Product Divisors

Mark Gius

April 14, 2011

1 Introduction

While reading Section 1.3.2, a sample MIX program designed to determine the first 100 primes briefly mentioned an optimization that centered around the idea that if you have checked every factor of X up to $\sqrt{X}$ then you can stop and declare the number prime. The root of this optimization is a claim that for each pair of factors of a number, one must be less than $\sqrt{X}$ and the other must be greater. I wanted to see why.

2 Proof/Analysis

Let's start with the claim.

$$\text{if } x = yz \text{ then } y > \sqrt{x} \text{ and } z < \sqrt{x} \text{ or } y = z$$

My first thought was to prove that every possibility other than the one suggested above was invalid. This led to examples of why y and z cannot both be greater or less than $\sqrt{x}$.

$$\begin{aligned} \text{Assume } y, z &> \sqrt{x} \\ yz &> x \\ yz &= x \end{aligned}$$

Contradiction

$$\begin{aligned} \text{Assume } y, z &< \sqrt{x} \\ yz &< x \\ yz &= x \end{aligned}$$

Contradiction

However, I was unsatisfied with this, because while it shows clearly that y and z cannot both be greater or less than $\sqrt{x}$, it fails to show that one must be greater and the other less, and Proof by Lack of Other Options doesn't seem like a very good way of going about things.

At this point I thought about how I could express a product in a different way such that the assertion I found in the book would become more apparent. What I came up was this:

$$x = y \times z$$
$$x = (\sqrt{x} \times \frac{i}{j}) \times (\sqrt{x} \times \frac{j}{i})$$

This definition is rather nice for a number of reasons. For one, it handles the case where y and z are equal, whereas most of my previous scratch work handled these cases separately. For another, it defines x as a product of it's own square root, which allows us to clearly show the relationship between the two product roots y and z in such a way that the greater than / less than relationship is clear. Because the two fractions involving i and j are inverses, one side of the product always rises as the other falls. The two fractions involving i and j cancel each other out, leaving the multiplication two square roots, which is trivial.

So, the assertion in the book is correct, shown clearly by defining a product with square roots and two inverted fractions as above.

3 Limitations

I believe this only works for values of X that are positive and greater than 1. I'm very confident that it only works for positive numbers, but the greater than 1 restriction is only a hunch.