> *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 $b \equiv 0 \bmod p$.

Solution:
Suppose p divides ab but p does not divide a. Then $\gcd(p, a) = 1$ (otherwise, there is $d > 1$ such that $d|p$ and $d|a$, and since p is prime $d = p$ but p does not divide a). By the theorem above, there exist $x, y \in \mathbb{Z}$ such that

$$ax + py = 1.$$

Multiplying this equation by b gives:

$$abx + pby = b.$$

Since p divides ab and p obviously divides pb, then p divides any linear combination of ab and pb. Hence p divides $b = (ab)x + (pb)y$.

The rest of the problem follows from the fact that $p|a$ if and only if $a \equiv 0 \bmod p$.

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.

Solution:
See the book or your class notes.

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).

Solution:
See the book or your class notes.

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

Solution:
See the book or your class notes.

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 $26x \equiv 4 \bmod 100$.

Solution:

1. $50 = 13 \cdot 3 + 11$, $13 = 11 + 2$, $11 = 2 \cdot 5 + 1$. Thus, the gcd is 1.
2. One particular solution is found by reversing Euclid's algorithm (and then multiplying through by 2). In particular, $13 \cdot 4 - 50 = 2$. By a theorem in class, since $\gcd(50, 13) = 1$, all the solutions of $13x + 50y = 2$ are given by:
$$x = 4 + 50t, \quad y = -1 - 13t, \qquad \text{for all } t \in \mathbb{Z}.$$
3. A solution to the equation $13x + 50y = 1$ is given by $x = 27$ and $y = -7$. The equation $13 \cdot 27 - 7 \cdot 50 = 1$ implies that
$$13 \cdot 27 \equiv 1 \bmod 50$$
and so, 27 is a multiplicative inverse of 13 modulo 50.
4. We first solve $13x \equiv 2 \bmod 50$. In fact, we have already seen that $13 \cdot 4 - 50 = 2$. Thus $x \equiv 4 \bmod 50$ is the unique solution. Thus, all solutions to $26x \equiv 4 \bmod 100$ are $x = 4$ and $x = 4 + 50 = 54$ modulo 100 (again by a theorem proved in class).

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).

Solution:
Since the set $\{0,1,2,3,4,5,6\}$ is a complete residue system modulo 7 and since $a^2 = (-a)^2$, we can conclude that $\{0^2, 1^2, 2^2, 3^2\} = \{0,1,4,2\}$ is a complete system of squares modulo 7 (i.e. the squares are congruent to either $0, 1, 2$ or 4 modulo 7).

Now, suppose that there are integers x, y, z such that $x^2 - 7y^3 + 21z^5 = 3$. Then:

$$3 = x^2 - 7y^3 + 21z^5 \equiv x^2 \bmod 7$$

but this, $x^2 \equiv 3 \bmod 7$ is impossible by our previous remark.

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

Solution:
Notice that $2^8 = 256 \equiv (-1) \bmod 257$. Thus, $2^{25} = (2^8)^3 \cdot 2 \equiv -2 \bmod 257$. Finally:

$$100 \cdot 2^{25} - 57 \equiv -200 - 57 \equiv -257 \equiv 0 \bmod 257.$$

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?

Solution:
We need to find the remainder of 102 modulo 12:

$$102 = 12 \cdot 8 + 6, \quad \text{and so} \quad 102 \equiv 6 \bmod 12.$$

Thus, the time is 6 o'clock. By the way, is that in the PM or AM? Suppose the time now is 2PM (which is $14:00$, the 14th hour of the day). Then we need to find the remainder of $114 = 100 + 14$ modulo 24:

$$114 = 24 \cdot 4 + 18, \quad \text{and so} \quad 114 \equiv 18 \bmod 24$$

and the time is 6 PM.

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

Solution:
First, we try a few numbers. For $n = 1$, $2^2 + 5 = 9 = 3 \cdot 3$. For $n = 2$, $2^4 + 5 = 21 = 3 \cdot 7$. For $n = 3$, $2^8 + 5 = 261$ which is divisible by 3. Let us prove that every number $2^{2^n} + 5$ is divisible by 3 and therefore composite. Since $2^2 \equiv 1 \bmod 3$, we also have $2^{2^n} = (2^2)^{2^{n-1}} \equiv 1 \bmod 3$ for all $n > 0$. Hence:

$$2^{2^n} + 5 \equiv 6 \equiv 0 \bmod 3.$$

Question 6. Find the smallest positive integer n such that

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

Solution:
Simplifying, we need to solve the system:

$$n \equiv 1 \bmod 3, \quad n \equiv 0 \bmod 5, \quad n \equiv 3 \bmod 7.$$

Since $n \equiv 0 \bmod 5$, then $n = 5a$. Since $n \equiv 1 \bmod 3$ and $n \equiv 3 \bmod 7$ then $n \equiv 10 \bmod 21$ (solve $n = 1 + 3x = 3 + 7y$, so $3x - 7y = 2$). Hence, we need to solve:

$$5a \equiv 10 \bmod 21$$

and clearly $a = 2$ works. Thus, $n \equiv 10 \bmod 105$ and $n = 10$ is the smallest valid solution.

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?

Solution:
Let x be the number of bananas. Then:

$$x \equiv 6 \bmod 11, \quad \text{and} \quad x \equiv 0 \bmod 17.$$

Hence, $x = 17a$ for some integer a. Thus, we need to solve $17a \equiv 6 \bmod 11$ or $17a + 11b = 6$. Clearly, $a = 1, b = -1$ work. Thus $a = 1$ and $x \equiv 17 \bmod 187$. The smallest possible number is 17.

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?

Solution:
Notice that $72 = 2^3 \cdot 3^2$. Thus, 8 divides n and so 8 divides the three last digits $0y2 = y2$. The only two digit numbers divisible by 8 and ending in 2 are 32 or 72, so $y = 3$ or 7.

The number n is also divisible by 9, thus the sum of its digits $7+2+x+2+0+y+2 = x+y+13$ is a multiple of 9. So $x+y+4$ is a multiple of 9. If $y = 3$ then $x+7$ must be a multiple of 9, and the only possibility is $x = 2$. If $y = 7$ then $x + 11$ must be a multiple of 9, which implies that $x = 7$. Therefore:

$$n = 7222032 = 72 \cdot 100306, \quad \text{or} \quad n = 7272072 = 72 \cdot 101001.$$

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

Solution:
By the properties of congruences we know that $36^{100} \equiv 2^{100} \bmod 17$ because $36 \equiv 2 \bmod 17$. Moreover, $2^4 \equiv 16 \equiv -1 \bmod 17$. Therefore:

$$36^{100} \equiv 2^{100} \equiv (2^4)^{25} \equiv (-1)^{25} \equiv -1 \equiv 16 \bmod 17.$$

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

Solution:
Note that $42 = 2 \cdot 3 \cdot 7$. First, notice that if n is even or odd, $n^7 - n$ will always be even, and so it is divisible by 2. Also, if $n \equiv 0, 1$ or $2 \bmod 3$, it is an easy calculation to check that $n^7 - n \equiv 0 \bmod 3$. And likewise (although a little more work), one checks that for $n \equiv 0, 1, 2, 3, 4, 5, 6 \bmod 7$ we also get $n^7 - n \equiv 0 \bmod 7$, and so 7 divides $n^7 - n$, for all $n \geq 1$.

Thus, since $n^7 \equiv n \bmod 7$ and $n^7 \equiv n \bmod 6$ and $\gcd(6, 7) = 1$, we obtain $n^7 \equiv n \bmod 42$, for all n.

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

Solution:
Note that $5555 + 2222 = 7777 \equiv 0 \bmod 7$. Thus, $5555 \equiv -2222 \bmod 7$ and $2222 = 2100 + 122 \equiv 122 \equiv 105+17 \equiv 3 \bmod 7$. One also calculates that $3^6 \equiv 1 \bmod 7$ and $2222 = 6 \cdot 370 + 2$ and $5555 = 925 \cdot 6 + 5$. Finally:

$$5555^{2222} + 2222^{5555} \equiv (-3)^{2222} + 3^{5555} \equiv ((-3)^6)^{370} \cdot (-3)^2 + (3^6)^{925} \cdot 3^5 \equiv 1 \cdot 2 + 1 \cdot 5 \equiv 0 \bmod 7.$$

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).

Solution:
Let us begin working modulo 5 and 7 separately. One calculates:

$$3^6 \equiv 3^4 \cdot 3^2 \equiv 9 \equiv 4 \bmod 5, \quad 2^6 \equiv 2^2 \equiv 4 \bmod 5, \quad 3^6 \equiv 2^6 \equiv 1 \bmod 7.$$

Thus:

$$3^{6n} - 2^{6n} \equiv 4^n - 4^n \equiv 0 \bmod 5, \quad 3^{6n} - 2^{6n} \equiv 1 - 1 \equiv 0 \bmod 7.$$

Thus, since 5 and 7 are relatively prime, $3^{6n} - 2^{6n} \equiv 0 \bmod 35$.

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

Solution:
Let us calculate modulo 17:

$$\begin{aligned}
14! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \bmod 17 \\
&\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot (-8) \cdot (-7) \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \bmod 17 \\
&\equiv 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot (-7) \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \bmod 17 \\
&\equiv 3 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot (-7) \cdot (-6) \cdot (-5) \cdot (-3) \bmod 17 \\
&\equiv 3 \cdot 6 \cdot 8 \cdot (-6) \cdot (-3) \bmod 17 \\
&\equiv 8 \bmod 17
\end{aligned}$$

where, in order, we have used that $2 \cdot (-8) \equiv -16 \equiv 1 \bmod 17$, and $4(-4) \equiv 1 \bmod 17$, and $5 \cdot 7 \equiv (-5)(-7) \equiv 1 \bmod 17$, and $3 \cdot 6 \equiv (-3)(-6) \equiv 1 \bmod 17$.

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).

Solution:
Suppose n is odd. The numbers n and $n-2$ satisfy a Bezout's identity of the form

$$n - (n-2) = 2.$$

Therefore, by Theorem (b) at the beginning of this document, the GCD of n and $n-2$ divides 2. But it cannot be equal to 2 because n is odd and 2 does not divide n. Thus, the GCD must be 1.

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

Solution:
The integers $x = 7k+6$ and $y = 6k+5$ satisfy a Bezout's identity of the form $6x - 7y = 1$ because:

$$6(7k+6) - 7(6k+5) = 36 - 35 = 1.$$

Thus, by Theorem (b) above, the GCD of x and y must be 1.

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

Solution:
Suppose $17p + 1 = n^2$ for some $n \geq 1$. Then $n^2 - 1 = 17p$ and, therefore,

$$17p = (n+1)(n-1).$$

By the Fundamental Theorem of Arithmetic, the prime factorization of $(n+1)(n-1)$ is precisely $17p$, thus the factor $(n+1)$ is equal to $1, p, 17$ or $17p$ (and in the last case $n-1 = 1$, so $n = 2$). The cases $n+1 = 1$ and $n+1 = 17p$ are impossible (because, respectively, they imply $n = 0$ and $17p = 3$). If $n+1 = p$ then $17 = n-1$ and $n = 18$ so $p = 19$. If $n+1 = 17$ then $n-1 = p$ and $n = 16$, so $p = 15$, which is not a prime, so it is not a valid choice.

Hence the only possible case is $p = 19$, so $17p + 1 = 17 \cdot 19 + 1 = 324 = 18^2$.

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

Solution:
We shall prove that $n(n-1)(2n-1)$ is congruent to 0 modulo 2 and modulo 3. Thus, we can conclude that $n(n-1)(2n-1) \equiv 0 \bmod 6$. Indeed, if $n \equiv 0$ or 1 modulo 2, then $n(n-1) \equiv 0 \bmod 2$.

Also, if $n \equiv 0 \bmod 3$ then $n \equiv 0 \bmod 3$, if $n \equiv 1 \bmod 3$ then $(n-1) \equiv 0 \bmod 3$ and if $n \equiv 2 \bmod 3$ then $(2n-1) \equiv 0 \bmod 3$. Thus, in all cases $n(n-1)(2n-1) \equiv 0 \bmod 3$, as desired.

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.

Solution:
The congruence $3x \equiv 1 \bmod 18$ does not have solutions because $\gcd(3, 18)$ is not a divisor of 1. The congruence $3x \equiv 1 \bmod 19$ does have solutions because $\gcd(3, 19) = 1$. The equation $ax \equiv 1 \bmod 18$ only has solutions when $\gcd(a, 18) = 1$ (find them all). The equation $ax \equiv 1 \bmod 19$ has solutions for any $1 \leq a \leq 18$, because then $\gcd(a, 19) = 1$, because 19 is prime.

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.

Solution:
Just a number of calculations...