Key Topics

• $p$ is sufficient for $q$ if $p \Rightarrow q$.
• $p$ is necessary for $q$ if $\neg p \Rightarrow \neg q$ (or, $q \Rightarrow p$).
• $p$ is necessary and sufficient for $q$ if $p \Leftrightarrow q$.

Warmup

**Theorem 0.1 (Primality Test)** If $p$ is a prime number and $p > 2$ then $2^{p-1} \equiv 1 \pmod{p}$.

1. If $2^{128} \equiv 4 \pmod{129}$, what can you conclude? **129 is not prime.**
2. If $2^{560} \equiv 1 \pmod{561}$, what can you conclude? **Nothing.**
3. If $n$ is a number such that $2^{n-1} \equiv 0 \pmod{n}$, what can you conclude? **Either $n \leq 2$ or $n$ is not prime.**
4. How can you tell for certain that a number is prime? **The simplest way is to try dividing $n$ by every prime number less than its square root. There are more efficient tests, but they are beyond the scope of this course.**

**Theorem 0.2 (Raven Theorem)** All ravens are black.

Suppose we want to find a counterexample to the statement “All birds are black.” What information does Theorem 0.2 give us about such a counterexample? **The counterexample must be a bird that is not a raven.**

Let $x$ be a real number, and say we want to ensure that $x^2 + 1 > 5$. Find conditions on $x$ that are...

1. Necessary and sufficient. $|x| > 2$
2. Necessary, but not sufficient. $x \neq 0$
3. Sufficient, but not necessary. $x > 10$
4. Neither necessary nor sufficient. $x > 0$
Hypothesis Testing

Theorem 0.3 (Bezout’s Theorem) If \( \gcd(a, b) = 1 \) then there exist \( x \) and \( y \) such that \( ax + by = 1 \).

Theorem 0.4 (The Prime Property) If \( p \) is prime, then \( p \) has the following property: if \( p | ab \) then \( p | a \) or \( p | b \).

1. Suppose we have two integers \( a \) and \( b \) and want to find \( x \) and \( y \) such that \( ax + by = 1 \). We know that the condition \( \gcd(a, b) = 1 \) is sufficient, but is it necessary?
   Yes: suppose that \( \gcd(a, b) = d > 1 \), then \( ax + by = dnx + dmy = d(nx + my) \), which is divisible by \( d \) and therefore not equal to 1.

2. Suppose we want to find \( x \) and \( y \) such that \( ax + by = 7 \). Is the condition \( \gcd(a, b) = 1 \) necessary? Is it sufficient?
   It is sufficient, since if \( ax + by = 1 \) then \( (7x)a + (7y)b = 7 \). It is not necessary... take \( a = 7, b = 0 \) as a counterexample.

3. Consider the statement “If \( \gcd(a, b) \leq 3 \) then there exist \( x \) and \( y \) such that \( ax + by = 1 \).” What must a counterexample to this statement look like?
   Must have \( \gcd(a, b) = 2 \) or \( 3 \).

4. Is it necessary that \( p \) be prime in order for it to have the prime property?
   No. \( p \) can also be 0 or 1.

5. Prove or find a counterexample: If \( p \) is prime and \( ab \equiv 0 \pmod{p} \) then \( a \equiv 0 \pmod{p} \) or \( b \equiv 0 \pmod{p} \).
   True, since when put in divisibility notation this is the same as the Prime property.

6. Prove or find a counterexample: If \( n \geq 2 \) and \( ab \equiv 0 \pmod{n} \) then \( a \equiv 0 \pmod{n} \) or \( b \equiv 0 \pmod{n} \).
   False. \( n = 6, a = 3, b = 2 \) is a counterexample.