> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain (*Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*)
>
> Pierre de Fermat (annotation on a copy of Diophantus' "Arithmetica").

Please note:

1. Calculators are not allowed in the exam.
2. **You must always** provide full explanations for all your answers. You must include your work.

Theory Question 1. Write a precise statement for Fermat's Little Theorem and prove it.

Theory Question 2. Write a precise definition of Euler's phi function. Write a precise statement for Euler's theorem and prove it.

Theory Question 3. Prove Wilson's Theorem: if p is a prime then $(p-1)! \equiv -1 \bmod p$.

Theory Question 4. Write precise statements for the following theorems/conjectures (you do not need to prove them):

1. Prime Number Theorem.
2. Dirichlet's theorem on primes in arithmetic progressions.
3. Goldbach's Conjecture.
4. Twin Prime Conjecture.
5. Chinese Remainder Theorem
6. Fermat's Last Theorem.

Just in case you need them, the following are all the primes below 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Question 1. Find 3 primes in each category:

1. Find 3 primes $p \equiv 1 \bmod 3$.
2. Find 3 primes $p \equiv 2 \bmod 3$.
3. Find 3 primes $p \equiv 1 \bmod 5$.
4. Find 3 primes $p \equiv 2 \bmod 5$.

5. Find 3 primes $p \equiv 3 \bmod 5$.
6. Find 3 primes $p \equiv 4 \bmod 5$.
7. Are there any primes $p \equiv 3 \bmod 21$? Why? Why not?
8. Are there any primes $p \equiv 3 \bmod 22$? Why? Why not?
9. Are there infinitely many primes in each category above? How do you know?

Question 2. Use a Sieve method to find all the prime numbers between 105 and 115. Explain how you did it.

Question 3. Find the smallest positive integer n such that

$$\begin{aligned} n &\equiv 1 \bmod 3, \\ n &\equiv 2 \bmod 4, \\ n &\equiv 3 \bmod 5. \end{aligned}$$

You must use the method that appears in the proof of the Chinese Remainder Theorem.

Question 4. Find the smallest positive integer that leaves remainders of $2, 4, 6$ when divided by $3, 5, 7$, respectively. You must use the Chinese Remainder Theorem.

Question 5. Solve the following quadratic congruences:

- Find all solutions of $x^2 \equiv 1 \bmod 133$
- Prove that there are no solutions: $x^2 \equiv 2 \bmod 133$
- Find (at least) one solution: $x^2 \equiv 93 \bmod 133$

Note: Trial and error will yield no points. Hint: Use the Chinese Remainder Theorem ($133 = 7 \cdot 19$).

Question 6. Show that $37^{100} \equiv 13 \bmod 17$. Hint: Use Fermat's Little Theorem.

Question 7. Show that if p and q are distinct primes then $p^{q-1} + q^{p-1} \equiv 1 \bmod pq$.

Question 8. Use Euler's theorem to find the first digit (starting from the right-hand side of the expansion, i.e., the units digit) of the decimal expansion of 7^{1000}.

Question 9. Prove that for any natural number $n \geq 1$, $3^{6n} - 2^{6n}$ is never prime.

Question 10. Find as many prime factors as possible of the number $N = 3^{10!} - 1$.

Question 11. Let $a, n > 0$ be natural numbers. Find as many prime factors as possible of the number $N = a^{n!} - 1$.

Question 12. Are there infinitely many primes p such that $(p, p+2, p+4)$ are all primes? Why? Are there infinitely many primes p such that $(p, p+2, p+6, p+8, p+12, p+14)$ are all primes? Why? Make a generalization of the Twin Prime conjecture for 6-tuples, i.e. make an educated conjecture for the existence of 6-tuples of primes.