

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 **November 19**. I will provide feedback and then you must submit a final version incorporating this feedback. The final due date is **December 16**.
- 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

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

Prove this theorem and explain the RSA cryptosystem.

- Wilson’s Theorem says that an integer $n \geq 2$ 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:

$$p_k(x_1, \dots, x_n) = x_1^k + x_2^k + x_3^k + \dots + x_n^k,$$

$$e_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}.$$

Prove *Newton's identities* relating these polynomials:

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

- 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

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

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 equation $x^2 + ax + b = 0$ has discriminant $\Delta = a^2 - 4b$, which tells us when the equation has a repeated root. In fact, any polynomial of any degree has a discriminant. Investigate this and compute the discriminant of the cubic equation $x^3 + ax^2 + bx + c = 0$.

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

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

We will see later that this polynomial has rational coefficients (in fact, integer coefficients). Prove that $\Phi_n(x)$ is irreducible over \mathbb{Q} .