1. Find, read, and try to understand a proof of the Schröder-Bernstein Theorem, which states: Let A and B be sets. If there exists an injective mapping $f : A \to B$ and an injective mapping $g : B \to A$, then there exists a bijective mapping $h : A \to B$. If you look online, it might help to search for "Schroeder-Bernstein." You don't have to turn in anything for this problem.

2. Given a set A, first let $\mathcal{P}_o(A)$ be the power set of A without the empty set — i.e., $\mathcal{P}_o(A)$ is the set of all nonempty subsets of A. A mapping $\kappa : \mathcal{P}_o(A) \to A$ is called a *choice function* if $\kappa(S) \in S$ for all $S \in \mathcal{P}_o(A)$. In other words, a choice function "picks out" an element of every nonempty subset of A. Show that a choice function cannot be an injective mapping if A has at least two elements. (Please don't do this by referring to the relative cardinalities of the sets — it's easier than that. What's more interesting is the question: does a choice function exist for every set A? The *Axiom of Choice* states that the answer is yes, but its truth is not accepted universally.)

3. Let A, B, and C be sets and let $f : A \to B$ and $g : B \to C$ be mappings. Let $h : A \to C$ be the composition mapping defined by

$$h(a) = g(f(a)) \text{ for every } a \in A .$$

(a) Show that if both f and g are injective, then so is h.
(b) Show that if both f and g are surjective, then so is h. Conclude that if f and g are both bijective, then so is h.
(c) Make up an example where neither f nor g is bijective, but h is bijective.

4. For this problem, you may assume the following fact, whose proof appears in Chapter 2 of the monograph: every nonzero $a \in \mathbb{N}$ has a unique factorization

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

as the product of powers of prime numbers (the p_j are prime).

(a) Show that

$$(n_1, n_2) \mapsto 3^{n_1} 7^{n_2}$$

is an injective mapping from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{N}$. It's also easy to construct an injective mapping from $\mathbb{N}$ into $\mathbb{N} \times \mathbb{N}$ (please do so). Conclude from the Schröder-Bernstein Theorem that $\mathbb{N} \times \mathbb{N}$ is countably infinite.

(b) Let

$$\mathbb{N}^k = \mathbb{N} \times \mathbb{N} \times \cdots \mathbb{N} \;\; k \text{ times} .$$

Show that $\mathbb{N}^k$ is countably infinite.

5. Recall from class and the monograph that when $a \geq 1$ is an integer,

$$\mathbb{Z}_a = \{0, 1, 2, \ldots, a-1\}$$

and

$$\mathbb{Z}_a^* = \{k \in \mathbb{Z}_a : \gcd(k, a) = 1\} ;$$

that is, $\mathbb{Z}_a^*$ is the set of all integers in $\mathbb{Z}_a$ coprime with a. In class, I showed that if $k \in \mathbb{Z}_a^*$ there exists $l \in \mathbb{Z}_a$ such that

$$\langle\!\langle kl \rangle\!\rangle_a = k \overline{\times} l = 1 .$$

(Alternatively, $kl \equiv 1 \mod a$.) In other words, if $k \in \mathbb{Z}_a^*$, then k has a "multiplicative inverse" with respect to the operation $\overline{\times}$ on $\mathbb{Z}_a$. Show that the converse is true. In other words, show that if $k \in \mathbb{Z}_a$ has a multiplicative inverse with respect to $\overline{\times}$, then $k \in \mathbb{Z}_a^*$. (Suggestion: if $k \notin \mathbb{Z}_a^*$, then $k = mn$ and $a = mq$ for some m, n, and q in $\mathbb{Z}_a$. Why? Thus $\langle\!\langle kq \rangle\!\rangle_a = 0$. Again, why? If k had a multiplicative inverse l, that would require $\langle\!\langle q \rangle\!\rangle_a = 0$. Again, why? Thus $q = 0$ because $q \in \mathbb{Z}_a$ — but that's impossible because $0 < a = mq$.)

6. Recall the definition of the binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!} \;,$$

where $n \in \mathbb{N}$ and $0 \le k \le n$. Note: it always sort of surprised me that it comes out to be an integer — not obvious. In this problem, you'll prove by induction that when p is prime, p is a divisor of $\binom{p}{k}$ when $1 \le k \le p-1$.

(a) p is a divisor of $\binom{p}{1}$. Why?

(b) Suppose you've shown that p is a divisor of $\binom{p}{m}$ for all m satisfying $1 \le m \le k$, where $1 \le k < p-1$. Note that

$$\binom{p}{k} = \binom{p}{k+1}\frac{k+1}{p-k} \;,$$

so

$$(k+1)\binom{p}{k+1} = (p-k)\binom{p}{k} \;.$$

Why does it follow that p is a divisor of $\binom{p}{k+1}$? (Suggestion: by induction assumption, p is a divisor of the right-hand side.)

(c) Conclude by induction that p is a divisor of $\binom{p}{k}$ for all k satisfying $1 \le k \le p-1$.

7. In class, we talked about Euler's Theorem, which states that $k^{\phi(a)} \equiv 1 \mod a$ whenever $k \in \mathbb{Z}_a^*$, where $\phi(a)$ is the number of elements in $\mathbb{Z}_a^*$. In this problem, I'll try to step you through a proof of a special case of Euler's Theorem. It's called Fermat's Little Theorem, and it asserts that if $p \in \mathbb{N}$ is prime, then $k^{p-1} \equiv 1 \mod p$ whenever $1 \le k \le p-1$.

(a) First of all, why is Fermat's Little Theorem just a special case of Euler's Theorem? Think about what $k \in \mathbb{Z}_p^*$ means. Also, what's $\phi(p)$?

(b) Given p, $k^{p-1} \equiv 1 \mod p$ clearly holds for $k = 1$. Now suppose that $m < p-1$ and we've shown that $k^{p-1} \equiv 1 \mod p$ for all k such that $1 \le k \le m-1$. Let's show that $m^{p-1} \equiv 1 \mod p$. First note that

$$\begin{aligned} m^p &= (1+m-1)^p \\ &= 1 + \binom{p}{1}(m-1) + \binom{p}{2}(m-1)^2 + \cdots + \binom{p}{p-1}(m-1)^{p-1} + (m-1)^p \end{aligned}$$

by binomial expansion. In the previous problem you showed that p is a divisor of $\binom{p}{k}$ when $1 \le k \le p-1$. Conclude (and explain why) that

$$m^p \equiv 1 + (m-1)^p \mod p$$

and therefore, by induction assumption, that

$$m^p \equiv m \mod p \;.$$

It follows that $m\left(m^{p-1}-1\right) \equiv 0 \mod p$ and therefore that $m^{p-1} \equiv 1 \mod p$. Why? (Recall that since $m \in \mathbb{Z}_p^*$, you can find $l \in \mathbb{Z}_p^*$ such that $lm \equiv 1 \mod p$.) At this point, you've completed an inductive proof of Fermat's Little Theorem.

8. It turns out that the following extension of Fermat's Little Theorem holds: if $k \in \mathbb{N}$ is positive and p is prime, then $\langle\!\langle k^{p-1} \rangle\!\rangle_p = 1$ unless k is a multiple of p.

(a) Prove it (it's easy).

(b) Euler's Theorem extends similarly. Given a natural number $a > 1$, under what conditions on the positive integer k is it true that $\langle\!\langle k^{\phi(a)} \rangle\!\rangle_a = 1$? Remember, $k \geq a$ is possible here — i.e. we're not assuming that $k \in \mathbb{Z}_a$.

9. The Hellman-Diffie-Merkle key-establishment scheme works because an eavesdropper has a hard time figuring out e from $\langle\!\langle b^e \rangle\!\rangle_p$ even if the large prime p and the base $b \in \mathbb{Z}_p^*$ are public knowledge. To find e, the eavesdropper has to solve the following *discrete logarithm problem*: find the "mod p logarithm" to the base b of the number $\langle\!\langle b^e \rangle\!\rangle_p$. The discrete logarithm problem turns out to be computationally taxing. Nobody knows a good way to solve it except by trying, one by one, the numbers in $\mathbb{Z}_p$ until you hit upon e. The worst-case size of that computation grows linearly in p and hence exponentially in the number of digits or bits required to specify p.

It turns out, moreover, that discrete logarithms aren't even uniquely determined. I.e., given a prime p and base $b \in \mathbb{Z}_p^*$, more than one $e \in \mathbb{Z}_p^*$ might solve $\langle\!\langle b^e \rangle\!\rangle_p = m$, where $m \in \mathbb{Z}_p^*$. For $p = 7$ and $m = 4$, find one value of $b \in \mathbb{Z}_p^*$ for which only one solution $e \in \mathbb{Z}_p^*$ to $\langle\!\langle b^e \rangle\!\rangle_p = 4$ exists and one value of $b \in \mathbb{Z}_p^*$ for which two solutions $e \in \mathbb{Z}_p^*$ to $\langle\!\langle b^e \rangle\!\rangle_p = 4$ exist.

10. I've been telling you that modern encryption schemes work because eavesdroppers (and everybody else) have a hard time finding things like prime factorizations and discrete logarithms. Meanwhile, the encryptors have to compute huge powers of huge numbers mod huge primes p. With some justification, you might ask whether that's any easier. Turns out it is.

One popular technique for computing powers mod p is the *method of repeated squares.* Consider, for example, finding $7^9 \mod 13$. First you expand the exponent 9 in binary — 9 in binary is 1001. So

$$\langle\!\langle 7^9 \rangle\!\rangle_{13} = \langle\!\langle 7 \rangle\!\rangle_{13} \times \langle\!\langle 7^8 \rangle\!\rangle_{13} = 7\ \langle\!\langle 7^8 \rangle\!\rangle_{13} .$$

Now, $\langle\!\langle 7^2 \rangle\!\rangle_{13} = \langle\!\langle 49 \rangle\!\rangle_{13} = 10$, so $\langle\!\langle 7^4 \rangle\!\rangle_{13} = \langle\!\langle 10^2 \rangle\!\rangle_{13} = 9$, and $\langle\!\langle 7^8 \rangle\!\rangle_{13} = \langle\!\langle 9^2 \rangle\!\rangle_{13} = 3$. Finally,

$$\langle\!\langle 7^9 \rangle\!\rangle_{13} = \langle\!\langle 7 \times \langle\!\langle 7^8 \rangle\!\rangle_{13} \rangle\!\rangle_{13} = \langle\!\langle 7 \times 3 \rangle\!\rangle_{13} = 8 .$$

See how that went?

(a) Find $11^{100} \mod 101$. (This one is easy — Euler and Fermat could do it in a flash. BTW 11, 100, and 101 are in decimal here.)

(b) Find $11^{99} \mod 101$ using the method of repeated squares. Check your answer by multiplying it by 11, modding out by 101, and equating with the answer to (a).