QUIZ
MATH-UA 0248-001 THEORY OF NUMBERS
November, 9, 2020, 3.30-4.45pm
If doing at a different time, choose 1h15 time slot
CLASS NOTES, BOOKS, NOTES FROM THE RECITATION ARE
AUTHORIZED
Submit your quiz by email as the homework

1. give the definition of a quadratic residue mod p, where p is a prime number

2. give the definition of the Legendre symbol

3. formulate Euler's criterion (give the statement, no proof)

4. formulate and prove Gauss criterion (give the statement and the proof)

5. give a proof of quadratic reciprocity in the form $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ where p and q are odd primes.

6. why there is no primitive roots mod 8?

7. give a proof of Lagrange theorem: Let p be a prime number. Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

$p \nmid a_n$ be a polynomial of degree n. Then the congruence $f(x) \equiv 0 \ (mod \ p)$ has at most n incongruent solutions mod p.

8. give the idea of the proof of the fact that there are primitive roots mod p (Explain what is the main idea, in your opinion. You are free to choose to provide more or less details).