Throughout, \(N\) denotes the set \(\{1, 2, 3, \ldots\}\) of positive integers. The notation \(a \mid b\) is to be read “\(a\) divides \(b\).” By “prime number,” we always mean “positive prime number.”

**Exercise 1**

Prove by induction that for all \(n \in N\), we have \(6 \mid n(n+1)(n+2)\).

*Lazy proof.* This is the \(d = 3\) case of Exercise 2. \(\square\)

*Redundant proof.* The base case \(n = 1\) holds because \(6 = 1 \cdot 2 \cdot 3\). To do the inductive step, suppose that \(6\) divides \(n(n+1)(n+2)\) for some fixed \(n\). We must show that \(6\) divides the expression

\[
(n+1)((n+1)+1)((n+1)+2) = (n+1)(n+2)(n+3)
= n(n+1)(n+2) + 3(n+1)(n+2).
\]

By the inductive hypothesis, it remains to show the claim: \(6 \mid 3(n+1)(n+2)\). Indeed, \(2\) divides \((n+1)(n+2)\) because one of \(n+1, n+2\) must be even, so the claim follows from scaling by \(3\) on both sides. This completes the induction. \(\square\)

**Exercise 2**

Prove by induction that for all \(n, d \in N\), we have \(d! \mid n(n+1) \cdots (n + d - 1)\).

*First Proof.* For all \(N \in N\), let \(P(N)\) denote the following claim: “If \(n + d = N\), then \(d!\) divides \(n(n+1) \cdots (n + d - 1)\).” It suffices to show \(P(N)\) for all \(N\), which we do by induction on \(N\).

The base case \(N = 1\) is vacuously true, as there do not exist \(n, d \geq 1\) such that \(n + d = 1\). To do the inductive step, suppose that \(P(N)\) holds. Consider arbitrary \(n, d \in N\) such that \(n + d = N + 1\). Then \((n - 1) + d = n + (d - 1) = N\), so by the inductive hypothesis,

\[
\begin{align*}
(2) & \quad d! \mid (n-1)((n-1)+1) \cdots ((n-1)+d-1), \\
(3) & \quad (d-1)! \mid n(n+1) \cdots (n+(d-1)-1).
\end{align*}
\]

Above (2) and (3) respectively entail

\[
\begin{align*}
(4) & \quad d! \mid n(n+1) \cdots (n + d - 2)(n-1), \\
(5) & \quad d! \mid n(n+1) \cdots (n + d - 2)d.
\end{align*}
\]

So \(d\) divides \(n(n+1) \cdots (n + d - 2)((n-1) + d)\). Therefore, \(P(N + 1)\) holds, completing our induction. \(\square\)

*Remark 1.* The following proof is very similar to the first proof. I am including it here so that you can see the commonality between them.
Second proof. For \( n, d \in \mathbb{N} \), let \( Q(n, d) \) be the claim that \( d! \mid n(n+1) \cdots (n+d-1) \). Let \( R(d) \) be the claim, “\( Q(n, d) \) holds for all \( n \).” It suffices to show \( R(d) \) for all \( d \), which we do by induction on \( d \).

The base case \( d = 1 \) holds because \( 1! = 1 \) divides \( n \) for all \( n \in \mathbb{N} \). Suppose \( R(d-1) \) holds. To show \( R(d) \), we will show \( Q(n, d) \) for all \( n \), which we do by induction on \( n \). The base case \( n = 1 \) holds because \( d! \) divides \( 1(2) \cdots (1 + d - 1) = d! \). Now, suppose there exists \( n > 1 \) such that \( Q(n-1, d) \) holds, meaning

\[
d! \mid (n-1)((n-1)+1) \cdots ((n-1)+d-1).
\]

Since \( R(d-1) \) also holds, we also know \( Q(n, d-1) \), meaning

\[
(d-1)! \mid n(n+1) \cdots (n+(d-1)-1).
\]

Simplifying (6) and multiplying (7) by \( d \) on both sides, we respectively get

\[
d! \mid (n-1)(n+1) \cdots (n+d-2),
\]

\[
d! \mid dn(n+1) \cdots (n+d-2).
\]

As in the first proof, we deduce \( d! \mid n(n+1) \cdots (n+d-1) \), meaning \( Q(n, d) \) holds. As this completes the induction on \( n \), we know \( R(d) \) holds, which completes the induction on \( d \). \( \square \)

Exercise 3

Prove that for all \( n, d \in \mathbb{N} \), one and only one of \( n, n+1, \ldots, n+d-1 \) is a multiple of \( d \).

Proof by induction. Let \( P(n) \) be the claim: “For all \( d \in \mathbb{N} \), exactly one of \( n, n+1, \ldots, n+d-1 \) is a multiple of \( d \).” We will show \( P(n) \) holds for all \( n \) by inducting on \( n \).

The base case \( n = 1 \) is equivalent to, “For any \( d \in \mathbb{N} \), exactly one of \( 1, \ldots, d \) is a multiple of \( d \),” which is true. Suppose \( P(n) \) holds. We must prove that, for any given \( d \), exactly one of \( n+1, \ldots, n+d \) is a multiple of \( d \). By the inductive hypothesis, one of the following possibilities, but not both, is true:

1. \( n \) is a multiple of \( d \).
2. Exactly one element of \( S = \{n+1, \ldots, n+d-1\} \) is a multiple of \( d \).

In case (1), we deduce that \( n + d \) is a multiple of \( d \) but no element of \( S \) is a multiple of \( d \). In case (2), exactly one element of \( S \) is a multiple of \( d \), but \( n \) is not a multiple of \( d \), which means \( n + d \) cannot be a multiple of \( d \). In both cases, we get our desired result, so \( P(n+1) \) holds and the induction is complete. \( \square \)

Proof without induction. Fix \( n, d \in \mathbb{N} \). Let \( X_d = \{0, \ldots, d-1\} \) and \( Y_{n,d} = \{n, \ldots, n+d-1\} \). Each element \( k \in Y_{n,d} \) has some remainder \( r_k \in X_d \) upon long division by \( d \). It is sufficient to show that the map \( k \mapsto r_k \) is a bijection \( Y_{n,d} \rightarrow X_d \), as this will imply \( 0 \) has exactly one preimage in \( Y_{n,d} \), which will be the desired multiple of \( d \).

An injective map between finite sets of the same cardinality is bijective, so it remains to show injectivity. We want to show that if \( a, b \in Y_{n,d} \) such that \( r_a = r_b \), then \( a = b \). Without loss of generality, take \( a < b \). The division algorithm says we can write \( a = dq_a + r_a \) and \( b = dq_b + r_b \) for some \( q_a, q_b \in \mathbb{N} \). Then \( b - a = d(q_b - q_a) + (r_b - r_a) = d(q_b - q_a) \), whence \( d \) divides \( b - a \). But \( n \leq a, b \leq n + d - 1 \), so \( 0 \leq b - a \leq d - 1 \). Therefore, \( b - a = 0 \), completing the proof. \( \square \)

Exercise 4

Prove by contradiction that there are infinitely many primes of the form \( 4n + 3 \) (where \( n \) is an integer).
Proof. The idea is to modify Euclid’s proof. Let \( \mathcal{P}_3 \) be the set of primes of the form \( 4n + 3 \). Suppose \( \mathcal{P}_3 \) is finite.

Let \( N = 1 + 2 \prod_{p \in \mathcal{P}_3} p \). Reducing modulo 4, we see that a product of odd primes is always congruent to either 1 or 3 (mod 4). In either case, \( N \equiv 1 + 2 \equiv 3 \pmod{4} \). If the only primes in the factorization of \( N \) were congruent to either 1 or 2 (mod 4), then \( N \) would be one of 0, 1, or 2 (mod 4), a contradiction, so \( N \) must be divisible by some prime of the form \( 4n + 3 \). But this implies \( 1 = N - 2 \prod_{p \in \mathcal{P}_3} p \) is also divisible by that prime, a contradiction. \( \square \)

Remark 2. You can check for yourself that if we tweak certain numbers in the above proof, then we get a proof that there are infinitely many primes of the form \( 6n + 5 \).

Remark 3. We probably won’t get to it in this course, but: Dirichlet’s theorem on arithmetic progressions is a much deeper result, asserting that whenever \( a, b \in \mathbb{N} \) are relatively prime, then there are infinitely many primes of the form \( an + b \).