How do proofs that primes are infinite fail?

William Gasarch

Abstract.

1. INTRODUCTION. Let P be a proof that the primes are infinite. What happens if you try to use P on a domains where the number of primes is finite? By seeing where P fails, you get more insight into what it was about $\mathbb{Z}$ that made P work.

We first need to clarify what a prime is. The following definitions are standard.

Definition 1. Let D be an integral domain.

(a) A *unit* is a $u \in \mathrm{D}$ such that there exists $v \in \mathrm{D}$ with $uv = 1$. We let U be the set of units if the domain is understood.

(b) An *irreducible* is a $p \in \mathrm{D} - \mathrm{U}$ such that if $p = ab$ then either $a \in \mathrm{U}$ or $b \in \mathrm{U}$. We let I be the set of irreducibles if the domain is understood.

(c) A *prime* is a $p \in \mathrm{D}$ such that if p divides ab then either p divides a or p divides b. In any integral domain all primes are irreducible. There are integral domains with irreducibles that are not primes. The set $\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$ is one such example: (a) The element 2 is irreducible, yet (b) 2 is not prime since 2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ but 2 does not divide either $1 + \sqrt{-5}$ or $1 + \sqrt{-5}$.

(d) We impose an equivalence relation on I: p and q are equivalent if there exists $u \in \mathrm{U}$ such that $p = uq$. We say I *is infinite up to units* if the number of equivalence classes is infinite. In this paper *infinite* will mean *infinite up to units*.

We consider the following domains.

Notation 1.

(a) *An algebraic integer is a number that satisfies a monic polynomial over $\mathbb{Z}$. Let A be the set of algebraic integers.*

(b) $\mathbb{Q}_2$ *is the set* $\{\frac{a}{b} \colon b \equiv 1 \pmod 2\}$.

Theorem 2.

ACKNOWLEDGEMENTS.

WILLIAM GASARCH received his doctorate in computer science from Harvard in 1985, advised by Harry R. Lewis. His thesis was titled *Recursion-theoretic techniques in complexity theory and combinatorics*. He was hired by the University of Maryland in the Fall of 1985, becoming Associate Professor in 1991, and Full Professor in 1998. He has the largest collection of satires of Nobelist Bob Dylan's music and is an active blogger.
Department of Computer Science, University of Maryland, College Park, MD 20742
gasarch@cs.umd.edu