long. Of course this will include white space because typeset mathematical formulas always need white space.
- The paper should include a series of small results and definitions, leading up to the proof of an interesting theorem. The definitions, statements and proofs should be written clearly and correctly.
- The paper should include an abstract and bibliography.
- The first draft must be submitted to me by **Thursday March 9**. I will provide feedback and then you must submit a final version incorporating this feedback. The final due date is **the day that would be the day of our final exam, which has not been released yet (as far as I know)**.
- I will be happy to set up Zoom appointments to discuss possible topics.

Some Possible Topics.

- We say that a point in the Cartesian plane is *constructible* if it can be obtained from the points $(0,0)$ and $(1,0)$ using "straightedge and compass", as in Euclidean geometry. Prove that the point (x,y) is constructible if and only if the real numbers x,y can be expressed in terms of integers and square roots.
- The RSA cryptosystem is based on the following theorem. Let $p,q\in\mathbb{Z}$ be prime numbers with $p\neq q$. Then for all integers $m,k\in\mathbb{Z}$ we have

  $$pq\,\big|\,(m-m^{(p-1)(q-1)k+1}).$$

  Prove this theorem and explain the RSA cryptosystem.
- Wilson's Theorem says that an integer $n\geqslant 2$ is prime if and only if $(n-1)!+1$ is divisible by n. Prove this theorem.

- The ring of *Gaussian integers* is defined as follows:

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\}.$$

  Prove that this ring is a Euclidean domain and describe its prime elements.

- The *power sum* and *elementary* symmetric polynomials are defined as follows:

$$\begin{aligned} p_k(x_1, \ldots, x_n) &= x_1^k + x_2^k + x_3^k + \cdots + x_n^k, \\ e_k(x_1, \ldots, x_n) &= \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k}. \end{aligned}$$

  Prove *Newton's identities* relating these polynomials:

$$ke_k = e_k p_1 - e_{k-1} p_2 + e_{k-2} p_3 - \cdots + (-1)^k e_1 p_{k-1} + (-1)^{k-1} p_k.$$

- Consider a cubic equation $x^3 + px + q = 0$ with real coefficients p, q. If $(q/2)^2 + (p/3)^3 < 0$ then the equation has only real roots. Prove that these roots can be expressed as

$$x = r \cos\left(\theta + \frac{2\pi k}{3}\right) \qquad \text{for } k = 0, 1, 2,$$

  for some positive real number $r > 0$ and some angle θ.

- The general quartic equation

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

  is solvable by radicals. Discuss the solution.

- The quadratic polynomial $x^2 + ax + b = (x - r)(x - s)$ has discriminant $\Delta = (r - s)^2 = a^2 - 4b$, which tells us when the equation has a repeated root. In fact, any polynomial has a discriminant. Higher degree polynomials also have discriminants. If $f(x)$ can be factored as $f(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$ then its discriminant is defined as

$$\Delta_f = \prod_{i<j} (r_i - r_j)^2.$$

  The discriminant of a polynomial $f(x)$ can always be expressed in terms of the coefficients. Find this formula in the case of degree 3.

- Let $\omega = e^{2\pi i/n}$. The *n-th cyclotomic polynomial* is defined as

$$\Phi_n(x) = \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(k,n)=1}} (x - \omega^k).$$

  Prove that $x^n - 1$ equals the product of $\Phi_d(x)$ for integers $1 \leqslant d \leqslant n$ dividing n. For example, $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$. Use this rule to compute the polynomials $\Phi_n(x)$ for $1 \leqslant n \leqslant 8$. Use induction to prove that $\Phi_n(x)$ always has integer coefficients.

- The ring of quaternions $\mathbb{H}$ was the first known example of a non-commutative ring. To be specific, $\mathbb{H}$ consists of expressions of the form $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with $a, b, c, d \in \mathbb{R}$, where the abstract symbols $\mathbf{i}, \mathbf{j}, \mathbf{k}$ satisfy

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}.$$

  Check that these rules do indeed define a ring (except for commutative multiplication). Show that the quadratic polynomial $x^2 + 1$ has infinitely many roots in $\mathbb{H}$, which shows that Descartes' Theorem fails for non-commutative rings.