As long as algebra and geometry have been separated, their progress have been slow and their uses limited; but when these two sciences have been united, they have lent each mutual forces, and have marched together towards perfection.
Joseph Louis Lagrange.

Question 1. The following is a table of powers of 2 modulo 13:

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}
2	4	8	3	6	12	11	9	5	10	7	1

1. Without finding them, how many primitive roots are there in $\mathbb{Z}/13\mathbb{Z}$?
2. Find **all** primitive roots modulo 13.
3. Use the table to find **all** quadratic residues modulo 13.

Question 2. Is 45 a quadratic residue modulo 47?

Question 3. Is -13 a square modulo 37?

Question 4. Is 14 a quadratic residue modulo 65?

Question 5. Find the following values of the Legendre symbol:

$$\left(\frac{113}{127}\right), \quad \left(\frac{113}{131}\right), \quad \left(\frac{113}{137}\right), \quad \left(\frac{210}{229}\right).$$

The numbers $113, 127, 131, 137$ are primes.

Question 6. Find the value of the following Legendre symbol: $\left(\frac{4699}{4703}\right)$. Note that 4703 is prime but 4699 is not!

Question 7. Find all solutions (if any) of the equations:

$$x^2 + 21x + 82 \equiv 0 \mod 137, \quad x^2 + 5x + 3 \equiv 0 \mod 37, \quad x^2 + 5x + 7 \equiv 0 \mod 37$$

Question 8. Prove that the equation $x^2 - 137y^2 = 113$ has no integer solutions.

Question 9. For what primes p is -5 a quadratic residue? For what primes p is -10 a quadratic residue? Are there infinitely many primes p such that -10 is a quadratic residue modulo p? Hint: Use Quadratic Reciprocity!

Question 10. Are there two odd primes p, q such that $p \neq q$, $p \equiv q \equiv 3 \mod 4$ and such that p is a quadratic residue modulo q and q is a quadratic residue modulo p? What is the smallest odd prime q such that 3 is a quadratic residue modulo q and q is a quadratic residue modulo 3?

Question 11. Use induction to show that, for all n, there exists a set of n distinct odd primes $\{p_1, \ldots, p_n\}$ such that

$$\left(\frac{p_i}{p_j}\right) = 1$$

for all $1 \leq i, j \leq n$ with $i \neq j$, i.e. every prime in the list is a quadratic residue modulo any other prime in the list.

Question 12. Suppose that p and q are twin primes. Is it possible that 2 is a quadratic residue for both p and q? Is 2 necessarily a quadratic residue of p or q? Find twin primes p and q such that 2 is a quadratic residue modulo p but not modulo q.

Question 13. The number $p = 4003$ is prime.

1. The number 372 has exact order 2001 modulo 4003. Find a primitive root modulo p.
2. The number 285 has exact order 87 modulo p, and the number 2163 has exact order 46 modulo p. Find another primitive root mod p.
3. Given that $2^{87} \equiv 2163 \mod 4003$ and $2^{46} \equiv 285 \mod 4003$, prove that 2 is also a primitive root modulo 4003.

Question 14. (Extra credit: read Section 8.9.2 in the book, then answer the following questions). The fraction 3/14 has decimal expansion $0.2\overline{142857}$ so we say that the period has length 6 and the position of the first digit in the period (within the expansion of the fractional part) is the second digit of the expansion. Without actually doing the long division (i.e., use congruences instead as in the book), find out the length of the period, and the position of the first digit in the period, for each of these fractions:

1. 2/35.
2. 11/208.
3. 5/17.
4. 1/97.
5. 282475249/19400.