Key:

Question 1

(a)
$$200 = 3 \cdot 57 + 29$$
$$57 = 1 \cdot 29 + 28$$
$$29 = 1 \cdot 28 + 1 \leftarrow \text{last nonzero.}$$
$$28 = 28 \cdot 1 + 0$$

So $\gcd(200, 57) = 1$.

(b) We find one through the Euclidean Algorithm

$$1 = 29 - 1 \cdot 28$$
$$= 29 - 1 \cdot (57 - 1 \cdot 29) = 2 \cdot 29 - 1 \cdot 57$$
$$= 2 \cdot (200 - 3 \cdot 57) - 1 \cdot 57 = 2 \cdot 200 - 7 \cdot 57$$

So one solution is $(2, -7)$.

All solutions are $(2 + 57k, -7 - 200k)$ for any integer k.

(c) Yes! We can get a solution by multiplying the solution in (b) by 15.

So $(30, -105)$ is a solution.

Question 2

(a) $a \equiv b \bmod m$ means $m \mid (b-a)$. //

(b) $\ldots, -15, -5, 5, 15, 25, \ldots$
alternatively, those integers of the form $5+10k$. //

(c) 3, 7, 11, 19, 23, 31, 39, 43, 47 //

Question 3

(a) We use the solution from #1, b.
So the answer is $x \equiv 2 \pmod{57}$. //

(b) All incongruent solutions are $x \equiv 4, 9, 14 \pmod{15}$.
[One could use the Euclidean algorithm on $6x+15y=3$.
Or you could find 1 (like $x \equiv 4 \bmod 15$) and add $\frac{15}{\gcd(6,15)} = 5$ a few times.] //

(c) There are 5 solutions to $15x \equiv 10 \bmod 80$, as $\gcd(15,80) = 5$ and $5 \mid 80$.

Since $\gcd(15,90) = 15$ and $15 \nmid 90$, there are no solutions to $15x \equiv 10 \bmod 90$. //

Question 4

(a) If p is prime, and $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$. //

(b) We know $2^4 \equiv 1 \mod 5$ from FLT.

So $2^{18} \equiv (2^4)^4 \cdot 2^2 \equiv 1^4 \cdot 2^2 \equiv 4 \mod 5$, and so

$x \equiv 4 \mod 5$. //

[It is possible to just do it, of course].

Question 5

There are many ways to succeed, but all start by noticing this is asking for a solution to $10x = 35y + 28z + 3$, or equivalently $10x - 35y - 28z = 3$, with $x, y, z \geq 0$.

Method #1: $\gcd(10, 35) = 5$ and $4 \cdot 10 - 1 \cdot 35 = 5$.

So we look at $5w - 28z = 3$, which has one solution $(w, z) = (23, 4)$.

So $23 \cdot 5 - 4 \cdot 28 = 3 \implies 23 \cdot (4 \cdot 10 - 1 \cdot 35) - 4 \cdot 28 = 3$

$\implies 92 \cdot 10 - 23 \cdot 35 - 4 \cdot 28 = 3$.

So $(x, y, z) = (92, 23, 4)$ is a solution. //

Method #2: look mod 10.

Then $35y + 28z + 3 \equiv 0 \mod 10$, or rather

$5y + 8z \equiv 7 \mod 10$.

We see that $(y, z) = (1, 4)$ is a solution.

Getting rid of mods, this says

$10x = 35 \cdot 1 + 28 \cdot 4 + 3 = 150$, so

$(x, y, z) = (15, 1, 4)$ is a solution. //

There are many more!

Question 6

(a) As $\gcd(a,b)=1$, there are x,y such that

$$ax+by=1.$$

Then $acx + bcy = c$. As $a \mid a$, and $a \mid bc$, we know $a \mid acx+bcy = c$. So $a \mid c$. //

Note: this is just like the proof of $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

(b) $ac \equiv bc \bmod m \rightsquigarrow m \mid ac-bc = c(a-b)$.

As $\gcd(m,c)=1$, we get $m \mid (a-b)$ by part (a) above. So $a \equiv b \bmod m$. //

Question 7

(a) Given (x,y) with $ax+by=c$, we have $ax-c=-by$, so that $b \mid ax-c$, so that $ax \equiv c \bmod b$.
Conversely, if $ax \equiv c \bmod b$, then $b \mid ax-c$.
So there is some k with $bk = ax-c$, or equivalently $ax + b(-k) = c$. Then $(x,-k)$ is a solution to $ax+by=c$. /

(b) No! for instance, $2 \cdot 2 \equiv 0 \bmod 4$,
but $2 \not\equiv 0 \bmod 4$.

(There are infinitely many possibilities. But the modulus must be composite!)

Question 8

(a) Suppose (x,y,z) satisfy $x^2+y^2=3z^2$, and d is a prime with $d \mid x, y$. As $d \mid x$, $d \mid y$, we know from unique factorization that $d^2 \mid x^2$, $d^2 \mid y^2$ (as one d is contributed by each factor of x or y).

Alternatively, $d \mid x$ means $dk = x$ for some k. Then $d^2k^2 = x^2$, so $d^2 \mid x^2$.

So $d^2 \mid x^2, y^2$. ~~Then~~ Then $d^2 \mid x^2+y^2$, their sum. //

(b) We know $d^2 \mid x^2+y^2 = 3z^2$. So $d^2 \mid$ ~~$3z$~~ $3z^2$.
If $d \mid 3$, then $d=3$. And then $3 \mid z^2 \Longrightarrow 3 \mid z$.
Otherwise, $d^2 \mid 3z^2$ and $d \nmid 3$, so that $d \mid z^2 \Rightarrow d \mid z$.
[Recall, if d is prime, then $d \mid xy \Rightarrow d \mid x$ or $d \mid y$].
So $d \mid z$. If (x,y) have a common factor, then it also divides z. So in any primitive solution, $\gcd(x,y)=1$. //

(c) $x^2+y^2=3z^2 \Longrightarrow 3 \mid x^2+y^2 \Longrightarrow x^2+y^2 \equiv 0 \bmod 3$. //

(d)

y mod 3 \ x mod 3	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

In this table, we have the possibilities for $x^2+y^2 \bmod 3$. Remember, there are only 3 "numbers" mod 3! Notice, the only case where there is 0 is when ~~x~~ $x \equiv y \equiv 0 \bmod 3$. //

(e) If $x \equiv y \equiv 0 \bmod 3$, then $3 \mid x$, $3 \mid y$. By (b), $3 \mid z$ too. So this solution is not primitive. But by (c), any solution has ~~3...~~ $x^2+y^2 \equiv 0 \bmod 3$. So no solution is primitive. // [In fact, there are no solutions

Question 9

(a) if $a \equiv 1 \bmod 4$, $b \equiv 1 \bmod 4$, then $ab \equiv 1 \cdot 1 \equiv 1 \bmod 4$. //

(b) If all primes are of form $4n+1$, then by (a) their product is of the form $4n+1$. But N is of the form $4n+3$. So at least one prime dividing N is of shape $4n+3$. //

(c) If $3 \mid N$, then as $3 \mid 3$, we know $3 \mid N - 3 = 4p_1p_2\cdots p_n$. But 3 is not in the factorization $4p_1p_2\cdots p_n$, so $3 \nmid N$.
If $p_i \mid N$, then as $p_i \mid 4p_1p_2\cdots p_n$, we know $p_i \mid N - 4p_1p_2\cdots p_n = 3$. But clearly $p_i \nmid 3$, as $p_i \neq 3$. So $p_i \nmid N$. //

(d) We found a prime congruent to 3 mod 4 that's not in our supposed list of <u>all</u> primes congruent to 3 mod 4! That's clearly impossible, and we have reached a contradiction. There are infinitely many primes congruent to 3 mod 4. //

Question 10

(a) if $z \neq 0$, then $x^2 - y^2 = z^2 \rightsquigarrow \left(\frac{x}{z}\right)^2 - \left(\frac{y}{z}\right)^2 = 1$.

So $\left(\frac{x}{z}, \frac{y}{z}\right)$ is a rational solution to $X^2 - Y^2 = 1$.

(b) Plugging in $(-1, 0)$ gives $(-1)^2 - 0 = 1$. ✓

(c) $y = m(x+1)$.

(d) Clearly $(-1,0)$ is a point, as we checked this in b,c.

$$Y = m\left(\frac{1+m^2}{1-m^2} + 1\right) = m\left(\frac{1+m^2+1-m^2}{1-m^2}\right) = m\left(\frac{2}{1-m^2}\right).$$

And
$$\left(\frac{1+m^2}{1-m^2}\right)^2 - \left(\frac{2m}{1-m^2}\right)^2 = \frac{1}{(1-m^2)^2}\left[(1+m^2)^2 - (2m)^2\right]$$

$$= \frac{1}{(m^2-1)^2}\left[1 + 2m^2 + m^4 - 4m^2\right]$$

$$= \frac{1}{(1-m^2)^2}\left[1 - 2m^2 + m^4\right] = \frac{(1-m^2)^2}{(1-m^2)^2} = 1.$$

So we explicitly verified that the other point is $\left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2}\right)$

[You could also use poly. long division or the quad. formula].

(e) The solutions are $\left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2}\right)$ for any rational $m \neq \pm 1$

(f). Notice m is rational. So $m = \frac{u}{v}$.

Then $\left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2}\right) = \left(\frac{v^2+u^2}{v^2-u^2}, \frac{2uv}{v^2-u^2}\right)$.

Translating back to $x^2 - y^2 = z^2$, we get

$$(v^2+u^2)^2 - (2uv)^2 = (v^2-u^2)^2.$$

So $\begin{cases} x = v^2+u^2 \\ y = 2uv \\ z = v^2-u^2 \end{cases}$ where u, v are any integers.

[I note that some details about $u = v$ are brushed under the rug, + that's okay.]