Prove that for all integers \( n \), \( 6 \mid n \iff 2 \mid n \land 3 \mid n \).

(Where the notation \( "k \mid n" \) means "\( k \) divides \( n \), i.e., \( n \mod k = 0 \), for all integers \( n \) and \( k \neq 0 \).)

- **FIRST**, write the statement symbolically, to make its logical structure obvious. As given, the statement is already mostly symbolic (except for the quantifier). But we should expose the logical structure of the predicate "|" by spelling out its meaning:

\[
\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 6k) \iff (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k)
\]

This allows us to work with each sub-statement more easily.

- **SECOND**, write the outline of the proof, based on the statement’s logical structure.

Assume \( n \in \mathbb{Z} \).

Assume \( (\exists k \in \mathbb{Z}, n = 6k) \).

Let \( k_0 \in \mathbb{Z} \) be such that \( n = 6k_0 \).

\[
\ldots
\]

Then, \( (\exists k \in \mathbb{Z}, n = 6k) \Rightarrow (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k) \).

Assume \( (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k) \).

Let \( k_0 \in \mathbb{Z} \) be such that \( n = 2k_0 \), and let \( k_1 \in \mathbb{Z} \) be such that \( n = 3k_1 \).

\[
\ldots
\]

Then, \( (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k) \Rightarrow (\exists k \in \mathbb{Z}, n = 6k) \).

Then, \( (\exists k \in \mathbb{Z}, n = 6k) \iff (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k) \).

Then, \( \forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 6k) \iff (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k) \).

- **THIRD**, do the scratch work (figure out how to fill in the "\ldots" in the proof outline).

  - For the first "\ldots", we have the following

    **givens**: \( n \in \mathbb{Z} \), \( k_0 \in \mathbb{Z} \), \( n = 6k_0 \);

    **goals**: \( (\exists k \in \mathbb{Z}, n = 2k) \), \( (\exists k \in \mathbb{Z}, n = 3k) \).

    This one is simple: \( n = 6k_0 \Rightarrow n = 2(3k_0) = 3(2k_0) \).

  - For the second "\ldots", we have the following

    **givens**: \( n \in \mathbb{Z} \), \( k_0 \in \mathbb{Z} \), \( k_1 \in \mathbb{Z} \), \( n = 2k_0 \), \( n = 3k_1 \);

    **goals**: \( (\exists k \in \mathbb{Z}, n = 6k) \).

    This is the part of the proof that requires the most creativity. One obvious thing to try is to equate both expressions for \( n \): \( 2k_0 = 3k_1 \). It’s not entirely clear what to do next, but think about what this is saying: the integer \( 3k_1 \) is equal to \( 2k_0 \), i.e., the integer \( 3k_1 \) is even, i.e., \( 2 \) is a factor of \( 3k_1 \). Since \( 2 \neq 3 \), \( 2 \) is a factor of \( 3k_1 \) iff \( 2 \) is a factor of \( k_1 \), i.e., \( k_1 = 2k_2 \) for some \( k_2 \in \mathbb{Z} \). But then, \( n = 3k_1 = 3(2k_2) = 6k_2 \).

    Equivalently, we can reach the same conclusion as follows: \( 2k_0 = 3k_1 \iff k_0 = \frac{3}{2}k_1 \). This means that \( \frac{3k_1}{2} \) is equal to an integer \( (k_0) \). The only way this can happen is if \( 3k_1 \) is even, and this can only happen if \( k_1 \) is even. (The rest of the argument is the same.)

- **FOURTH**, write up the entire proof nicely.

Assume \( n \in \mathbb{Z} \).

Assume \( (\exists k \in \mathbb{Z}, n = 6k) \).

Let \( k_0 \in \mathbb{Z} \) be such that \( n = 6k_0 \).

Then, \( n = 2(3k_0) \) so \( \exists k \in \mathbb{Z}, n = 2k \) (pick \( k = 3k_0 \)).

Then, \( n = 3(2k_0) \) so \( \exists k \in \mathbb{Z}, n = 3k \) (pick \( k = 2k_0 \)).

Then, \( (\exists k \in \mathbb{Z}, n = 6k) \Rightarrow (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k) \).
Assume \((\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k)\).
Let \(k_0 \in \mathbb{Z}\) be such that \(n = 2k_0\), and let \(k_1 \in \mathbb{Z}\) be such that \(n = 3k_1\).
Then, \(n = 2k_0 = 3k_1\) so the integer \(3k_1\) is even.
Since \(2 \neq 3\), \(2\) must be a factor of \(k_1\) in order to be a factor of \(3k_1\), i.e., \(\exists k \in \mathbb{Z}, k_1 = 2k\).
Let \(k_2 \in \mathbb{Z}\) be such that \(k_1 = 2k_2\).
Then, \(n = 3k_1 = 3(2k_2) = 6k_2\) so \(\exists k \in \mathbb{Z}, n = 6k\).
Then, \((\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k) \Rightarrow (\exists k \in \mathbb{Z}, n = 6k)\).
Then, \((\exists k \in \mathbb{Z}, n = 6k) \Leftrightarrow (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k)\).

Then, \(\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 6k) \Leftrightarrow (\exists k \in \mathbb{Z}, n = 2k) \land (\exists k \in \mathbb{Z}, n = 3k)\).

---

**Prove or disprove that for all real numbers \(x\), there is a real number \(y\) such that \(xy^2 \neq y - x\).**

- **First**, write the statement symbolically, to make its logical structure obvious.

\[
\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy^2 \neq y - x
\]

- **Second**, investigate the statement to try and figure out whether it is true or false (since this is a “prove or disprove” question).

\[
xy^2 \neq y - x \iff xy^2 + x \neq y \\
\iff x(y^2 + 1) \neq y \\
\iff x \neq \frac{y}{y^2 + 1}
\]

\((y^2 \geq 0 \Rightarrow y^2 + 1 \geq 1)\)

The question is: can we always pick a value for \(y\) to guarantee this inequality, no matter what \(x\) is equal to? This seems likely — after all, we are free to choose \(y\) in any way we like to satisfy the inequality. However, it is not immediately obvious exactly how to choose an appropriate value for \(y\).

At this point, having decided that we suspect the statement to be true, it is worth writing down an outline of the proof before doing more scratch work — this will help to ensure that we do not make mistakes in the logical dependencies between various parts of the statement.

- **Third**, write the outline of the proof, based on the statement’s logical structure.

  Assume \(x \in \mathbb{R}\).

  Let \(y_0 = \ldots \) # an expression dependent on \(x\)

  Then, \(y_0 \in \mathbb{R}\). # this should be obvious

  \(\ldots\)

  Then, \(xy_0^2 \neq y_0 - x\). # we wish to reach this conclusion

  Then, \(\exists y \in \mathbb{R}, xy^2 \neq y - x\).

Then, \(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy^2 \neq y - x\).

- **Fourth**, continue with the scratch work. At this point, we are trying to figure out how to choose \(y_0\).

  - We could try to solve for \(y\) in the equation \(xy^2 = y - x\), using the quadratic formula, then make sure to pick \(y_0\) different from the roots.

    This would work. But I don’t want to start mucking about with the quadratic formula at this point; partly out of laziness, partly because the alternative will be a good way to showcase the use of another proof technique!

    - Instead, let’s try to introduce cases to make the proof of each case very simple. What cases should we consider?
* The one quantity that we have no control over is $x$, so our cases should depend on the value of $x$.
* Are there particular properties of $x$ that are related to what we are trying to prove?
* Nothing obvious comes to mind. So let’s try to think of particular values of $x$ that might make the statement easy to prove.
* Part of the expression is the product $xy^2$. This simplifies to $y^2$ when $x = 1$. But it simplifies even more when $x = 0$...
* When $x = 0$, the expression becomes: “$0 \neq y_0$”. That’s very easy to satisfy: just pick $y_0 = 1$, for example.
* What about when $x \neq 0$? Is there a value of $y_0$ we could choose that would obviously make the inequality true? Again, we can use the fact that we have a product on the left-hand-side: if we pick $y_0 = 0$, then the expression becomes “$0 \neq -x$”, which is true in this case.

Admittedly, there is an element of trial-and-error to the process of choosing cases. We can easily spend a long time trying out many possibilities that do not lead to a simplified proof, before finally finding one that does.

• **Fifth**, write up the entire proof nicely.

Assume $x \in \mathbb{R}$.

Then, either $x = 0$ or $x \neq 0$.

Assume $x = 0$.

Let $y_0 = 1$.

Then, $y_0 \in \mathbb{R}$.

Also, $xy_0^2 = 0(1)^2 = 0 \neq 1 = 1 - 0 = y_0 - x$.

So $\exists y \in \mathbb{R}, xy^2 \neq y - x$.

Assume $x \neq 0$.

Let $y_0 = 0$.

Then, $y_0 \in \mathbb{R}$.

Also, $xy_0^2 = x(0)^2 = 0 \neq -x = y_0 - x$. # since $x \neq 0$ by assumption

So $\exists y \in \mathbb{R}, xy^2 \neq y - x$.

In every case, $\exists y \in \mathbb{R}, xy^2 \neq y - x$.

Then, $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy^2 \neq y - x$.

---

Prove that every integer greater than 2 can be factored into a product of primes.

[Note from François: This proof relies on a fact known as the Principle of Well Ordering, something that is equivalent to induction (as you will learn in CSC 236 H). Why do I include it on this handout? As an example of the sort of proof that is just a little beyond what we expect you to be able to tackle in CSC 165 H.]

• **First**, write the statement symbolically, to make its logical structure obvious. The phrase “can be factored into a product of primes” is an existential statement in disguise, but one where, in addition, there is variability in the number of primes used in the product. We’ll incorporate that into our representation by using ellipsis (...) where appropriate.

$$\forall n \in \mathbb{Z}^+, n \geq 2 \Rightarrow \exists k \in \mathbb{Z}^+, \exists p_1 \in \mathbb{Z}^+, \ldots, \exists p_k \in \mathbb{Z}^+, p_1 \text{ is prime} \land \cdots \land p_k \text{ is prime} \land n = p_1 \cdots p_k$$

Now, this is not immediately obvious from the statement, but a proof by contradiction will work best in this case. So let’s write down the negation of the statement.

$$\exists n \in \mathbb{Z}^+, n \geq 2 \land \forall k \in \mathbb{Z}^+, \forall p_1 \in \mathbb{Z}^+, \ldots, \forall p_k \in \mathbb{Z}^+, p_1 \text{ is prime} \land \cdots \land p_k \text{ is prime} \Rightarrow n \neq p_1 \cdots p_k$$
• **Second**, write the proof. Remember that we’re doing a proof by contradiction. I will write the complete proof all at once, instead of trying to lead you through the thought process of finding the proof—because this is not the kind of proof that we expect you to be able to come up with on your own (not yet, anyway)!

Assume \( \exists n \in \mathbb{Z}^+ , n > 2 \land \forall k \in \mathbb{Z}^+ , \forall p_1 \in \mathbb{Z}^+ , \ldots , \forall p_k \in \mathbb{Z}^+ , p_1 \) is prime \( \land \cdots \land p_k \) is prime \( \Rightarrow n \neq p_1 \cdots p_k \).

Let \( n_0 \) be a smallest counter-example:

- \( n_0 > 2 \land \forall k \in \mathbb{Z}^+ , \forall p_1 \in \mathbb{Z}^+ , \ldots , \forall p_k \in \mathbb{Z}^+ , p_1 \) is prime \( \land \cdots \land p_k \) is prime \( \Rightarrow n_0 \neq p_1 \cdots p_k \),
- but every integer smaller than \( n_0 \) can be factored into a product of primes, *i.e.,*

\[
\forall n \in \mathbb{Z}^+ , 2 < n < n_0 \Rightarrow \exists k \in \mathbb{Z}^+ , \exists p_1 \in \mathbb{Z}^+ , \ldots , \exists p_k \in \mathbb{Z}^+ , p_1 \text{ is prime } \land \cdots \land p_k \text{ is prime } \land n = p_1 \cdots p_k \quad (1)
\]

(such a value of \( n_0 \) exists by the Principle of Well Ordering).

Then, either \( n_0 \) is prime, or \( n_0 \) is not prime.

Assume \( n_0 \) is prime.

Then \( n_0 \) is its own prime factorization, *i.e.*, \( \exists k \in \mathbb{Z}^+ , \exists p_1 \in \mathbb{Z}^+ , \ldots , \exists p_k \in \mathbb{Z}^+ , p_1 \) is prime \( \land \cdots \land p_k \) is prime \( \land n_0 = p_1 \cdots p_k \) (pick \( k = 1 \) and \( p_1 = n_0 \)), a contradiction.

Assume \( n_0 \) is not prime.

Then by definition, there are integers \( a, b \in \mathbb{Z}^+ \) such that \( 2 \leq a, b < n_0 \) and \( n_0 = ab \).

Then by statement (1) above, we know

- \( \exists k_1 \in \mathbb{Z}^+ , \exists p_1 \in \mathbb{Z}^+ , \ldots , \exists p_{k_1} \in \mathbb{Z}^+ , p_1 \) is prime \( \land \cdots \land p_{k_1} \) is prime \( \land a = p_1 \cdots p_{k_1} \),
- \( \exists k_2 \in \mathbb{Z}^+ , \exists p_1' \in \mathbb{Z}^+ , \ldots , \exists p_{k_2} ' \in \mathbb{Z}^+ , p_1 ' \) is prime \( \land \cdots \land p_{k_2}' \) is prime \( \land b = p_1' \cdots p_{k_2}' \).

Then \( \exists k \in \mathbb{Z}^+ , \exists p_1 \in \mathbb{Z}^+ , \ldots , \exists p_k \in \mathbb{Z}^+ , p_1 \) is prime \( \land \cdots \land p_k \) is prime \( \land n_0 = p_1 \cdots p_k \) (pick \( k = k_1 + k_2 \) and \( p_1 , \ldots , p_{k_1} , p_{k_1} + 1 , \ldots , p_{k_1} + k_2 = p_1 , \ldots , p_{k_1} , p_1 ' , \ldots , p_1 ' , p_2 ' , \ldots , p_k ' \)), a contradiction.

In either case, we get a contradiction.

Hence, \( \forall n \in \mathbb{Z}^+ , n \geq 2 \Rightarrow \exists k \in \mathbb{Z}^+ , \exists p_1 \in \mathbb{Z}^+ , \ldots , \exists p_k \in \mathbb{Z}^+ , p_1 \) is prime \( \land \cdots \land p_k \) is prime \( \land n = p_1 \cdots p_k \).

• If you found this proof hard to read, here is a version where the notion of “factoring into a product of primes” is stated in English (instead of symbolically).

Assume \( \exists n \in \mathbb{Z}^+ , n \geq 2 \land n \) cannot be factored into a product of primes.

Let \( n_0 \) be a smallest counter-example:

- \( n_0 \geq 2 \land n_0 \) cannot be factored into a product of primes,
- but every integer smaller than \( n_0 \) can be factored into a product of primes

(such a value of \( n_0 \) exists by the Principle of Well Ordering).

Then, either \( n_0 \) is prime, or \( n_0 \) is not prime.

Assume \( n_0 \) is prime.

Then \( n_0 \) is its own prime factorization, a contradiction.

Assume \( n_0 \) is not prime.

Then by definition, there are integers \( a, b \in \mathbb{Z}^+ \) such that \( 2 \leq a, b < n_0 \) and \( n_0 = ab \).

Then by statement (1) above, we know

- \( a \) can be factored into a product of primes,
- \( b \) can be factored into a product of primes.

Then, the product of all the prime factors of \( a \) together with all the prime factors of \( b \) is a prime factorization of \( n_0 \), a contradiction.

In either case, we get a contradiction.

Hence, \( \forall n \in \mathbb{Z}^+ , n \geq 2 \Rightarrow n \) can be factored into a product of primes.