Comments on homework from graders.

1. It should not look like rough work.
   You should use complete sentences. Pages should be stapled. It should be neat.
   You should treat this the same way as an essay in an humanities class or a lab report in a science class.

Example: Question 2 asked you to prove that if $p$ is a prime number, then $\sqrt{p}$ is irrational.

Correct way to start the proof:
Assume for a contradiction that $\sqrt{p}$ is rational.
So, $\exists a, b \in \mathbb{Z}$, $b \neq 0$, such that $\sqrt{p} = \frac{a}{b}$, and we can assume that $a$ and $b$ have no common factors.
Then $\sqrt{p} = \frac{a}{b} \Rightarrow p = \frac{a^2}{b^2} \Rightarrow pb^2 = a^2 \Rightarrow p|a^2$.

Incorrect way to start the proof:
$\sqrt{p} = \frac{a}{b}$ (circled)
$p = \frac{a^2}{b^2} \Rightarrow pb^2 = a^2 \Rightarrow p|a^2$.

What are $a$, $b$? Where did they come from?
What are you doing?

2. Some trouble with negation. Especially with the phrasing around the math.
Tip: Try saying your answer out loud to see if it sounds right.

Example: Let's negate the Cauchy definition:

An infinite sequence of real numbers \((x_n) = (x_1, x_2, \ldots)\)

is Cauchy if \(\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ such that } \forall m, n \geq N, \quad |x_m - x_n| < \varepsilon\).

The negation is:

An infinite sequence of real numbers \((x_n) = (x_1, x_2, \ldots)\)

is not Cauchy if \(\exists \varepsilon > 0 \text{ such that } \forall N \in \mathbb{N}, \exists m, n \geq N \text{ such that } |x_m - x_n| \geq \varepsilon\).

Incorrect:

An infinite sequence of real numbers \((x_n) = (x_1, x_2, \ldots)\)

is not Cauchy if \(\exists \varepsilon > 0, \forall N \in \mathbb{N} \text{ such that } \exists m, n \geq N \text{ such that } |x_m - x_n| \geq \varepsilon\).

"such that" means "satisfying the following"

So "\(\forall N \in \mathbb{N} \text{ such that } \)" means you're only considering the \(N \in \mathbb{N}\) satisfying some following property, which may not be all \(N\).

3. Be careful using things we haven't proved in class or in the lecture notes. You most likely won't get credit.
Real world application: The RSA cryptosystem

Say you want to send and receive encrypted messages. How do you do it?

You could just have a secret code (private-key cryptosystem). OK for a small group, but impractical at a large scale: imagine if a bank had to create a separate secret code for every online banking customer.

**Public-key cryptosystem.** Then our separate keys to encrypt and decrypt messages:
- the public key, used to encrypt messages, is posted publicly, so anyone can send you an encrypted message.
- the private key, used to decrypt messages, is kept secret.

The RSA cryptosystem is a public-key cryptosystem. There are 3 things that make it work:
1. Modular arithmetic can be computed quickly.
2. Factoring integers is hard!
3. The following theorem:

**Theorem (Fuller)** Let $p$ and $q$ be distinct prime numbers.
Set $n = pq$ and $\phi(n) = (p-1)(q-1)$. Let $e \in \mathbb{Z}$ be such that $\gcd(e, \phi(n)) = 1$. Let $d \in \mathbb{Z}$ be such that $ed \equiv 1 \pmod{\phi(n)}$.

Then, for any $m \in \mathbb{Z}$,

\[ (m^e)^d \equiv m \pmod{n} \]

**To show** that such a $d$ exists, follow from...
RSA

1. Choose random large (~1024 bits) distinct primes numbers $p$ and $q$.
2. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
3. Choose $1 < e < \phi(n)$ such that $\gcd(e, \phi(n)) = 1$. A common choice for $e$ is $2^{16} + 1$.
4. Compute (via the Euclidean Algorithm) $1 < d < \phi(n)$ such that $de \equiv 1 \pmod{\phi(n)}$.

Public key: the pair $e$ and $n$.

Private key: $d$.

A message is first encoded as an integer $1 \leq m \leq n$ (or series of such) in some standard way.

The encrypted message is then $1 \leq s \leq n$ such that

$$ s \equiv m^e \pmod{n} $$

By the above, Theorem, we can decrypt it since

$$ sd \equiv (m^e)^d \equiv m \pmod{n} $$

Security comes from the fact that to find $d$, given $e$ and $n$, we need to compute $\phi(n)$, which means we need to factor $n$. This is very hard!

However, in practice, this algorithm is modified slightly and/or combined with private key security for more security.
Historical note: Named after Rivest, Shamir, and Adleman, who were the first to publicly describe the algorithm in 1977. But it had been discovered earlier, in 1973, by Cocks who worked for British intelligence, and his work wasn’t declassified until 1997.