> *It is not knowledge, but the act of learning, not possession but the act of getting there, which grants the greatest enjoyment.*
>
> In a letter from Carl Friedrich Gauss to Farkas Bolyai (September 2nd, 1808).

Note: The final exam will be similar to the first and second prelim in format, except that the final exam will be longer (2 hours). Also, the final exam will cover all the material we have covered, with an emphasis on newer material. In order to review, you should:

1. Review the first and second midterm exams and their solutions.
2. Review the practice problems for the first and second midterm exams.
3. Review the homework assignments and their solutions.

But most importantly, study your class notes and/or the book!

Theory Question 1. Any of the theory questions in previous practice tests.

Theory Question 2. Prove the Primitive Element Theorem: Let $p > 2$ be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ has a primitive root, i.e., there is a congruence $a \mod p$ of order exactly $p-1$. (You may use the theorem on the number of roots of polynomials over fields, but you certainly need to state it precisely and correctly).

Theory Question 3. Prove the following Lemma: Let p be an odd prime and let g be a primitive root modulo p. Let $a \in \mathbb{Z}$ with $(a, p) = 1$, and let n be the smallest positive integer such that $g^n \equiv a \mod p$. Then, n is even if and only if a is a quadratic residue modulo p.

Theory Question 4. Prove: if p is an odd prime, then -1 is a square mod p if and only if $p \equiv 1 \mod 4$. (You may use the previous lemma).

Theory Question 5. Write a precise statement for the Law of Quadratic Reciprocity.

Theory Question 6. Write a precise definition of the following:

1. Quadratic residue modulo m.
2. Legendre symbol.
3. Primitive root.

Question 1.
1. Find all the units in $\mathbb{Z}/28\mathbb{Z}$.
2. Find the multiplicative inverse of each unit in $\mathbb{Z}/28\mathbb{Z}$.
3. Prove that $a^{12} \equiv 1 \bmod 28$, for each unit a in $\mathbb{Z}/28\mathbb{Z}$.
4. Prove that $a^6 \equiv 1 \bmod 28$, for each unit a in $\mathbb{Z}/28\mathbb{Z}$.

Question 2. Find the least non-negative residue of

$$19! + (13!)^{44} \bmod 23.$$

Explain how you calculated it and **state any theorems** you used.

Question 3. Let $\varphi(n)$ be the Euler "phi" function.
1. Find $\varphi(125)$. **Explain** how you did it.
2. Let $N = 3^{10!} - 1$. Is N divisible by 125? **Justify** your answer and **state** any name any theorems that you use.

Question 4. Find the multiplicative inverse of 113 modulo 137.

Question 5. Find all the integral points in the line $L : 137x + 113y = 5$.

Question 6. Find all the integral points in the line $L : 185x + 111y = 7$.

Question 7. Is 31 a quadratic residue modulo 67?

Question 8. Show that the hyperbola $C : x^2 - 67y^2 = 31$ has no integral points.

Question 9. Let g be a primitive root modulo 29.
1. How many primitive roots are there modulo 29?
2. Find a primitive root g modulo 29.
3. Use g mod 29 to find **all** the primitive roots modulo 29.
4. Use the primitive root g mod 29 to express all the quadratic residues modulo 29 as powers of g.
5. Find all the quadratic residues modulo 29, and all the quadratic non-residues modulo 29.
6. Is 5 a quadratic residue modulo 29? If so, is 5 congruent to a fourth power modulo 29?
7. Use the primitive root g mod 29 to calculate all the congruence classes that are congruent to a fourth power.
8. Show that the equation $x^4 - 29y^4 = 5$ has no integral solutions.