Notre Dame Journal of Formal Logic
Volume 34, Number 3, Summer 1993

Quadratic Residues and $x^3 + y^3 = z^3$ in Models of IE_1 and IE_2

STUART T. SMITH

Abstract It is unknown whether the fragment of arithmetic IE_1 (or even the stronger system $I\Delta_0$) proves that every odd prime has a quadratic nonresidue. We show that one direction of the quadratic reciprocity law holds in IE_1 when one of the primes is standard. Thus an odd prime q which has no quadratic nonresidues must satisfy $\left(\frac{q}{p}\right) = 1$ for every standard prime p. We show that if q is a prime $\neq 2, 3$ in a model of IE_1 and $n = 1, 2, 3$, or 4, then $q = x^2 + ny^2$ for some x, y if and only if $\left(\frac{-n}{q}\right) = 1$. This result for $n = 3$ enables us to prove in IE_2 that $x^3 + y^3 = z^3$ has no nontrivial solution.

1 Introduction A number of articles have appeared which were motivated by the question of how much induction is necessary in order to prove elementary results in number theory. More precisely, axiom systems are considered which contain the axioms for discretely ordered semirings (i.e, 1 is the least positive element) together with the induction scheme for some class of formulas in the language $\mathcal{L} = \{+, \cdot, <, 0, 1\}$. Peano arithmetic (in which induction holds for *all* $\mathcal{L}$-formulas) is the best known such system, but it is too strong for our purposes, as it proves all of the results of classical number theory. We are interested in weaker systems, the so-called fragments of arithmetic.

The weakest such system is open induction (*IOpen*), in which induction is assumed only for quantifier-free formulas. Shepherdson showed in [7] that *IOpen* is too weak to prove the irrationality of $\sqrt{2}$, or to prove that $x^3 + y^3 = z^3$ has only trivial solutions. The model he constructed contains no nonstandard primes, so in particular the set of primes is not cofinal. In Wilkie [13], van den Dries [2], Smith [9], and Smith [11], open induction is strengthened by the addition of algebraic axioms, such as normality or the existence of g.c.d.'s, but the resulting systems are shown still to be very weak.

Received August 10, 1992; revised November 18, 1992