Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate.- Leonhard Euler.

Please note:

1. Calculators are not allowed in the exam.
2. You may assume the following axioms and theorems:
   (a) **Axiom**: The natural numbers $\mathbb{N}$ satisfies the Well Ordering Principle, i.e., every non-empty subset of natural numbers contains a least element.
   (b) **Theorem:** Let a, b, c be integers. The linear equation $ax + by = c$ has a solution if and only if $\gcd(a, b)$ divides c.
3. **You must** provide full explanations for all your answers. You must include your work.

Theory Question 1. Prove that if p is prime and $p|ab$ then either $p|a$ or $p|b$. Explain why the previous statement can be re-written as follows: if p is a prime and $ab \equiv 0 \bmod p$ then $a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p$.

Theory Question 2. Prove the existence part of the Fundamental Theorem of Arithmetic, i.e., every natural number $n > 1$ can be written as a product of primes.

Theory Question 3. Prove the uniqueness part of the Fundamental Theorem of Arithmetic, i.e., every natural number $n > 1$ can be written uniquely as a product of primes, up to a reordering of the prime-power factors (you may assume Theory Question 2).

Theory Question 4. Prove Euclid's theorem on the infinitude of primes, i.e., prove that there exist infinitely many prime numbers.

Question 1. Use Euclid's algorithm to:

1. Find the greatest common divisor of 13 and 50.
2. Find all solutions of the linear diophantine equation $13x + 50y = 2$.
3. Find the multiplicative inverse of 13 modulo 50. Find the multiplicative inverse of 50 modulo 13.
4. Find all solutions to $26x \equiv 4 \bmod 100$.

Question 2. Prove that the equation $x^2 - 7y^3 + 21z^5 = 3$ has no solution with x, y, z in $\mathbb{Z}$ (Hint: Calculate all possible squares modulo 7).

Question 3. Show that 257 divides $100 \cdot 2^{25} - 57 = 3355443143$.

Question 4. What time does a clock read 100 hours after it reads 2 o'clock? If the time is now 2PM, after 100 hours, will it be in the PM or in the AM?

Question 5. Show that $2^{2^n} + 5$ is composite for every positive integer n.

Question 6. Find the smallest positive integer n such that

$$n \equiv 7 \bmod 3, \quad n \equiv 5 \bmod 5, \quad n \equiv 3 \bmod 7.$$

Question 7. A troop of 17 monkeys store their bananas in 11 piles of equal size with a twelfth pile of 6 left over. When they divide the bananas into 17 equal groups, none remain. What is the smallest number of bananas they can have?

Question 8. The seven digit number $n = 72x20y2$, where x and y are digits, is divisible by 72. What are the possibilities for x and y?

Question 9. Show that $36^{100} \equiv 16 \bmod 17$.

Question 10. Show that $42|n^7 - n$ for all positive n.

Question 11. Show that $5555^{2222} + 2222^{5555}$ is divisible by 7.

Question 12. Prove that for any natural number $n \geq 1$, $3^{6n} - 2^{6n}$ is divisible by 35 (Hint: work modulo 5 and modulo 7, separately).

Question 13. Find the remainder when 14! is divided by 17.

Question 14. Prove that if n is odd, then n and $n - 2$ are relatively prime. (Hint: Use the theorem (b) at the beginning of this document).

Question 15. Prove that if $k \geq 1$, the integers $6k + 5$ and $7k + 6$ are relatively prime.

Question 16. Find all primes p such that $17p + 1$ is a square.

Question 17. Show that $n(n - 1)(2n - 1)$ is divisible by 6 for every $n > 0$.

Question 18. Does $3x \equiv 1 \bmod 18$ have a solution? What about $3x \equiv 1 \bmod 19$? Determine for which integers $1 \leq a \leq 17$ the equation $ax \equiv 1 \bmod 18$ has solutions. Do the same modulo 19.

Question 19. Verify that:

1. The numbers $0, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}$ are a complete set of representatives modulo 11.
2. The numbers $0, 2, 2^2, 2^3, 2^4, 2^5, 2^6$ are not a complete set of representatives modulo 7.