+-

-

Introduction to computing theory I.

First Midterm — scoring guide

November 3, 2023

General principles.

The aim of the scoring guide is for the correctors to evaluate the papers in a uniform manner. The purpose of this guide is not to give a detailed description of the complete solution of the tasks; the described steps are worth a maximum score they can be considered as an outline of a solution.

The partial marks indicated in the guide are awarded to the solver only if the related idea is included in the thesis as a step of a clear, clearly described and justified solution. That way

for example, the mere description of the knowledge, definitions, and items included in the material is worthless without their application (even if one of the described facts actually plays a role in the solution). Considering that the score indicated in the guide is for the solver taking into account the above (in whole or in part) is entirely the responsibility of the grader.

Sub-points are awarded for all ideas and thoughts that can play a meaningful role in a solution

and from which, with a suitable addition to the thought process described in the thesis, the problem would be solved flawlessly available. If a solver starts several, significantly different solutions to a task, then if all described solutions or solution parts are correct, or

can be completed correctly, then the solution initiative with the most sub-points is evaluated. However, if among the attempted solutions, there are correct ones and also those containing (significant) errors, and it is not clear from the thesis, which one the solver thought was correct, then the solution initiative with fewer points is evaluated (even if this score is 0).

The sub-scores in the guide can be divided further if necessary. From what is described in the guide, a different good solution is of course worth maximum points, but without proof only the items and statements in the presentation (lectures) can be referred to, for other things the proof should also be written.

1. The value of the two fractions gives an integer for those values of n for which $n \equiv 2$ (mod 21) and $n \equiv 5$ (mod 166). (1 point)
   The resulting congruence system is solved using the learned method. From the first congruence, $n = 21k + 2$ for some integer$k$. Substituting this into the second: $21k + 2 \equiv 5$ (mod 166). Subtracting 2 from both sides a, we get $21k \equiv 3$ (mod 166). (2 points)
   Since $(21, 166) = 1$ (because they have no common prime factor) and $1 \vee 3$, therefore, according to the learned theorem, the linear congruence can be solved and has only one solution modulo 166. (1 point)
   Multiplying both sides of the congruence by 8 yields $168k \equiv 24$ (mod 166), that is, $2k \equiv 24$ (mod 166). (1 point)

   (This transformation was not an equivalent step because (166, 2) = 2 and thus the congruence 168k ≡ 24 (mod 166) dividing by 8 would not return the original shape.) (0 points)

   Dividing both sides by 2: $k \equiv 12$ (mod 83), where the modulus was divided by 2 because$(2, 166) = 2$. (1 point)
   Hence $k \equiv 12$ (mod 166) or$k \equiv 95$ (mod 166). (1 point)
   Of these, $k \equiv 12$ (mod 83) is not a solution to the linear congruence, because $21 \cdot 12 = 252 \not\equiv 3$ (mod 166).
   (This false root is due to the non-equivalent step.) Since, according to the above, the linear congruence has only one solution modulo 166, it is therefore $k \equiv 95$ (mod 166). (1 point)
   Therefore, $k = 166l + 95$ for some integer l. Substituting this back:
   $n = 21k + 2 = 21(166l + 95) + 2 = 3486l + 1997$. (1 point)
   Since this only for $l = 0$ occurs between 1 and 2023, $n = 1997$ is the only integer corresponding to the condition for the problem. (1 point)

Applying the theorem on solvability and the number of solutions can be derived from $k \equiv 95$ (mod 166) also by checking the solution. The linear congruence created during the solution can of course be solved with other learned methods, so even with the Euclidean algorithm; working with this in turn, $166k \equiv 0$ (mod 166), $21k \equiv 3$ (mod 166), $19k \equiv -21$ (mod 166), $2k \equiv 24$ (mod 166), finally $k \equiv -237 \equiv 95$ (mod 166) congruences arise. Then 1 point out of 5 points for solving the linear congruence is worth the fact that the solver applies the algorithm (which you don't necessarily have to name, it's enough if its application clearly demonstrates this through); it is worth an additional 1 point to verify that the procedure is learned can be used without dividing (that is, skipping the first phase) because (21, 166) = 1; finally 3 points for the calculation.

2. **First solution.**
We calculate the remainder of 10^{23} when divided by 9998 using the method of repeated squaring. (1 point)
For this, we find the reminders of 10^1, 10^2, 10^4, 10^8, 10^{16} powers (always squaring the previous and taking the remainder of the obtained result). These are: 10, 100, 2, 4, 16. (3 points)
Since 23 = 1 + 2 + 4 + 16, (1 point)
therefore, we first calculate the powers $10^3 = 10^1 \cdot 10^2$, then $10^7 = 10^3 \cdot 10^4$, finally $10^{23} = 10^7 \cdot 10^{16}$ mod 9998 (by multiplying with the corresponding remainders previously calculated and the results obtained). These are: 1000, 2000 and 2006. (3 points)
Multiplying the congruence $10^{23} \equiv 2006$ (mod 9998) by 6: $6 \cdot 10^{23} \equiv 6 \cdot 2006 = 12036 \equiv 2038$ (mod 9998).
Thus, the required remainder is 2038. (2 points)

For a full-fledged solution, it is not necessary to describe the steps behind the performed operations in the above details, it is sufficient to communicate the correct calculations. According to the above scoring, the first 1 point goes to the one who realizes that the task can be solved using the method of repeated squaring (and at least indicates that the algorithm is starting to be applied). However, since the task does not require the learned algorithm application, therefore any calculation that leads to a correct result and **is theoretically correct** will receive a maximum score - even if it is unnecessarily complicated or does not correspond to the exact application of the algorithm. However, if a solution does not (exactly) follow the algorithm, then the correctness of the calculations and that the conclusions drawn from them need justification. Thus, if a solver just provides a calculation which is not the exact algorithm without explanation, then it cannot receive maximum points; such solutions can be awarded a maximum of 5 points out of the first 8 points awarded for the application of the algorithm.

Second solution.
Note that $10^4 = 10000 \equiv 2$ (mod 9998). (2 points)
Raising this to the 5th power: $10^{20} \equiv 2^5 = 32$ (mod 9998). (3 points)
Multiplying both sides by $10^3 = 1000$: $10^{23} \equiv 32000 \equiv 2006$ (mod 9998). (3 points)
Multiplying this by 6: $6 \cdot 10^{23} \equiv 6 \cdot 2006 = 12036 \equiv 2038$ (mod 9998).
Thus, the required remainder is 2038. (2 points)

3. The normal vector of the plane S of the ground is $\underline{n} = \overrightarrow{AB}$ (2 points)
since it is perpendicular to the plane S (because the sides of the rectangle are perpendicular to the plane of the base). (1 point)
Let the position vectors pointing to A and B be denoted by $\underline{a}$ and $\underline{b}$, respectively,
$\underline{n} = \overrightarrow{AB} = \underline{b} - \underline{a} = (4;2;1) - (1;4;2) = (3;-2;-1)$. (1 point)
Thus, writing the equation of S based on n and A: $3x - 2y - z = -7$. (3 points)

The points on the z-axis are those for which $x=y=0$ is satisfied. Substituting this into the equation of S, $-z=-7$, that is $z=7$ results. Thus, S intersects the z-axis at $(0;0;7)$. (3 points)

4. Suppose that $\alpha\cdot\underline{a}+\beta\cdot\underline{b}+\gamma\cdot\underline{c}+\delta\cdot\underline{d}=0$ holds for some scalars $\alpha,\beta,\gamma,\delta\in R$. (1 point)
Substituting the vectors $\underline{a},\underline{b},\underline{c},\underline{d}$ and performing the operations into the following system of linear equations, we get

$$\begin{aligned}\alpha+4\beta&=0\\ \alpha+5\beta&=0\\ 17\alpha+19\beta+2\gamma+4\delta&=0\\ 23\alpha+29\beta+5\gamma+p\cdot\delta&=0\end{aligned}$$ (1 point)

Subtracting the first from the second equation gives $\beta=0$. Substituting this back into either of the first two equations, $\alpha=0$ results. (2 points)
Thus, the system consisting of the third and fourth equations is simplified to:
$2\gamma+4\delta=0, 5\gamma+p\cdot\delta=0$. (0 points)
Here, subtract $\frac{5}{2}$ times the former from the latter: $(p-10)\cdot\delta=0$. (1 point)
If $p\neq10$, this equation gives $\delta=0$. Substituting this back into the equation $2\gamma+4\delta=0$,it follows that$\gamma=0$, too. (1 point)
Thus, according to what we learned, for every value $p\neq10$, the vectors $\underline{a},\underline{b},\underline{c},\underline{d}$are linearly independent (because $\alpha\cdot\underline{a}+\beta\cdot\underline{b}+\gamma\cdot\underline{c}+\delta\cdot\underline{d}=¿$ is possible only in the case $\alpha=\beta=\gamma=\delta=0$). (2 points)
If, on the other hand, $p=10$, then the equation $(p-10)\cdot\delta=0$is meaningless. Then, for example, $\gamma=2,\delta=-1,\alpha=\beta=0$ is the solution of the above system of linear equations (that is, $2\underline{c}-\underline{d}=0$). (1 point)
Thus, according to what was learned, in the case of $p=10$, then $\underline{a},\underline{b},\underline{c},\underline{d}$ are linearly dependent. (1 point)

If a solver only observes that d = 2c in the case of $p=10$, then he can therefore receive the score according to the penultimate 1 point; and if from this he correctly draws and justifies the conclusion that in the case of $p=10$, the vectors a, b, c and d are linearly dependent (because d = 0a + 0b + 2c), then the last 1 point, too.
If a solver only examines $d\in span\{a,b,c\}$ for which p values it is fulfilled and incorrectly thinking that this is sufficient to test for linear independence constitutes a basic principle error and thus (assuming correct calculation and result) it can only be awarded a maximum of 3 points (in the sense that it cannot be added to the points 1+2 just written, but one of the two will be given at the most). This of course, does not apply to a solution that first shows the linear independence of a, b, c, then, referring to the newly arriving vector lemma, he asserts that the four vectors are linearly independent equivalent to $d\notin span\{a,b,c\}$; such a solution can, in principle, can be flawless and can obviously get maximum points.

5. **First solution.**
If the first term of the arithmetic sequence formed by the first three coordinates of a vector $\underline{v}\in V$ is α, and its difference is δ, then from the text of the problem $\underline{v}=(\alpha,\alpha+\delta,\alpha+2\delta,2\alpha+4\delta,4\alpha+8\delta)^T$. (2 points)
Therefore, every $\underline{v}\in V$ can be written as follows: $\underline{v}=\alpha\cdot(1,1,1,2,4)^T+\delta\cdot(0,1,2,4,8)^T$. (2 points)
This means that $\underline{b_1}=(1,1,1,2,4)^T\wedge\underline{b_2}=(0,1,2,4,8)^T$ vectors form a generator system in V (2 points)
On the other hand, $\underline{b_1}$ and $\underline{b_2}$ are linearly independent, because no vector is a scalar multiple of the other. (2 points)
Thus $\{\underline{b_1},\underline{b_2}\}$ is a basis of V, (1 point)
that is, $dim\,V=2$. (1 point)

Second solution.

We use the learned procedure to create a basis for V. (0 points)
To do this, we first choose an arbitrary vector $b1 \in V$, with $\underline{b_1} \neq 0$: for example, $\underline{b_1} = (1,0,-1,-2,-4)^T$. (2 points)
Then $\underline{b_1}$ is not a generating system in V, for example, because in $\langle \underline{b_1} \rangle$ all vectors has 0 in the second coordinate, so we can easily choose a $\underline{b_2} \in V$, with $\underline{b_2} \notin \langle \underline{b_1} \rangle$: for example, let $\underline{b_2} = (0,1,2,4,8)^T$. (2+1 points)
Now we need to check that $V = \langle \underline{b_1}, \underline{b_2} \rangle$ is already true. For this, let us take an arbitrary $\underline{v} \in \langle \underline{b_1}, \underline{b_2} \rangle$. Then $\underline{v} = \alpha \underline{b_1} + \beta \underline{b_2}$ for some scalars α, β, (1 point)
that is, $\underline{v} = (\alpha, \beta, -\alpha+2\beta, -2\alpha+4\beta, -4\alpha+8\beta)^T$. (1 point)
We show that every vector $\underline{v} \in V$ can be written in this form. Indeed, if the first two coordinates of a $\underline{v} \in V$ are α and β, respectively, then the difference of the arithmetic series formed by the first three coordinates is $\beta - \alpha$, so the third coordinate of $\underline{v}$ is $\beta + (\beta - \alpha) = -\alpha + 2\beta$. Hence, the fourth and fifth coordinates of $\underline{v}$ are indeed
$-2\alpha+4\beta \wedge -4\alpha+8\beta$, respectively, because the last three coordinates form a geometric series with quotient 2. (1 point)
Thus $\{\underline{b_1}, \underline{b_2}\}$ already form a generator system in V. (1 point)
Following the learned procedure, we obtained a basis $\{\underline{b_1}, \underline{b_2}\}$ in V, from which $\dim V = 2$. (1 point)

(The "solutions" that refer only to the fact that by fixing the first two coordinates of a vector $\underline{v} \in V$, the others are already clearly defined, so that "the elements of V have two free parameters", therefore $\dim V = 2$, then this statement needs to be proven in one of the above ways, and thus in itself is worth only 1 point.)

6. Let a be an arbitrary Fermat liar of 1024. Then $1 \leq a \leq 1023$, $(a, 1024) = 1$ and $a^{1023} \equiv 1$ (mod 1024) (according to the definition of a Fermat liar). (1 point)
Since $1024 = 2^{10}$, according to the learned theorem, $\varphi(1024) = 2^{10} - 2^9 = 512$. (1 point)
Since $(a, 1024) = 1$, the Euler-Fermat theorem can be applied: (1 point)
The $a^{512} \equiv 1$ (mod 1024). (1 point)
Squaring this: $a^{1024} \equiv 1^2 = 1$ (mod 1024). (1 point)
Thus, $1 \equiv a^{1024} = a^{1023} \cdot a \equiv 1 \cdot a = a$ (mod 1024), that is, $a \equiv 1$ (mod 1024). (3 points)
From this, $1 \leq a \leq 1023$ gives $a = 1$. (1 point)
Also, 1 is obviously a Fermat liar of 1024, as $(1, 1024) = 1$ and $1^{1023} = 1 \equiv 1$ (mod 1024), (1 point)
Therefore, the only Fermat liar of 1024 is 1. (0 points)
(To obtain 3 points according to the above scoring, it is necessary to convincingly justify that $a^{1023} \equiv 1$ (mod 1024) and then $a \equiv 1$ (mod 1024) indeed follows from $a^{1024} \equiv 1$ (mod 1024) congruences.)