Math 312, Comments on practice problems for in-class exam

1. Find all solutions to the congruence $6x + 4 \equiv 2 \pmod{40}$.

This is the same as the congruence $6x \equiv -2 \pmod{40}$. It has a solution since the gcd of 6 and 40 is 2, which divides 38. In fact, by Theorem 3.10 it has precisely two solutions. The Euclidean algorithm gives

\[
40 = 6 \cdot 6 + 4 \\
6 = 4 \cdot 1 + 2 \\
4 = 2 \cdot 2 + 0
\]

Thus $2 = 6 \cdot 1 + 4 \cdot (-1) = 6 \cdot 1 + (40 \cdot (1) + 6 \cdot (-6))(-1) = 7 \cdot 6 - 40 \cdot 1$. So $x = 7$ is a solution to $6x \equiv 2 \pmod{40}$, and hence $x = -7$ (or $x = 33$) is a solution to $6x \equiv -2 \pmod{40}$.

To find the other solution, we need to come up with $x_0$ and $y_0$ such that $6x_0 + 40y_0 = 0$.

Taking $x_0 = -20$ and $y_0 = 3$ works, and thus $x = 33 + x_0 = 13$ gives another solution to $6x \equiv -2 \pmod{40}$.

2. Let $a$ and $b$ be integers and $d = \gcd(a, b)$. What are the possible values of $\gcd(a + b, a - b)$? Give your answer in terms of $d$, and prove that it is correct. Give an example to show that each possibility is realized.

Let $r = \gcd(a + b, a - b)$. Note that $(a + b) + (a - b) = 2a$, and hence $r \mid 2a$. Moreover, $(a + b) - (a - b) = 2b$, and so also $r \mid 2b$. Hence $r \mid \gcd(2a, 2b)$. Now argue $\gcd(2a, 2b) = 2d$, showing $r \mid 2d$. On the other hand, clearly $d \mid (a + b)$ and $d \mid (a - b)$, and since $r$ is a linear combination of $(a + b)$ and $(a - b)$, we have $d \mid r$. Hence $r = d$ or $r = 2d$. Both of these can happen as evidenced by the examples $a = 5, b = 4$ ($r = d$) and $a = 5, b = 3$ ($r = 2d$).

3. Find a positive integer $n$ such that $10^n \equiv 1 \pmod{363825}$. You may use the fact that $363825 = 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$.

As written, there is no such $n$. The reason is that $10^n x + 363825y$ must always be a multiple of 5, and therefore $10^n \equiv 1 \pmod{363825}$ implies that $5 \mid 1$, which is absurd. The question is more interesting if we replace 363825 by 14553, which is $3^3 \cdot 7^2 \cdot 11$. Note that

\[
\phi(3^3 \cdot 7^2 \cdot 11) = \phi(3^3) \cdot \phi(7^2) \cdot \phi(11) \\
= (3^2 \cdot 2) \cdot (7 \cdot 6) \cdot 10 \\
= 18 \cdot 42 \cdot 10 \\
= 7560
\]

Since $\gcd(14553, 10) = 1$, we may apply Euler’s theorem to get $10^{7560} \equiv 1 \pmod{14553}$.

4. Let $S$ be the set of primes of the form $10k + 3$ or $10k + 7$. Prove that $S$ is infinite: that is, there are infinitely many primes whose last digit is either 3 or 7.
Assume that $S$ is finite, and let $p_1, \ldots, p_n$ be all the primes (except 3) whose last digit is either 3 or 7. Consider

$$N = 10p_1 \cdots p_n + 3$$

Then $N$ is not divisible by 3, for if so then $3 \mid p_1 \cdots p_n$, which implies $3 = p_i$ for some $i$, which is a contradiction. Moreover, $N$ is not divisible by any of the $p_i$, for if so then $p_i \mid 3$, implying that $p_i = 3$, again giving a contradiction. Finally, $N$ is not divisible by 2. Thus all the prime factors of $N$ have last digit either 1 or 9. But the product of two numbers with last digit 1 or 9 again has last digit 1 or 9, as a simple calculation modulo 10 shows. It follows that $N$ has last digit either 1 or 9. But clearly $N$ has last digit 3, and this contradiction finishes the proof.