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

A much stronger system is $I\Delta_0$, in which induction is assumed to hold for all formulas having only bounded quantifiers. (See Paris and Wilkie [6].) As noted in Macintyre and Marker [5], it is unknown whether $I\Delta_0$ proves the cofinality of the set of primes, or the existence of quadratic nonresidues for all odd primes. It is the latter question which interests us here.

We will in fact work in IE_1, an intermediate system between *IOpen* and $I\Delta_0$. IE_1, or bounded existential induction, was introduced by Wilmers in [14]. In IE_1 we assume induction holds for all bounded *existential* formulas. (Actually, as is noted in [14], no proof is known that IE_1 is strictly weaker than $I\Delta_0$.) Some of the algebraic properties of models of IE_1 are developed in [9], Smith [10], and Smith [12].

In Section 2 we review the definitions and elementary facts about the systems IE_n. We show in Section 3 that we can use an inductive argument in IE_1 on the modulus m to show that certain finite elements are quadratic nonresidues for m, provided m satisfies certain congruence conditions. This enables us to prove one direction of the quadratic reciprocity law when one of the primes is standard. This in turn enables us to place limitations on odd primes which have no quadratic nonresidues, if such a thing is possible in a model of IE_1.

In Section 4 we show that a result for $\mathbb{N}$ is provable in IE_1 for small values of n. Specifically, we show in IE_1 that if q is a prime $\neq 2, 3$ and $n = 1, 2, 3$, or 4, then $q = x^2 + ny^2$ for some x and $y \Leftrightarrow \left(\frac{-n}{q}\right) = 1$. Our descent argument breaks down for larger n, and in any case this result does not hold in $\mathbb{N}$ for $n = 5$, since $\left(\frac{-5}{7}\right) = 1$ but 7 is not of the form $x^2 + 5y^2$.

In Section 5 we use the above characterization of primes of the form $x^2 + 3y^2$ to show that in IE_2, $x^3 + y^3 = z^3$ has no nontrivial solutions. The proof is adapted from an argument due to Browkin which appears in Sierpinski's book [8].

2 Preliminaries In this section we review the definitions of the axiom systems IE_n and list some basic results.

Definition 2.1 [14] Let $\mathcal{L}$ be the first-order language $\{+, \cdot, <, 0, 1\}$. Define

$$
\begin{aligned}
E_0 = U_0 &= \{\theta(\vec{x}) : \theta(\vec{x}) \quad \text{is an open formula}\},\\
E_{n+1} &= \{\exists y_1 < t_1(\vec{x}) \cdots \exists y_m < t_m(\vec{x})\theta(\vec{x}, y_1 \cdots y_m) :\\
&\qquad \theta \in U_n \quad \textit{and} \quad t_1, \ldots, t_m \quad \textit{are} \quad \mathcal{L}-\textit{terms}\},\\
U_{n+1} &= \{\forall y_1 < t_1(\vec{x}) \cdots \forall y_m < t_m(\vec{x})\theta(\vec{x}, y_1 \cdots y_m) :\\
&\qquad \theta \in E_n \quad \textit{and} \quad t_1, \ldots, t_m \quad \textit{are} \quad \mathcal{L}-\textit{terms}\},\\
\nabla_n &= \{\theta(\vec{x}) : \theta \quad \text{is logically equivalent to an } E_n\text{-formula and to a}\\
&\qquad U_n-\textit{formula}\}.
\end{aligned}
$$

If T is an $\mathcal{L}$-theory, the definition of ∇_n relativizes to T. Thus $\psi(\vec{x})$ is *provably* ∇_n *over* T if $\psi(\vec{x})$ is equivalent over T both to an E_n-formula and to a U_n-formula.

We are particularly interested in formulas which are provably ∇_1 over a given theory T. For suppose $\psi(\vec{x})$ is such a formula and suppose that $\varphi(\vec{x})$ is some quantified formula which contains $\psi(\vec{x})$ as a subformula. Then for purposes of determining the quantifier complexity of φ we can regard ψ as though it were quantifier-free. For example,

$$\exists y < t(\vec{x})\psi \quad \textit{and} \quad \exists y < t(\vec{x})\neg\psi$$

will both be equivalent over T to E_1-formulas. (Abusing terminology, we will refer to them both as E_1-formulas.)

Definition 2.2 [14] (i) The system IE_n consists of the axioms for discretely ordered semi-rings, together with the induction schema for all E_n-formulas θ:

$$\forall \vec{y}\,[(\theta(0, \vec{y}) \wedge \forall x\,(\theta(x, \vec{y}) \to \theta(x+1, \vec{y}))) \longrightarrow \forall x \theta(x, \vec{y})]\,.$$

(IE_0 will be denoted by *IOpen*.)

(ii) The system LE_n consists of the axioms for discretely ordered semirings, together with the following *least number principle* for all E_n-formulas θ:

$$\forall \vec{y}\,[\exists x \theta(x, \vec{y}) \longrightarrow \exists x\,(\theta(x, \vec{y}) \wedge \forall z < x \neg\theta(z, \vec{y}))]\,.$$

Semirings which are models of IE_n or LE_n will be denoted by M, M', etc. The basic properties of IE_n are developed in [14]. We will need the following two facts:

Theorem 2.3 [14] *For every $n \geq 0$, we have*

$$IE_{n+1} \Longrightarrow IE_n \Longleftrightarrow LE_n.$$

Lemma 2.4 [12] *Let $\theta(x, \vec{y})$ be an E_n-formula. Then*

$$IE_n \vdash \forall \vec{y}\Big[\Big(\exists w \theta(w, \vec{y}) \wedge \exists z \forall x\big(\theta(x, \vec{y}) \longrightarrow x \leq z\big)\Big) \longrightarrow \exists z\Big(\theta(z, \vec{y}) \wedge \forall x\big(\theta(x, y) \longrightarrow x \leq z\big)\Big)\Big].$$

That is, IE_n proves that any nonempty bounded E_n-definable set has a greatest element.

We also need to know that certain relations are provably ∇_1 over IE_1 or *IOpen*.

Lemma 2.5 Kaye [4] *$x|y$ is provably ∇_1 over IOpen.*

Proof: Here $x|y$ means x divides y, where $0|0$ and $0 \nmid y$ for $y \neq 0$. The formula $x|y$ has the E_1 definition $\exists z \leq y(xz = y)$, and is equivalent over *IOpen* to the U_1-formula

$$y = 0 \vee [y > 0 \wedge \forall z \leq y \forall r < y(y = zx + r \longrightarrow r = 0)]\,.$$

Lemma 2.6 [4] *$x \equiv y \bmod z$ is provably ∇_1 over IOpen.*

Proof: The formula $x \equiv y \bmod z$ has the E_1 definition $(\exists w \leq x + y)[x = wz + y \vee y = wz + x]$, and is equivalent over *IOpen* to the formula $(z = 0 \wedge x = y) \vee [z > 0 \wedge \forall w \leq x + y((x = y + w \vee y = x + w) \to z|w)]$. This formula is U_1 by Lemma 2.5.

Lemma 2.7 [14] $IE_1 \vdash \forall x[x > 0 \to \forall y((x, y) = 1 \to \exists z < x(yz \equiv 1 \bmod x))]$.

Corollary 2.8 *If $M \models IE_1$ and p is a prime in M, then M/pM is a field. More generally, if $m \in M$, $m > 1$ and $a \in M$ is such that $(a, m) = 1$, then a is invertible in M/mM.*

Lemma 2.9 [9] *$(x, y) = z$ is provably ∇_1 over IE_1.*

Proof: If $z = 1$, this follows from Lemma 2.7. The proof for arbitrary z in [9] is a generalization of Wilmers' proof for $z = 1$.

Finally, we note that one can prove in IE_1 (in fact in *IOpen*) that $x \equiv y \bmod z$ defines a congruence relation, and if $z > 0$ then every x is congruent to a unique w such that $w < z$.

3 Quadratic residues Let $M \models IE_1$ and suppose $m \in M, m > 1$. For any $a \in M$, we can ask whether the congruence $x^2 \equiv a \bmod m$ has any solutions in M. As in the case of $\mathbb{N}$, if the answer is yes *and* $(a, m) = 1$, then we say that a is a quadratic residue for m; otherwise a is a quadratic nonresidue for m.

We note some elementary facts.

Lemma 3.1 *Let $M \models IE_1$ and suppose $m \in M$, $m > 1$. Then for any $a, b \in M$, we have:*

(i) If $x^2 \equiv a \bmod m$ has a solution and $x^2 \equiv b \bmod m$ has a solution, then $x^2 \equiv ab \bmod m$ has a solution.

(ii) If $x^2 \equiv a \bmod m$ has a solution where we assume also that $(a, m) = 1$, and if $x^2 \equiv b \bmod m$ has no solution, then $x^2 \equiv ab \bmod m$ has no solution.

(iii) If $x^2 \equiv a \bmod m$ has a solution and $m' | m$, then $x^2 \equiv a \bmod m'$ has a solution.

Proof: (i) and (iii) are trivial. To prove (ii), suppose $c \in M$ is such that $c^2 = a \bmod m$. Since $(a, m) = 1$, clearly $(c, m) = 1$, so by Lemma 2.7, there is a $d \in M$ such that $cd \equiv 1 \bmod m$. Then $d^2a \equiv d^2c^2 \equiv 1 \bmod m$, so if $e \in M$ were such that $e^2 \equiv ab \bmod m$ we would have $(de)^2 \equiv d^2ab \equiv b \bmod m$, contradicting our assumption on b.

When $m \in M$ is a prime, say $m = q$, we can define the Legendre symbol $\left(\frac{c}{q}\right)$ in the usual way:

$$\left(\frac{c}{q}\right) = \begin{cases} 0 & \text{if } q | c\,, \\ 1 & \text{if } q \nmid c \text{ and } c \text{ is a quadratic residue for } q\,, \\ -1 & \text{if } q \nmid c \text{ and } c \text{ is a quadratic nonresidue for } q. \end{cases}$$

The generalization of this symbol to the case where q is composite (the *Jacobi* symbol) does not have the properties we will need, so we will use only the Legendre symbol.

As is implied by the previous paragraph, we are particularly interested in the case where $m \in M$ is prime. If m is a *standard* prime, say $m = p \in \mathbb{N}$, we have that the usual results from $\mathbb{N}$ hold (in addition to those listed in Lemma 3.1). Specifically, half of the elements $1, 2, \cdots, \frac{p-1}{2}$ of M/pM are quadratic residues and the other half are quadratic nonresidues; also the product of two quadratic nonresidues is a quadratic residue.

The proofs of these facts use counting arguments which do not go over to the non-standard case. Thus in [5] the question is raised as to whether one can prove in $I\Delta_0$ that every prime has a quadratic nonresidue. (They note that if we adjoin the Δ_0-Pigeonhole Principle to $I\Delta_0$, then the proof can be carried out.)

In $\mathbb{N}$ we have the famous law of quadratic reciprocity, which says that if p and q are distinct odd primes then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *unless* both p and q are congruent to 3 modulo 4, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. The question arises as to what happens to this law in $M \models IE_1$ (of course it continues to hold if both primes are standard). We will show that if p is standard and q is an arbitrary prime, then $\left(\frac{p}{q}\right) = 1 \Rightarrow \left(\frac{q}{p}\right) = 1$ unless both primes are congruent to 3 modulo 4, in which case $\left(\frac{p}{q}\right) = 1 \Rightarrow \left(\frac{q}{p}\right) = -1$. In particular, we will show that many elements (if not most primes) of M have quadratic nonresidues.

Our first result in this direction is the following:

Lemma 3.2 *Let $M \models IE_1$ and suppose $m \in M$, $m \equiv 3 \, mod \, 4$. Then -1 is a quadratic nonresidue for m.*

Proof: Note that although our language $\mathcal{L}$ does not contain a minus sign, the above conclusion can be expressed as

$$\neg\exists x(x^2 + 1 \equiv 0 \, mod \, m).$$

By the remark after Lemma 2.9, it suffices to consider those x for which $x < m$; thus -1 is a quadratic nonresidue for m if and only if

$$M \models \neg\exists x < m(x^2 + 1 \equiv 0 \, mod \, m).$$

Using Lemma 2.6, we see that the set of $m \in M$ such that $m \equiv 3 \, mod \, 4$ and -1 is a quadratic *residue* for m is E_1-definable. If it is nonempty, it must have a least element $a \in M$. There is by assumption a $b \in M$ such that $b < a$ and $b^2 + 1 \equiv 0 \, mod \, a$; replacing b by $a - b$ if necessary, we can assume that b is even. The above congruence implies

$$b^2 + 1 = ac$$

for some $c \in M$. Since $b < a$, we have $ac = b^2 + 1 < a^2$ and so $c < a$. Now $b^2 + 1 \equiv 1 \, mod \, 4$ because b is even, hence $ac \equiv 1 \, mod \, 4$. But $a \equiv 3 \, mod \, 4$, so $c \equiv 3 \, mod \, 4$ as well. The equation $b^2 + 1 = ac$ implies that $b^2 + 1 \equiv 0 \, mod \, c$, so

$$M \models \exists x(x^2 + 1 \equiv 0 \, mod \, c)$$

where $c \equiv 3 \, mod \, 4$. This contradicts the minimality of a.

In particular, if $M \models IE_1$ and $q \in M$ is an odd prime for which -1 is a quadratic residue, then $q \equiv 1 \, mod \, 4$. We would like to prove the converse, which of course holds when q is standard. The problem is that the analogous descent argument to Lemma 3.2 does not work. Even in $I\Delta_0$, where we can restrict this argument to primes, there does not seem to be any contradiction to be derived from assuming that $q \equiv 1 \, mod \, 4$ is the minimal prime for which -1 is a quadratic *nonresidue*. Moreover, the usual methods for finding a square root for -1 modulo q involve functions, such as the factorial function, which are not available to us even in $I\Delta_0$.

We can prove related results by a similar argument, where in general we will have to consider more cases. For example, the following result (actually its corollary) will be needed later in the discussion at the end of this section.

Lemma 3.3 *Let $M \models IE_1$ and suppose $m \in M$, where $m \equiv 5, 8, 10, 11, 16, 17, 20, 22,$ or $23 \, mod \, 24$. Then -3 is a quadratic nonresidue for m.*

Proof: As in Lemma 3.2, we let $a \in M$ be the minimal counterexample for m and we let $b \in M$ be such that $b < a$ and $b^2 + 3 = 0 \, mod \, a$; replacing b by $a - b$ if necessary, we can assume that $3 \nmid b$. Thus $b^2 + 3 \equiv 4, 7$ or $19 \, mod \, 24$.

Now $b^2 + 3 = ac$ for some $c \in M$; since $b < a$ and $a \geq 5$ (by the congruence condition in the hypothesis), then $b^2 + 3 < a^2$ and so $c < a$. Obviously -3 is a quadratic residue for c; it remains only to show that c satisfies one of the congruences in the hypothesis of the lemma, and then c will contradict the minimality of a. We consider the three possible values for $b^2 + 3$ modulo 24 in turn.

(a) Suppose $b^2 + 3 \equiv 4 \, mod \, 24$. Since $b^2 + 3 = ac$ we have $ac \equiv 4 \, mod \, 24$; thus $a \not\equiv 8 \, mod \, 24$ and $a \not\equiv 16 \, mod \, 24$. If $a \equiv 5, 11, 17$, or $23 \, mod \, 24$ then $c \equiv 20 \, mod \, 24$, and vice versa. If $a \equiv 10$ or $22 \, mod \, 24$ then $c \equiv 10$ or $22 \, mod \, 24$. Thus c satisfies the hypothesis of the lemma.

(b) Suppose $b^2 + 3 \equiv 7 \, mod \, 24$, so $ac \equiv 7 \, mod \, 24$; then $a \not\equiv 8, 10, 16, 20$ or $22 \, mod \, 24$. If $a \equiv 5 \, mod \, 24$ then $c \equiv 11 \, mod \, 24$ and vice versa; if $a \equiv 17 \, mod \, 24$ then $c \equiv 23 \, mod \, 24$ and vice versa.

(c) Suppose $b^2 + 3 \equiv 19 \, mod \, 24$, so $ac \equiv 19 \, mod \, 24$. Again $a \not\equiv 8, 10, 16, 20$, or $22 \, mod \, 24$. If $a \equiv 5 \, mod \, 24$ then $c \equiv 23 \, mod \, 24$ and vice versa; if $a \equiv 11 \, mod \, 24$ then $c \equiv 17 \, mod \, 24$ and vice versa.

Corollary 3.4 *Let $M \models IE_1$ and suppose $q \in M$, $q > 3$ is prime and -3 is a quadratic residue for q. Then $q \equiv 1 \, mod \, 6$.*

We can similarly prove:

Lemma 3.5 *(i) Let $M \models IE_1$ and suppose $m \in M$, where $m \equiv 3$ or $5 \, mod \, 8$. Then 2 is a quadratic nonresidue for m.*

(ii) Let $M \models IE_1$ and suppose $m \in M$, where $m \equiv 5$ or $7 \, mod \, 8$. Then -2 is a quadratic nonresidue for m.

Corollary 3.6 *(i) Let $M \models IE_1$ and suppose $q \in M$ is prime and 2 is a quadratic residue for q. Then $q \equiv 1$ or $7 \, mod \, 8$.*

(ii) Let $M \models IE_1$ and suppose $q \in M$ is prime and -2 is a quadratic residue for q. Then $q \equiv 1$ or $3 \, mod \, 8$.

We can continue in this manner, eventually salvaging one direction of the quadratic reciprocity law when one prime is standard.

Lemma 3.7 *Let $M \models IE_1$ and let $p \in M$ be a standard prime such that $p \equiv 1 \, mod \, 8$. Let $m \in M$, $p \nmid m$, be a quadratic nonresidue for p. Then p is a quadratic nonresidue for m.*

Proof: We first must show that the set of $m \in M$ for which the lemma does not hold is E_1-definable. Because p is standard, the assumption $\neg \exists x < p(x^2 \equiv m \, mod \, p)$ can be replaced by a finite disjunction of congruences, the choice of which varies with p. For example, if $p = 17$ then m is a quadratic nonresidue for p if and only if $m \equiv 3, 5, 6, 7, 10, 11, 12$, or $14 \, mod \, 17$. By Lemma 2.6, this formula is provably ∇_1 over IE_1.

The set of counterexamples for m is thus E_1-definable, and we assume it is nonempty. By LE_1, it contains a least element $a \in M$. We will show that a is infinite.

Clearly $a > 1$, so if a is finite we can write $a = 2^r \cdot s$, where $r \geq 0$ and s is odd. Now 2 is a quadratic residue for p, hence so is 2^r; in order for a to be a quadratic nonresidue for p, it must be the case that a (hence s) has an odd prime factor q which is a quadratic nonresidue for p. Since q is standard, by ordinary quadratic reciprocity we have that p is a quadratic nonresidue for q (and so for a). But then a is not a counterexample.

Now for some $b < a$, we have

$$b^2 \equiv p \, mod \, a,$$

where by replacing b by $a - b$ if necessary we can assume that $p \nmid b$. Thus

$$b^2 = p \pm ac$$

for some $c \in M$, $c > 0$. But a is infinite and p finite, so the sign above cannot be negative, and we have $b^2 = p + ac$. Furthermore, $b < a$ and so $c < a$; also clearly $p \nmid c$. Looking modulo p, we have

$$0 \neq b^2 \equiv ac \bmod p,$$

where $\left(\frac{a}{p}\right) = -1$. Hence $\left(\frac{c}{p}\right) = -1$, whereas since $b^2 = p + ac$ we have that p is a quadratic residue for c. Since $c < a$, this contradicts the minimality of a.

The corresponding lemma for $p \equiv 5 \bmod 8$ is more complicated, since in this case $\left(\frac{2}{p}\right) = -1$.

Lemma 3.8 *Let $M \models IE_1$ and let $p \in M$ be a standard prime such that $p \equiv 5 \bmod 8$. Let $m \in M$, $p \nmid m$, satisfy one of the following conditions:*

(a) $m \equiv 0 \bmod 8$, or
(b) $m \equiv 1, 3, 4, 5,$ or $7 \bmod 8$ and m is a quadratic nonresidue for p, or
(c) $m \equiv 2$ or $6 \bmod 8$ and m is a quadratic residue for p.

Then p is a quadratic nonresidue for m.

Proof: Clearly the set of counterexamples for m is E_1-definable, as in Lemma 3.7. We assume that it is nonempty and we let a denote its minimal element. We show that a is infinite.

Clearly $a > 1$, and if a is finite we can write $a = 2^r \cdot s$ with $r \geq 0$ and s odd. If $r \geq 3$ then $a \equiv 0 \bmod 8$; but since $p \equiv 5 \bmod 8$, we have that p is a quadratic nonresidue for 8, hence for a. This contradicts the assumption that a is a counterexample to the lemma. Thus $r \leq 2$.

If $r = 0$ or 2 then $a \equiv 1, 3, 4, 5,$ or 7 modulo 8, so by assumption $\left(\frac{a}{p}\right) = -1$. Moreover, $a = s$ or $a = 4s$, so $\left(\frac{s}{p}\right) = -1$. In particular, $s > 1$ and s has an odd prime factor q such that $\left(\frac{q}{p}\right) = -1$. By ordinary quadratic reciprocity, $\left(\frac{p}{q}\right) = -1$, so p is a quadratic nonresidue for a. Again this contradicts the assumption that a is a counterexample.

If $r = 1$ then $a = 2s$ with s odd, so $a \equiv 2$ or $6 \bmod 8$. By assumption, then, $\left(\frac{a}{p}\right) = 1$; but $\left(\frac{2}{p}\right) = -1$ so $\left(\frac{s}{p}\right) = -1$ as well, and the argument continues as above. Therefore a must be infinite.

As in Lemma 3.7, we have

$$b^2 = p + ac$$

for some $b < a$, $c < a$ such that $p \nmid b$; therefore $p \nmid c$ either. Modulo 8 we have

$$b^2 \equiv 5 + ac \bmod 8,$$

so $a \not\equiv 0 \bmod 8$. Therefore one of cases (b) or (c) applies. We deal with them in turn.

(b) If $a \equiv 1, 3, 4, 5,$ or $7 \bmod 8$ and $\left(\frac{a}{p}\right) = -1$, then since $b^2 \equiv ac \bmod p$ we have $\left(\frac{c}{p}\right) = -1$ as well. In the congruence $b^2 \equiv 5 + ac \bmod 8$ there are two possibilities:

(1) Suppose b is odd. Then $b^2 \equiv 1 \, mod \, 8$, so $ac \equiv 4 \, mod \, 8$. If $a \equiv 1, 3, 5,$ or $7 \, mod \, 8$ then $c \equiv 4 \, mod \, 8$ and vice versa, so c contradicts the minimality of a.

(2) Suppose b is even. Then b^2 is even, so ac is odd. Thus a and c are both odd, so again c satisfies the hypotheses of case (b) and contradicts the minimality of a.

(c) If $a \equiv 2$ or $6 \, mod \, 8$ and $\left(\frac{a}{p}\right) = 1$, then since $b^2 \equiv ac \, mod \, p$ we have $\left(\frac{c}{p}\right) = 1$ as well. Now since a is even and p is odd, the equation $b^2 = p + ac$ implies that b is odd. Thus $b^2 \equiv 1 \, mod \, 8$, and since $p \equiv 5 \, mod \, 8$ we must have $ac \equiv 4 \, mod \, 8$. Since $a \equiv 2$ or $6 \, mod \, 8$, then $c \equiv 2$ or $6 \, mod \, 8$ also, and so c contradicts the minimality of a.

Lemmas 3.7 and 3.8 together enable us to deal with standard primes p such that $p \equiv 1 \, mod \, 4$. When we turn to the case where $p \equiv 3 \, mod \, 4$, the situation becomes more complicated; for instance, when $m = q$ is a standard odd prime, we must distinguish between the cases $q \equiv 1 \, mod \, 4$ and $q \equiv 3 \, mod \, 4$. The following two lemmas provide the analogues to Lemmas 3.7 and 3.8.

Lemma 3.9 *Let $M \models IE_1$ and let $p \in M$ be a standard prime such that $p \equiv 7 \, mod \, 8$. Let $m \in M$, $p \nmid m$, satisfy one of the following conditions:*

(a) $m \equiv 0$ or $4 \, mod \, 8$ (i.e. $4|m$), or
(b) $m \equiv 1, 2,$ or $5 \, mod \, 8$ and m is a quadratic nonresidue for p, or
(c) $m \equiv 3, 6,$ or $7 \, mod \, 8$ and m is a quadratic residue for p.

Then p is a quadratic nonresidue for m.

Proof: As in the previous cases, the set of $m \in M$ for which the lemma does not hold is E_1-definable. Assume it is nonempty and let $a \in M$ be the minimal counterexample. We show that a is infinite.

Since 1 does not satisfy any of the conditions in the hypothesis of the lemma, we have $a > 1$. *Suppose a is finite*; then, we can write $a = 2^r \cdot s \in \mathbb{N}$ with $r \geq 0$ and s odd. If $r \geq 2$ then $4|a$; but $p \equiv 3 \, mod \, 4$ so p is a quadratic nonresidue for 4, hence for a. This contradicts the assumption that a is a counterexample to the lemma. Hence $r = 0$ or 1, and case (a) does not hold.

Now $\left(\frac{2}{p}\right) = 1$. In case (b), then, we have that $s \equiv 1$ or $5 \, mod \, 8$ (i.e. $s \equiv 1 \, mod \, 4$) and $\left(\frac{s}{p}\right) = -1$. Thus $s > 1$. Write $s = t^2 u \in \mathbb{N}$, where u is squarefree and $(t, u) = 1$. Then $\left(\frac{u}{p}\right) = -1$, so $u > 1$. Also, since $s \equiv 1 \, mod \, 4$ and $t^2 \equiv 1 \, mod \, 4$, we have $u \equiv 1 \, mod \, 4$.

Suppose u has a prime factor q such that $q \equiv 1 \, mod \, 4$ and $\left(\frac{q}{p}\right) = -1$. By ordinary quadratic reciprocity, p is a quadratic nonresidue for q, hence for a. This contradicts the assumption that a is a counterexample.

Thus if we write $u = vw \in \mathbb{N}$ where all of the prime factors of v are congruent to 1 modulo 4 and all of the prime factors of w are congruent to 3 modulo 4, the previous paragraph shows that v is a quadratic residue for p, hence w is not. (In particular, $w > 1$.) Now $v \equiv 1 \, mod \, 4$, hence $w \equiv 1 \, mod \, 4$ as well; since $w \in \mathbb{N}$ is squarefree, it has an even number of prime factors. An odd number of them must be quadratic nonresidues for p and an odd number must be quadratic residues for p. In particular, there is at least one $q \equiv 3 \, mod \, 4$ dividing w which is a quadratic residue for p. By ordinary quadratic reciprocity, p is a quadratic *nonresidue* for q, hence for a; this contradicts our assumption on a. Thus case (b) does not hold for a.

We are left with case (c). Here we have $s \equiv 3$ or $7 \bmod 8$ (i.e. $s \equiv 3 \bmod 4$, so in particular $s > 1$) and $\left(\frac{s}{p}\right) = 1$. Again writing $s = t^2u$, this time $u \equiv 3 \bmod 4$. Let $u = vw$ as before; again v must be a quadratic residue for p, hence so is w. But this time $w \equiv 3 \bmod 4$ so w has an *odd* number of prime factors; therefore again w has at least one prime factor $q \equiv 3 \bmod 4$ such that $\left(\frac{q}{p}\right) = 1$. As before, this leads to a contradiction. We conclude that a must be infinite.

As in Lemma 3.7, we have

$$b^2 = p + ac$$

for some $b < a$, $c < a$ such that $p \nmid b$, so $p \nmid c$ either. We consider the three cases in the lemma in turn.

(a) If $a \equiv 0$ or $4 \bmod 8$, then b must be odd, hence $b^2 \equiv 1 \bmod 4$. But then the equation $b^2 = p + ac$ yields

$$1 \equiv 3 + 0 \cdot c \bmod 4,$$

which is impossible. Therefore this case does not apply.

(b) Suppose $a \equiv 1, 2$, or $5 \bmod 8$ and $\left(\frac{a}{p}\right) = -1$. Since

$$0 \not\equiv b^2 \equiv ac \bmod p,$$

we also have that $\left(\frac{c}{p}\right) = -1$. On the other hand, since $b^2 = p + ac$, clearly p is a quadratic residue for c. Considering the equation $b^2 \equiv p + ac \bmod 8$, there are three possibilities for b^2:

(1) Suppose b is odd. Then $b^2 \equiv 1 \bmod 8$, so $1 \equiv 7 + ac \bmod 8$, hence $ac \equiv 2 \bmod 8$. Since $a \equiv 1, 2$, or $5 \bmod 8$, we have that $c \equiv 1, 2$, or $5 \bmod 8$. Thus c contradicts the minimality of a.

(2) Suppose $2|b$ but $4 \nmid b$. Then $b^2 \equiv 4 \bmod 8$, so $4 \equiv 7 + ac \bmod 8$, hence $ac \equiv 5 \bmod 8$. This rules out the possibility that $a \equiv 2 \bmod 8$, hence $a \equiv 1$ or $5 \bmod 8$. We conclude that $c \equiv 1$ or $5 \bmod 8$, and again c contradicts the minimality of a.

(3) Suppose $4|b$. Then $b^2 \equiv 0 \bmod 8$, so $0 \equiv 7 + ac \bmod 8$. Thus $ac \equiv 1 \bmod 8$, so $a \not\equiv 2 \bmod 8$. We therefore have $a \equiv 1$ or $5 \bmod 8$, so $c \equiv 1$ or $5 \bmod 8$. Thus c contradicts the minimality of a.

We have shown that in case (b), the minimality of a is always contradicted by c. Now we consider case (c).

(c) Suppose $a \equiv 3, 6$, or $7 \bmod 8$ and $\left(\frac{a}{p}\right) = 1$. Since

$$0 \not\equiv b^2 \equiv ac \bmod p,$$

we also have that $\left(\frac{c}{p}\right) = 1$. Clearly p is a quadratic residue for c as well. We again look at the three possible values for b^2 in the congruence $b^2 \equiv p + ac \bmod 8$.

(1) Suppose b is odd. Again $ac \equiv 2 \bmod 8$. Since $a \equiv 3, 6$, or $7 \bmod 8$, we have that $c \equiv 3, 6$, or $7 \bmod 8$, so c contradicts the minimality of a.

(2) Suppose $2|b$ but $4 \nmid b$. Then $ac \equiv 5 \bmod 8$ as before, so $a \not\equiv 6 \bmod 8$. Therefore $a \equiv 3$ or $7 \bmod 8$, so $c \equiv 3$ or $7 \bmod 8$; so c contradicts the minimality of a.

(3) Suppose $4|b$. Then $b^2 \equiv 0 \, mod \, 8$ so $ac \equiv 1 \, mod \, 8$. Hence $a \not\equiv 6 \, mod \, 8$, so $a \equiv 3$ or $7 \, mod \, 8$. We conclude that $c \equiv 3$ or $7 \, mod \, 8$, and again c contradicts the minimality of a.

In all cases we arrive at a contradiction, so the set of counterexamples to the lemma must be empty.

Lemma 3.10 *Let $M \models IE_1$ and let $p \in M$ be a standard prime such that $p \equiv 3 \, mod \, 8$. Let $m \in M$, $p \nmid m$, satisfy one of the following conditions:*

(a) $m \equiv 0$ or $4 \, mod \, 8$ (i.e. $4|m$), or
(b) $m \equiv 1, 5$, or $6 \, mod \, 8$ and m is a quadratic nonresidue for p, or
(c) $m \equiv 2, 3$, or $7 \, mod \, 8$ and m is a quadratic residue for p.

Then p is a quadratic nonresidue for m.

Proof: The proof is analogous to that of Lemma 3.9 and is left to the reader.

If in the previous four lemmas we restrict our attention to the case where m is *prime*, say $m = q \in M$, we obtain one direction of the quadratic reciprocity law.

Theorem 3.11 *Let $M \models IE_1$ and let $p, q \in M$ be primes, where p is standard. If $\left(\frac{p}{q}\right) = 1$, then $\left(\frac{q}{p}\right) = 1$ unless both p and q are congruent to 3 modulo 4, in which case $\left(\frac{q}{p}\right) = -1$.*

Suppose now that IE_1 cannot prove that every odd prime has a quadratic nonresidue. Let $M \models IE_1$ and let $q \in M$ be a prime which has no quadratic nonresidues. (Then q must be infinite.) In particular, $\left(\frac{-1}{q}\right) = 1$, so by Lemma 3.2 we must have $q \equiv 1 \, mod \, 4$. (By Lemma 3.5 we in fact have $q \equiv 1 \, mod \, 8$.) Then by Theorem 3.11, $\left(\frac{q}{p}\right) = 1$ for *every* standard odd prime p.

The above condition enables us to place restrictions on the form of q. We know from [12] that any odd $m \in M$ greater than 1 can be written as $m = ab + 1$, where a is odd and b is a power of 2. (Recall that the relation "y is a power of the prime x" can be expressed in IE_1 via the formula $Pow(x, y)$ defined as follows:

$$x > 1 \wedge x|y \wedge \forall z \leq y \, ((1 < z \wedge z|y \rightarrow x|z).$$

It is easy to see that x must be prime for this formula to hold.) If $q = ab + 1$ is an odd prime with no quadratic nonresidues, we saw above that $8|b$. Note here that there seems to be no way in IE_1 of determining an exponent e of 2 such that "$b = 2^e$" holds in some sense, whereas in $I\Delta_0$ it is well-known that this can be done.

Similarly, if q is as above then in particular -3 is a quadratic residue for q, so $q \equiv 1 \, mod \, 6$ by Corollary 3.4. This means $3|ab$; but $3 \nmid b$ because $Pow(2, b)$ holds in M. Therefore $3|a$.

The previous paragraph shows in particular that any Fermat prime q (i.e., any prime $q = b + 1$ where b is a power of 2) has quadratic nonresidues. In fact this holds for any $m = b + 1$ such that $Pow(2, b)$, whether or not m is prime. The corresponding result for Mersenne primes (i.e., primes q such that $q + 1$ is a power of 2) is even easier, since we will have $q \equiv 3 \, mod \, 4$ and so -1 is a quadratic nonresidue for q by Lemma 3.2. We leave it to the reader to find other restrictions on a; for example, a must be congruent to either 0 or 3 modulo 5.

In view of the fact that at least one of a, b must be infinite, we ask whether it is possible to prove that *both* are infinite. For a, this would possibly involve extending the above congruence restrictions to all the standard primes and showing that no finite element of M can satisfy them all simultaneously.

The situation is different for b. In $\mathbb{N}$ we can prove that if $m \equiv 9 \, mod \, 16$, then -1 has no eighth root in $\mathbb{Z}/m\mathbb{Z}$. The proof involves examining the order of the group of units of $\mathbb{Z}/m\mathbb{Z}$ and noting that it is not divisible by 16. In IE_1 one could attempt an alternative proof along the lines of Lemma 3.2; the problem is that we can no longer conclude that $c < a$. Thus we do not even know if IE_1 proves that $b > 3$.

4 Representability by quadratic forms In this section we treat some cases of the following question: which elements (and in particular which primes) of a model $M \models IE_1$ can be expressed in the form $x^2 + ny^2$ for a particular integer n? Some results of this type for $\mathbb{N}$ go back to Fermat, and the problem for primes in $\mathbb{N}$ has been completely solved for each $n > 0$ (cf. Cox [1]). The question is intimately related to quadratic reciprocity since if $q = x^2 + ny^2$ then

$$x^2 \equiv -ny^2 \, mod \, q,$$

implying that $\left(\frac{-n}{q}\right) = 1$. For certain values of n, this necessary condition is also sufficient, even in IE_1.

Before discussing this further, we note that when such representations of a prime q exist, they are essentially unique. In fact we can show this to be the case in any discretely ordered GCD domain. The following proof is taken from Sierpinski's book [8].

Theorem 4.1 *Let R be a discretely ordered GCD domain, let $a, b \in R$ be positive elements of R, and let $q \in R$ be a positive prime element of R. If there exist $x, y \in R$ such that both are nonzero and $q = ax^2 + by^2$, then x and y are unique up to sign and up to the possibility of interchanging x and y in the case $a = b = 1$.*

Proof: If such x, y exist then clearly $(a, b) = 1$, for if d is a common divisor of a and b then $d|q$. Clearly $d = \pm q$ is impossible because a, b, x, y are all positive, therefore $d = \pm 1$. Similarly we can conclude $(x, y) = 1$.

Suppose in addition to $q = ax^2 + by^2$ we also have $q = ax_1^2 + by_1^2$ for some $x_1, y_1 \in R$. As above, we have $(x_1, y_1) = 1$. We suppose for convenience that $x, y, x_1, y_1 > 0$.

We note that

$$(axx_1 + byy_1)\,(xy_1 + yx_1) =$$
$$(ax^2 + by^2)x_1y_1 + (ax_1^2 + by_1^2)xy = q(x_1y_1 + xy).$$

Therefore either $q|axx_1 + byy_1$ or else $q|xy_1 + yx_1$ (or both).

Suppose the former, that is suppose $q|axx_1 + byy_1$. From our two expressions for q we can deduce that

$$q^2 = (axx_1 + byy_1)^2 + ab(xy_1 - yx_1)^2,$$

so if $q|axx_1 + byy_1$ we must in fact have $axx_1 + byy_1 = \pm q$ and so $xy_1 - yx_1 = 0$. Therefore

$$xy_1 = yx_1.$$

Since $(x, y) = 1$, this implies $x|x_1$ (cf. [9]), and similarly $(x_1, y_1) = 1$ implies $y_1|y$. Therefore we must have $x = x_1,\ y = y_1$.

Now suppose the latter possibility, i.e. $q|xy_1 + yx_1$. Our two expressions for q also give us the equation

$$q^2 = (axx_1 - byy_1)^2 + ab(xy_1 + yx_1)^2.$$

Now $ab \geq 1$; if $q|xy_1 + yx_1$, this equation implies that $q^2 \geq abq^2$, which can only happen if $a = b = 1$ and

$$axx_1 - byy_1 = 0.$$

That is, $xx_1 - yy_1 = 0$, so $xx_1 = yy_1$. An argument similar to that in the previous case yields $x = y_1$ and $y = x_1$.

We return to the question of which primes can be expressed in the form $x^2 + ny^2$. We begin with the case $n = 1$.

Theorem 4.2 *Let $M \models IE_1$ and let $q \in M$ be an odd prime. Then $q = x^2 + y^2$ for some $x, y \in M \iff \left(\frac{-1}{q}\right) = 1$.*

Proof: ($\Longrightarrow$) Obviously, as remarked earlier.

($\Longleftarrow$) We adapt the proof of Theorem 20 of Gupta [3]. Let $q \in M$ be an odd prime such that $\left(\frac{-1}{q}\right) = 1$. Then for some $u \in M$ such that $u < q$, we have $u^2 + 1 \equiv 0 \, mod \, q$. Therefore $u^2 + 1 = mq$ for some $m \in M$, where $m < q$. Thus the set of elements $m \in M$ such that $M \models \exists u < q \exists v < q (mq = u^2 + v^2)$ is nonempty. Since this set is also clearly E_1-definable, it contains a minimal element m_0. We must show that $m_0 = 1$.

Suppose $m_0 > 1$. We also have $m_0 < q$ because the above set contains an element $m < q$. Choose $x_0, y_0 \in M$ such that $x_0 < q,\ y_0 < q$, and

$$m_0 q = x_0^2 + y_0^2.$$

If $m_0|x_0$ and $m_0|y_0$, then $m_0^2|x_0^2 + y_0^2$ so $m_0|q$; this is impossible since q is prime and $1 < m_0 < q$. Therefore we can find x_1, y_1 such that $0 \leq x_1, y_1 < m_0$ and not both of x_1, y_1 are zero, and such that

$$x_0 \equiv x_1 \, mod \, m_0 \quad and \quad y_0 \equiv y_1 \quad mod \, m_0.$$

We are interested in $x_1^2 + y_1^2 \, mod \, m$, therefore if $x_1 > \frac{1}{2}m_0$ we can replace it by $m_0 - x_1$ without affecting the value of x_1^2 modulo m_0 (and similarly for y_1). Thus we can assume that we have found x_1, y_1 such that $0 \leq x_1, y_1 \leq \frac{1}{2}m_0$ and such that

$$x_1^2 + y_1^2 \equiv x_0^2 + y_0^2 \equiv 0 \, mod \, m_0.$$

The inequalities on x_1, y_1 imply

$$0 < x_1^2 + y_1^2 \leq \frac{1}{2}m_0^2 < m_0^2.$$

Therefore $x_1^2 + y_1^2 = m_1 m_0$ for some $m_1 \in M$ with $0 < m_1 < m_0$. Thus we have:

$$\begin{aligned} m_0^2 m_1 q &= (x_0^2 + y_0^2)(x_1^2 + y_1^2) \\ &= (x_0 x_1 + y_0 y_1)^2 + (x_0 y_1 - x_1 y_0)^2. \end{aligned}$$

(The second term might actually be $x_1y_0 - x_0y_1$, depending on which expression is nonnegative.)

Now modulo m_0, we have

$$x_0x_1 + y_0y_1 \equiv x_1^2 + y_1^2 \equiv 0 \, mod \, m_0 \quad and$$
$$x_0y_1 - x_1y_0 \equiv x_1y_1 - x_1y_1 \equiv 0 \, mod \, m_0.$$

Thus if we let $a = \frac{x_0x_1+y_0y_1}{m_0}$ and $b = \frac{x_0y_1-x_1y_0}{m_0}$ $\left(or \ \frac{x_1y_0-x_0y_1}{m_0}\right)$, we have $m_1q = a^2 + b^2$. Since $m_1 < q$ we have $a, b < q$. But then m_1 contradicts the minimality of m_0. This contradiction shows that $m_0 = 1$.

In $\mathbb{N}$, we have the additional equivalence for odd primes p that $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \ mod \, 4$, so Theorem 4.2 is usually expressed as $p = x^2 + y^2$ for some $x, y \iff p = 2$ or $p \equiv 1 \, mod \, 4$. As we remarked earlier, we do not know if $q \equiv 1 \, mod \, 4 \Longrightarrow \left(\frac{-1}{q}\right) = 1$ for odd primes q in models of IE_1.

In order to deal with other values of n, we need the following identity from [1]:

Proposition 4.3 *The following holds in any commutative ring:*

$$(x^2 + ny^2)(z^2 + nw^2) = (xz + nyw)^2 + n(xw - yz)^2$$
$$= (xz - nyw)^2 + n(xw + yz)^2.$$

We used this identity for $n = 1$ in the previous proof when we rewrote the product $(x_0^2 + y_0^2)(x_1^2 + y_1^2)$.

Now we can extend Theorem 4.2 to the cases $n = 2$ and $n = 3$:

Theorem 4.4 *Let $M \models IE_1$ and let $q \in M$ be a prime $\neq 2, 3$.*

(i) $q = x^2 + 2y^2$ *for some* $x, y \in M \iff \left(\frac{-2}{q}\right) = 1$.

(ii) $q = x^2 + 3y^2$ *for some* $x, y \in M \iff \left(\frac{-3}{q}\right) = 1$.

Proof: (i) We can adapt the proof of Theorem 4.2 here. We have

$$0 < x_1^2 + 2y_1^2 \leq \frac{3}{4}m_0^2 < m_0^2,$$

so $m_1 < m_0$ as before.

(ii) Again the proof of Theorem 4.2 applies, but this time the inequalities for $x_1^2 + 3y_1^2$ yield

$$0 < x_1^2 + 3y_1^2 \leq \frac{1}{4}m_0^2 + \frac{3}{4}m_0^2 = m_0^2,$$

implying $m_1 \leq m_0$. Equality holds only if m_0 is even and $x_1 = y_1 = \frac{1}{2}m_0$. We will show that this cannot happen if m_0 is minimal.

Suppose m_0 is even. Since

$$m_0q = x_0^2 + 3y_0^2$$

and $(x_0, y_0) = 1$ by the minimality of m_0, we must have that x_0 and y_0 are both odd. Therefore

$$m_0q \equiv 1 + 3 \equiv 0 \quad mod \, 4;$$

since q is odd, we conclude that $4|m_0$, say $m_0 = 4m_2$. Thus

$$4m_2q = x_0^2 + 3y_0^2.$$

Since x_0 and y_0 are both odd, there are two possible cases:

(a) Suppose $x_0 \equiv y_0 \, mod \, 4$. Then $4|x_0 + 3y_0$ and $4|x_0 - y_0$ (or $4|y_0 - x_0$). By Proposition 4.3 with $n = 3$, $z = w = 1$, we have

$$(x_0^2 + 3y_0^2) \cdot 4 = (x_0 + 3y_0)^2 + 3(x_0 - y_0)^2.$$

Therefore we conclude that

$$4m_2q = x_0^2 + 3y_0^2 = 4\left[\left(\frac{x_0 + 3y_0}{4}\right)^2 + 3\left(\frac{x_0 - y_0}{4}\right)^2\right]$$

and so we have

$$m_2q = \left(\frac{x_0 + 3y_0}{4}\right)^2 + 3\left(\frac{x_0 - y_0}{4}\right)^2.$$

But then m_2 contradicts the minimality of m_0.

(b) If $x_0 \equiv -y_0 \, mod \, 4$, then $4|x_0 - 3y_0$ (or $4|3y_0 - x_0$, depending on which one is nonnegative) and $4|x_0 + y_0$. This time we use the second formula in Proposition 4.3, i.e.

$$(x_0^2 + 3y_0^2) \cdot 4 = (x_0 - 3y_0)^2 + 3(x_0 + y_0)^2$$

and then continue as before.

We conclude that m_0 must be odd, so $0 < x_1^2 + 3y_1^2 < m_0^2$ and thus $m_1 < m_0$. The rest of the proof now proceeds as in Theorem 4.2.

The previous argument indicates that we will not be able to extend these results much past $n = 3$, because the proof that $m_1 < m_0$ will break down. Note, however, that the result for $n = 4$ is true:

Corollary 4.5 *Let $M \models IE_1$ and let $q \in M$ be an odd prime. Then $q = x^2 + 4y^2$ for some $x, y \in M \iff \left(\frac{-4}{q}\right) = 1$.*

Proof: This is a corollary of Theorem 4.2; for if $q = x^2 + 4y^2$ then q is a sum of two squares. Conversely, if the odd prime q is the sum of two squares $x^2 + y^2$, then one of x, y is even, say $y = 2z$. Thus $q = x^2 + 4z^2$. Similarly, $\left(\frac{-4}{q}\right) = 1 \iff \left(\frac{-1}{q}\right) = 1$.

As for $n = 5$, it is well known that the corresponding result fails even in $\mathbb{N}$. For instance, if we let $q = 7$ then $\left(\frac{-5}{7}\right) = 1$ since $3^2 \equiv -5 \, mod \, 7$, but 7 is not of the form $x^2 + 5y^2$. The correct result for $\mathbb{N}$ is that a prime p has the form $x^2 + 5y^2$ if and only if $p \equiv 1$ or $9 \, mod \, 20$. For a complete characterization of the primes of the form $x^2 + ny^2$ in $\mathbb{N}$, where $n > 0$, see [1].

5 The Equation $x^3 + y^3 = z^3$ In [9] we showed that IE_1 proves that the equation $x^n + y^n = z^n$ has no nontrivial solutions for $n = 4$, 6, and 10. Thus Fermat's last theorem is provable in IE_1 for certain even exponents. In this section we show that the results in Section 3 enable us to prove that Fermat's last theorem for $n = 3$ is provable in IE_2. We do not know if this can be improved to IE_1.

We adapt a proof by Browkin (which in turn is based on one by Carmichael) which appears in [8].

The first result we need is the following:

Lemma 5.1 *Let $M \models IE_2$ and suppose $s, a, b \in M$ are such that s is odd, $(a, b) = 1$, and $s^3 = a^2 + 3b^2$. Then there exist $\alpha, \beta \in M$ of opposite parity such that $(\alpha, 3\beta) = 1$ and*

$$s = \alpha^2 + 3\beta^2,$$
$$a = |\alpha^3 - 9\alpha\beta^2|,$$
$$b = |3\alpha^2\beta - 3\beta^3|.$$

Moreover, if $\alpha, \beta \in M$ are arbitrary satisfying the conditions in the conclusion and s, a, and b are defined as in the conclusion, then s is odd, $(a, b) = 1$, and $s^3 = a^2 + 3b^2$.

Proof: We prove the second part first. Let $M \models IE_2$ and let $\alpha, \beta \in M$ be of opposite parity such that $(\alpha, 3\beta) = 1$. Define s, a, and b as in the conclusion. Since α and β have opposite parity, $s = \alpha^2 + 3\beta^2$ must be odd. Also since the usual properties of g.c.d.'s hold in IE_2, in fact in IE_1 (c.f. [9]), we have that $(a, b) = (\alpha(\alpha^2 - 9\beta^2),\ 3\beta(\alpha^2 - \beta^2)) = (\alpha^2 - 9\beta^2, \alpha^2 - \beta^2)$ because $(\alpha, 3\beta) = 1$, $(\alpha, \alpha^2 - \beta^2) = 1$, and $(3\beta, \alpha^2 - 9\beta^2) = 1$. Now $(\alpha^2 - \beta^2) - (\alpha^2 - 9\beta^2) = 8\beta^2$, $9(\alpha^2 - \beta^2) - (\alpha^2 - 9\beta^2) = 8\alpha^2$, so $(\alpha^2 - 9\beta^2, \alpha^2 - \beta^2)$ divides $(8\alpha^2, 8\beta^2)$. But $(8\alpha^2, 8\beta^2) = 8(\alpha^2, \beta^2) = 8$ since $(\alpha, \beta) = 1$; since α and β have opposite parity, $\alpha^2 - 9\beta^2$ and $\alpha^2 - \beta^2$ are odd, so $(\alpha^2 - 9\beta^2, \alpha^2 - \beta^2) = 1$. We conclude that $(a, b) = 1$.

Finally, a straightforward substitution shows that $s^3 = a^2 + 3b^2$ when s, a, and b are as above.

Now we prove the main direction of the lemma. Suppose the set of counterexamples for s to the lemma is nonempty. The fact that s is such a counterexample can be expressed as:

$$\begin{aligned}
&(\exists a \le s^3)(\exists b \le s^3)\big[s^3 = a^2 + 3b^2 \wedge \\
&(a, b) = 1 \wedge \neg 2|s\big] \wedge \\
\neg&(\exists \alpha \le s)(\exists \beta \le s)\big[s = \alpha^2 + 3\beta^2 \wedge \\
&(a = \alpha^3 - 9\alpha\beta^2 \vee a = 9\alpha\beta^2 - \alpha^3) \\
&\wedge (b = 3\alpha^2\beta - 3\beta^3 \vee b = 3\beta^3 - 3\alpha^2\beta) \\
&\wedge \alpha \not\equiv \beta \bmod 2 \wedge (\alpha, 3\beta) = 1\big].
\end{aligned}$$

This is an E_2-definable set which we are assuming is nonempty; since IE_2 is equivalent to LE_2, it has a least element which we also denote by s. Let $a, b \in M$ be such that the first clause in the above formula is satisfied for this minimal choice of s.

Since s is odd, the smallest possible value it could have is 1, in which case $a = 1$, $b = 0$. But then $\alpha = 1$, $\beta = 0$ contradict the assumption that s is a counterexample. Thus $s > 1$.

It is easy to show in IE_2 (in fact in IE_1) that any $s > 1$ has a prime factor. For the set of factors of s which are greater than 1 is E_1-definable and nonempty, therefore it has a least element, which is then obviously prime. Let q be a prime factor of s. Since s is odd, q is as well. Write $s = qt$.

We show that $3 \nmid s$, thus in particular $q > 3$. If $3|s$ then $3|s^3 = a^2 + 3b^2$, and so $3|a$. Then $9|s^3$ and $9|a^2$, so $3|b$, contradicting the assumption that $(a, b) = 1$. We conclude that $3 \nmid s$.

Since $(a, 3b) = 1$ and $s^3 = a^2 + 3b^2$, then $(s, a) = 1$ and $(s, 3b) = 1$. In particular, $(q, a) = 1$ and $(q, 3b) = 1$. Now $a^2 + 3b^2 \equiv 0 \bmod q$, so $0 \not\equiv a^2 \equiv$

$-3b^2 \bmod q$. Therefore -3 is a quadratic residue for q. By Theorem 4.4 (ii),

$$q = \alpha_1^2 + 3\beta_1^2$$

for some $\alpha_1, \beta_1 \in M$. Clearly α_1 and β_1 have opposite parity and $(\alpha_1, 3\beta_1) = 1$. By the reverse direction of this lemma, which we have already proved, if $c = |\alpha_1^3 - 9\alpha_1\beta_1^2|$ and $d = |3\alpha_1^2\beta_1 - 3\beta_1^3|$, then $(c, d) = 1$ and $q^3 = c^2 + 3d^2$.

For convenience, we continue the argument in R, the ring obtained from M by adjoining negative elements. Thus we will not have to worry that all our expressions are nonnegative. Also, since any or all of a, b, c, or d can be replaced by their negatives, we can drop the absolute value signs in the expressions for these elements.

We claim that $ad - bc$ and $ad + bc$ are not both divisible by q. For

$$(ad - bc)(ad + bc) = (ad)^2 - (bc)^2 = (a^2 + 3b^2)d^2$$
$$-b^2(c^2 + 3d^2) = t^3q^3d^2 - b^2q^3 = q^3(t^3d^2 - b^2).$$

If $q \mid ad - bc$ and $q \mid ad + bc$, then $q \mid 2ad$ and $q \mid 2bc$. Since q is odd, $q \mid ad$ and $q \mid bc$. But $(q, a) = (q, b) = 1$, so $q \mid d$ and $q \mid c$. This contradicts the fact that $(c, d) = 1$.

Thus one of $ad - bc$ or $ad + bc$ is not divisible by q. But

$$(ad - bc)(ad + bc) = q^3(t^3d^2 - b^2).$$

Therefore if $q \nmid ad - bc$ then $q^3 \mid ad + bc$, and if $q \nmid ad + bc$ then $q^3 \mid ad - bc$. Now

$$t^3q^6 = s^3q^3 = (a^2 + 3b^2)(c^2 + 3d^2).$$

By Proposition 4.3,

$$t^3q^6 = (ac \pm 3bd)^2 + 3(ad \mp bc)^2.$$

Choose the signs so that the expression in the second set of parentheses is divisible by q^3. Then the expression in the first set of parentheses is also divisible by q^3, so for the appropriate choice of signs we have

$$u = \frac{ac \pm 3bd}{q^3} \in R$$
$$\text{and} \quad v = \frac{ad \mp bc}{q^3} \in R.$$

It then follows that

$$t^3 = u^2 + 3v^2.$$

We claim that $(u, v) = 1$. For $uc + 3vd = \frac{ac^2 + 3ad^2}{q^3} = a$, $ud - vc = \frac{\pm(3bd^2 + bc^2)}{q^3} = \pm b$ and $(a, b) = 1$. Therefore $(u, v) = 1$ as well.

Now $s = qt$ so $t < s$. Since $t^3 = u^2 + 3v^2$ with $(u, v) = 1$, the fact that s is the *minimal* counterexample to the lemma implies that there exist $\alpha_2, \beta_2 \in M$ such that $\alpha_2 \not\equiv \beta_2 \bmod 2$, $(\alpha_2, 3\beta_2) = 1$, and (replacing α_2, β_2 by their negatives if necessary):

$$t = \alpha_2^2 + 3\beta_2^2,$$
$$u = \alpha_2^3 - 9\alpha_2\beta_2^2,$$
$$v = 3\alpha_2^2\beta_2 - 3\beta_2^3.$$

We now combine our representations for t and q to derive a contradiction to the assumption that s is a counterexample to the lemma. Let

$$\alpha = \alpha_1\alpha_2 + 3\beta_1\beta_2,$$
$$\beta = \alpha_2\beta_1 - \beta_2\alpha_1.$$

Since $\alpha_1 \not\equiv \beta_1 \bmod 2$ and $\alpha_2 \not\equiv \beta_2 \bmod 2$, we have $\alpha \not\equiv \beta \bmod 2$. We have

$$s = qt = (\alpha_1^2 + 3\beta_1^2)(\alpha_2^2 + 3\beta_2^2) = \alpha^2 + 3\beta^2$$

by Proposition 4.3. Also the proof that $(u, v) = 1$ provides formulas for a and b:

$$\begin{aligned} a = uc + 3vd &= (\alpha_2^3 - 9\alpha_2\beta_2^2)(\alpha_1^3 - 9\alpha_1\beta_1^2) \\ &\quad + 3(3\alpha_2^2\beta_2 - 3\beta_2^3)(3\alpha_1^2\beta_1 - 3\beta_1^3) \\ &= \alpha^3 - 9\alpha\beta^2, \\ \pm b = ud - vc &= (\alpha_2^3 - 9\alpha_2\beta_2^2)(3\alpha_1^2\beta_1 - 3\beta_1^3) \\ &\quad - (3\alpha_2^2\beta_2 - 3\beta_2^3)(\alpha_1^3 - 9\alpha_1\beta_1^2) \\ &= 3\alpha^2\beta - 3\beta^3. \end{aligned}$$

Since $\alpha | a$ and $\beta | b$ and since $(a, b) = 1$, we must have $(\alpha, \beta) = 1$. Replacing α, β by $|\alpha|$, $|\beta|$ respectively, we arrive at a contradiction to the assumption that s is a counterexample to the lemma. This completes the proof.

Now we can prove Fermat's last theorem for exponent 3 in IE_2.

Theorem 5.2 $IE_2 \vdash \forall x \forall y \forall z (x^3 + y^3 = z^3 \rightarrow (x = 0 \vee y = 0))$.

Proof: Let $M \models IE_2$ and suppose M contains a nontrivial solution to the equation $x^3 + y^3 = z^3$. Consider the set of elements $m \in M$ satisfying

$$m > 0 \wedge \exists x < m \exists y < m \exists z < m (m = xyz \wedge x^3 + y^3 = z^3).$$

We are assuming this E_1-definable set to be nonempty, therefore it has a least element m. Let $x, y, z \in M$ be such that $m = xyz$ and $x^3 + y^3 = z^3$. Clearly $(x, y) = (x, z) = (y, z) = 1$, for any common divisor of two of them would also divide the third and enable us to produce a smaller solution.

As in the previous lemma, we find it more convenient to continue the argument in the ring R obtained from M by adjoining negative elements. Replacing z by $-z$ in R yields the equation $x^3 + y^3 + z^3 = 0$, which is symmetric in x, y, and z. Clearly at least one of x, y, z is even, and since they are pairwise relatively prime we conclude that *exactly* one of them is even. The aforementioned symmetry enables us to assume that z is even and that x and y are odd. Rewrite the equation as $x^3 + y^3 = z^3$, where now $x, y, z \in R$, all are nonzero, z is even, and x, y are odd.

Thus $x + y$ and $x - y$ are even, say $x + y = 2u$ and $x - y = 2w$. Therefore $x = u + w$, $y = u - w$. Since $(x, y) = 1$ we conclude that $(u, w) = 1$. Also x and y are both odd, so $u \not\equiv w \bmod 2$. Substituting the above expressions for x and y in the equation $x^3 + y^3 = z^3$ yields $(u + w)^3 + (u - w)^3 = z^3$, or $2u(u^2 + 3w^2) = z^3$. We consider two cases, depending on whether or not 3 divides u.

(a) Suppose $3 \nmid u$, so $(3, u) = 1$. Then $(u, u^2 + 3w^2) = 1$, and since $u \not\equiv w \bmod 2$ we have that $u^2 + 3w^2$ is odd. Therefore $(2u, u^2 + 3w^2) = 1$. But

$$2u(u^2 + 3w^2) = z^3,$$

so $2u = t^3$ and $u^2 + 3w^2 = s^3$ for some $s, t \in R$. (This fact is provable in IE_1; cf. [9].) Since $u^2 + 3w^2$ is odd, so is s. By Lemma 5.1, there exist $\alpha, \beta \in R$ such that $u = \alpha^3 - 9\alpha\beta^2$, $\alpha \not\equiv \beta \, mod \, 2$, and $(\alpha, 3\beta) = 1$. Then

$$t^3 = 2u = 2\alpha(\alpha - 3\beta)(\alpha + 3\beta).$$

Now $\alpha - 3\beta$ and $\alpha + 3\beta$ are odd and $(\alpha, 3\beta) = 1$, so the three elements 2α, $\alpha - 3\beta$, and $\alpha + 3\beta$ are pairwise relatively prime. Therefore there exist σ, τ, and ρ in R such that $2\alpha = \sigma^3$, $\alpha - 3\beta = \tau^3$, and $\alpha + 3\beta = \rho^3$, and where $t = \sigma\tau\rho$. But then

$$\sigma^3 = \tau^3 + \rho^3$$

is a solution to the equation of the theorem, where $|\sigma\tau\rho|^3 = |t^3| = |2u| = |x + y| < |xyz|^3$, contradicting the minimality of $|xyz|$.

Actually we must justify this by showing that $|\sigma\tau\rho| > 0$. But $|\sigma\tau\rho| = |x + y|$; if $|x + y| = 0$ then $x = -y$, in which case $z = 0$ which contradicts our assumptions on x, y, z.

(b) Suppose $3|u$, say $u = 3v$. Substituting for u in the equation $2u(u^2 + 3w^2) = z^3$, we have

$$6v(9v^2 + 3w^2) = z^3, \quad or$$
$$18v(3v^2 + w^2) = z^3.$$

Now $u \not\equiv w \, mod \, 2$ so $v \not\equiv w \, mod \, 2$. Therefore $3v^2 + w^2$ is odd. Also $(u, w) = (3v, w) = 1$, so we conclude that $(18v, 3v^2 + w^2) = 1$. Thus $18v = t^3$ and $3v^2 + w^2 = s^3$ for some $s, t \in R$. Now s is odd because v and w have opposite parity. Also $(v, w) = 1$, so by Lemma 5.1 there exist $\alpha, \beta \in R$ such that $w = \alpha^3 - 9\alpha\beta^2$, $v = 3\alpha^2\beta - 3\beta^3$, $\alpha \not\equiv \beta \, mod \, 2$, and $(\alpha, 3\beta) = 1$. Since $18v = t^3$, we have

$$18(3\beta)(\alpha^2 - \beta^2) = t^3, \quad or$$
$$27 \cdot 2\beta(\alpha + \beta)(\alpha - \beta) = t^3.$$

Now $\alpha + \beta$ and $\alpha - \beta$ are both odd and $(\alpha, \beta) = 1$, so 2β, $\alpha + \beta$, and $\alpha - \beta$ are pairwise relatively prime. Therefore there exist σ, τ, and ρ in R such that $2\beta = \sigma^3$, $\alpha + \beta = \tau^3$, and $\alpha - \beta = \rho^3$, and where $t = 3\sigma\tau\rho$. But then

$$\sigma^3 = \tau^3 + \rho^3$$

is a solution to the equation of the theorem, where $|3\sigma\tau\rho|^3 = |t^3| = |18v| = |6u| = 3|x + y| < 3|xyz|^3$. In particular, $|\sigma\tau\rho| < |xyz|$, and $|\sigma\tau\rho| > 0$ as in case (a). We have thus contradicted the minimality of $|xyz|$.

6 Open questions

Question 5.1 Does IE_1 prove that if $q \equiv 1 \, mod \, 4$ is prime then $\left(\frac{-1}{q}\right) = 1$? Is this provable in $I\Delta_0$?

Question 5.2 Is the converse to Theorem 3.11 provable in IE_1 or in $I\Delta_0$? Can anything be said about the case when p and q are both nonstandard?

Question 5.3 Does IE_1 (or $I\Delta_0$) prove that if $m \equiv 5 \, mod \, 8$ then -1 has no fourth root modulo m? More generally, if $m = 2^r \cdot s$ with s odd and r finite, then -1 has no 2^r-th root modulo m?

Question 5.4 What can be said about primes of the form $x^2 + ny^2$ for $n > 4$ in IE_1?

Question 5.5 Can Fermat's last theorem for exponent 3 be proved in IE_1?

Question 5.6 Does IE_2 prove other cases of Fermat's last theorem for odd exponents?

REFERENCES

[1] Cox, D., *Primes of the Form* $x^2 + ny^2$, John Wiley & Sons, New York, 1989.

[2] van den Dries, L., "Some model theory and number theory for models of weak systems of arithmetic," pp. 346–362 in *Model Theory of Algebra and Arithmetic*, edited by L. Pacholski, Lecture Notes in Mathematics 834, Springer, Berlin, 1980.

[3] Gupta, H., *Selected Topics in Number Theory*, Abacus Press, London, 1980.

[4] Kaye, R., "Diophantine and parameter-free induction," Ph.D. dissertation, Manchester University, 1987.

[5] Macintyre, A. and D. Marker, "Primes and their residue rings in models of open induction," *Annals of Pure and Applied Logic*, vol. 43 (1989), pp. 57–77.

[6] Paris, J. and A. Wilkie, "Δ_0 sets and induction", pp. 237–248 in *Open Days in Model Theory and Set Theory*, edited by W. Guzicki, Proceedings of the Jadwisin, Poland, Logic Conference 1981, Leeds University, 1983 .

[7] Shepherdson, J. C., "A nonstandard model for a free variable fragment of number theory," *Bull. Acad. Polon. Sci.*, vol. 12 (1964), pp. 79–86.

[8] Sierpinski, W., *Elementary Theory of Numbers*, Panstwowe Wydawnictwo Naukowe, Warszawa, 1964.

[9] Smith, S. T., "Fermat's last theorem and Bezout's theorem in GCD domains," *Journal of Pure and Applied Algebra*, vol. 79 (1992), pp. 63–85.

[10] Smith, S. T., "On the diophantine equation $x^{10} \pm y^{10} = z^2$," *Journal of Pure and Applied Algebra*, vol. 79 (1992), pp. 87–108.

[11] Smith, S. T., "Building discretely ordered Bezout domains and GCD Domains," forthcoming in *Journal of Algebra*.

[12] Smith, S. T., "Prime numbers and factorization in IE_1 and weaker systems," *Journal of Symbolic Logic*, vol. 57, (1992), pp. 1057–1085.

[13] Wilkie, A., "Some results and problems on weak systems of arithmetic," pp. 285–296 in *Logic Colloquium '77*, edited by A. J. Macintyre, North–Holland, Amsterdam, 1978.

[14] Wilmers, G., "Bounded existential induction," *The Journal of Symbolic Logic*, vol. 50, (1985), pp. 72–90.

Raymond and Beverly Sackler Faculty of Exact Sciences
School of Mathematical Sciences
Tel Aviv University
Ramat-Aviv, 69978 Israel