1. (a) State the law of quadratic reciprocity. **(2 points)**

   (b) Compute the value of the Legendre symbol

$$\left(\frac{15}{2027}\right).$$

   (Take for granted that 2027 is a prime.) **(4 points)**

Solution. (a) The law of quadratic reciprocity states that if $p, q > 2$ are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

(b) Applying the multiplicativity of the Legendre symbol, that $2027 \equiv 3 \bmod 4, 5 \equiv 1 \bmod 4$, and finally that 2 is a quadratic non-residue modulo both 3 and 5 (which are easy case-by-case calculations),

$$\left(\frac{15}{2027}\right) = \left(\frac{3}{2027}\right)\left(\frac{5}{2027}\right) = -\left(\frac{2027}{3}\right)\left(\frac{2027}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = -(-1)(-1) = -1.$$

2. (a) Define prime numbers. (Note: you have to give the definition of primes that we used in the class, not the equivalent definition of irreducibles.) **(2 points)**

   (b) Give those primes $p \geq 2$ that can be written as the sum of two consecutive integers. **(4 points)**

   Solution. (a) An integer $p \neq 0, \pm 1$ is a prime by definition, if the following holds. Whenever $p \mid ab$ for some $a, b \in \mathbf{Z}$, $p \mid a$ or $p \mid b$.

   (b) Two consecutive inteegers, say, n and $n+1$ are of different parity, hence their sum $2n+1$ is always odd. As a consequence, the only even positive prime number 2 cannot be written as the sum of two consecutive integers. On the other hand, if the prime p is odd, say, $p = 2n+1$, then $p = n + (n+1)$, and here, n and $n+1$ are consecutive integers. That is, all positive primes except for 2 can be written as the sum of two consecutive integers.

3. (a) Define the number-theoretic function φ. **(2 points)**

   (b) Solve the equation $2\varphi(n) = n$ in $n \in \mathbf{N}$. **(4 points)**

Solution. (a) The function φ is defined as follows: for any $n \in \mathbf{N}$, let $\varphi(n)$ be the number of residue classes modulo n which are coprime to n.

(b) We claim that the set of solutions is $\{n = 2^k : k \in \mathbf{N}\}$. First, such numbers are indeed solutions, since for $n = 2^k$ $(k \in \mathbf{N})$, we apply the formula

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right),$$

which simplifies, when the only prime divisor of n is 2, to

$$\varphi(n) = n\left(1 - \frac{1}{2}\right) = \frac{n}{2}.$$

This shows that such numbers are indeed solutions.

As for the converse, observe that $n = 2\varphi(n)$ implies that $2 \mid n$. Then the numbers $2, 4, \ldots, n$ are not coprime to n, therefore, the other half of the residue classes $1, 3, \ldots, n-1$ all have to be coprime to n. This shows that n has no odd prime divisor, hence it has to be of the given form.

4. (a) State our proposition about $\gcd(a, b)$ and integer combinations of a and b. **(2 points)**

   (b) Assume $a, b, n \in \mathbf{N}$ such that $n > ab$ and $\gcd(a, b) = 1$. Prove that there exist $x, y \in \mathbf{N}$ such that $ax + by = n$. **(4 points)**

Solution. (a) The proposition says that if $a, b \in \mathbf{Z}$, then $\gcd(a, b)$ can be written as the integer combination of a and b, that is, there exist $u, v \in \mathbf{Z}$ such that $au + bv = \gcd(a, b)$.

(b) By our theorem about linear diophantine equations, since $\gcd(a, b) = 1 \mid n$, there exist integers x_0, y_0 such that $ax_0 + by_0 = n$, fix such a pair of x_0, y_0. Now take the smallest integer t satisfying that

$$x_0 + tb > 0,$$

that is, let t be the smallest integer exceeding $-x_0/b$ (in formula, $t = \lfloor -x_0/b \rfloor + 1$). Set then $x = x_0 + tb$, $y = y_0 - ta$, and we claim that this pair does the job. First,

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + by_0 + tab - tab = ax_0 + by_0 = n.$$

It is also clear that $x, y \in \mathbf{Z}$, and by the definition of t, $x = x_0 + tb > 0$, therefore, $x \in \mathbf{N}$. To see that also $y \in \mathbf{N}$, it suffices to see that $ax \leq ab$, since it would imply $by = n - ab > 0$, that is, $y > 0$. Assume then by contradiction that $ax > ab$. Then $x > b$, which means that $x - b > 0$, that is, $x_0 + (t - 1)b > 0$, which contradicts the minimal choice of t.