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 of 13.
3. Use the table to find **all** quadratic residues modulo 13.

Solution:

1. From the given table we clearly see that 2 is a primitive root. Then, there are $\varphi(\varphi(13)) = \varphi(12) = \varphi(4)\varphi(3) = 4$ primitive roots.
2. The primitive roots coincide with those powers 2^n with n relatively prime to 12, i.e. $n = 1, 5, 7, 11$ and the primitive roots are 2, 6, 7 and 11.
3. Since 2 is a primitive root, the quadratic residues are those 2^n with n **even**. Hence, the quadratic residues are $4, 3, 12, 9, 10, 1$ (and there are $6 = \frac{13-1}{2}$ of them).

Question 2. Is 45 a quadratic residue modulo 47?

Solution:
Notice that $45 = 9 \cdot 5$, so

$$\left(\frac{45}{47}\right) = \left(\frac{9 \cdot 5}{47}\right) = \left(\frac{9}{47}\right) \cdot \left(\frac{5}{47}\right) = 1 \cdot \left(\frac{5}{47}\right).$$

Now, we use quadratic reciprocity. Since $5 \equiv 1 \bmod 4$ then:

$$\left(\frac{5}{47}\right) = \left(\frac{47}{5}\right) = \left(\frac{2}{5}\right) = -1$$

where we have used quadratic reciprocity and then the fact that $47 \equiv 2 \bmod 5$. Therefore, 45 is not a quadratic residue modulo 47.

Here is an alternative way: $45 \equiv -2 \bmod 47$. Thus:

$$\left(\frac{45}{47}\right) = \left(\frac{-2}{47}\right) = \left(\frac{-1}{47}\right) \cdot \left(\frac{2}{47}\right)$$

Since $47 \equiv 7 \bmod 8$, 2 is a QR and since $47 \equiv 3 \bmod 4$, -1 is not a square modulo 47, and so:

$$\left(\frac{45}{47}\right) = \left(\frac{-1}{47}\right)\left(\frac{2}{47}\right) = (-1) \cdot 1 = -1.$$

Question 3. Is -13 a square modulo 37?

Solution:
By the properties of the Legendre symbol:

$$\left(\frac{-13}{37}\right) = \left(\frac{13}{37}\right) \cdot \left(\frac{-1}{37}\right) = \left(\frac{13}{37}\right) \cdot 1 = \left(\frac{13}{37}\right)$$

where we have used the fact that $37 \equiv 1 \bmod 4$ and, thus, -1 is a quadratic residue modulo 37. Now we shall use Quadratic Reciprocity. Since $13 \equiv 1 \bmod 4$ and $37 \equiv 11 \bmod 13$:

$$\left(\frac{13}{37}\right) = \left(\frac{37}{13}\right) = \left(\frac{11}{13}\right)$$

and, again by Quadratic Reciprocity and $13 \equiv 1 \bmod 4$:

$$\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right).$$

Finally, since $11 \equiv 3 \bmod 8$, the number 2 is not a square modulo 11 and so:

$$\left(\frac{-13}{37}\right) = \left(\frac{13}{37}\right) = \left(\frac{2}{11}\right) = -1.$$

Hence, -13 is not a quadratic residue modulo 37.

Question 4. Is 14 a quadratic residue modulo 65?

Solution:
We need to check whether $x^2 \equiv 14 \bmod 65$ has solutions. By the Chinese Remainder theorem, and since $65 = 5 \cdot 13$, this equation has solutions if and only if the system:

$$\begin{cases} x^2 \equiv 14 \equiv 4 \bmod 5 \\ x^2 \equiv 14 \equiv 1 \bmod 13 \end{cases}$$

has solutions. But, clearly, these systems have solutions. Therefore, the original system has a solution as well. For example, a solution of the system $x \equiv 2 \bmod 5$ and $x \equiv 1 \bmod 13$ will work. Thus $x \equiv 27 \bmod 65$ is a solution of $x^2 \equiv 14 \bmod 65$.

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.

Solution:
For this, use the law of quadratic reciprocity. In the last one, first factor 210.

$$\left(\frac{113}{127}\right) = 1, \quad \left(\frac{113}{131}\right) = 1, \quad \left(\frac{113}{137}\right) = -1,$$

$$\left(\frac{210}{229}\right) = \left(\frac{2}{229}\right)\left(\frac{3}{229}\right)\left(\frac{5}{229}\right)\left(\frac{7}{229}\right) = (-1)\cdot 1\cdot 1\cdot(-1) = 1.$$

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

Solution:
The number 4699 factors as $37 \cdot 127$, and notice that they are both 1 mod 4, thus, by the properties of the Legendre symbol and quadratic reciprocity:

$$\left(\frac{4699}{4703}\right) = \left(\frac{-4}{4703}\right) = \left(\frac{-1}{4703}\right)\cdot\left(\frac{4}{4703}\right) = \left(\frac{-1}{4703}\right) = -1$$

because $4703 \equiv 3 \bmod 4$. Another way, using Quadratic Reciprocity:

$$\left(\frac{4699}{4703}\right) = \left(\frac{37}{4703}\right)\left(\frac{127}{4703}\right) = \left(\frac{4703}{37}\right)\cdot\left(-\left(\frac{4703}{127}\right)\right) = \left(\frac{4}{37}\right)\cdot\left(-\left(\frac{4}{127}\right)\right) = -1.$$

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

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

Solution:
Use the quadratic formula. First one needs to calculate the discriminants of the equations:

$$21^2 - 4\cdot 82 = 113, \quad 5^2 - 4\cdot 3 = 13, \quad 5^2 - 4\cdot 7 = -3.$$

Since:

$$\left(\frac{113}{137}\right) = -1, \quad \left(\frac{13}{37}\right) = -1, \quad \left(\frac{-3}{37}\right) = 1$$

the first equations have no solutions and the third one does. In fact $16^2 \equiv -3 \bmod 37$ and the solutions are 8 and 24 modulo 37 and

$$(x-8)(x-24) \equiv x^2 + 5x + 7 \bmod 37.$$

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

Solution:
Suppose that (x, y) is a solution in integers and reduce the equation modulo 137, to obtain $x^2 \equiv 113 \bmod 137$. But in problem 1 we saw that $(113/137) = -1$, so 113 is not a quadratic residue modulo 137 and $x^2 \equiv 113 \bmod 137$ cannot have solutions. Contradiction.

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!

Solution:
Use quadratic reciprocity:

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right).$$

Thus, -5 is a QR if -1 is a QR and $p \equiv \pm 1 \bmod 5$, or -1 is not a QR and $p \equiv 2, 3 \bmod 5$. Notice that -1 is a QR if and only if $p \equiv 1 \bmod 4$, so one can express all this in terms of congruences modulo 20 (do it!). Similarly, one can treat the question about -10 (in this case the answer will be modulo 40). And there are infinitely many such primes (use Dirichlet's theorem).

Question 10. Are there two odd primes p, q such that $p \neq q$, $p \equiv q \equiv 3 \bmod 4$ 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?

Solution:
The answer to the first question is no (use quadratic reciprocity). For the second question, we need to find p such that p is a QR modulo 3 and 3 is a QR modulo p. Hence, p must be 1 modulo 4, and p must be 1 modulo 3. By the Chinese Remainder Theorem, $p \equiv 1 \bmod 12$. The first such prime is 13.

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.

Solution:
We will show that this can be done with all $p_i \equiv 1 \bmod 4$. For $n = 1$ it is clear. Now let $\{p_1, \ldots, p_{n-1}\}$ be a set of such primes, i.e. $p_i \equiv 1 \bmod 4$ and $(p_i/p_j) = 1$ for $i \neq j$. Then, by Dirichlet's theorem on primes in arithmetic progressions there are infinitely many primes p such that $p \equiv 1 \bmod 4p_1p_2 \cdots p_{n-1}$. Let p_n be one of them. In particular, $p_n \equiv 1 \bmod 4$ and $p_n \equiv 1 \bmod p_i$ for all $1 \leq i \leq n - q$ (by the Chinese Remainder Theorem). Hence:

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

for all $1 \leq i \leq n - 1$ as desired.

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.

Solution:
Suppose p and q are twin, with $q = p + 2$. The number 2 is a QR modulo a prime t if and only if $t \equiv \pm 1 mod 8$. Suppose 2 is a QR modulo p, then $p \equiv \pm 1 \bmod 8$ but then $p + 2 \equiv 3$ or 1 modulo 8. Hence, if 2 is a QR for $q = p + 2$, then p cannot be 1 modulo 8, but there is no problem if $p \equiv -1 \bmod 8$ and $q \equiv 1 \bmod 8$. For example, 71 and 73 are both primes (twin) and 2 is a QR for both of them.

If p and $q = p + 2$ are twin primes but $p \equiv 3 \bmod 8$ then $q \equiv 5 \bmod 8$ and for neither of them 2 is a QR. For example, 11 and 13.

By our first remarks, if 2 is a QR for p but not for $q = p + 2$ then $p \equiv 1 \bmod 8$. For example, 17 and 19.

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 $2^{87} \equiv 2163 \bmod 4003$ and $2^{46} \equiv 285 \bmod 4003$, prove that 2 is also a primitive root modulo 4003.

Solution:

1. Let us assume (as they tell us to do) that 372 has exact order 2001 modulo 4003. A number is a primitive root modulo 4003 if its order is exactly $4003-1 = 4002 = 2001 \cdot 2$. Notice that $-1 \equiv 4002$ has order 2 modulo 4003. Since $(2001, 2) = 1$, then the order of $(-1) \cdot 372$ is equal to $2 \cdot 2001 = 4002$. Therefore, $-372 \equiv 3631 \bmod 4003$ is a primitive root.
2. Suppose $\text{ord}(285) = 87$ and $\text{ord}(2163) = 46$. Notice that $4002 = 2 \cdot 3 \cdot 23 \cdot 29$ and $87 = 3 \cdot 29$ and $46 = 2 \cdot 23$. Since $(87, 46) = 1$ then $\text{ord}(285 \cdot 2163) = 87 \cdot 46 = 4002$. Hence, $285 \cdot 2163 \equiv 3996 \bmod 4003$ is also a primitive root.
3. We are given $2^{87} \equiv 2163 \bmod 4003$ and $2^{46} \equiv 285 \bmod 4003$. Recall the formula:

$$\text{ord}(a^n) = \frac{\text{ord}(a)}{(\text{ord}(a), n)}.$$

Thus:

$$46 = \text{ord}(2163) = \text{ord}(2^{87}) = \frac{\text{ord}(2)}{(\text{ord}(2), 87)}$$

and

$$87 = \text{ord}(285) = \text{ord}(2^{46}) = \frac{\text{ord}(2)}{(\text{ord}(2), 46)}.$$

Hence:

$$\text{ord}(2) = 46 \cdot (\text{ord}(2), 87) = 87 \cdot (\text{ord}(2), 46).$$

Consequently, the order of 2 is divisible by 46 and by 87. Since these two numbers are relatively prime, $\text{ord}(2)$ is divisible by $46 \cdot 87 = 4002$. Since the order of any number modulo p divides $p - 1$, we conclude that $\text{ord}(2) = 4002$ and 2 is a primitive root.

Question 14 (Extra credit)**.** 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, 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.

Solution:
In the solutions for this problem I am referring to the notation of Section 8.9 and Theorem 8.9.8 in the book.

1. $2/35 = 0.0\overline{571428}$. Here $35 = 5 \cdot 7$ so $M = 1$ and the repeating part of the decimal expansion starts with the second digit, and the order of 10 modulo 7 is 6, i.e., $\mathrm{ord}_7(10) = 6$. Hence, the length of the period is 6.
2. $11/208 = 0.0528\overline{846153}$. Here $208 = 2^4 \cdot 13$ so $M = 4$ and the repeating part of the decimal expansion starts with the $M + 1 = 5$th digit, and the order of 10 modulo 13 is 6, i.e., $\mathrm{ord}_{13}(10) = 6$. Hence, the length of the period is 6.
3. $5/17 = 0.\overline{2941176470588235}$. Here 17 is prime so $M = 0$ and the repeating part of the decimal expansion starts with the $M + 1 = 1$st digit, and the order of 10 modulo 17 is 16, i.e., $\mathrm{ord}_{17}(10) = 16$. Hence, the length of the period is 16.
4. $1/97 = 0.\overline{01030927835051546391752577319 59\ldots}$. Here 97 is prime so $M = 0$ and the repeating part of the decimal expansion starts with the $M + 1 = 1$st digit, and the order of 10 modulo 97 is 96, i.e., $\mathrm{ord}_{97}(10) = 96$. Hence, the length of the period is 96.
5. $282475249/19400 = 14560.579\overline{8453608247422680412371\ldots}$. Here $19400 = 2^3 \cdot 5^2 \cdot 97$ where 97 is prime so $M = 3$ and the repeating part of the decimal expansion starts with the $M + 1 = 4$th digit, and the order of 10 modulo 97 is 96, i.e., $\mathrm{ord}_{97}(10) = 96$. Hence, the length of the period is 96.