

Formalizing and Autoformalizing Euclid's Lemma in $\mathbb{N}$ aproche

BY PETER KOEPKE

Mathematical Institute and Hausdorff Center for Mathematics, University of Bonn

Workshop on Natural Formal Mathematics (NatFoM)

Brasilia, Brazil, 6 October 2025



Overview

Euclid's Lemma: $p \mid a b \rightarrow p \mid a$ **or** $p \mid b$

Wikipedia proof

Some principles of the $\mathbb{N}$ aproche natural proof assistant

Hand-coded $\mathbb{N}$ aproche formalization of the Wikipedia proof

$\mathbb{N}$ aproche formalization generated by ChatGPT conversation

Euclid's Lemma

Wikipedia:

Euclid's lemma—If a prime p divides the product ab of two integers a and b , then p must divide at least one of those integers a or b .

Naproche, hand-coded:

Theorem. (title = Euclids Lemma) *Let p be a prime number and $p \mid m * n$. Then $p \mid m$ or $p \mid n$.*

Naproche, using ChatGPT:

Lemma. (Euclid's lemma) *If p is prime and p divides $(a * b)$ then p divides a or p divides b .*

Generalized Euclid's Lemma

Wikipedia:

*if n divides ab and is *coprime* with a then it divides b .*

Naproche, hand-coded:

Theorem. (title = Euclids Lemma) *For all nonzero natural numbers n, a, b if $n \mid a * b$ and n and a are coprime then n divides b .*

Naproche, using ChatGPT:

Lemma. (Euclid's lemma) *For all a, b, n if n divides $(a * b)$ and a and n are coprime then n divides b .*

A Hand-coded Naproche formalization of the Wikipedia proof

Suppose that $n \mid ab$ and that n and a are coprime (that is, their greatest common divisor is 1). One has to prove that n divides b . Since $n \mid ab$, there exists an integer q such that

$$nq = ab.$$

Without loss of generality, one can suppose that n, q, a , and b are positive, since the divisibility relation is independent of the signs of the involved integers.

To prove the theorem by strong induction, we suppose that it has been proved for all smaller values of ab . There are three cases:

1. If $n = a$, coprimality implies $n = 1$, and n divides b trivially.
2. If $n < a$, then subtracting nb from both sides gives

$$n(q - b) = (a - n)b.$$

Thus, n divides $(a - n)b$. Since we assumed that n and a are coprime, it follows that $a - n$ and n must be coprime. (If not, their greatest common divisor d would divide their sum a as well as n , contradicting our assumption.)

The conclusion therefore follows by induction hypothesis, since $0 < (a - n)b < ab$.

3. If $n > a$ then subtracting aq from both sides gives

$$(n - a)q = a(b - q).$$

Thus, $n - a$ divides $a(b - q)$. Since (as in the previous case), $n - a$ and a are coprime, and since $0 < b - q < b$, then the induction hypothesis implies that $n - a$ divides $b - q$; that is, $b - q = r(n - a)$ for some integer r . So, $(n - a)q = ar(n - a)$, and, by dividing by $n - a$, one has $q = ar$. Therefore, $ab = nq = anr$, and by dividing by a , one gets $b = nr$, the desired conclusion.

Lemma. For all nonzero natural numbers n, a, b if $n \mid a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n \mid a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n \mid b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$$n - a \neq 0 \text{ and } q = a * r.$$

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b . □

Variables have to be declared (“typed”) before use

Lemma. For all *nonzero natural numbers* n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be *nonzero natural numbers* such that $n|a * b$ and n and a are coprime. Take a *natural number* q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a *natural number* r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b .

□

Inductive variables need to be explicitly quantified and introduced in the proof:

Lemma. *For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .*

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b . □

Hypotheses have to be explicitly assumed in the proof

Lemma. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime+. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b .

□

Take ... such that constructs introduce existential witnesses

Lemma. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime.
Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$.
Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b . □

Case constructs: Case ... [the current thesis holds]. qed

Lemma. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b .



After case constructs, the complement of the case assumptions is assumed

Lemma. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b . □

Natural language connectives

Lemma. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$$n - a \neq 0 \text{ and } q = a * r.$$

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b .

□

Natural language filler words

Lemma. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. **Then** $n = 1$ and $n|b$. qed.

Case $a > n$. **Then** $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b .

□

Strong induction along $<$

Lemma. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b .

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n|a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$n - a \neq 0$ and $q = a * r$.

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b . □

Hand-coded proof versus proof produced by ChatGPT interaction

Proof. (method = induction on $a * b$) Let n, a, b be nonzero natural numbers such that $n \mid a * b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n \mid b$. qed.

Case $a > n$. Then $q \geq b$. Indeed if $q < b$ then $n * q < a * b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a - n) * b$. n and $a - n$ are coprime. $(a - n) * b < a * b$. $(a - n) * b$ is inductively smaller than $a * b$. Thus n divides b . qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n - a$ divides $a * (b - q)$. $n - a$ and a are coprime. $a * (b - q) < a * b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a).$$

$$n - a \neq 0 \text{ and } q = a * r.$$

$$a * (n * r) = n * (a * r) = n * q = a * b.$$

Then $n * r = b$ and n divides b . □

Proof. (by induction on $(a * b)$) Let a, b, n be natural numbers.

Suppose n divides $(a * b)$ and a and n are coprime. Take a natural number q such that $(n * q) = (a * b)$. Suppose $0 < a$ and $0 < b$ and $0 < n$ and $0 < q$.

Case $n = a$. Then a and a are coprime. Hence $a = 1$. Therefore n divides b . End.

Case $n < a$. Take a natural number i such that $a = n + i$. Then $(a * b) = ((n + i) * b) = ((n * b) + (i * b))$. Hence $(n * q) = ((n * b) + (i * b))$.

Not $q < b$.

Proof. Suppose $q < b$. Then $(n * q) < (n * b)$. Hence $(a * b) = (n * q) < (n * b) \leq ((n * b) + (i * b)) = (a * b)$. contradiction. End.

Therefore $b \leq q$. Take a natural number t such that $q = b + t$. Then $(n * q) = (n * (b + t)) = ((n * b) + (n * t))$. Hence $(i * b) = (n * t)$.

$a - n$ and n are coprime.

Proof. Suppose d is a natural number and d divides $(a - n)$ and d divides n . Then d divides $((a - n) + n)$ and $((a - n) + n) = a$. a and n are coprime and $d = 1$. End.

We have $0 < ((a - n) * b)$ and $((a - n) * b) < (a * b)$. n divides b . End.

Case $a < n$. Take a natural number j such that $n = a + j$. Then $(n * q) = ((a + j) * q) = ((a * q) + (j * q))$ and $(a * b) = ((a * q) + (j * q))$.

Not $b < q$.

Proof. Suppose $b < q$. Then $(a * b) < (a * q)$. Hence $(a * b) < (a * q) \leq ((a * q) + (j * q)) = (a * b)$. contradiction. End.

Therefore $q \leq b$. Take a natural number s such that $b = q + s$. Then $(a * (b - q)) = (a * s)$. We have $(n * q) = (a * b)$. $(n * q) = ((a + j) * q)$. Hence $((a + j) * q) = (a * b)$. $(a * b) = (a * (q + s))$. Hence $((a + j) * q) = (a * (q + s))$. We have $((a + j) * q) = ((a * q) + (j * q))$. We have $(a * (q + s)) = ((a * q) + (a * s))$. Hence $((a * q) + (j * q)) = ((a * q) + (a * s))$. Therefore $(j * q) = (a * s)$.

j and a are coprime.

Proof. Suppose d is a natural number and d divides j and d divides a . Then d divides $(j + a)$ and $(j + a) = n$. a and n are coprime and $d = 1$. End.

We have $0 < (j * q)$ and $(j * q) < (a * b)$. j divides s . Take a natural number r such that $s = (r * j)$. Then $(j * q) = (a * s) = (a * (r * j)) = ((a * r) * j)$. Therefore $q = (a * r)$. Hence $(a * b) = (n * q) = (n * (a * r)) = (a * (n * r))$. Thus $b = (n * r)$. Therefore n divides b . End. □

Interacting with ChatGPT

Start from file `01.ftl.tex`

Iterate from $n = 1$

Check file `n.ftl.tex` in $\text{\LaTeX}$ and $\text{\Naproche}$

(Human) feedback/instructions to ChatGPT

ChatGPT produces file `[n+1].ftl.tex`

$n := n + 1$

Repeat (until $n = 107$)

Interacting with ChatGPT

Start from file `01.ftl.tex`

Iterate from $n = 1$

Check file `n.ftl.tex` in $\text{\LaTeX}$ and $\text{\Naproche}$

(Human) feedback/instructions to ChatGPT

ChatGPT produces file `[n+1].ftl.tex`

$n := n + 1$

Repeat (until $n = 107$)

01.ftl.tex:

A Natural Language Formalization of Euclid's Lemma in Naproche

Peter Koepke
University of Bonn

2025

Abstract

Euclid's lemma is a fundamental result and tool in elementary num-

...

Axiom 11. $(m * n) * l = m * (n * l)$.

Axiom 12. $m * 1 = m = 1 * m$.

Axiom 13. $m * 0 = 0 = 0 * m$.

Axiom 14. $m * (n + l) = (m * n) + (m * l)$ and $(n + l) * m = (n * m) + (l * m)$.

Axiom 15. If $l + m = l + n$ or $m + l = n + l$ then $m = n$.

Axiom 16. Assume that l is nonzero. If $l * m = l * n$ or $m * l = n * l$ then $m = n$.

Axiom 17. If $m + n = 0$ then $m = 0$ and $n = 0$.

We name two more natural numbers:

Definition 18. $2 = 1 + 1$.

Definition 19. $3 = 2 + 1$.

Me: The attached file is a correct LaTeX file that also proofchecks in Naproche. Please use it as a template for our further conversation.

ChatGPT: Thanks — I've received your file 01.ftl.tex. Since you said it is already LaTeX-correct *and* passes Naproche proofchecking, we can safely treat it as our working template.

...

Me: Please extend the file by a new subsection on the nonstrict order on the natural numbers. Call the extended file 02.ftl.tex so that I can download it.

ChatGPT: Nachgedacht für 1m 33s

Done! I added a new LaTeX subsection and a fresh forthel block with a conservative, Naproche-friendly development of the **nonstrict order** ($\leq$): its definition ..., and standard lemmas You can download the extended file here:

Download 02.ftl.tex

04.ftl.tex:

Definition 18. $2 = 1 + 1$.

Definition 19. $3 = 2 + 1$.

1.2 Nonstrict Order on the Natural Numbers

Signature 20. Let $_ \leq _$ denote a relation between natural numbers and natural numbers.

Definition 21. For natural numbers m, n , we define $m \leq n$ iff there exists a natural number k such that $n = m + k$.

Lemma 22 (Reflexivity). For every natural number m , we have $m \leq m$.

Proof. Take $k = 0$. Then $m + 0 = m$. Hence $m \leq m$. $\square$

...

Me: The error message of the Naproche parsing reads:

"[Parser] (line 166 of "/home/peter/HOME/C/25/10/NatFoM/Chat/04.ftl.tex") (line 166, column 26): unexpected relation"

This is because the Signature command is wrong and superfluous. The new symbol $\leq$ is introduced by the Definition command as written.

ChatGPT:

Nachgedacht für 5s

You're right — that signature block was both unnecessary and syntactically off for a relation introduced via a definition. I've removed it so the symbol $\leq$ is introduced solely by the definition, matching your style and Naproche's expectations.

Here's the corrected file:

Download 05.ftl.tex

1.2 Nonstrict Order on the Natural Numbers

Definition 20. $m \leq n$ iff there exists k such that $n = m + k$.

Lemma 21 (Reflexivity). $m \leq m$.

Proof. Take $k = 0$. Then $m + 0 = m$. Hence $m \leq m$. □

Lemma 22 (Zero is minimum). $0 \leq n$.

Proof. Take $k = n$. Then $0 + k = n$. Hence $0 \leq n$. □

Lemma 23 (Successor step). If $m \leq n$ then $m \leq n + 1$.

Proof. Assume $m \leq n$. Then there exists k such that $n = m + k$. Take $k' = k + 1$. Then $m + k' = m + (k + 1) = (m + k) + 1 = n + 1$. Hence $m \leq n + 1$. □

Lemma 24 (Transitivity). If $m \leq n$ and $n \leq p$ then $m \leq p$.

Proof. Assume $m \leq n$ and $n \leq p$. Then there exist a, b with $n = m + a$ and $p = n + b$. We prove that there exists c with $p = m + c$ by induction on b .

Base. If $b = 0$ then $p = n + 0 = n$. Take $c = a$. Then $m + c = m + a = n = p$. Hence $m \leq p$.

Step. Assume the statement for b . Suppose $p = n + (b + 1) = (n + b) + 1$. By the inductive hypothesis there exists c with $n + b =$

Me: Please leave away the names of lemmas. The “take” commands in the proofs should be like “take k such that k

ChatGPT: Done — I:

- removed all lemma names in square brackets,
- changed proof steps to the more idiomatic ForTheL style:
“Take k such that $k = ...$.”

Here's the updated file:

Download 06.ftl.tex

28.ftl.tex:

Lemma 33. If $m \leq n$ or $n \leq m$ then $m < n$ or $m = n$ or $n < m$.

Proof. Assume $m \leq n$. Then $m = n$ or $m < n$. Hence $m < n$ or $m = n$ or $n < m$. Assume $n \leq m$. Then $n = m$ or $n < m$. Hence $m < n$ or $m = n$ or $n < m$. Therefore $m < n$ or $m = n$ or $n < m$. $\square$

Lemma 34. If $m < n$ then $m + 1 \leq n$.

Proof. Assume $m < n$. Take i such that $n = m + (i + 1)$. Then $n = (m + 1) + i$. Take k such that $k = i$. Then $n = (m + 1) + k$. Hence $m + 1 \leq n$. $\square$

Lemma 35. $m \leq n$ or $n \leq m$.

Proof. We prove by induction on n .

Base. If $n = 0$ then $0 \leq m$. Hence $m \leq n$ or $n \leq m$.

...

Me: LaTeX works, Naproche works except for the last inductive proof. We will discuss tomorrow how inductive proofs are structured in Naproche. Good night.

ChatGPT: Great — LaTeX and Naproche are both passing except for the last induction proof, which we can refine tomorrow.

Have a good night!<#1F319>

When you're ready, just upload the latest .ftl.tex file again so we can adjust the induction proof structure together.

Me: Good morning, do you still have 28.ft.tex available?

Me: Naproche does induction along a dedicated binary relation $\prec$. To do induction along the $<$ relation along the natural numbers requires to embed $<$ into $\prec$.

ChatGPT:

Nachgedacht für 1m 32s

That matches Naproche's approach. I've added the embedding you need:

1.3 Induction via the well-founded relation $\prec$

Axiom 37. If $m < n$ then $m \prec n$.

Lemma 38. $m \leq n$ or $n \leq m$.

Proof. We prove by induction on n . Base. If $n = 0$ then $0 \leq m$. Hence $m \leq n$ or $n \leq m$. Step. Assume $m \leq n$ or $n \leq m$. If $m \leq n$ then $m \leq n + 1$. Assume $n \leq m$. Then $n = m$ or $n < m$. If $n = m$ then $m \leq n + 1$. Assume $n < m$. Then $n + 1 \leq m$. Hence $m \leq n + 1$ or $n + 1 \leq m$. Therefore $m \leq n$ or $n \leq m$ holds for all n . qed. $\square$

...

ChatGPT:

Nachgedacht für 45s

All set. I moved **all induction-related material** into its own subsection at the end of the document and fixed the nesting issue:

- Removed the misplaced axiom from inside the earlier subsection.
- Cut the induction-based **comparability** lemma from the nonstrict-order subsection.
- Added a new subsection:
Induction via the well-founded relation $\prec$

Me: OK. An inductive proof requires that the inductive variables are explicitly universally quantified in the statement of the lemma.

ChatGPT: Exactly — Naproche requires something like

```
\begin{lemma}
```

```
For all  $m, n$ ,  $m \leq n$  or  $n \leq m$ .
```

```
\end{lemma}
```

38.ftl.tex:

Axiom 35. If $m < n$ then $m \prec n$.

Lemma 36. For all n $m \leq n$ or $n \leq m$.

Proof by induction on n . Let n be a natural number.

Case $n = 0$. Then $0 \leq m$. End.

Then n is nonzero. We have $m \leq n$ or $n \leq m$. If $m \leq n$ then $m \leq n + 1$. If $n \leq m$ then $n = m$ or $n < m$. If $n = m$ then $m \leq n + 1$. If $n < m$ then $n + 1 \leq m$. $\square$

...

Me: Congratulations, accepted by LaTeX and Naproche. We shall continue to improve the induction proof later today.

ChatGPT: Excellent — I'm glad to hear that 38.ftl.tex passes both LaTeX and Naproche!

We can definitely refine the induction proof further later today — for example, making it even more elegant or factoring out a helper lemma about the successor case.

Me: Naproche is able, with the help of an inbuilt automated theorem prover, to prove the inductive lemma on its own with the minimal inductive proof: `\begin{proof}[by induction on $n$] \end{proof}`

ChatGPT:

Nachgedacht für einige wenige Sekunden

Nachgedacht für 4 Sekunden

Nice—let's switch to the ultra-minimal version. I've replaced the last proof by

```
\begin{proof}[by induction on $n$]
\end{proof}
```

Prime Numbers

Let p and d stand for natural numbers.

Definition 49. p is prime iff $p \neq 0$ and $p \neq 1$ and for all d if d divides p then $d = 1$ or $d = p$.

Definition 50. A prime number is a prime natural number.

Lemma 51. If p is prime then $p \neq 0$ and $p \neq 1$.

Proof. By definition of prime $p \neq 0$ and $p \neq 1$. □

Lemma 52. If p is prime then $0 < p$.

Proof. We have $0 \leq p$. Not $p = 0$. Therefore $0 < p$. □

Lemma 53. If p is prime and d divides p and not $d = 1$ then $d = p$.

Proof. Suppose p is prime and d divides p and not $d = 1$. By definition of prime $d = 1$ or $d = p$. Not $d = 1$. Therefore $d = p$. □

Lemma 54. If p is prime then p divides p .

Proof. Take i such that $i = 1$. Then $p = p * i$. Therefore p divides p . □

Me: The file checks alright. All variables are correctly declared in one way or the other. Can we now have a short subsection on prime numbers. Perhaps it is a good idea to predeclare a variable $\$p\$$ for prime numbers and $\$d\$$ for divisors.

ChatGPT: Excellent — glad to hear everything checks now.

Yes, we can add a **short subsection on prime numbers**, ...

Me: Please include Naproche proofs.

ChatGPT:

Nachgedacht für 50s

Added a concise **Prime Numbers** subsection with compact Naproche-friendly proofs, matching your style:

Me: Only keep the two definitions in the subsection on prime numbers. The lemmas will not be needed.

ChatGPT: Got it — we can trim the subsection down to just the two **definitions** (“ $\$p\$$ is prime” and “prime number”).

Let a, b, n stand for natural numbers.

Lemma 60 (Euclid's lemma). If n divides $a * b$ and a and n are coprime then n divides b .

*Proof by strong induction on $a * b$.* Suppose n divides $a * b$ and a and n are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = 0$. Then $a * b = 0$. If $a = 0$ then $b = 0$. Therefore n divides b . End. If not $a = 0$ then $a = 1$ since a and 0 are coprime. Hence $b = 0$. Therefore n divides b . End.

Case $n = a$. Then a and a are coprime. Hence $a = 1$. Therefore n divides b . End.

Case $n < a$. Take a natural number i such that $a = n + i$. Then $a * b = (n + i) * b = n * b + i * b$. Hence $n * q = n * b + i * b$. We have $a \neq 0$ and $n \neq 0$ in this case. Hence $0 < n$. Not $q < b$. Proof. Suppose $q < b$. Then $n * q < n * b$. Hence $a * b = n * q < n * b \leq n * b + i * b = a * b$. contradiction. End. Therefore $b \leq q$. Take a natural number t such that $q = b + t$. Then $n * q = n * (b + t) = n * b + n * t$. Hence $i * b = n * t$. Moreover $a - n$ and n are coprime. Proof. Suppose d divides $a - n$ and d divides n . Then d divides $(a - n) + n = a$. Since a and n are coprime, $d = 1$. End. We have $0 < (a - n) * b$ and $(a - n) * b < a * b$. By induction hypothesis n divides b . End.

Me: Could you translate the following proof from Wikipedia into a Naproche lemma and proof and put it at the end of our file?

Suppose that $n \mid a \cdot b$ and that n and a are coprime (that is, their greatest common divisor is 1). One has to prove that n divides b . Since $n \mid a \cdot b$, there exists an integer q such that $n \cdot q = a \cdot b$. Without loss of generality, one can suppose that n, q, a , and b are positive, since the divisibility relation is independent of the signs of the involved integers. To prove the theorem by strong induction, we suppose that it has been proved for all smaller values of ab . There are three cases: If $n = a$, coprimality implies $n = 1$, and n divides b trivially. If $n < a$, then subtracting $n \cdot b$ from both sides gives $n \cdot (q - b) = (a - n) \cdot b$. Thus, n divides $(a - n) \cdot b$. Since we assumed that n and a are coprime, it follows that $a - n$ and n must be coprime. (If not, their greatest common divisor d would divide their sum a as well as n , contradicting our assumption.) The conclusion therefore follows by induction hypothesis, since $0 < (a - n) \cdot b < ab$

Let a, b, n stand for natural numbers.

Lemma 60 (Euclid's lemma). If n divides $a * b$ and a and n are coprime then n divides b .

*Proof by strong induction on $a * b$.* Suppose n divides $a * b$ and a and n are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = 0$. Then $a * b = 0$. If $a = 0$ then $b = 0$. Therefore n divides b . End. If not $a = 0$ then $a = 1$ since a and 0 are coprime. Hence $b = 0$. Therefore n divides b . End.

Case $n = a$. Then a and a are coprime. Hence $a = 1$. Therefore n divides b . End.

Case $n < a$. Take a natural number i such that $a = n + i$. Then $a * b = (n + i) * b = n * b + i * b$. Hence $n * q = n * b + i * b$. We have $a \neq 0$ and $n \neq 0$ in this case. Hence $0 < n$. Not $q < b$. Proof. Suppose $q < b$. Then $n * q < n * b$. Hence $a * b = n * q < n * b \leq n * b + i * b = a * b$. contradiction. End. Therefore $b \leq q$. Take a natural number t such that $q = b + t$. Then $n * q = n * (b + t) = n * b + n * t$. Hence $i * b = n * t$. Moreover $a - n$ and n are coprime. Proof. Suppose d divides $a - n$ and d divides n . Then d divides $(a - n) + n = a$. Since a and n are coprime, $d = 1$. End. We have $0 < (a - n) * b$ and $(a - n) * b < a * b$. By induction hypothesis n divides b . End.

.....

Me: Not bad, but there are many parser mistakes. Can you first insert sufficiently many brackets to get rid of ambiguity errors. Note that we do not have a priority of $*$$ over $+$$.

ChatGPT:

Nachgedacht für 41s

Nachgedacht für 37s

96.ftl.tex:

d divides $((a-n)+n)$ and $((a-n)+n) = a$. a and n are coprime and $d = 1$. End. We have $0 < ((a-n)*b)$ and $((a-n)*b) < (a*b)$. n divides b . End.

Case $a < n$. Take a natural number j such that $n = a + j$. Then $(n*q) = ((a+j)*q) = ((a*q)+(j*q))$ and $(a*b) = ((a*q)+(j*q))$. Not $b < q$. Proof. Suppose $b < q$. Then $(a*b) < (a*q)$. Hence $(a*b) < (a*q) \leq ((a*q)+(j*q)) = (a*b)$. contradiction. End. Therefore $q \leq b$. Take a natural number s such that $b = q + s$. Then $(a*(b-q)) = (a*s)$. Thus $(j*q) = (a*s)$. j and a are coprime. Proof. Suppose d is a natural number and d divides j and d divides a . Then d divides $(j+a)$ and $(j+a) = n$. a and n are coprime and $d = 1$. End. We have $0 < (j*q)$ and $(j*q) < (a*b)$. j divides s . Take a natural number r such that $s = (r*j)$. Then $(j*q) = (a*s) = (a*(r*j)) = ((a*r)*j)$. Therefore $q = (a*r)$. Hence $(a*b) = (n*q) = (n*(a*r)) = (a*(n*r))$. Thus $b = (n*r)$. Therefore n divides b . End. $\square$

.....

Me: Now Naproche fails at the line Thus “ $(j * q) = (a * s)$.” Could you prove and replace the line by a longer chain of equations so that Naproche could check the single steps?

ChatGPT: ... In the meantime, here is a Naproche-friendly replacement for the line

Thus $(j * q) = (a * s)$.

Drop that line and insert the following small steps instead (all symbols in $\$...\$$, with explicit parentheses):

We have $\$(n * q) = (a * b)\$$.

From $\$n = a + j\$$ we get $\$(n * q) = ((a + j) * q)\$$.

Hence $\$((a + j) * q) = (a * b)\$$.

From $\$b = q + s\$$ we get $\$(a * b) = (a * (q + s))\$$.

Hence $\$((a + j) * q) = (a * (q + s))\$$.

We have $\$((a + j) * q) = ((a * q) + (j * q))\$$.

We have $\$(a * (q + s)) = ((a * q) + (a * s))\$$.

Hence $\$((a * q) + (j * q)) = ((a * q) + (a * s))\$$.

Therefore $\$(j * q) = (a * s)\$$.

d divides $((a-n)+n)$ and $((a-n)+n) = a$. a and n are coprime and $d = 1$. End. We have $0 < ((a-n)*b)$ and $((a-n)*b) < (a*b)$. n divides b . End.

Case $a < n$. Take a natural number j such that $n = a + j$. Then $(n*q) = ((a+j)*q) = ((a*q) + (j*q))$ and $(a*b) = ((a*q) + (j*q))$. Not $b < q$. Proof. Suppose $b < q$. Then $(a*b) < (a*q)$. Hence $(a*b) < (a*q) \leq ((a*q) + (j*q)) = (a*b)$. contradiction. End. Therefore $q \leq b$. Take a natural number s such that $b = q + s$. Then $(a*(b-q)) = (a*s)$. We have $(n*q) = (a*b)$. $(n*q) = ((a+j)*q)$. Hence $((a+j)*q) = (a*b)$. $(a*b) = (a*(q+s))$. Hence $((a+j)*q) = (a*(q+s))$. We have $((a+j)*q) = ((a*q) + (j*q))$. We have $(a*(q+s)) = ((a*q) + (a*s))$. Hence $((a*q) + (j*q)) = ((a*q) + (a*s))$. Therefore $(j*q) = (a*s)$. j and a are coprime. Proof. Suppose d is a natural number and d divides j and d divides a . Then d divides $(j+a)$ and $(j+a) = n$. a and n are coprime and $d = 1$. End. We have $0 < (j*q)$ and $(j*q) < (a*b)$. j divides s . Take a natural number r such that $s = (r*j)$. Then $(j*q) = (a*s) = (a*(r*j)) = ((a*r)*j)$. Therefore $q = (a*r)$.

Me: Excellent!! The file works: a guided AI translation of a modest proof from Wikipedia. Could you now improve the readability and appearance of the document by putting fitting comments outside the forthel environments and by structuring proofs by using paragraphs in a meaningful way.

ChatGPT:

Nachgedacht für 59s

Nice! I've made a readability pass without changing any math content:

- Added a short **informal guide paragraph** (outside any forthel block) right before the final induction proof to orient the reader—what the proof is doing and how the cases are organized.
- Inside the **induction proof**, I introduced **paragraph breaks** (blank lines) at natural places:
 - after the initial assumptions,
 - between the setup and the case split,
 - before each Case ... line,
 - and after each End. that closes a case.

Wikipedia proof versus proof produced by ChatGPT interaction

Suppose that $n \mid ab$ and that n and a are coprime (that is, their greatest common divisor is 1). One has to prove that n divides b . Since $n \mid ab$, there exists an integer q such that

$$nq = ab.$$

Without loss of generality, one can suppose that n, q, a , and b are positive, since the divisibility relation is independent of the signs of the involved integers.

To prove the theorem by strong induction, we suppose that it has been proved for all smaller values of ab . There are three cases:

1. If $n = a$, coprimality implies $n = 1$, and n divides b trivially.
2. If $n < a$, then subtracting nb from both sides gives

$$n(q - b) = (a - n)b.$$

Thus, n divides $(a - n)b$. Since we assumed that n and a are coprime, it follows that $a - n$ and n must be coprime. (If not, their greatest common divisor d would divide their sum a as well as n , contradicting our assumption.)

The conclusion therefore follows by induction hypothesis, since $0 < (a - n)b < ab$.

3. If $n > a$ then subtracting aq from both sides gives

$$(n - a)q = a(b - q).$$

Thus, $n - a$ divides $a(b - q)$. Since (as in the previous case), $n - a$ and a are coprime, and since $0 < b - q < b$, then the induction hypothesis implies that $n - a$ divides $b - q$; that is, $b - q = r(n - a)$ for some integer r . So, $(n - a)q = ar(n - a)$, and, by dividing by $n - a$, one has $q = ar$. Therefore, $ab = nq = anr$, and by dividing by a , one gets $b = nr$, the desired conclusion.

Proof. (by induction on $(a * b)$) Let a, b, n be natural numbers.

Suppose n divides $(a * b)$ and a and n are coprime. Take a natural number q such that $(n * q) = (a * b)$. Suppose $0 < a$ and $0 < b$ and $0 < n$ and $0 < q$.

Case $n = a$. Then a and a are coprime. Hence $a = 1$. Therefore n divides b . End.

Case $n < a$. Take a natural number i such that $a = n + i$. Then $(a * b) = ((n + i) * b) = ((n * b) + (i * b))$. Hence $(n * q) = ((n * b) + (i * b))$.

Not $q < b$.

Proof. Suppose $q < b$. Then $(n * q) < (n * b)$. Hence $(a * b) = (n * q) < (n * b) \leq ((n * b) + (i * b)) = (a * b)$. contradiction. End.

Therefore $b \leq q$. Take a natural number t such that $q = b + t$. Then $(n * q) = (n * (b + t)) = ((n * b) + (n * t))$. Hence $(i * b) = (n * t)$.

$a - n$ and n are coprime.

Proof. Suppose d is a natural number and d divides $(a - n)$ and d divides n . Then d divides $((a - n) + n)$ and $((a - n) + n) = a$. a and n are coprime and $d = 1$. End.

We have $0 < ((a - n) * b)$ and $((a - n) * b) < (a * b)$. n divides b . End.

Case $a < n$. Take a natural number j such that $n = a + j$. Then $(n * q) = ((a + j) * q) = ((a * q) + (j * q))$ and $(a * b) = ((a * q) + (j * q))$.

Not $b < q$.

Proof. Suppose $b < q$. Then $(a * b) < (a * q)$. Hence $(a * b) < (a * q) \leq ((a * q) + (j * q)) = (a * b)$. contradiction. End.

Therefore $q \leq b$. Take a natural number s such that $b = q + s$. Then $(a * (b - q)) = (a * s)$. We have $(n * q) = (a * b)$. $(n * q) = ((a + j) * q)$. Hence $((a + j) * q) = (a * b)$. $(a * b) = (a * (q + s))$. Hence $((a + j) * q) = (a * (q + s))$. We have $((a + j) * q) = ((a * q) + (j * q))$. We have $(a * (q + s)) = ((a * q) + (a * s))$. Hence $((a * q) + (j * q)) = ((a * q) + (a * s))$. Therefore $(j * q) = (a * s)$.

j and a are coprime.

Proof. Suppose d is a natural number and d divides j and d divides a . Then d divides $(j + a)$ and $(j + a) = n$. a and n are coprime and $d = 1$. End.

We have $0 < (j * q)$ and $(j * q) < (a * b)$. j divides s . Take a natural number r such that $s = (r * j)$. Then $(j * q) = (a * s) = (a * (r * j)) = ((a * r) * j)$. Therefore $q = (a * r)$. Hence $(a * b) = (n * q) = (n * (a * r)) = (a * (n * r))$. Thus $b = (n * r)$. Therefore n divides b . End. $\square$

Me:

How would you describe our chat that led from natural numbers to Euclid's lemma.

ChatGPT:

That's a wonderful question — the entire conversation can be described as a **guided formalization journey**.

...

6. Result

By the end, we had a complete Naproche document:

- Mathematically rigorous,
- Fully parsed and checked,
- Written in natural, readable language,
- Progressing from the Peano axioms to Euclid's Lemma.

Me:

How would ~~you~~ I describe our chat that led from natural numbers to Euclid's lemma.

~~ChatGPT~~ Me:

That's a ~~wonderful~~ difficult question — the entire conversation can be described as a ~~guided formalization journey~~.

- An interesting, isolated experiment,
- Talking to a willing pupil with a particular mix of language abilities, mathematical abilities, no real “understanding”, making odd mistakes, ...
- Encouraging and surprising, that the chat converged to a correct document.
- How can the interaction with ChatGPT be structured to achieve general, reliable results?
- How does chatting (fine-tuning?) compare to a few, well-formulated prompts?
- ...

Thank you!