In this exam all variables are integers. Solutions mean integer solutions.

1. (25 points) True or False. Determine if the following statements are true. Explain your answers.
   (1). For all real numbers \( x \geq 2 \), we have
   \[
   \frac{\ln 2}{4} \cdot \frac{x}{\ln x} < \pi(x) < 30 \ln 2 \cdot \frac{x}{\ln x}.
   \]
   (2). Let \( \mu(n) \) be the Möbius Function. Then the function \( \sum_{d|n} \mu(d) \) is multiplicative.

2. (25 points) (1). Compute
   \[
   n = \sum_{e|304} \phi(e) d(e) \sigma(e) \mu(e)
   \]
   (2). Does the equation \( x^2 \equiv 2019 \pmod{n} \) have any solution? Here \( n \) is the number from part (1).

3. (25 points) Show that there are infinitely many odd prime numbers \( p \) such that 2 is a quadratic non-residue modulo \( p \) and \( -2 \) is a quadratic residue modulo \( p \).

4. (25 points)
   (1). Show that the equation \( x^2 \equiv 17 \pmod{71} \) has no solution.
   (2). Does this mean 17 is a primitive root modulo 71? If yes, explain why. If not, check directly whether 17 is a primitive root modulo 71.
   (3). Find a primitive root module 142.

Solutions on next page
Solutions:

1. (1). True. If \( x \geq 8 \) this is the statement of Tchebychev’s Theorem in Chapter 8. For \( 2 \leq x \leq 8 \) the inequality can be checked directly.

(2). True. Let \( n = n_1^2 \cdot m \) where \( m \) is square free. Then \( \sum_{d^2 \mid n_1} \mu(d) = \sum_{d^2 \mid n_1} \mu(d) \). By Theorem 6.5 this is 0 unless \( n_1 = 1 \) (in which case it is equal to 1). In other words it is 1 if \( n \) is square free, 0 if not. So, say in another way, \( \sum_{d^2 \mid n} \mu(d) = \mu^2(n) \). Now it is clear that this function is multiplicative.

2. (1). All four functions are multiplicative. So \( \sum_{e \mid 304} \phi(e) d(e) \sigma(e) \mu(e) \) is also multiplicative. If \( n = p^k \) where \( p \) prime, then \( \sum_{e \mid p^k} \phi(e) d(e) \sigma(e) \mu(e) = \phi(1) \cdot d(1) \cdot \sigma(1) \cdot \mu(1) + \phi(p) \cdot d(p) \cdot \sigma(p) \cdot \mu(p) = 1 + (p-1) \cdot 2 \cdot (p+1) \cdot (-1) = 3 - 2p^2 \).

So \( \sum_{e \mid 304} \phi(e) d(e) \sigma(e) \mu(e) = (3 - 2 \cdot 2^2) \cdot (3 - 2 \cdot 19^2) = (-5) \cdot (-719) = 3595 \).

(2). By Chinese Remainder Theorem, the equation has solution if and only if both \( x^2 \equiv 2019 \pmod 5 \) and \( x^2 \equiv 2019 \pmod {719} \) have solution. For the first: \( (\frac{2019}{5}) = (\frac{3}{5}) = 1 \). For the second: check that 719 is prime, then

\[
\frac{2019}{719} = \left(\frac{-138}{719}\right) = \left(\frac{-1}{719}\right) \cdot \left(\frac{2}{719}\right) \cdot \left(\frac{3}{719}\right) \cdot \left(\frac{3}{719}\right) = (-1) \cdot 1 \cdot 1 \cdot (-719/23) = \frac{6}{23} = 1.
\]

(Computation using quadratic reciprocity law. Fill in the detail for the last step.) So the original equation has solution. (In fact 1203 is a solution.)

3. By assumption \( (\frac{3}{p}) = -1 \) and \( (\frac{-2}{p}) = (\frac{-1}{p}) \cdot (\frac{2}{p}) = 1 \) which means \( (\frac{-1}{p}) = -1 \). This happens if and only if \( p \equiv 3 \pmod 8 \).

Assume there are only finitely many prime numbers that are congruent to 3 modulo 8. Call them \( p_1, \ldots, p_r \). Consider \( N = (p_1 p_2 \cdots p_r)^2 + 2 \). Then \( N \equiv 3 \pmod 8 \). If \( p \mid N \) is a prime factor, then \( (p_1 p_2 \cdots p_r)^2 \equiv -2 \pmod p \). Therefore \( (\frac{-2}{p}) = 1 \). Check that this means \( p \equiv 1 \pmod 8 \) or \( p \equiv 3 \pmod 8 \). However \( N \equiv 3 \pmod 8 \). Therefore it has at least one prime factor \( p \) such that \( p \equiv 3 \pmod 8 \). By assumption, \( p \mid p_1 p_2 \cdots p_r \) and \( p \mid N \). Thus \( p \mid 2 \) which is a contradiction.

4. (1). \( (\frac{17}{71}) = (\frac{7}{17}) = (\frac{3}{17}) = -1 \), so the equation has no solution.

(2). This only means 17 is a quadratic non-residue modulo 71, but it does not guarantee 17 is a primitive root modulo 71. However this shows (by Theorem 9.2) the order of 17 modulo 71 (which must divide \( \varphi(71) = 70 \)) is not 35 nor any factor of 35 (so cannot be 1, 5 or 7), and cannot be 2 since 17 \( \equiv \pm 1 \pmod 71 \). So we only need to check if the order can be 10 (which is equivalent to 17^5 \( \equiv -1 \pmod 71 \)), or if the order can be 14 (which is equivalent to 17^7 \( \equiv -1 \pmod 71 \)). Here indeed 17^5 \( \equiv -1 \) (as 17^2 = 289 \( \equiv 5 \)), so 17^5 \( \equiv 5^2 \cdot 17 = 425 = 71 \cdot 6 - 1 \equiv -1 \pmod {71} \)). So 17 is not a primitive root modulo 71.

(3). To be a primitive root, it must be a quadratic non-residue. Quick check finds that \( (\frac{2}{71}) = 1 \) and \( (\frac{4}{71}) = 1 \) so these small numbers are not primitive roots modulo 71. In fact \( (\frac{4}{71}) = -1 \) and 7 is indeed a primitive root modulo 71 (thus also primitive root modulo 142 as 7 is odd). But one needs to check like in (2) above. Another way: check that \( (\frac{-2}{71}) = (\frac{3}{71}) \cdot (\frac{2}{71}) = -1 \), and it is easier to verify \( -2 \equiv -1 \pmod {71} \) and \( (-2)^2 \equiv -1 \pmod {71} \). So -2 is a primitive root modulo 71. To get a primitive root modulo 142 = 2 \cdot 71, by \( \frac{72}{142} \equiv 142 \), we just need to find an odd primitive root modulo 71, so 69 = (-2) + 71 works.