# Math 430: Number Theory — Spring 2021

## Final Exam - take home — 4/5 May 2021

- This is an open-book, open-note exam. You may use any proven result from our textbook with a proper **citation**: a reference to the page number and particular result being used. Using *unproven* statements (like unassigned exercises) is generally not allowed - some exam questions may have themselves been taken from the unassigned exercises.
- Likewise, if you use the internet to look up any definitions or theorems, you should keep a list of all webpages you visit and **cite** their web addresses/links with your submission.
- The instructor (me) reserves the right to ask any student to explain their answers to any or all questions on the exam. If the student is unable to provide a satisfactory answer, it will be assumed that the work submitted was not done in an earnest manner and the solution in question will receive no credit.

---

**Question 1.**

- Use the greatest integer function to find the highest power of 2 that divides 10!.
- Find the full prime decomposition of 10!, written in standard form. You must show all of your work.
- Prove that if $n \in \mathbb{Z}$ such that $n^3$ is a perfect square, then $n$ is a perfect square.

---

**Question 2.** Show that $\phi(n^2) = n\,\phi(n)$, and more generally that $\phi(n^k) = n^{k-1}\phi(n)$.

(This should remind you of Calculus.)

---

**Question 3.** Find the following, showing all of your computations and explanations:

- all integers in $(\mathbb{Z}/7\mathbb{Z})^\times$ that are **not** quadratic residues modulo 7
- the number of integers between 1 and 76 that are relatively prime to 76
- a positive integer that is three more than a multiple of 11 and whose last two digits are 32.

---

**Question 4.** Find the six values of $m$ for which 3 has order 4 modulo $m$.

That is, find the moduli $m$ for which $\mathrm{ord}_m(3) = 4$.

---

**Question 5.**

- Which of the integers $16, 25, 26, 27, 28, 35$ have primitive roots? Explain your answer in detail.
- Verify that 2 is a primitive root modulo 13.
- Find a primitive root modulo $13^k$ where $k \geq 2$. Explain.
- Find a primitive root modulo $2 \cdot 13^k$ where $k \geq 1$. Explain.
- How many incongruent primitive roots are there modulo $2 \cdot 13^{k+2}$ where $k \geq 0$? Explain.

---

**Question 6.** Let $p$ be an odd prime.

- Prove the following formula for the Legendre symbol $(-3/p)$:

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 6 \\ -1 & \text{if } p \equiv 5 \mod 6 \end{cases}$$

- Consider the integer $n^2 - n + 1$ for $n \geq 3$. Show that every prime divisor of this number that is larger than 3 must be of the form $6k + 1$.

---

**Question 7.** For this problem it is given that 107 is a prime number.

- Use Quadratic Reciprocity to determine whether or not 7 is a quadratic residue modulo 107.
- Use the last result to find a one-digit integer, positive or negative, that is congruent to $7^{53} \mod 107$. (**Hint**: the exponent here is not random.)
- Use the last result to find the order of 7 modulo 107.

---

**Question 8.** Find two solutions to the following quadratic congruence:

$$x^2 + 7x + 11 \equiv 0 \mod 139.$$

If this congruence has no solutions, explain how you know. You may not use any calculators for this question.

---