Introduction to the Theory of Computing I
1st retake of First midterm
Grading guide

November.15,2024

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. Since $(7,8)=1$, a number is divisible by both 7 and 8 if and only if it is divisible by 56. (1 point)
   In other words, $n\equiv 0\ (mod\ 56)$ and $n\equiv 10\ (mod\ 22)$ result from the conditions of the problem. (1 point)
   The resulting congruence system is solved using the learned method.
   From the first congruence, $n=56k$ follows for some integer k. Substituting this into the second:
   $56k\equiv 10\ (mod\ 22)$, that is, $12k\equiv 10(mod\ 22)$. (2 points)
   Since $(12,22)=2\vee 10$, therefore the congruence can be solved according to the learned theorem (and it will have two solutions modulo 10). (1 point)
   Dividing both sides by 2: $6k\equiv 5\ (mod\ 11)$, where the modulus had to be divided by $(22,2)=2$.
   Multiplying both sides by 2: $12k\equiv 10(mod\ 11)$, that is, $k\equiv 10\ (mod\ 11)$. Multiplying by 2 was an equivalent step because $(2,11)=1$ (that is, the solution set did not change). So $k=11l+10$ for some integer l. (3 points)
   Substituting this back: $n=56(11l+10)=616l+560$. (1 point)
   Since this number lies between 0 and 1000 exactly if $l=0$, therefore there is only one number, which is 560, that meet the conditions of the task. (1 point)

2. We use the Euclidean algorithm. (So this score goes to the person who recognizes that this algorithm must be used - even if it is not mentioned separately.) (2 points)
   Dividing (48n + 12) by (33n + 8) with a remainder: 48n + 12 = 1 · (33n + 8) + 15n + 4.
   Dividing (33n + 8) by (15n + 4) gives: 33n + 8 = 2 · (15n + 4) + 3n.
   Dividing (15n + 4) by 3n with a remainder: 15n + 4 = 5 · 3n + 4. (4 points)

Since the number formed from the last two digits of n is 88, which is divisible by 4, therefore n and 3n are also divisible by 4. Thus, when 3n is divided by 4, the remainder is 0. (2 points)
Thus, the greatest common divisor (which is the last non-zero remainder) is 4. (2 points)

3. **(a)** Rewriting the equation system of e yields $\frac{x-2}{-4}=\frac{y-7}{p}=\frac{z-6}{3}$, from which the direction vector of e can be read: $\underline{v}_e=(-4;p;3)$. (1 point)

Similarly, rewriting the system of equations of f yields $\frac{x+9}{2}=\frac{y}{1/2}=\frac{z-5/2}{-3/2}$, from which the direction vector of f can be read as: $\underline{v}_f=(2;1/2;-3/2)$. (2 points)

Two lines are parallel if and only if their direction vectors are parallel, i.e. if $\underline{v}_e$ and $\underline{v}_f$ are constant (non-zero) multiples of each other, i.e. if there exists a number $\lambda\in R$ such that $\underline{v}_e=\lambda\cdot\underline{v}_f$. (1 point)
That is, $-4=2\lambda, p=\frac{1}{2}\cdot\lambda, 3=-3/2\cdot\lambda$, which gives $\lambda=-2$, and hence $p=-1$. (1 point)
So the two lines are parallel if and only if $p=-1$. (1 point)

(b) Two lines are perpendicular if and only if their direction vectors are perpendicular, (1 point)
that is, if $\underline{v}_e\cdot\underline{v}_f=0$. (1 point)
So $0=-4\cdot2+p\cdot\frac{1}{2}+3\cdot(\frac{-3}{2})=\frac{-25}{2}+\frac{p}{2}$, from which $p=25$. (1 point)

So the two lines are perpendicular if and only if $p=25$. (1 point)

If a solver writes the direction vectors incorrectly, after losing the 1+2 points for determining the direction vectors, he/she can still get the additional sub-scores. However, if the solution becomes easier as a result of the error, points can only be given for parts that essentially correspond to the above.

4. Let $\underline{z}$ be such a vector. Then $\underline{z}\in Span\{\underline{u},\underline{v}\}$ means that $\underline{z}$ can be expressed from $\underline{u}$ and $\underline{v}$ by a linear combination, that is, there exist scalars α,β such that $\alpha\cdot\underline{u}+\beta\cdot\underline{v}=\underline{z}$. (3 points)
Then, after performing the operations, we get the following:

$$\underline{z}=\begin{pmatrix}2\alpha-\beta\\ \alpha\\ \beta\\ -\alpha+3\beta\end{pmatrix}. \text{ (2 points)}$$

That is, according to the conditions of the task, we get the following system of equations. (2 points)
$2\alpha-\beta=\beta$
$-\alpha+3\beta=\alpha+5$
The first equation gives $\alpha=\beta$. Substituting this into the second, $\alpha=\beta=5$. (1 point)
Thus, the only element of the generated subspace $Span\{\underline{u},\underline{v}\}$ satisfying the conditions is the vector $\underline{z}=(5;5;5;10)^{\mathsf{T}}$. (2 points)

5. We show that the system $\underline{a},\underline{b},\underline{c}+\underline{d}$ is definitely linearly independent.

Solution 1.
Since the system a,b,c is linearly independent, so are the system a,b. (1 point)

However, since the system $\underline{a},\underline{b},\underline{d}$ is already linearly dependent, according to the lemma of the newly arriving vector, $\underline{d}\in Span\{\underline{a},\underline{b}\}$, i.e. there exist scalars α,β such that $\alpha\cdot\underline{a}+\beta\cdot\underline{b}=\underline{d}$. (2 points)

Suppose that $\lambda_1\cdot\underline{a}+\lambda_2\cdot\underline{b}+\lambda_3\cdot(\underline{c}+\underline{d})=\underline{0}$ holds for some scalars $\lambda_1,\lambda_2,\lambda_3$. (1 point)

Substituting into this the relationship $\alpha\cdot\underline{a}+\beta\cdot\underline{b}=\underline{d}$ and then rearranging the equation $(\lambda_1+\lambda_3\cdot\alpha)\cdot\underline{a}+(\lambda_2+\lambda_3\cdot\beta)\cdot\underline{b}+\lambda_3\cdot\underline{c}=\underline{0}$ is obtained (2 point)

Since the vectors $\underline{a},\underline{b},\underline{c}$ are linearly independent, this is only possible if $(\lambda_1+\lambda_3\cdot\alpha)=0$ and $(\lambda_2+\lambda_3\cdot\beta)=0$ and $\lambda_3=0$. (2 points)

It immediately follows also that $\lambda_1=0$ and $\lambda_2=0$. (1 point)

Thus, a linear combination of the vectors $\underline{a},\underline{b},\underline{c}+\underline{d}$ can be the null vector if and only if all three coefficients are 0, so according to the theorem learned in the lecture, the vectors are linearly independent. (1 point)

Solution 2.

Assume indirectly that the vectors $\underline{a},\underline{b},\underline{c}+\underline{d}$ are linearly independent.

Since the vectors $\underline{a},\underline{b},\underline{c}$ are linearly independent, so are the vectors $\underline{a},\underline{b}$. (1 point)

However, since $\underline{a},\underline{b},\underline{c}+\underline{d}$ are already linearly dependent, $\underline{c}+\underline{d}\in Span\{\underline{a},\underline{b}\}$ according to the newly arriving vector lemma. (2 points)

Similarly, since the system $\underline{a},\underline{b},\underline{d}$ is also linearly dependent, therefore, according to the newly arrived vector lemma, $\underline{d}\in Span\{\underline{a},\underline{b}\}$. (2 points)

Since all subspaces are closed for addition and multiplication by the scalar, then $-\underline{d}\in Span\{\underline{a},\underline{b}\}$, and thus $\underline{c}=(\underline{c}+\underline{d})+(-1)\cdot\underline{d}\in Span\{\underline{a},\underline{b}\}$, (3 points)

which contradicts the fact that the vectors $\underline{a},\underline{b},\underline{c}$ are linearly independent. (2 points)

So the system $\underline{a},\underline{b},\underline{c}+\underline{d}$ is indeed linearly independent.

6. Consider the remainder of the division of the number $a^{\varphi(b)}+b^{\varphi(a)}$ by a or b. (1 point)

Obviously, $a^{\varphi(b)}\equiv 0(mod\,a)$ and $b^{\varphi(a)}\equiv 0(mod\,b)$. (1 point)

Since $(a,b)=1$, according to the Euler–Fermat theorem, $a^{\varphi(b)}\equiv 1(mod\,b)$ and $b^{\varphi(a)}\equiv 1(mod\,a)$. (1 point)

That is, $a^{\varphi(b)}+b^{\varphi(a)}\equiv 0+1\equiv 1(mod\,a)$ and $a^{\varphi(b)}+b^{\varphi(a)}\equiv 1+0\equiv 1(mod\,b)$. (2 points)

Thus, according to the equivalent definition of congruence, $a^{\varphi(b)}+b^{\varphi(a)}-1$ is divisible by both a and b, (3 points)

and since $(a,b)=1$, so $a^{\varphi(b)}+b^{\varphi(a)}-1$ is also divisible by ab. (1 points)

That is, the number $a^{\varphi(b)}+b^{\varphi(a)}$ gives a remainder of 1 when divided by ab. (1 point)