HW 2 FEEDBACK

Dear Students,

It is good to see that the overall mathematical writing in HW 2 is much better than that of HW 1. However, there are still some points we would like to discuss in the following.

1. Comments on Math

(1) For Q.2 (b), a few students responded by saying decrypt $m^7 \pmod{31}$ by multiplying by m^{24} to get $m^{31} \pmod{31}$, then use Fermat's little theorem to obtain $m^{31} \equiv m \pmod{31}$. This method assumes that you know what the value of m is, which is something unreasonable. Decryption is meaningful only if (and in practice) you do not have complete information of the original text.

(2) Consider the matrix $\begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix} \pmod{26}$ in Q.18. We observe that quite a number of you make the mistake that

$$\begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix} \text{ is invertible if and only if } \det \begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix} \neq 0. \tag{1.1}$$

This is incorrect as you are now working with **a ring $\mathbb{Z}_{26}$ instead of a field**. In a linear algebra class, you only encounter matrices over $\mathbb{R}$ or $\mathbb{C}$. In fact, $\mathbb{R}$ or $\mathbb{C}$ are fields in which (1.1) is valid.

The correct statement in $\mathbb{Z}_{26}$ is that $\begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix} \pmod{26}$ is invertible if and only if $\det \begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix}$ is invertible $\pmod{26}$ (multiplicatively). The last statement is also equivalent to $\det \begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix}$ being coprime to 26.

(3) In Q. 26, it is worth pointing out that the Fermat's Little Theorem $x^{p-1} \equiv 1 \pmod{p}$ (where p is a prime) **only holds for $p \nmid x$!** A large proportion of students forgot about this.

2. Comments on Math Writing

(1) **Prove by Contradiction in Q. 26.** It could be the first time for some of you to see prove by contradiction. Therefore, we think it may be a good idea to briefly go through how does this work.

Recall that we want to show that 'if p is a prime satisfying $p \equiv 3$ (mod 4), then $x^2 \equiv -1 \pmod{p}$ has no solution'.

You should start your proof by **assuming the negation of the conclusion is true**, i.e., you should write something like "Suppose contrary, there exists $x \in \mathbb{Z}_p$ such that $x^2 \equiv -1 \pmod{p}$" in the beginning. Many of you omit this in the proof.

Date: September 26, 2018.

Having this assumption, you should figure out where do contradiction(s) arise. In the following, we present an example on how to argue properly:

Suppose contrary, there exists $x \in \mathbb{Z}_p$ such that $x^2 \equiv -1 \pmod p$. Since $p \equiv 3 \pmod 4$, $(p-1)/2$ is an odd positive integer. We have

$$-1 \;=\; (-1)^{\frac{p-1}{2}} \;\equiv\; (x^2)^{\frac{p-1}{2}} \;=\; x^{p-1} \pmod p. \tag{2.1}$$

It is clear that $p \nmid x$; otherwise, we have $-1 \equiv x^2 \equiv 0 \pmod p$ which is impossible. Then by Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod p$. Together with (2.1), it follows that $-1 \equiv 1 \pmod p$. However, as p cannot be 2, we have a contradiction ! Therefore, our assumption is false and the equation $x^2 \equiv -1 \pmod p$ does not admit any solution.

(2) Do not forget those quantifiers like "there exists", "for any", "for some" etc. in your proof. They are very important!!!

(3) Here, we use Q. 18 of HW 2 as an example. Suppose now you want to apply a formula by plugging-in some numbers into it. For example, compute

$$\det \begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix}$$

by using the formula

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;=\; ad - bc.$$

We observe that many of you write something like

$$\text{"}ad - bc \;=\; (1)(1) - (6)(1) \;=\; -5\text{"}$$

in your answer but without defining what exactly are a, b, c, d. This is something improper.

In fact, simply write

$$\det \begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix} \;=\; (1)(1) - (6)(1) \;=\; -5$$

would be good enough. The message is that **if you want to introduce any notation, variable etc., you should define it properly before using it.**

(4) **Please help the graders by explaining what are the meanings of your mathematical expressions and tell us what you are doing.** It would be great if you could avoid random expressions floating around. For example, we observe that many of you write something like

$$5 \begin{pmatrix} 1 & -1 \\ -6 & 1 \end{pmatrix} \;\equiv\; \begin{pmatrix} 5 & -5 \\ -30 & 5 \end{pmatrix} \;\equiv\; \begin{pmatrix} 5 & 21 \\ 22 & 5 \end{pmatrix} \pmod{26}$$

out of nowhere. **Please tell us what are you computing for**. In this case, it is so much better if you simply add a line before it, e.g., "The inverse of $\begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix} \pmod{26}$ is ". Even if you put a box around it is not decent enough.

Here is another example. Some of you used Euclidean algorithm to compute the inverse of $5 \pmod{26}$ (In fact, this is unnecessary. This can be done by inspection.). Before writing out all the numbers and expressions involved in the Euclidean algorithm, please add a line "In the following, we use the Euclidean algorithm to compute the inverse of 5 $\pmod{26}$. "

(5) As in the feedback of HW 1, try to write your argument in **complete sentences** instead of phrases.

(6) **Misuse of Arrows.** Many of you attempted to connect the phrases or equations by "$\rightarrow$", "$\Rightarrow$". However, we have encountered many occasions in which these arrows were used incorrectly!!! They have meanings in mathematics and please do not use them arbitrarily. To avoid confusion, it would be great to stop using unnecessary arrows and write your sentences in full.

(7) Try not to write something non-standard like "$(-1)^{\text{odd }\#}$", "$\gcd(\det, 26)$" in mathematical expressions.