> 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.

Read through your notes for the proofs of the theorems of Fermat, Euler and Wilson, and also for the statements of the other theorems and conjectures.

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 $p \equiv 1 \mod 3$.
2. Find 3 primes $p \equiv 2 \mod 3$.
3. Find 3 primes $p \equiv 1 \mod 5$.
4. Find 3 primes $p \equiv 2 \mod 5$.
5. Find 3 primes $p \equiv 3 \mod 5$.
6. Find 3 primes $p \equiv 4 \mod 5$.
7. Are there any primes $p \equiv 3 \mod 21$? Why? Why not?
8. Are there any primes $p \equiv 3 \mod 22$? Why? Why not?
9. Are there infinitely many primes in each category above? How do you know?

Solution:
For parts (1) through (6), simply look through a table of primes and find primes that fit the description. For part (7), there is only one prime $p \equiv 3 \mod 21$, which is $p = 3$. All other numbers that are congruent to $n \equiv 3 \mod 21$ have a factor of 3, and they are not primes, because $n = 3 + 21k = 3(1 + 7k)$.

For part (8), yes, there are primes that are $p \equiv 3 \mod 22$, for example 47. For part (9): by Dirichlet's theorem on arithmetic progressions, if $(a, m) = 1$ then there are infinitely many primes of the form $p \equiv a \mod m$. Thus, there are infinitely many primes in the categories of parts (1) through (6) and (8), and only one in category (7).

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

Solution:
We perform a sieve on the numbers:

$$105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115$$

Notice that $11^2 = 121$ and so $\sqrt{115} < 11$. Thus, if any of those numbers is not prime, they must have a prime factor less than 11. Hence, it is enough to cross out the multiples of $2, 3, 5$, and 7. In order to start the sieve, notice that:

$$105 \equiv 1 \mod 2,\ 105 \equiv 0 \mod 3,\ 105 \equiv 0 \mod 5,\ 105 = 7 \cdot 15 \equiv 0 \mod 7.$$

Hence, $106, 108, 110, 112$ and 114 are multiples of 2. The numbers $105, 108, 111, 114$ are multiples of 3. The numbers $105, 110$ and 115 are multiples of 5 and the numbers $105, 112$ are multiples of 7. Therefore, the numbers $107, 109$ and 113 are the only primes between 105 and 115.

Question 3. Find the smallest positive integer n such that

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

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

Solution:
First, we solve three easier problems: $n_1 \equiv 1, 0, 0 \mod 3, 4, 5$ (respectively), $n_2 \equiv 0, 1, 0 \mod 3, 4, 5$ (resp.) and $n_3 \equiv 0, 0, 1 \mod 3, 4, 5$ (resp.).

For example, to solve for n_1, we must have $n_1 = 20k \equiv 1 \mod 3$ so $k = 2$ works and $n_1 \equiv 40 \mod 60$. Similarly, $n_2 \equiv 45 \mod 60$ and $n_3 \equiv 36 \mod 60$.

Hence, the solution we are looking for is:

$$n \equiv 1 \cdot n_1 + 2 \cdot n_2 + 3 \cdot n_5 \equiv 40 + 90 + 108 \equiv 58 \mod 60.$$

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.

Solution:
We are looking for $x \equiv 2, 4, 6 \mod 3, 5, 7$ (respectively). Note that this can be written as $x \equiv -1, -1, -1 \mod 3, 5, 7$. Therefore, $x \equiv -1 \equiv 104 \mod 105$ works. By the Chinese Remainder Theorem, that is the unique solution modulo 105.

Question 5. Solve the following quadratic congruences:

- Find all solutions of $x^2 \equiv 1 \mod 133$

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

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

Solution:

- Find all solutions of $x^2 \equiv 1 \mod 133$. First reduce modulo 7 and 19: and solve $x^2 \equiv 1 \mod 7$ and $x^2 \equiv \mod 19$. Thus, we are looking for $x \equiv \pm 1 \mod 7, 19$. There are four solutions modulo 133 (find them using the Chinese Remainder Theorem, e.g. solve $x \equiv 1 \mod 7, x \equiv 18 \mod 19$):

$$x \equiv 1, 20, 113, 132 \mod 133.$$

- Prove that there are no solutions: $x^2 \equiv 2 \mod 133$. Suppose there is an integer x such that $x^2 \equiv 2 \mod 133$. Then it is also true that $x^2 \equiv 2 \mod 19$. But 2 is not a square modulo 19:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^2	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1

- Find (at least) one solution: $x^2 \equiv 93 \mod 133$. If there is a solution, x also satisfies $x^2 \equiv 93 \equiv 2 \mod 7$ and $x^2 \equiv 17 \mod 19$. Notice that $3^2 \equiv 2 \mod 7$ and (by the table above) $6^2 \equiv 17 \mod 19$. Let us solve, using the Chinese Remainder Theorem, the system: $x \equiv 3 \mod 7$ and $x \equiv 6 \mod 19$. This yields: $x \equiv 101 \mod 133$. (There are other solutions, e.g. the congruence $x \equiv 25 \mod 133$ is another solution of $x^2 \equiv 93 \mod 133$.)

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

Solution:
First $37^{100} \equiv 3^{100} \mod 17$ because $37 \equiv 3 \mod 17$. By Fermat's Little Theorem, and since $(37, 17) = 1$, we have that $3^{16} \equiv 1 \mod 17$. Moreover, $100 = 6 \cdot 16 + 4$ and so:

$$37^{100} \equiv 3^{100} \equiv (3^{16})^6 \cdot 3^4 \equiv 1 \cdot 3^4 \equiv 27 \cdot 3 \equiv 10 \cdot 3 \equiv 30 \equiv 13 \mod 17.$$

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

Solution:
Since p and q are distinct (and therefore relatively prime), it suffices separately modulo p and modulo q. By Fermat's Little theorem one has $n^{p-1} \equiv 1 \mod p$ and $n^{q-1} \equiv 1 \mod q$ for all n not equivalent to 0 modulo p or q respectively. Thus:

$$p^{q-1} + q^{p-1} \equiv 1 + 0 \equiv 1 \mod q, \quad p^{q-1} + q^{p-1} \equiv 0 + 1 \equiv 1 \mod p.$$

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}.

Solution:
First, $\phi(10) = \phi(2)\phi(5) = 4$. In order to find out the last digit of the decimal expansion of a number, one needs to calculate its least non-negative residue modulo 10. Thus:

$$7^{1000} \equiv (7^4)^{250} \equiv 1 \mod 10$$

where we have used the fact that $7^4 \equiv 1 \mod 10$, by Euler's theorem (which applies in this case because $(7, 10) = 1$). Therefore the last digit is a 1.

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

Solution:
Show that 5 and 7 are always divisors of $3^{6n} - 2^{6n}$, using Fermat's little theorem (i.e., show that $3^{6n} - 2^{6n} \equiv 0 \mod 7$).

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

Solution:
Clearly, N is even (so $2|N$) and 3 does not divide N. By Fermat's little theorem, if $(a, p) = 1$ then $a^{(p-1)t} - 1$ is divisible by p, for any integer $t \geq 1$ (why?). Thus, if $p > 3$ and $p - 1$ divides 10! then p divides N. Notice that:

$$10! = 10 \cdot 9 \cdot 8 \cdots 3 \cdot 2 \cdot 1 = 2^8 3^4 5^2 7.$$

Let us make a list of primes and the value of $p - 1$:

p	5	11	13	17	19	23	29	31	37
$p-1$	2^2	$2 \cdot 5$	$2^2 \cdot 3$	2^4	$2 \cdot 3^2$	$2 \cdot 11$	$2^2 \cdot 7$	$2 \cdot 3 \cdot 5$	$2^2 \cdot 3^2$

Hence, from the factorization of 10! and the table we see that $p = 2, 5, 11, 13, 17, 19, 29, 31, 37, \ldots$ are all divisors of N.

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

Solution:
See the solution to the previous problem. Those primes p such that $p - 1$ divides $n!$, and $(p, a) = 1$, are divisors.

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.

Solution:
$(p, p+2, p+4)$ cannot be all prime because one number is divisible by 3. Similarly, $(p, p+2, p+6, p+8, p+12, p+14)$ cannot be all primes because one is divisible by 5.