(1) For integers a, b, write the definition of "$a \mid b$."

(2) Write the definition of $a \equiv b \pmod{n}$.

(3) Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$.

   (a) When does the equation $ax \equiv b \pmod{n}$ have an integer solution for x?

   (b) When does a have an inverse modulo n?

(4) Suppose that $n \in \mathbb{Z}_{\geq 2}$ and $a \in \mathbb{Z}$. Show that there is $x \in [n-1]$ such that $ax \equiv 0 \pmod{n}$ if and only if $\gcd(a, n) \neq 1$.

(5) What is the last digit of the number 7^{100}?

(6) This exercise will show that there are infinitely many primes of the form $4n + 3$.

   (a) Show that p is a prime then $p = 2$ or $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

   (b) Suppose there are only finitely many primes of the form $4n + 3$ and call them $p_1, \ldots, p_k$. Consider the number $N = 4(p_1 \cdots p_k) - 1$. Arrive at a contradiction.

(7) Show that if n is an odd number and $n = x^2 + y^2$ for integers x, y, then $n \equiv 1 \pmod{4}$.

(8) Let $n \in \mathbb{N}$ with $n \geq 2$. Show that $n \mid (n-1)!$ if and only if n is composite.

(9) Show that there are no $x, y \in \mathbb{Z}$ for which $3x^2 - 5y^2 = 15$.

(10) This exercise will show that there are infinitely many primes of the form $4n + 1$.

   (a) Why does a proof similar to that in Question (6) fail in this case?

   (b) Suppose there are only finitely many primes of the form $4n + 1$ and call them $p_1, \ldots, p_k$. Consider the number $N = 4(p_1 \cdots p_k)^2 + 1$. Arrive at a contradiction. (Remember, we proved that if p is an odd prime and there is $x \in \mathbb{Z}$ with $x^2 \equiv -1 \pmod{p}$, then $p \equiv 1 \pmod{4}$)

(1) $a \mid b$ if and only if there exists $c \in \mathbb{Z}$ with $b = ca$.

(2) $a \equiv b \pmod{n}$ if and only if $n \mid (a - b)$.

(3) (a) $ax \equiv b \pmod{n}$ has a solution for x if and only if $\gcd(a, n) \mid b$.

(b) a has an inverse modulo n if and only if $\gcd(a, n) = 1$.

(4) We proved this in class, so look back on your notes.

(5) We calculate

$$7^{100} \equiv (-1)^{50} \pmod{10} \equiv 1^{25} \pmod{10} \equiv 1 \pmod{10}.$$

Thus, the last digit of 7^{100} is 1.

(6) (a) If $n \equiv 0, 2 \pmod{4}$, then $2 \mid n$, so n is not a prime unless $n = 2$. Thus all primes have $p \equiv 1, 3 \pmod{4}$.

(b) We first note that $2, p_1, \ldots, p_k \nmid N$ as this can only be possible if they were to divide -1, which is not the case. Thus, let $N = q_1 \ldots q_n$ be the prime factorization. As none of the p_i's nor 2 divide N, it must be the case that $q_i \equiv 1 \pmod{4}$ for all i. Thus, $N \equiv 1^n \pmod{4} \equiv 1 \pmod{4}$; a contradiction as we already know that $N \equiv -1 \pmod{4} \not\equiv 1 \pmod{4}$.

(7) We note that $0^2 \equiv 0 \pmod{4}$, $1^2 \equiv 1 \pmod{4}$, $2^2 \equiv 0 \pmod{4}$ and $3^2 \equiv 1 \pmod{4}$. We also know that if n is odd, then $n \equiv 1, 3 \pmod{4}$. However, by checking the above cases, we see that $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$, so if $n = x^2 + y^2$ for n odd, then $n \equiv 1 \pmod{4}$.

(8) It was pointed out that $n = 4$ is a counterexample to this statement. However, one direction is true. Suppose p is a prime and that $p \mid (p-1)!$. As p is prime, by Euclid's lemma, there is some $k \in [p-1]$ such that $p \mid k$; a contradiction. Thus $p \nmid (p-1)!$.

For the other direction, let's show that if $n \geq 5$ is composite, then $n \mid (n-1)!$. Write $n = ab$ where $2 \leq a, b \leq n-1$ and first suppose that $a \neq b$. In this case, $a, b \in [n-1]$, so as $a \neq b$, each of a and b appear when multiplying out $(n-1)!$. Thus, there is some integer $c \in \mathbb{Z}$ with $(n-1)! = cab = cn$, so $n \mid (n-1)!$. On the other hand, suppose $a = b$, and $a, b \neq 2$. From this, we note that $n = ab > 2b$, and as $a = b$, $2b \neq a$ and $2b, a \in [n-1]$. Thus, by similar reasoning as above, a and $2b$ appear when multiplying out $(n-1)!$, so there is some integer $c \in \mathbb{Z}$ for which $(n-1)! = ca(2b) = 2cn$. Thus, $n \mid (n-1)!$.

(9) Suppose that there did exist such x, y, then it must be the case that

$$3x^2 \equiv 0 \pmod{5}, \quad -5y^2 \equiv 0 \pmod{3}.$$

As $3, 5$ are primes, this means that there are $m, n \in \mathbb{Z}$ for which $x = 5m$ and $y = 3n$. Thus, $3(5m)^2 - 5(3n)^2 = 15$, so $5m^2 - 3n^2 = 1$. Taking this equation modulo 3 yields

$$5m^2 \equiv 1 \pmod{3}.$$

As $5 \cdot 2 = 10 \equiv 1 \pmod{3}$, multiplying both sides of this equation by 2 yields $m^2 \equiv 2 \pmod{3}$. However, we have previously shown that this equation has no solution; a contradiction.

(10) This exercise will show that there are infinitely many primes of the form $4n + 1$.

(a) The main issue with a proof similar to that in Question (6) is that multiplying together integers of the form $4n + 3$ can yield an integer of the form $4n + 1$.

(b) We first note that $2, p_1, \ldots, p_k \nmid N$ as this can only be possible if they were to divide 1. Thus, there is some prime p with $p \mid N$. However, $p \neq 2, p_1, \ldots, p_k$, so it must be the case that $p \equiv 3 \pmod{4}$. However, as $p \mid N$, $N \equiv 0 \pmod{p}$. However, this implies that $(2p_1 \cdots p_k)^2 \equiv -1 \pmod{p}$. However, we showed that this can only be the case if $p \equiv 1 \pmod{4}$; a contradiction.