HW 6 FEEDBACK

(1) **Sec. 13.3, Q. 2 (a)** Most students know they should argue by contradiction for this part. This is a good start. However, a significant number of students only wrote down something like:

'Suppose contrary. Then by the Chinese Remainder Theorem (CRT), we can combine the congruences and thus y is a square $(\mathrm{mod}\, n)$*, which is impossible from the question!'.*

This is not good enough. If you write down the given information carefully, you will see that a bit more explanation is needed to arrive at the desired conclusion.

More precisely, the question only tells you (0.1) in the suggested answer below. Applying CRT to (0.1) does not guarantee y is square $(\mathrm{mod}\, n)$. Instead, the proper way is to apply CRT to (0.2).

In any case, having only the keywords (in this case, 'CRT') in your answer is not good enough. You are expected to give sufficient and valid explanation.

For this part, one of the possible answers is the following:

Proof. Suppose contrary, y are both squares $(\mathrm{mod}\, p)$ and $(\mathrm{mod}\, q)$. There exists $s_1 \in \mathbb{Z}_p, s_2 \in \mathbb{Z}_q$ such that

$$\begin{cases} s_1^2 \equiv y \ (\mathrm{mod}\, p) \\ s_2^2 \equiv y \ (\mathrm{mod}\, q). \end{cases} \tag{0.1}$$

By the Chinese Remainder Theorem, there exists $s_0 \in \mathbb{Z}_n$ such that

$$\begin{cases} s_0 \equiv s_1 \ (\mathrm{mod}\, p) \\ s_0 \equiv s_2 \ (\mathrm{mod}\, q). \end{cases} \tag{0.2}$$

Therefore, we have

$$s_0^2 \equiv s_1^2 \equiv y \ (\mathrm{mod}\, p)$$

and

$$s_0^2 \equiv s_2^2 \equiv y \ (\mathrm{mod}\, q).$$

Apply once again the Chinese Remainder Theorem to the last two congruences, it follows that $s_0^2 \equiv y \ (\mathrm{mod}\, n)$. In other words, y is a square $(\mathrm{mod}\, n)$, which is a contradiction! The result follows. □

(2) **Sec. 13.3 Q.2 (d)** Once again, many students only wrote down the answer *'Bob can compute* $\gcd(n, b^2 - y)$ *to obtain* p*'* without explaining why this is the case. In fact, this is just the quadratic sieve that has been covered in class. Explain the reasoning behind just takes a few sentences!

Date: October 26, 2018.

(3) **Sec. 13.3 Q.2 (d)** Some students attempted to explain the reasoning behind by saying that *'Since* $p \mid (b^2 - y)$*, we have* $\gcd(b^2 - y, n) = p$*.'* This is clearly false. Recall that $n = pq$, where p, q are distinct primes. If $q \mid (b^2 - y)$, then you do not have $\gcd(b^2 - y, n) = p$! You should argue why such case is impossible. Indeed, if this is the case, you have $n \mid (b^2 - y)$, i.e., y is a square $(\mathrm{mod}\, n)$ and this is not possible by the question.

(4) **Sec. 13.3 Q.3 (b)**. Some students thought if we have $p^2 \mid (x + y)(x - y)$, then it follows immediately that $p^2 \mid (x + y)$ or $p^2 \mid (x - y)$. In general, this is not correct. In order to have the desired conclusion of this question, you have to take into account the given fact that $x, y \not\equiv 0 \ (\mathrm{mod}\, p)$ and use this to argue why $p \mid (x + y)$ and $p \mid (x - y)$ cannot simultaneously hold.

It is important to keep in mind that the statement *'if* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*'* only holds when p is a prime. In this question, we have square of a prime instead!