A Calculational Proof for the Fundamental Theorem of Arithmetic

João Paixão and Lucas Rufino

September 20, 2020

1 Bags of Primes

Let R and S be bags of primes and p and q are bags with a single prime.

Lemma 1.1 (Connection between $\vee$ and $\sqcup$)**.** $p \in R \vee p \in S \iff p \in R \sqcup S$

Lemma 1.2. $R \sqcup p \sqsubseteq S \sqcup p \iff R \sqsubseteq S$

Lemma 1.3. $R \sqcup p \sqsubseteq S \iff R \sqcup p \sqsubseteq S \wedge p \in S$

Lemma 1.4. $p \in R \iff R \setminus p \sqcup p = R$

2 Number Theory

Let n and m be natural numbers and p and q are primes.

Lemma 2.1 (Euclid)**.** $p \mid n \vee p \mid m \iff p \mid n \cdot m$

Lemma 2.2. $n \cdot p \mid m \cdot p \iff n \mid m$

Lemma 2.3. $n \cdot p \mid m \iff n \cdot p \mid m \wedge p \mid m$

Lemma 2.4. $p \mid n \iff (n/p) \cdot p = n$

3 Connection

Definition 3.1. $F(R \sqcup p) = F(R) \cdot p$ with $F(\emptyset) = 1$

Is F well-defined?

Lemma 3.1 (F distributes $\sqcup$ over $\cdot$)**.** $F(R \sqcup S) = F(R) \cdot F(S)$

Proof. Induction on S in $\sqsubseteq$
Base case: $S = \emptyset$

$$
\begin{aligned}
& F(R \sqcup \emptyset) \\
\iff & \quad \{ \text{ Union with empty set } \} \\
& F(R)
\end{aligned}
$$

Induction case: $S = S' \sqcup p$

$$
\begin{aligned}
& F(R \sqcup S) \\
\iff & \quad \{ \text{ Definition of } S \ \} \\
& F(R \sqcup S' \sqcup \{p\}) \\
\iff & \quad \{ \text{ Definition 3.1 } \} \\
& F(R \sqcup S') \cdot p \\
\iff & \quad \{ \text{ Induction Step } \} \\
& F(R) \cdot F(S') \cdot p \\
\iff & \quad \{ \text{ Definition 3.1 } \} \\
& F(R) \cdot F(S' \sqcup \{p\}) \\
\iff & \quad \{ \text{ Definition of } S \ \} \\
& F(R) \cdot F(S)
\end{aligned}
$$

□

Lemma 3.2. $p \mid q \iff p \in q$

Lemma 3.3. $p \mid F(R) \iff p \in R$

Proof. Induction on the size of bag R.
Base case: $R = \emptyset$

$$
\begin{aligned}
& p \mid F(R) \\
\iff & \quad \{ \text{ Definition of } R \ \} \\
& p \mid F(\emptyset) \\
\iff & \quad \{ \text{ Definition 3.1 } \} \\
& p \mid 1 \\
\iff & \quad \{ \ p > 1 \ \} \\
& FALSE \\
\iff & \quad \{ \text{ Property of } \emptyset \ \} \\
& p \in \emptyset \\
\iff & \quad \{ \text{ Definition of } R \ \} \\
& p \in R
\end{aligned}
$$

Induction: $q \in R$

$$
\begin{aligned}
& p \mid F(R) \\
\iff & \quad \{ \text{ Lemma 1.4 } \} \\
& p \mid F(R \setminus q \sqcup q) \\
\iff & \quad \{ \text{ Definition 3.1 } \} \\
& p \mid F(R \setminus q) \cdot q \\
\iff & \quad \{ \text{ Lemma 2.1 } \} \\
& p \mid F(R \setminus q) \vee p \mid q \\
\iff & \quad \{ \text{ Lemma 3.2 } \} \\
& p \mid F(R \setminus q) \vee p \in q \\
\iff & \quad \{ \text{ Induction Step } \} \\
& p \in R \setminus q \vee p \in q \\
\iff & \quad \{ \text{ Lemma 1.1 } \} \\
& p \in R \setminus q \sqcup q \\
\iff & \quad \{ \text{ Lemma 1.4 } \} \\
& p \in R
\end{aligned}
$$

□

Theorem 3.4. $F(R) \mid F(S) \iff R \sqsubseteq S$

Proof. • Induction on the size of bag R.

- Base case: $R = \emptyset$

$$
\begin{aligned}
& F(R) \mid F(S) \\
\iff & \quad \{ \text{ Definition of } R \text{ } \} \\
& F(\emptyset) \mid F(S) \\
\iff & \quad \{ \text{ Definition 3.1 } \} \\
& 1 \mid F(S) \\
\iff & \quad \{ \text{ 1 is bottom element of } \mid \text{ } \} \\
& TRUE \\
\iff & \quad \{ \text{ 1 is bottom element of } \sqsubseteq \text{ } \} \\
& \emptyset \sqsubseteq S \\
\iff & \quad \{ \text{ Definition of } R \text{ } \} \\
& R \sqsubseteq S
\end{aligned}
$$

- Induction: $p \in R$

Case 1: $p \notin S$.

$$
\begin{aligned}
& F(R) \mid F(S) \\
\iff & \quad \{ \text{ Lemma 1.4 } \} \\
& F(R \setminus p \sqcup p) \mid F(S) \\
\iff & \quad \{ \text{ Definition 3.1 } \} \\
& F(R \setminus p) \cdot p \mid F(S) \\
\iff & \quad \{ \text{ Lemma 2.3 } \} \\
& F(R \setminus p) \cdot p \mid F(S) \wedge p \mid F(S) \\
\iff & \quad \{ \text{ Lemma 3.3 (Euclid) } \} \\
& F(R \setminus p) \cdot p \mid F(S) \wedge p \in S \\
\iff & \quad \{ \ p \notin S \ \} \\
& FALSE \\
\iff & \quad \{ \ p \notin S \ \} \\
& R \setminus p \sqcup p \sqsubseteq S \wedge p \in S \\
\iff & \quad \{ \text{ Lemma 1.3 } \} \\
& R \setminus p \sqcup p \sqsubseteq S \\
\iff & \quad \{ \text{ Lemma 1.4 } \} \\
& R \sqsubseteq S
\end{aligned}
$$

Case 2: $p \in S$

$$
\begin{aligned}
& F(R) \mid F(S) \\
\iff & \quad \{ \text{ Lemma 1.4 on both } \} \\
& F(R \setminus p \sqcup p) \mid F(S \setminus p \sqcup p) \\
\iff & \quad \{ \text{ Definition 3.1 } \} \\
& F(R \setminus p) \cdot p \mid F(S \setminus p) \cdot p \\
\iff & \quad \{ \text{ Lemma 2.2 } \} \\
& F(R \setminus p) \mid F(S \setminus p) \\
\iff & \quad \{ \text{ Induction Step } \} \\
& R \setminus p \sqsubseteq S \setminus p \\
\iff & \quad \{ \text{ Lemma 1.2 } \} \\
& R \setminus p \sqcup p \sqsubseteq S \setminus p \sqcup p \\
\iff & \quad \{ \text{ Lemma 1.4 } \} \\
& R \sqsubseteq S
\end{aligned}
$$

$\square$

Corollary 3.4.1 (Uniqueness of Prime Factorization)**.** $F(R) = F(S) \iff R = S$.

Proof.

$$
\begin{array}{ll}
& F(R) = F(S) \\
\iff & \quad \{ \text{ Antisymmetry of } \mid \ \} \\
& F(R) \mid F(S) \wedge F(S) \mid F(R) \\
\iff & \quad \{ \text{ Theorem 3.4 on both terms } \} \\
& R \sqsubseteq S \wedge S \sqsubseteq R \\
\iff & \quad \{ \text{ Antisymmetry of } \sqsubseteq \ \} \\
& R = S
\end{array}
$$

□

Theorem 3.5. F is surjective.

Theorem 3.6 (Existence of Prime Factorization)**.**

F^{-1} exists!

4 Irrationality of $\sqrt{p}$

Lemma 4.1 (Even $\neq$ Odd)**.** $2 \cdot m \neq 2 \cdot n + 1$

Lemma 4.2 (Irrationality of $\sqrt{p}$)**.** $m^2 \neq n^2 \cdot p$

Proof.

$$
\begin{array}{ll}
& m^2 \neq n^2 \cdot p \\
\Longleftarrow & \quad \{ \text{ Leibniz } \} \\
& F^{-1}(m^2) \neq F^{-1}(n^2 \cdot p) \\
\Longleftarrow & \quad \{ \text{ Leibniz } \} \\
& |F^{-1}(m^2)| \neq |F^{-1}(n^2 \cdot p)| \\
\iff & \quad \{ \text{ Lemma 3.1 } \} \\
& |F^{-1}(m) \sqcup F^{-1}(m)| \neq |F^{-1}(n) \sqcup F^{-1}(n) \sqcup F^{-1}(p)| \\
\iff & \quad \{ \text{ Connection between } \sqcup \text{ and } + \ \} \\
& |F^{-1}(m)| + |F^{-1}(m)| \neq |F^{-1}(n)| + |F^{-1}(n)| + |F^{-1}(p)| \\
\iff & \quad \{ \text{ Arithmetic } \} \\
& 2 \cdot |F^{-1}(m)| \neq 2 \cdot |F^{-1}(n)| + 1 \\
\iff & \quad \{ \text{ Even} \neq \text{Odd } \} \\
& TRUE
\end{array}
$$

□