Introduction to the Theory of Computing I
First midterm-Grading guide
Oct.25,2024

General principles.

The aim of the scoring guide is for the correctors to evaluate the papers in a uniform manner. The aim of the guide is not to provide a detailed description of the complete solution of the tasks; the described steps can be considered as an outline of a solution that will achieve a maximum score.

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. Thus, for example, the mere description of the knowledge, definitions, and theorems included in the material is not worth points without their application (even if, by the way, one of the described facts actually plays a role in the solution). Considering whether the score indicated in the guide is due to the solver (in part or in whole) taking into account the above, is entirely the responsibility of the corrector.

Partial points are awarded for all ideas and thoughts that can have a meaningful role in a solution and from which, with a suitable addition to the thought process described in the thesis, a flawless solution to the task could be obtained. If a solver starts several, significantly different solutions to the same task, then the maximum score that can be given is one. If each described solution or solution part is correct or can be supplemented to be correct, then the solution initiative with the most partial points is evaluated. However, if there are several solution attempts that are both correct and contain (significant) errors, and the thesis does not reveal which one the solver considered correct, then the solution attempt with fewer points is evaluated (even if this score is 0).

The sub-scores in the guide can be divided further if necessary. A good solution different from the one described in the guide is of course worth maximum points, but without proof you can only refer to the theorems and statements in the presentation.

1. From the conditions of the problem, $48n \equiv n + 1(mod277)$. Rearranged: $47n \equiv 1\ (mod277)$. (1+1 point)
   Since $(47,277) = 1$ (because 47 is prime and $47 \nmid 277$), the resulting linear congruence can be solved according to the learned theorem and has 1 solution modulo 277. (1 point)
   Multiplying both sides by 6: $282n \equiv 6(mod277)$, i.e. $5n \equiv 6(mod277)$. (1 point)
   Multiplying by 6, $(6,277)$ made it an equivalent step (that is, the solution set did not change). (1 point)
   Because of $6 \equiv 560(mod277)$, this is equivalent to: $5n \equiv 560(mod277)$. (1 point)
   Dividing both sides by 5: $n \equiv 112(mod277)$, (1 point)
   where the modulus did not change due to $(277,5) = 1$. (1 point)
   Since all steps taken were equivalent, the resulting $n \equiv 112(mod277)$ is indeed a solution to the linear congruence. (Here, instead of the equivalence of the steps, we can refer to the fact that since the number of solutions is 1 modulo 277, it can only be 112, so it really is a solution; and, of course, we can also check that 112 is correct.)
   Thus, among the numbers between 1 and 500, $n = 112$ and $n = 389$ meet the conditions of the task. (2 point)

   The linear congruence can of course also be solved with the learned Euclidean algorithm.

2. The conditions of the problem give $n \equiv 7(mod36)$ and $n \equiv 9(mod64)$. (3 points)
   The resulting congruence system is solved using the learned method. From the first congruence, $n = 36k + 7$ for some integer k. Substituting this into the second: $36k + 7 \equiv 9$ (mod 64). (2 points)
   By subtracting 7 from both sides, we get the linear congruence $36k \equiv 2\ (mod\ 64)$. (1 point)

However, since $(36, 64) = 4 \nmid 2$, this has no solution according to the learned theorem. (3 points)
Thus, the congruence system also has no solution, i.e. there are no integers n satisfying the conditions (not even between 1 and 2024). (1 point)

If a solver cannot correctly write the congruence system resulting from the text of the task and therefore solves another congruence system, he can only get as many of the 7 points remaining after losing the first 3 points as can be matched with the above solution. Thus, the following 2 + 1 points can be given for the correct calculation resulting from the incorrect congruence system. However, if the linear congruence obtained in this way can be solved, then the last 3 + 1 points according to the scoring can no longer be given for that (even flawless) solution.

3. Let $Q = (x, y, z)$ be the intersection point of the lines e_1 and e_2.
Form the parametric system of e_1, we obtain $x = 6 + t, y = 1 - \frac{1}{2}t$ and $z = -t$. (1 point)
As Q must also satisfy the equation of e_2, we have $\frac{(6+t)-2}{4} = \left(1 - \frac{1}{2}t\right) + 6 = \frac{1-(-t)}{3}$ (1 point)
From $\frac{(6+t)-2}{4} = \left(1 - \frac{1}{2}t\right) + 6$, we find $t = 8$ (1 point)
And $t = 8$ satisfies the second equality $\left(1 - \frac{1}{2}t\right) + 6 = \frac{1-(-t)}{3}$ (1 point)
So $Q = (14, -3, -8)$. (1 point)
Since the line through P and Q is perpendicular to S, the normal vector $\underline{n} = \overrightarrow{PQ}$ (1 point)
So $\underline{n} = \overrightarrow{PQ} = (6, -4, -14)$ (1 point).
From this and P, we can already write the equation of S: 3x − 2y − 7z = −20. (1 point)
On the y-axis are the points whose x and z coordinates are 0. From this, we get the equation −2y = −20 for the intersection of S and the y-axis. Thus, S intersects the y-axis, namely at the point (0; 10; 0). (2 points)

4. **(a)** The statement is (always) true. (0 points)
Because $d \in Span\{a, b, c\}$ there exist scalars α, β, γ for which $d = \alpha a + \beta b + \gamma c$. (1 point)
We show that here $\alpha = 0$. If $\alpha \neq 0$, then by rearrangement we would get the equation $a = -\frac{\beta}{\alpha}b - \frac{\gamma}{\alpha}c + \alpha d$. (1 point)
From this, however, $a \in Span\{b, c, d\}$ would follow, contrary to the statement of the problem. Thus, $\alpha = 0$ really follows. (2 points)
From this and the equation above, $d = \beta b + \gamma c$, which proves the statement $d \in Span\{b, c\}$. (1 point)

(b) The statement can be true or false. (0 point)
To show this, we first show an example where the statement is true. For example, let a and b be two non-parallel plane vectors (that is, vectors in R^2) and let $b = c = d$. (For example, $a = (1; 0)$ and $b = c = d = (0; 1)$.) (0 point)
Then $a \notin Span\{b, c, d\}$ is true, since from the vectors $b = c = d$ only the plane vectors parallel to them can be expressed by linear combination and a is not such a vector. (1 point)
On the other hand, the statements $d \in Span\{a, b, c\}$ and $b \in Span\{c, d\}$ are also true because $d = 0 \cdot a + 1 \cdot b + 0 \cdot c$ and $b = 1 \cdot c + 0 \cdot d$. (1 point)

We now show an example where the statement is false. For example, let a, b and c be three space vectors (that is, vectors in R^3) that do not lie in the same plane and let $d = c$. (For example, $a = (1; 0; 0), b = (0; 1; 0)$ and $c = d = (0; 0; 1)$.) (0 point)
Then $d \in Span\{a, b, c\}$ is true because $d = 0 \cdot a + 0 \cdot b + 1 \cdot c$. (1 point)

Also $a \notin Span\{b, c, d\}$ is also true, because from the vectors b and $c = d$ only the vectors of the plane defined by them (passing through the origin) can be expressed by linear combination and a is not such. (1 point)
However, the statement $b \in Span\{c, d\}$ is not true now, because from the vector $c = d$ only the vectors parallel to it can be expressed by linear combination and b is not like this (otherwise a, b and c would fall in the same plane). (1 point)

Of course, countless other good examples can be shown that $b \in Span\{c, d\}$ is true and also that it is not.
In each case, these are scored in such a way that the provision of specific examples is worth no points in itself, and the justification of their correctness is worth 2 or 3 points in the true and false cases, respectively. In both cases, a partial score can only be given if the solver has made his objective clear - that is, that he wants to show an example of whether the statement is true or false - and his example really meets this objective.

5. Suppose that $\alpha \cdot u + \beta \cdot v + \gamma \cdot w = 0$ holds for some scalars $\alpha, \beta, \gamma \in R$. (1 points)
Substituting the vectors u, v, w and performing the operations, we arrive at the following system of linear equations: (2 points)

$$\alpha - 2\beta = 0$$
$$-3\alpha + 6\beta = 0$$
$$\alpha + \beta + 4\gamma = 0$$
$$\alpha + 4\beta + 9\gamma = 0$$

From the first equation $\alpha = 2\beta$. Entering this in the third and fourth: $3\beta + 4\gamma = 0$ and $6\beta + 9\gamma = 0$. (1 point)
Subtracting the double of the former from the latter equation: $\gamma = 0$. Substituting this (for example) back into the equation $3\beta + 4\gamma = 0$ gives $\beta = 0$, from which $\alpha = 0$ because of $\alpha = 2\beta$. (3 points)
Thus, according to what was learned, u, v, w are linearly independent (because $\alpha u + \beta v + \gamma w = 0$ is only possible in the case $\alpha = \beta = \gamma = 0$). (1+2 points)

Of course, the problem can be solved based on the original definition of linear independence (that is, by showing that none of u, v and w can be expressed as a linear combination of the other two). Then 2–2 points are awarded for the justification of the statements $u \notin Span\{v, w\}$ and $v \notin Span\{u, w\}$, and 3 points for the justification of the statement $w \notin Span\{u, v\}$; and the missing 3 points are for the correct application of the definition (thus including the knowledge that, following this path, the verification of all three statements is necessary to show linear independence). The system of linear equations resulting from the solution can also be solved by Gaussian elimination (even though this is not included in the first midterm material). If someone works like this, then for the elimination, the third and fourth according to the above scoring are awarded 1+2 points, the scoring of the other parts corresponds to the above.

6. $n^{201} \equiv n(mod275)$ is satisfied exactly if the congruences $n^{201} \equiv n(mod11)$ and $n^{201} \equiv n(mod25)$ are true. Indeed: $n^{201} \equiv n(mod275)$ by the (second, equivalent) definition of congruence means that $275 \mid n^{201} - n$; namely, a number is exactly divisible by 275 if it is divisible by both 11 and 25 ($5^2 \cdot 11 = 275, (25,11) = 1$, and due to the fundamental theorem of arithmetic). (1 point)
Thus, we will examine separately for what n these two congruences are satisfied.
First, we show that $n^{201} \equiv n(mod11)$ is true for all integers n. (0 points)
If $11 \mid n$, then $11 \mid n^{201}$ is also obviously true, so the congruence $n^{201} \equiv n(mod11)$ holds (because both sides give a remainder of 0 when divided by 11). (1 point)
If, on the other hand, $11 \nmid n$, then $(n, 11) = 1$ (because 11 is prime). Thus, $n^{\varphi(11)} \equiv 1(mod11)$ results from the Euler-Fermat theorem. Here $\varphi(11) = 10$, again because 11 is prime. (1 point)
Raising the obtained congruence to the 20th power, then multiplying both sides by n, $n^{200} \equiv 1(mod11)$, then $n^{201} \equiv n(mod11)$ really follows in the case of $11 \nmid n$. (1 point)
However, the congruence $n^{201} \equiv n(mod\ 25)$ no longer holds for all n. Indeed, if $5 \mid n$, then n^{201} is obviously divisible by 25 (in fact, even by 5^{201}). Thus, if $5 \mid n$, but $25 \nmid n$, then $n^{201} \not\equiv n(mod25)$. (1 point)

We show that $n^{201} \equiv n(mod\ 25)$ holds for all other integers n; that is, it is also true for n's not divisible by 5 and divisible by 25. (0 points)
If 25 | n, then, as above, $25 \mid n^{201}$ is also true, so $n^{201} \equiv n\ (mod 25)$ holds. (0 points)
If, on the other hand, $5 \nmid n$, then $(25, n) = 1$, because 25 and n have no common prime divisor. (1 point)
$\varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 20$ as learned. (1 point)
Thus, applying the Euler-Fermat theorem to n and 25: $n^{20} \equiv 1$ (mod 25). (1 point)
By raising the obtained congruence to the 10th power and then multiplying both sides by n, $n^{200} \equiv 1\ (mod\ 25)$ and then$n^{201} \equiv n\ (mod\ 25)$ indeed follows in all $5 \nmid n$ cases. (1 point)
Summarizing the above, we have thus obtained that $n^{201} \equiv n\ (mod\ 275)$ does not hold for exactly those integers n for which $5 \mid n$ and $25 \nmid n$. The number of these between 1 and 275 is 55 − 11 = 44 (because the number of n divisible by 5 is 55, and the number of those divisible by 25 is 11). Thus, the number of n between 1 and 275 for which $n^{201} \equiv n\ (mod 275)$ holds: 275 − 44 = 231. (1 point)

If a solver only gets so far as to find out by directly applying the Euler-Fermat theorem (and multiplying the obtained congruence by n) that $n^{201} \equiv n(mod\ 275)$ holds for all n for which $(n, 275) = 1$, then he/she can get 2+1 points for this partial result. Only two points is awarded if the solver forgets about the condition $(n, 275) = 1$ and thus believes that the congruence is true for all n.
And if a solver uses the Euler-Fermat theorem incorrectly in the sense that he mistakenly believes that (n, 275) = 1 is a necessary and sufficient condition for the fulfillment of the congruence in the problem (and thus, for example, thinks that ϕ (275) is the corresponding n's), he/she can only get 1 of these 2 points.