Test 1  Duration: 50 minutes

This test has 3 questions on 6 pages, for a total of 21 points.

- All questions are long-answer; you should give complete arguments and explanations for all your solutions; answers without justifications will not be marked.
- Continue on the back of the page if you run out of space.
- This is a closed-book examination. None of the following are allowed: documents, cheat sheets or electronic devices of any kind (including calculators, cell phones, etc.)

First Name: ___________________________________ Last Name: ___________________________________

Student-No: ___________________________________

Signature: ___________________________________

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points:</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>21</td>
</tr>
<tr>
<td>Score:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Student Conduct during Examinations**

1. Each examination candidate must be prepared to produce, upon the request of the invigilator or examiner, his or her UBCcard for identification.

2. Examination candidates are not permitted to ask questions of the examiners or invigilators, except in cases of supposed errors or ambiguities in examination questions, illegible or missing material, or the like.

3. No examination candidate shall be permitted to enter the examination room after the expiration of one-half hour from the scheduled starting time, or to leave during the first half hour of the examination. Should the examination run forty-five (45) minutes or less, no examination candidate shall be permitted to enter the examination room once the examination has begun.

4. Examination candidates must conduct themselves honestly and in accordance with established rules for a given examination, which will be articulated by the examiner or invigilator prior to the examination commencing. Should dishonest behaviour be observed by the examiner(s) or invigilator(s), pleas of accident or forgetfulness shall not be received.

5. Examination candidates suspected of any of the following, or any other similar practices, may be immediately dismissed from the examination by the examiner/invigilator, and may be subject to disciplinary action:
   - (i) speaking or communicating with other examination candidates, unless otherwise authorized;
   - (ii) purposely exposing written papers to the view of other examination candidates or imaging devices;
   - (iii) purposely viewing the written papers of other examination candidates;
   - (iv) using or having visible at the place of writing any books, papers or other memory aid devices other than those authorized by the examiner(s); and,
   - (v) using or operating electronic devices including but not limited to telephones, calculators, computers, or similar devices other than those authorized by the examiner(s) electronic devices other than those authorized by the examiner(s) must be completely powered down if present at the place of writing).

6. Examination candidates must not destroy or damage any examination material, must hand in all examination papers, and must not take any examination material from the examination room without permission of the examiner or invigilator.

7. Notwithstanding the above, for any mode of examination that does not fall into the traditional, paper-based method, examination candidates shall adhere to any special rules for conduct as established and articulated by the examiner.

8. Examination candidates must follow any additional examination rules or directions communicated by the examiner(s) or invigilator(s).
1. Let \( \{b_n\}_{n \geq 0} \) be a sequence defined by the properties:

- \( b_0 = -2, b_1 = 5 \); and
- \( b_{n+2} = 10b_{n+1} - 25b_n \).

Find the first positive integer \( n \) with the property that 2018 divides \( b_n \).

**Solution:** This problem is similar to Problem 11 from Practice Set 2 (see also Problem 3 from Practice Set 2)

The quadratic equation associated to this linear recurrence sequence is

\[ x^2 - 10x + 25 = 0 \]

which has the double root 5; this leads to search for the general term of the sequence of the form

\[ b_n = 5^n \cdot (\alpha n + \beta). \]

We solve for \( \alpha \) and \( \beta \) using the information that \( b_0 = -2 \) and \( b_1 = 5 \) and obtain

\[ \beta = -2 \text{ and } \alpha = 3. \]

We check by induction on \( n \) that \( b_n = 5^n \cdot (3n - 2) \). Indeed, the formula works for \( n = 0 \) and \( n = 1 \); so, we prove that it holds for all \( 0 \leq n \leq N \) (for some \( N \geq 1 \)) and then we check it for \( n = N + 1 \). We have

\[
\begin{align*}
  b_{N+1} &= 10b_N - 25b_{N-1} \\
  &= 10 \cdot 5^N (3N - 2) - 25 \cdot 5^{N-1} (3(N - 1) - 2) \\
  &= 5^{N+1} \cdot (2(3N - 2) - (3N - 5)) \\
  &= 5^{N+1} \cdot (3N + 1) \\
  &= 5^{N+1} \cdot (3(N + 1) - 2),
\end{align*}
\]

as claimed. So, the problem asks for the smallest positive integer \( n \) such that 2018 divides \( b_n = 5^n (3n - 2) \); this is equivalent (since 5 is coprime with 2018) with finding the smallest positive integer \( n \) such that

\[ 3n - 2 = 2018k \]

for some \( k \in \mathbb{N} \). We see that \( k = 1 \) does not work because 2020 is not a multiple of 3, but \( k = 2 \) works since 4038 is a multiple of 3; hence the answer is \( n = 1346 \).
2. Let \(m\) and \(n\) be positive integers such that
\[m^{2018} \cdot \phi(m) = n^{2018} \cdot \phi(n),\]
where \(\phi\) is the Euler’s \(\phi\)-function. Prove that \(m = n\).

**Solution: This problem is similar with Problem 3 from Practice Set 3.**

We let \(m = \prod_{i=1}^{r} p_i^{\alpha_i}\) and \(n = \prod_{j=1}^{s} q_j^{\beta_j}\) be the decomposition of \(m\), respectively \(n\) into a product of powers of primes. We allow for the possibility that either \(m\) or \(n\) equals 1 in which case \(r\) or \(s\) equal to 0. We will prove that \(m = n\) by induction on \(r + s\).

The base is \(r = s = 0\) which automatically yields \(m = n = 1\). Therefore we proved the base case of our induction. We assume now that we proved that \(m = n\) for all cases when \(r + s < k\) (for some integer \(k \geq 1\)) and next we prove that also when \(r + s = k\), we get \(m = n\).

Indeed, we let \(p\) be the largest prime number which divides either \(m\) or \(n\). Without loss of generality, we may assume \(p = p_1\). We claim that there exists \(j \in \{1, \ldots, s\}\) such that \(p = q_j\) (in this case we already know that \(s \geq 1\) since otherwise \(n = 1\) which would contradict the fact that \(m^{2018} \phi(m) > 1\)). Now, if \(q_j < p\) for all \(j = 1, \ldots, s\) (note that by our assumption, we already knew that \(p \geq q_j\) for each \(j\)), then also \(p > q_j - 1\) for each \(j\), and thus
\[p \nmid n^{2018}\phi(n) = \prod_{j=1}^{s} q_j^{2019\beta_j - 1}(q_j - 1),\]
because \(p\) is a prime number larger than each prime factor from the above product. So, indeed, there exists \(j\) such that \(p = q_j\). Without loss of generality we may assume \(j = 1\).

We claim that \(\alpha_1 = \beta_1\). Indeed, otherwise we may assume (without loss of generality) that \(\alpha_1 > \beta_1\). So, \(m^{2018} \phi(m) = n^{2018} \phi(n)\) yields
\[\prod_{i=1}^{r} p_i^{2019\alpha_i - 1}(p_i - 1) = \prod_{j=1}^{s} q_j^{2019\beta_j - 1}(q_j - 1),\]
and so,
\[p^{2019(\alpha_1 - \beta_1)} \cdot \prod_{i=2}^{r} p_i^{2019\alpha_i - 1}(p_i - 1) = \prod_{j=2}^{s} q_j^{2019\beta_j - 1}(q_j - 1).\]
Moreover, now we know that \(p > q_j\) for each \(j = 2, \ldots, s\), and hence
\[p \nmid \prod_{j=2}^{s} q_j^{2019\beta_j - 1}(q_j - 1).\]
This is a contradiction with the fact that \(p \mid p^{2019(\alpha_1 - \beta_1)} \cdot \prod_{i=2}^{r} p_i^{2019\alpha_i - 1}(p_i - 1)\) (because \(\alpha_1 > \beta_1\)). So, indeed \(\alpha_1 = \beta_1\), which yields that
\[\prod_{i=2}^{r} p_i^{2019\alpha_i - 1}(p_i - 1) = \prod_{j=2}^{s} q_j^{2019\beta_j - 1}(q_j - 1).\]
More precisely, if we let \(m_1 = \frac{m}{p_1}\) and \(n_1 = \frac{n}{q_1}\), then
\[m_1^{2018} \phi(m_1) = n_1^{2018} \phi(n_1).\]
But the number of prime factors for $m_1$ and $n_1$ is now $r-1$, respectively $s-1$, and thus by the inductive hypothesis we may conclude that $m_1 = n_1$. Because $p_1 = q_1$ and $\alpha_1 = \beta_1$, we get that also $m = n$, as desired.
3. Let $p \geq 5$ be a prime number and let $a$ and $b$ be coprime positive integers with the property that
\[ \sum_{i=1}^{p-1} \frac{1}{i^2} = \frac{a}{b}. \]
Prove that $p \mid a$.

Solution: This problem is similar to Problem 2 from Practice Set 3.
For each $i \in \{1, \ldots, p-1\}$ there exists a unique inverse of $i$ modulo $p$, i.e., there exists a bijective function
\[ f : \{1, \ldots, p-1\} \rightarrow \{1, \ldots, p-1\} \]
such that $f(i)$ is the inverse of $i$ modulo $p$. So,
\[ if(i) \equiv 1 \pmod{p}, \text{ and thus } i^2f(i)^2 \equiv 1 \pmod{p}. \]
Hence there exist positive integers $m_i$ such that
\[ \frac{1}{i^2} = \frac{f(i)^2}{pm_i + 1}. \]
Let $N = \prod_{i=1}^{p-1}(pm_i + 1)$ and for each $i$, we let $N_i = N/(pm_i + 1)$. Since $pm_i + 1 \equiv 1 \pmod{p}$ for each $i$, we conclude that $N$, and also each integer $N_i$ is congruent to 1 modulo $p$. Because
\[ a \equiv \sum_{i=1}^{p-1} \frac{1}{i^2} = \sum_{i=1}^{p-1} \frac{f(i)^2N_i}{N}, \]
we already conclude that $p \nmid b$ (since $p \nmid N$ and also $\gcd(a, b) = 1$). All we need to prove is that $p \mid a$ which would follow if we could prove that
\[ p \mid \sum_{i=1}^{p-1} f(i)^2N_i. \]
Indeed, if $p \mid \sum_{i=1}^{p-1} f(i)^2N_i$, then
\[ p \mid b \cdot \sum_{i=1}^{p-1} f(i)^2N_i = a \cdot N \]
and since $N \equiv 1 \pmod{p}$, then we would conclude that $p \mid a$.
Now, because $N_i \equiv 1 \pmod{p}$ for each $i$, then we obtain that
\[ \sum_{i=1}^{p-1} f(i)^2N_i \equiv \sum_{i=1}^{p-1} f(i)^2 \equiv \sum_{i=1}^{p-1} i^2 \pmod{p}, \]
where in the last congruence we used the fact that the function $f$ is a bijection on the set $\{1, \ldots, p-1\}$. On the other hand,
\[ \sum_{i=1}^{p-1} i^2 = \frac{(p-1)p(2p-1)}{6}. \]
Since $p \geq 5$, we obtain that $\gcd(p, 6) = 1$ and so, the integer $\frac{(p-1)p(2p-1)}{6}$ must be divisible by $p$. Thus

$$p \mid \sum_{i=1}^{p-1} f(i)^2N_i$$

and hence $p \mid a$, as desired.