Remarks: This is a long exam; **do as much of it as you can, and please take care to budget your time wisely.** Each problem is worth ten points; you may do the problems in any order (kindly indicate in your blue book which problem you are solving at any given time).

Please make sure to communicate your ideas by explaining your reasoning precisely and clearly. GOOD LUCK!

Problem 1. State and prove a test for a number n to be divisible by 9.

Problem 2. Factorize the Gaussian integer $189 + 42i$ into a product of Gaussian primes.

Problem 3. Find all integers x that **simultaneously** satisfy the equations

$$\begin{cases} 5x \equiv 2 \pmod{8}, \\ 6x \equiv 9 \pmod{15}. \end{cases}$$

Note: your answer should be in the form: $x \equiv a \pmod{m}$ for suitable a and m. It is also acceptable to give an answer that looks like: $x \equiv$ one of $a, b, c \pmod{m}$.

Problem 4. Which of the following congruences have solutions? (This is really an exercise in the Legendre symbol. Note that 73, 89, and 1019 are all prime numbers.)

(a) $x^2 \equiv -11 \pmod{73}$

(b) $x^2 \equiv 56 \pmod{89}$

(c) $x^2 \equiv 15 \pmod{1019}$.

Problem 5. Use Gauss' Lemma to compute $\left(\frac{-3}{23}\right)$.

Problem 6. In an application of the RSA cryptosystem, Alice encodes a message M by calculating $M_1 \equiv M^{11} \pmod{6161}$ and sending to Bob the encoded message M_1. Bob decodes the message by calculating $M \equiv M_1^d \pmod{6161}$ for a suitable d. What value of d does he use?

(Remark: it is easy to factor $6161 = 61 \times 101$, so this is not a secure choice of public key.)

Problem 7. Find the continued fraction of $\sqrt{5}$ and write down the first few convergents until you reach a convergent A_n/B_n for which you can prove that

$$\left| \frac{A_n}{B_n} - \sqrt{5} \right| < \frac{1}{500}.$$

Problem 8. Given that 2 is a primitive root mod 19, find all the solutions to the following equations:

(a) $x^3 \equiv 1 \pmod{19}$

(b) $x^5 \equiv 4 \pmod{19}$

(c) $x^8 \equiv -1 \pmod{19}$.

Problem 9. Give an example of a number a such that the Jacobi symbol $\left(\frac{a}{35}\right)$ is equal to 1, but the equation $x^2 \equiv a \pmod{35}$ has no solutions.

Problem 10. Let $d > 0$ such that d is not a square. Show that if the equation

$$x^2 - dy^2 = 3, \qquad x, y \in \mathbf{Z}$$

has a solution, then it has infinitely many solutions.

(Hint: Think of norms of elements in $\mathbf{Z}[\sqrt{d}]$ and use the fact that the equation $x^2 - dy^2 = 1$ has infinitely many solutions.)

Problem 11. Let p be a prime such that $\ell = 4p + 1$ is also prime.

a) Show that $2^{2p} \equiv -1 \pmod{\ell}$.

b) Show that 2 is a primitive root mod ℓ.