# Automating elementary number-theoretic proofs using Gröbner bases

John Harrison

Intel Corporation, JF1-13
2111 NE 25th Avenue, Hillsboro OR 97124, USA
johnh@ichips.intel.com

**Abstract.** We present a uniform algorithm for proving automatically a fairly wide class of elementary facts connected with integer divisibility. The assertions that can be handled are those with a limited quantifier structure involving addition, multiplication and certain number-theoretic predicates such as 'divisible by', 'congruent' and 'coprime'; one notable example in this class is the Chinese Remainder Theorem (for a specific number of moduli). The method is based on a reduction to ideal membership assertions that are then solved using Gröbner bases. As well as illustrating the usefulness of the procedure on examples, and considering some extensions, we prove a limited form of completeness for properties that hold in all rings.

## 1 Introduction

Various classes of mathematical problems, when expressed in formal logic, can be solved automatically by suitable algorithms. This is often valuable, if only for dealing with relatively uninteresting subtasks of larger formal proofs. Some algorithms implement decision procedures for theories or logical fragments known to be decidable, such as Cooper's algorithm [7] for Presburger arithmetic [17]. Others are more heuristic in nature, e.g. automated induction proofs employing conjecture generalization [4], though many of these can be understood in a general framework of proof planning [6].

Here we present a new algorithm for a useful class of elementary number-theoretic properties. We will introduce and motivate the procedure by focusing on the integers $\mathbb{Z}$, though we will see later that the procedure is only complete for properties that hold in the class of *all* rings. (Thus it is perhaps neither a heuristic method nor a decision procedure, but rather a heuristic application *of* a decision procedure outside its domain of completeness.) The formulas that can be handled are expressed in a first-order language. The terms can be built up using integer constants, negation, addition, subtraction and multiplication, as well as exponentiation with constant nonnegative exponents. (For example, $2x^2 - y^3(w - 42z)^9$ is allowed, but not $x^y$.) The formulas can be built from these terms using the equality symbol as well as three 'divisibility' relationships, all of which we consider as mere shorthands for other formulas using equality as the only predicate:

– $s \mid t$, read '$s$ divides $t$' abbreviates $\exists d.\, t = sd$
– $s \equiv t \pmod{u}$, read '$s$ is congruent to $t$ modulo $u$', abbreviates $\exists d.\, t - s = ud$
– coprime$(s, t)$, read '$s$ and $t$ are coprime', abbreviates $\exists x\ y.\ sx + ty = 1$.

Over the integers, coprime$(m, n)$ holds precisely if $m$ and $n$ have no common factors besides $\pm 1$. This equivalence is proved in many elementary number theory texts [2, 8].

We attempt to explain any algebraic terminology as it is used, but a reader may find it helpful to refer to an algebra textbook such as [21] for more on rings, polynomials and ideals. It is worth noting that we tend to blur the distinction between three distinct notions of 'polynomial': (i) a first-order formula in the language of rings, (ii) a polynomial itself as an algebraic object, and (iii) a polynomial function or its evaluation for a specific argument. When we want to emphasize the polynomial as a function we tend to write the arguments (so $p(\overline{x})$ rather than just $p$), and when treating it as an element of the ring of polynomials we tend to omit arguments, and perhaps emphasize that equations are to be understood as polynomial identities. Sometimes, however, we write the arguments just to emphasize which variables are involved in the polynomial. Over an infinite base ring such as $\mathbb{Z}$, two polynomials are equal as algebraic objects ($p = q$) if and only if the associated functions are equal on all arguments ($\forall \overline{x}.\, p(\overline{x}) = q(\overline{x})$). By contrast, over a 2-element ring the polynomials $x^2 + x$ and 0 are considered distinct even though they determine the same function.

## 2 Example

We will explain the procedure by a typical example first, proving this 'cancellation' property for congruences:

$$\forall a\ n\ x\ y.\ ax \equiv ay \pmod{n} \wedge \text{coprime}(a, n) \Rightarrow x \equiv y \pmod{n}$$

The first step is to expand away the number-theoretic predicates:

$$\begin{aligned} \forall a\ n\ x\ y.\ & (\exists d.\, ay - ax = nd) \wedge \\ & (\exists u\ v.\, au + nv = 1) \\ & \Rightarrow (\exists e.\, y - x = ne) \end{aligned}$$

and we then pull out the existential quantifiers in the antecedent:

$$\forall a\ n\ x\ y\ d\ u\ v.\, ay - ax = nd \wedge au + nv = 1 \Rightarrow \exists e.\, y - x = ne$$

We prove this by proving something related, but in general stronger, namely that over the ring $\mathbb{Z}[a, n, x, y, d, u, v]$ the polynomial $y - x$ is contained in the ideal generated by the polynomials in the antecedent ($ay - ax - nd$ and $au + nv - 1$) and the multiplier ($n$) for the existentially quantified variable:

$$(y - x) \in \text{Id}\,\langle ay - ax - nd, au + nv - 1, n\rangle$$

i.e. that there exist 'cofactor' polynomials $p(a,n,x,y,d,u,v)$, $q(a,n,x,y,d,u,v)$ and $r(a,n,x,y,d,u,v)$ such that the following is a polynomial identity:

$$\begin{aligned} y - x = {} & (ay - ax - nd)p(a,n,x,y,d,u,v) + \\ & (au + nv - 1)q(a,n,x,y,d,u,v) + \\ & nr(a,n,x,y,d,u,v) \end{aligned}$$

To see that the identity implies the original claim, note that if $ay - ax = nd$ and $au + nv = 1$, the identity reduces to $y - x = nr(a,n,x,y,d,u,v)$, which certainly implies $\exists e.\ y - x = ne$. In fact, it shows something stronger: there is a polynomial expression for the witness $e$ in terms of the other variables.

To prove the ideal membership goal, the most natural and straightforward technique is to apply Buchberger's algorithm [5] to find a Gröbner basis for the ideal, and then show that $y - x$ reduces to 0 w.r.t. this basis. A suitably instrumented version of the algorithm can actually produce the explicit cofactor polynomials, giving a simple 'certificate' of the result. For our example, one natural possibility for the cofactors is:

$$\begin{aligned} p(a,n,x,y,d,u,v) &= u \\ q(a,n,x,y,d,u,v) &= x - y \\ r(a,n,x,y,d,u,v) &= ud + vy - vx \end{aligned}$$

We can then verify the polynomial identity simply by normalizing both sides in some reasonable way.

## 3 Detailed procedure

We aim to reduce the initial problem to one or more sub-problems of the following standard form, where the $e_i(\overline{x})$, $a_i(\overline{x})$ and $p_{ij}(\overline{x})$ are polynomials in variables $\overline{x} = x_1, \ldots, x_l$:

$$\begin{aligned} \forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \exists y_1\ \cdots\ y_n.\ & p_{11}(\overline{x})y_1 + \cdots + p_{1n}(\overline{x})y_n = a_1(\overline{x}) \wedge \\ & \cdots \wedge \\ & p_{k1}(\overline{x})y_1 + \cdots + p_{kn}(\overline{x})y_n = a_k(\overline{x}) \end{aligned}$$

We need to test whether this formula holds over the integers, and we do it by testing the following ideal membership problem in $\mathbb{Z}[x_1, \ldots, x_l, u_1, \ldots, u_k]$, where the $u_i$ are fresh variables not occurring in the original problem:

$$\begin{aligned} & (a_1u_1 + \cdots + a_ku_k) \\ & \in \mathrm{Id}\,\langle e_1, \ldots, e_m, (p_{11}u_1 + \cdots + p_{k1}u_k), \ldots (p_{1n}u_1 + \cdots + p_{kn}u_k)\rangle \end{aligned}$$

(Note that we are considering *integer* polynomials only in the ideal membership.) In the common special case $k = 1$, as in the example of the previous section, we do not need to introduce the auxiliary variables, but can use simply:

$$a_1 \in \mathrm{Id}\,\langle e_1, \ldots, e_m, p_{11}, \ldots, p_{1n}\rangle$$

**Incompleteness over the integers**

The standard problem above takes in the degenerate case ($n = 0$ and $k = 0$) of proving that a Diophantine equation has no solutions over the integers: $\forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \bot$. Since this is known to be undecidable [16] while ideal membership over the integers is decidable [1] it follows that our test based on ideal membership cannot be both sound and complete. And indeed, it is not hard to find examples of incompleteness, where the existential assertion holds over $\mathbb{Z}$ but the corresponding ideal membership does not. The following are all variations on a theme that $x^2 + x$ is always even:

- $\forall x.\ \exists a.\ x^2 + x = 2a$ holds over the integers, yet $(x^2 + x) \notin \mathrm{Id}\,\langle 2 \rangle$.
- $\forall x\ y.\ y = 1 \Rightarrow \exists a.\ x^2 + x = (y + 1)a$ holds over the integers, yet $(x^2 + x) \notin \mathrm{Id}\,\langle y - 1, y + 1 \rangle$
- $\forall x\ y.\ \exists a\ b.\ x^2 + x = (y + 1)a + (y - 1)b$ yet $(x^2 + x) \notin \mathrm{Id}\,\langle y - 1, y + 1 \rangle$

Nevertheless, we will show (i) that our procedure is sound, and (ii) that it is complete for properties that hold in *all rings*, not just in the integers.

**Soundness**

Consider first the special case $k = 1$, when we just test

$$a_1 \in \mathrm{Id}\,\langle e_1, \ldots, e_m, p_{11}, \ldots, p_{1n} \rangle$$

If this ideal membership assertion holds, then concretely there are cofactor polynomials $f_1, \ldots, f_m, g_1, \ldots, g_n$ such that

$$e_1 f_1 + \cdots + e_m f_m + p_{11} g_1 + \cdots + p_{1n} g_n = a_1$$

Evaluating when $\bigwedge_{i=1}^{m} e_i(\overline{x}) = 0$ we get

$$p_{11}(\overline{x}) g_1(\overline{x}) + \cdots + p_{1n}(\overline{x}) g_n(\overline{x}) = a_1(\overline{x})$$

which does indeed show that there exist $y_1, \ldots, y_n$ such that

$$p_{11}(\overline{x}) y_n + \cdots + p_{1n}(\overline{x}) y_n = a_1(\overline{x})$$

and from the cofactors in the ideal membership, we obtain a simple and explicit proof of the original formula, with witnesses for the existentially quantified variables that are polynomials in the other variables. In the general case (not requiring $k = 1$), suppose that the ideal membership holds:

$$\begin{array}{l} (a_1 u_1 + \cdots + a_k u_k) \\ \in \mathrm{Id}\,\langle e_1, \ldots, e_m, (p_{11} u_1 + \cdots + p_{k1} u_k), \ldots, (p_{1n} u_1 + \cdots + p_{kn} u_k) \rangle \end{array}$$

which means explicitly we have a polynomial identity of the form:

$$\begin{array}{l} (a_1 u_1 + \cdots + a_k u_k) = \\ e_1(\overline{x}) r_1(\overline{x}, \overline{u}) + \cdots + e_m(\overline{x}) r_m(\overline{x}, \overline{u}) + \\ (p_{11} u_1 + \cdots + p_{k1} u_k) q_1(\overline{x}, \overline{u}) + \cdots + (p_{1n} u_1 + \cdots + p_{kn} u_k) q_n(\overline{x}, \overline{u}) \end{array}$$

with the $q_i$ and $r_i$ polynomials in $\mathbb{Z}[x_1, \ldots, x_l, u_1, \ldots, u_k]$. Let us separate each $q_i(\overline{x}, \overline{u})$ into:

$$q_i(\overline{x}, \overline{u}) = c_i(\overline{x}) + d_i(\overline{x}, \overline{u})$$

where $c_i(\overline{x})$ does not involve any of the $u_i$, and all monomials in $d_i(\overline{x}, \overline{u})$ contain at least one of the $u_i$. Similarly we decompose $r_i(\overline{x}, \overline{u})$ into:

$$r_i(\overline{x}, \overline{u}) = s_i(\overline{x}, \overline{u}) + t_i(\overline{x}, \overline{u})$$

where each monomial in $s_i(\overline{x}, \overline{u})$ has degree 1 in exactly one of the $u_i$ (e.g. $3u_1$ or $x_5^2 u_2$) and each monomial in $t_i(\overline{x}, \overline{u})$ either does not involve any $u_i$, involves more than one, or has a degree higher than 1 in one of them (e.g. 42, $7u_1u_2$, $xu_3^2$). Now:

$$\begin{array}{l}(a_1u_1 + \cdots + a_ku_k) = \\ e_1(\overline{x})s_1(\overline{x}, \overline{u}) + \cdots + e_m(\overline{x})s_m(\overline{x}, \overline{u}) + \\ e_1(\overline{x})t_1(\overline{x}, \overline{u}) + \cdots + e_m(\overline{x})t_m(\overline{x}, \overline{u}) + \\ (p_{11}u_1 + \cdots + p_{k1}u_k)c_1(\overline{x}) + \cdots + (p_{1n}u_1 + \cdots + p_{kn}u_k)c_n(\overline{x}) + \\ (p_{11}u_1 + \cdots + p_{k1}u_k)d_1(\overline{x}, \overline{u}) + \cdots + (p_{1n}u_1 + \cdots + p_{kn}u_k)d_n(\overline{x}, \overline{u})\end{array}$$

Note that all terms on the LHS have degree exactly 1 in just one of the $u_i$. Thus all terms on the right that are not of that form must cancel, leaving:

$$\begin{array}{l}(a_1u_1 + \cdots + a_ku_k) = \\ e_1(\overline{x})s_1(\overline{x}, \overline{u}) + \cdots + e_m(\overline{x})s_m(\overline{x}, \overline{u}) + \\ (p_{11}u_1 + \cdots + p_{k1}u_k)c_1(\overline{x}) + \cdots + (p_{1n}u_1 + \cdots + p_{kn}u_k)c_n(\overline{x})\end{array}$$

Evaluating when $\bigwedge_{i=1}^{m} e_i(\overline{x}) = 0$ gives:

$$\begin{array}{l}(a_1u_1 + \cdots + a_ku_k) = \\ (p_{11}u_1 + \cdots + p_{k1}u_k)c_1(\overline{x}) + \cdots + (p_{1n}u_1 + \cdots + p_{kn}u_k)c_n(\overline{x})\end{array}$$

Successively setting $u_i = 1$ and $u_j = 0$ for all $j \neq i$, we find that for all $1 \leq i \leq k$ the following holds:

$$a_i = c_1(\overline{x})p_{i1}(\overline{x}) + \cdots + c_n(\overline{x})p_{in}(\overline{x})$$

which does indeed show that there exist $y_1, \ldots, y_n$ such that

$$\begin{array}{l}p_{11}(\overline{x})y_1 + \cdots + p_{1n}(\overline{x})y_n = a_1(\overline{x}) \wedge \\ \cdots \wedge \\ p_{k1}(\overline{x})y_1 + \cdots + p_{kn}(\overline{x})y_n = a_k(\overline{x})\end{array}$$

and once again we obtain explicit polynomials $y_i = c_i(\overline{x})$ as witnesses.

**Completeness over all rings**

We will now prove that the ideal membership assertion is equivalent to *the validity of the starting formula in all rings* (as usual, we mean commutative rings with 1). The reasoning in the previous section extends easily from $\mathbb{Z}$ to an arbitrary ring, showing that the ideal membership implies the validity of the starting formula in all rings. To establish the other direction, we first recall that a *Horn clause* is a first-order formula that is either of the form:

$$\forall v_1, \ldots, v_n.\, P_1[v_1, \ldots, v_n] \wedge \cdots \wedge P_n[v_1, \ldots, v_n] \Rightarrow Q[v_1, \ldots, v_n]$$

including the degenerate case

$$\forall v_1, \ldots, v_n.\, Q[v_1, \ldots, v_n]$$

or

$$\forall v_1, \ldots, v_n.\, P_1[v_1, \ldots, v_n] \wedge \cdots \wedge P_n[v_1, \ldots, v_n] \Rightarrow \bot$$

where $Q[v_1, \ldots, v_n]$ and all $P_i[v_1, \ldots, v_n]$ are atomic formulas. In particular, the axioms for commutative rings with 1 are just (implicitly universally quantified) equations, and are therefore Horn clauses. In fact, all truly *algebraic* axioms are just universally quantified equations, and thus Horn clauses. For example, we can add the infinite set of axioms $x^k = 0 \Rightarrow x = 0$ for all $k \geq 1$ to axiomatize the class of *reduced* rings (rings without nilpotent elements). However neither the integral domain axiom $xy = 0 \Rightarrow x = 0 \vee y = 0$ nor the field axiom $\neg(x = 0) \Rightarrow x^{-1}x = 1$ is a Horn clause, and so the special results we will note for Horn clause theories are not directly applicable, though analogous results can be derived for general theories by considering canonical resolution proofs [14].

In order to state these special properties of Horn clause theories, it is more convenient to consider first-order logic without special treatment of equality. By a standard result [13], a formula is valid in first-order logic with equality iff it is a general first-order consequence of the set of equivalence and congruence properties of equality for the language at issue. In particular, a formula holds in all rings iff it is a first-order consequence of the following axioms, all of which are Horn clauses:

$$\begin{aligned}
&x + y = y + x \\
&x + (y + z) = (x + y) + z \\
&x + 0 = x \\
&x + (-x) = 0 \\
&xy = yx \\
&x(yz) = (xy)z \\
&x1 = x \\
&x(y + z) = xy + xz \\
&x = x \\
&x = y \Rightarrow y = x \\
&x = y \wedge y = z \Rightarrow x = z \\
&x = x' \Rightarrow -x = -x' \\
&x = x' \wedge y = y' \Rightarrow x + y = x' + y' \\
&x = x' \wedge y = y' \Rightarrow xy = x'y'
\end{aligned}$$

If $\Gamma$ is a set of Horn clauses and $A$ an atomic formula or $\bot$, then $\Gamma \vdash A$ if and only if there is a 'Prolog-style' proof of $A$ from $\Gamma$, i.e. a tree whose nodes are atomic formulas, with $A$ as the top node, such that for every node $B$ in the tree, there is a clause in the axiom set that can be instantiated so its conclusion is $B$ and its antecedent atoms are the nodes below $B$ in the tree [10]. This special canonical proof format for deductions from Horn clauses allows us to deduce some interesting consequences. We start with a theorem due to Simmons [19, 12, 21]:

**Theorem 1.** *Let $p_1(\overline{x})$, ..., $p_r(\overline{x})$ and $p(\overline{x})$ be polynomials with integer coefficients over the variables $\overline{x} = x_1, \ldots, x_l$. Then the following holds in all commutative rings with 1:*

$$\forall x_1, \ldots, x_l.\, p_1(\overline{x}) = 0 \wedge \cdots \wedge p_r(\overline{x}) = 0 \Rightarrow p(\overline{x}) = 0$$

*iff the following ideal membership holds over $\mathbb{Z}[\overline{x}]$:*

$$p \in Id\langle p_1, \ldots, p_r \rangle$$

*in other words, if there are cofactor polynomials $q_1(\overline{x})$, ..., $q_r(\overline{x})$ with integer coefficients such that the following is a polynomial identity:*

$$p(\overline{x}) = p_1(\overline{x})q_1(\overline{x}) + \cdots + p_r(\overline{x})q_r(\overline{x})$$

*Proof. (Sketch.) The bottom-to-top direction is immediate, because given that identity, the right-hand side collapses to zero when all the $p_i(\overline{x})$ are zero. Conversely, if the top result holds in all rings, then there is a Prolog-style proof from the Horn clause axioms for rings and equality. By induction on this tree, for every equation $s(\overline{x}) = t(\overline{x})$ deduced, $s(\overline{x}) - t(\overline{x})$ is in the ideal generated by $p_1, \ldots, p_r$.* □

The following is essentially Theorem 7.0.6 ("Horn-Herbrand theorem") in [10]. It states that for deduction from Horn clauses we can strengthen the usual classical Herbrand theorem to one with the same 'existence property' as in intuitionistic logic:

**Theorem 2.** *Let $T$ be a set of Horn clauses and $A_i[y_1, \ldots, y_n]$ atomic formulas (in a language with at least one individual constant). Then*

$$T \models \exists y_1, \ldots, y_n.\, A_1[y_1, \ldots, y_n] \wedge \cdots \wedge A_k[y_1, \ldots, y_n]$$

*(where '$\Gamma \models P$' means '$P$ is a first-order consequence of $\Gamma$') if and only if there are ground terms $t_1, \ldots, t_n$ in the language such that:*

$$T \models A_1[t_1, \ldots, t_n] \wedge \cdots \wedge A_k[t_1, \ldots, t_n]$$

*Proof. (Sketch.) The bottom-to-top direction is immediate. For the other direction, note that the top is equivalent to*

$$T \cup \{(\forall y_1, \ldots, y_n.\, A_1[y_1, \ldots, y_n] \wedge \cdots \wedge A_k[y_1, \ldots, y_n] \Rightarrow \bot)\} \models \bot$$

*The usual 'Prolog style' backchaining proof for Horn clauses can only apply the extra clause once, and will give rise to the corresponding instantiation.* □

Thus we can deduce a corollary:

**Theorem 3.** *The following formula:*

$$\forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \exists y_1\ \cdots\ y_n.\ \begin{array}{l} p_{11}(\overline{x})y_1 + \cdots + p_{1n}(\overline{x})y_n = a_1(\overline{x}) \wedge \\ \cdots \wedge \\ p_{k1}(\overline{x})y_1 + \cdots + p_{kn}(\overline{x})y_n = a_k(\overline{x}) \end{array}$$

*holds in all rings iff there are terms $q_1(\overline{x}),\ldots,q_n(\overline{x})$ in the language of rings (i.e. polynomials with integer coefficients) such that the following holds in all rings:*

$$\forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \begin{array}{l} p_{11}(\overline{x})q_1(\overline{x}) + \cdots + p_{1n}(\overline{x})q_n(\overline{x}) = a_1(\overline{x}) \wedge \\ \cdots \wedge \\ p_{k1}(\overline{x})q_1(\overline{x}) + \cdots + p_{kn}(\overline{x})q_n(\overline{x}) = a_k(\overline{x}) \end{array}$$

*Proof.* *We can replace the variables $\overline{x}$ by constants, and regard the $e_i(\overline{x})$ as new (Horn) axioms. The result is then an immediate consequence of Theorem 2 and the Horn nature of the ring and equality axioms.* □

This leads us to the following:

**Theorem 4.** *The following formula:*

$$\forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \exists y_1\ \cdots\ y_n.\ \begin{array}{l} p_{11}(\overline{x})y_1 + \cdots + p_{1n}(\overline{x})y_n = a_1(\overline{x}) \wedge \\ \cdots \wedge \\ p_{k1}(\overline{x})y_1 + \cdots + p_{kn}(\overline{x})y_n = a_k(\overline{x}) \end{array}$$

*holds in all rings iff there are terms $q_1(\overline{x}),\ldots,q_n(\overline{x})$ and $r_{1j}(\overline{x}),\ldots,r_{mj}(\overline{x})$ in the language of rings (i.e. polynomials with integer coefficients) such that the following is a polynomial identity for each $j$ with $1 \leq j \leq k$:*

$$e_1(\overline{x})r_{1j}(\overline{x}) + \cdots + e_m(\overline{x})r_{mj}(\overline{x}) + p_{j1}(\overline{x})q_1(\overline{x}) + \cdots + p_{jn}(\overline{x})q_n(\overline{x}) = a_j(\overline{x})$$

*Proof.* *Just combine the previous theorem and Theorem 1.* □

The case $k = 1$ takes a particularly simple form, which was used in the motivating example of the previous section:

**Theorem 5.** *The formula:*

$$\forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \exists y_1\ \cdots\ y_n.\ p_1(\overline{x})y_1 + \cdots + p_n(\overline{x})y_n = a(\overline{x})$$

*holds in all rings iff the following ideal membership holds for integer polynomials:*

$$a \in Id\langle e_1, \ldots, e_m, p_1, \ldots, p_n \rangle$$

*Proof.* *Just a special case of the previous theorem.* □

The conclusion of Theorem 4 for general $k$ is not just a conjunction of independent ideal membership assertions, because we need to constrain the cofactors $q_i(\overline{x})$ to be the same for each one. However, by introducing auxiliary variables $u_1, \ldots, u_k$ we will show:

**Theorem 6.** *The following formula:*

$$\forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \exists y_1\ \cdots\ y_n.\ \begin{array}{l} p_{11}(\overline{x})y_1 + \cdots + p_{1n}(\overline{x})y_n = a_1(\overline{x}) \wedge \\ \cdots \wedge \\ p_{k1}(\overline{x})y_1 + \cdots + p_{kn}(\overline{x})y_n = a_k(\overline{x}) \end{array}$$

*holds in all rings iff the following ideal membership assertion, where the $u_i$ are fresh variables not occurring in the original problem, holds in $\mathbb{Z}[x_1, \ldots, x_l, u_1, \ldots, u_k]$:*

$$\begin{array}{l} (a_1u_1 + \cdots + a_ku_k) \\ \in Id\langle e_1, \ldots, e_m, (p_{11}u_1 + \cdots + p_{k1}u_k), (p_{1n}u_1 + \cdots + p_{kn}u_k)\rangle \end{array}$$

*Proof. The bottom-to-top direction was dealt with above under 'soundness'. For the other direction, note that by Theorem 4, the initial assertion is equivalent to the existence of $q_1(\overline{x}),\ldots,q_n(\overline{x})$ and $r_{1j}(\overline{x}),\ldots,r_{mj}(\overline{x})$ such that for all $1 \leq j \leq k$:*

$$e_1(\overline{x})r_{1j}(\overline{x}) + \cdots + e_m(\overline{x})r_{mj}(\overline{x}) + p_{j1}(\overline{x})q_1(\overline{x}) + \cdots + p_{jn}(\overline{x})q_n(\overline{x}) = a_j(\overline{x})$$

*Multiplying this identity by $u_j$ and summing over $1 \leq j \leq k$ we obtain*

$$\begin{array}{l} a_1u_1 + \cdots + a_ku_k = \\ e_1(\overline{x})(u_1r_{11}(\overline{x}) + \cdots + u_kr_{1k}(\overline{x})) + \cdots + \\ e_m(\overline{x})(u_1r_{m1}(\overline{x}) + \cdots + u_kr_{mk}(\overline{x})) + \\ (p_{11}u_1 + \cdots + p_{k1}u_k)q_1(\overline{x}) + \cdots + (p_{1n}u_1 + \cdots + p_{kn}u_k)q_n(\overline{x}) \end{array}$$

*which verifies the claimed ideal membership.* □

## 4 Reduction to standard form

In reducing the initial problem to standard form, we expand the number-theoretic predicates into existentially quantified equations. Note that the equivalence assumed between $\exists x\ y.\ sx + ty = 1$ and coprime$(s, t)$, in the usual sense of having no non-unit common factors, does not hold over an arbitrary ring (though it does in all principal ideal domains). For example, $x + 1$ and 2 are coprime over the polynomial ring $\mathbb{Z}[x]$, but there are no integer polynomials $p$ and $q$ such that $(x + 1)p(x) + 2q(x) = 1$. This means that even though the core reduction is complete w.r.t. the class of all rings, the initial processing into standard form relies on additional axioms. Moreover, we will sometimes want to exploit the integral domain property $st = 0 \Leftrightarrow s = 0 \vee t = 0$ (see below), which also fails in an arbitrary ring (e.g. $2 \cdot 3 = 0$ in $\mathbb{Z}/6$ but $2 \neq 0$ and $3 \neq 0$). This mismatch between a preprocessing step valid only in certain rings and a core procedure sound

and complete with respect to *all* rings gives our overall procedure a somewhat heuristic flavour.

But once we accept the mappings of the basic concepts down to algebraic statements, then we can translate a wide variety of assertions into the standard form. In particular, any Horn clause built up from the basic number-theoretic concepts works, e.g. our first example:

$$ax \equiv ay \pmod{n} \wedge \mathrm{coprime}(a, n) \Rightarrow x \equiv y \pmod{n}$$

as well as numerous others such as

$$\begin{array}{l}
d|a \wedge d|b \Rightarrow d|(a - b) \\
a|b \Rightarrow (ca)|(cb) \\
x|y \wedge y|z \Rightarrow x|z \\
(xd)|a \Rightarrow d|a \\
a|b \wedge c|d \Rightarrow (ac)|(bd) \\
\mathrm{coprime}(d, a) \wedge \mathrm{coprime}(d, b) \Rightarrow \mathrm{coprime}(d, ab) \\
\mathrm{coprime}(d, ab) \Rightarrow \mathrm{coprime}(d, a) \\
m|r \wedge n|r \wedge \mathrm{coprime}(m, n) \Rightarrow (mn)|r \\
x \equiv x' \pmod{n} \wedge y \equiv y' \pmod{n} \Rightarrow xy \equiv x'y' \pmod{n} \\
x \equiv y \pmod{m} \wedge n|m \Rightarrow x \equiv y \pmod{n} \\
\mathrm{coprime}(a, b) \wedge x \equiv y \pmod{a} \wedge x \equiv y \pmod{b} \Rightarrow x \equiv y \pmod{(ab)} \\
x^2 \equiv y^2 \pmod{(x + y)} \\
x^2 \equiv a \pmod{n} \wedge y^2 \equiv a \pmod{n} \Rightarrow n|((x + y)(x - y))
\end{array}$$

It is also clear we can solve problems of the form $P \Leftrightarrow Q$ by separating them into $P \Rightarrow Q$ and $Q \Rightarrow P$; more generally we can place a problem in conjunctive normal form and split up the conjuncts. For example, this deals with:

$$\begin{array}{l}
x \equiv y \pmod{n} \Rightarrow (\mathrm{coprime}(n, x) \Leftrightarrow \mathrm{coprime}(n, y)) \\
x \equiv 0 \pmod{n} \Leftrightarrow n|x \\
x + a \equiv y + a \pmod{n} \Leftrightarrow x \equiv y \pmod{n} \\
\mathrm{coprime}(xy, x^2 + y^2) \Leftrightarrow \mathrm{coprime}(x, y)
\end{array}$$

Additional negated equations can easily be absorbed into the conclusion using the integral domain property, passing from $\neg(t = 0) \wedge P \Rightarrow \exists \overline{y}.\ s(\overline{y}) = 0$ to $P \Rightarrow \exists \overline{y}.\ s(\overline{y})t = 0$, which allows us to handle things like:

$$\neg(c = 0) \Rightarrow ((ca)|(cb) \Leftrightarrow a|b)$$

Perhaps more interesting is that we can even handle existential quantifiers present in the original problem before the algebraic reduction, e.g.

$$\mathrm{coprime}(a, n) \Rightarrow \exists x.\ ax \equiv b \pmod{n}$$

We will treat a somewhat more general version of that problem in detail below ('extension with GCDs'). Here we will run through the basic binary Chinese Remainder Theorem, which also has an existential quantifier in the conclusion:

$$\forall a\ b\ u\ v.\ \mathrm{coprime}(a, b) \Rightarrow \exists x.\ x \equiv u \pmod{a} \wedge x \equiv v \pmod{b}$$

If we proceed as usual we obtain the goal:

$$\forall a\ b\ u\ v\ w\ z.\ aw + bz = 1 \Rightarrow \exists x\ d\ e.\ u - x = da \wedge v - x = eb$$

Since we have multiple equations under the existential quantifier, the reduction to ideal membership introduces two new variables $r$ and $s$:

$$(ur + vs) \in \mathrm{Id}\,\langle aw + bz - 1, r + s, ar, bs\rangle$$

and this is true since we have

$$ur+vs = (aw+bz-1)(rv-ru)+(r+s)(v+buz-bvz)+(ar)(uw-vw)+(bs)(vz-uz)$$

## 5 Extensions

Although the basic procedure above is already quite powerful, we can extend its scope by a number of perhaps ad hoc but quite natural refinements.

### Introduction of GCDs

It is often convenient to express properties using greatest common divisors (GCDs). One simple approach for handling $\gcd(a, b)$ is to replace it with a variable $g$ while adding as an additional hypothesis a characterizing theorem:

$$g \mid a \wedge g \mid b \wedge (\exists u\ v.\ au + bv = g)$$

This does not characterize $g$ uniquely because of the ambiguity over sign (or multiplication by a unit in a general ring), but any divisibility relationships are also invariant under such a change, so this is not a severe obstacle. For example, consider proving a basic condition for the solvability of a congruence:

$$\gcd(a, n) \mid b \Rightarrow \exists x.\ ax \equiv b\ (\mathrm{mod}\ n)$$

After the initial augmentation we get:

$$g \mid a \wedge g \mid n \wedge (\exists u\ v.\ au + nv = g) \wedge g \mid b \Rightarrow \exists x.\ ax \equiv b\ (\mathrm{mod}\ n)$$

and the usual expansion, normalization and prenexing yields:

$$gq = a \wedge gr = n \wedge au + nv = g \wedge gs = b \Rightarrow \exists x\ y.\ ax + yn = b$$

giving the ideal membership question

$$b \in \mathrm{Id}\,\langle gq - a, gr - n, au + nv - g, gs - b, a, n\rangle$$

which is true since

$$b = (gq - a)0 + (gr - n)0 + (au + nv - g)(-s) + (gs - b)(-1) + a(su) + n(sv)$$

The converse implication $\exists x.\ ax \equiv b\ (\mathrm{mod}\ n) \Rightarrow \gcd(a, n) \mid b$ can be proved in a similar way.

**Elimination using linear equations**

For a motivating example here, consider again the binary Chinese Remainder Theorem:

$$\forall a\ b\ u\ v.\ \text{coprime}(a, b) \Rightarrow \exists x.\ x \equiv u\ (\text{mod}\ a) \wedge x \equiv v\ (\text{mod}\ b)$$

If we proceed as before we obtain the goal:

$$\forall a\ b\ u\ v\ w\ z.\ aw + bz = 1 \Rightarrow \exists x\ d\ e.\ u - x = da \wedge v - x = eb$$

Earlier, we introduced auxiliary variables to handle the double equation. However, in this case it is fairly obvious that we can get an equivalent that just eliminates $x$ between the two equations:

$$\forall a\ b\ u\ v\ w\ z.\ aw + bz = 1 \Rightarrow \exists d\ e.\ v - u = eb - da$$

This gives a reduction to the ideal membership goal:

$$(v - u) \in \text{Id}\ \langle aw + bz - 1, b, -a\rangle$$

which is true since

$$v - u = (aw + bz - 1)(u - v) + b(zv - zu) + -a(wu - wv)$$

This elimination does not help with the ternary Chinese Remainder Theorem, whereas the method using auxiliary variables still works perfectly. However, on a heuristic level it seems prudent always to eliminate existentially quantified variables when there is a simple linear equation that allows us to do so.

**Sequential treatment of equations**

Our standard form requires each equation to be linear in the existentially quantified variables. However, note that linearity is irrelevant to Theorem 2, and only appears as a restriction in order to reduce witness-finding to ideal membership. So we can consider more general means of finding witnesses by building in techniques for nonlinearity. Elimination using linear equations, as in the previous example, may enable us to get round this restriction in some cases. Otherwise, we can at least find witnesses for those equations we can, and hope that they will then in turn allow us to solve the overall problem. For example, consider:

$$\gcd(a, b) \neq 0 \Rightarrow \exists a'\ b'.\ a = a' \gcd(a, b) \wedge b = b' \gcd(a, b) \wedge \text{coprime}(a', b')$$

Proceeding in the usual way, eliminating number-theoretic concepts, we obtain:

$$a = gx \wedge b = gy \wedge g = ua + vb \wedge \neg(g = 0) \Rightarrow \exists a'\ b'\ w\ z. a = a'g \wedge b = b'g \wedge a'w + b'z = 1$$

and as usual we eliminate the negated equational hypothesis using the integral domain property:

$$a = gx \wedge b = gy \wedge g = ua + vb \Rightarrow \exists a'\ b'\ w\ z. ag = a'g^2 \wedge bg = b'g^2 \wedge a'wg + b'zg = g$$

This does not fall into our subset because of the nonlinearity: in $a'wg$ we have two existentially quantified variables $a'$ and $w$ multiplied together. On the other hand, we might heuristically try to find witnesses by considering the equations one at a time. First

$$a = gx \wedge b = gy \wedge g = ua + vb \Rightarrow \exists a'.\, ag = a'g^2$$

gives the ideal membership assertion

$$(ag) \in \mathrm{Id}\left\langle gx - a, gy - b, ua + vb - g, g^2 \right\rangle$$

from whose solution

$$ag = (gx - a)(-g) + g^2x$$

we extract the witness $a' = x$. Similarly solving the next equation gives us $b' = y$. After inserting those, two equations in the problem are trivial and everything reduces to:

$$a = gx \wedge b = gy \wedge g = ua + vb \Rightarrow \exists w\ z.\, xwg + yzg = g$$

giving the ideal membership

$$g \in \mathrm{Id}\left\langle gx - a, gy - b, ua + vb - g, xg, yg \right\rangle$$

which is true since

$$g = (gx - a)(-u) + (gy - b)(-v) + (ua + vb - g)(-1) + (xg)u + (yg)v$$

and in particular we obtain the witnesses $w = u$, $z = v$.

## 6 Implementation

We have implemented a simple prototype of the routine, containing fewer than 100 lines of code, in the HOL Light theorem prover [9]; in version 2.20, it is included in the standard release. The implemented version does not yet use the extension to multiple equations using auxiliary variables, and some of the initial normalization is a little ad hoc. But it does include all the extensions in the previous section, and all the examples we have mentioned in this paper can be proved automatically by it. Here is a typical interaction, proving a slight generalization of the binary Chinese remainder theorem, not assuming that the moduli are coprime: if $a_1 \equiv a_2 \pmod{\gcd(n_1, n_2)}$ then there is an $x$ such that $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$. The user passes the desired result as a parameter to `INTEGER_RULE` on the first line, and after some informative messages, the required theorem is proved automatically:

```
# INTEGER_RULE
   `!a1 a2 n1 n2:int.
          (a1 == a2) (mod (gcd(n1,n2)))
          ==> ?x. (x == a1) (mod n1) /\ (x == a2) (mod n2)`;;
4 basis elements and 1 critical pairs
5 basis elements and 0 critical pairs
1 basis elements and 0 critical pairs
Translating certificate to HOL inferences
val it : thm =
  |- !a1 a2 n1 n2.
         (a1 == a2) (mod gcd (n1,n2))
         ==> (?x. (x == a1) (mod n1) /\ (x == a2) (mod n2))
```

We just use the normal Buchberger algorithm for polynomial ideals over $\mathbb{Q}$, implemented in HOL via `int_ideal_cofactors`. Properly speaking, we should use a version of Buchberger's algorithm tailored to the ring $\mathbb{Z}$ [11]. For example, consider proving just $x+y = 0 \wedge x-y = 0 \Rightarrow x = 0$. This does not hold in all rings (e.g. set $x = y = 1$ in the integers modulo 2). The Gröbner basis algorithm over the rationals, however, would appear to prove it giving coefficients of $1/2$ in the cofactors. However, testing ideal membership over $\mathbb{Z}$ is in general somewhat more difficult [1], and we have found almost no cases where the distinction mattered (most problems involve no explicit constants $|c| > 1$, which helps). Because the actual HOL Light proof proceeds rigorously by logical inference, no false result could be generated, but the proof construction step will fail if the ideal cofactors contain rationals.

## 7 Conclusions and related work

We are not aware of any related work on automating problems involving both multiplication and 'divisibility' concepts. Indeed, as we have noted, the problem is in general unsolvable and our procedure, though remarkably effective, is a combination of a preprocessing step tailored to the integers followed by a decision procedure complete only over the class of rings in general.

There are established results for decidability of universal linear formulas in the language of Presburger arithmetic including divisibility by non-constants [3, 15], though we are not aware of any actual implementation. Allowing a richer quantifier structure soon leads to undecidability, even in the linear case; for example multiplication can be defined in terms of divisibility, successor and 1 only [18], so even that theory is undecidable. In contrast, we allow more or less unrestricted use of multiplication, which in principle leads to undecidability. But the approach of seeking properties true in all rings seems to work very well.

We have found the procedure very useful in practice. Just as it is convenient to have automated provers for routine facts of linear arithmetic and propositional tautologies, being able to generate routine lemmas about divisibility with so little effort is a considerable help in proofs. In fact, we were inspired to create this procedure during the formal verification of an arithmetic algorithm, when we found ourselves repeatedly proving trivialities about divisibility by hand. The procedure has also been useful in some HOL proofs in pure mathematics, e.g. quadratic reciprocity.

In all the examples we have tried, the ideal membership goals are easy: our straightforward Gröbner basis algorithm works in a fraction of a second. It might be interesting to try some large (even if artificial) problems, such as $n$-ary Chinese remainder theorems for large $n$. Perhaps in such cases more care would be needed, e.g. over the monomial order in the Gröbner basis algorithm. At present we order the monomials by total degree then reverse lexicographic order of variables [21], ordering the variables themselves alphabetically. Other optimizations might be worthwhile, e.g. using reduced Gröbner bases or constructing the basis more incrementally when dealing with equations sequentially.

Also, it would be more satisfactory to use a Gröbner basis algorithm tailored to the integers. This would open up the possibility of dealing with a wider range of problems involving specific numbers. It is even conceivable that the approach could then be used to reason about machine arithmetic modulo $2^n$ in a useful way. Perhaps the results here could also be used in other situations where restricted quantifier instantiation is needed, e.g. checking that universally quantified polynomial equations are invariant over a program block.

## Acknowledgements

I am grateful to the anonymous referees for their valuable work; they offered everything from thought-provoking general observations to lists of subtle typos in doubly indexed variables.

## References

1. M. Aschenbrenner. Ideal membership in polynomial rings over the integers. *Journal of the American Mathematical Society*, 17:407–441, 2004.
2. A. Baker. *A Concise Introduction to the Theory of Numbers*. Cambridge University Press, 1985.
3. A. P. Beltyokov. Decidability of the universal theory of natural numbers with addition and divisibility (Russian). *Sem. Leningrad Otd. Mat. Inst. Akad. Nauk SSSR*, 40:127–130, 1974. English translation in Journal Of Mathematical Sciences, vol. 14, pp. 1436–1444, 1980.
4. R. S. Boyer and J. S. Moore. *A Computational Logic*. ACM Monograph Series. Academic Press, 1979.
5. B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Mathematisches Institut der Universität Innsbruck, 1965. English translation to appear in Journal of Symbolic Computation, 2006.
6. A. Bundy. A science of reasoning. In J.-L. Lassez and G. Plotkin, editors, *Computational Logic: Essays in Honor of Alan Robinson*, pages 178–198. MIT Press, 1991.
7. D. C. Cooper. Theorem proving in arithmetic without multiplication. In B. Melzer and D. Michie, editors, *Machine Intelligence 7*, pages 91–99. Elsevier, 1972.
8. G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, 5th edition, 1979.

9. J. Harrison. HOL Light: A tutorial introduction. In M. Srivas and A. Camilleri, editors, *Proceedings of the First International Conference on Formal Methods in Computer-Aided Design (FMCAD'96)*, volume 1166 of *Lecture Notes in Computer Science*, pages 265–269. Springer-Verlag, 1996.
10. W. Hodges. Logical features of Horn clauses. In D. M. Gabbay, C. J. Hogger, and J. A. Robinson, editors, *Handbook of Logic in Artificial Intelligence and Logic Programming, volume 1 (logical foundations)*, pages 449–503. Oxford University Press, 1993.
11. A. Kandri-Rody and D. Kapur. Algorithms for computing Gröbner bases of polynomial ideals over various Euclidean rings. In J. Fitch, editor, *EUROSAM 84: International Symposium on Symbolic and Algebraic Computation*, volume 174 of *Lecture Notes in Computer Science*, pages 195–206, Cambridge, England, 1984. Springer-Verlag.
12. A. Kandri-Rody, D. Kapur, and P. Narendran. An ideal-theoretic approach to word problems and unification problems over finitely presented commutative algebras. In J.-P. Jouannaud, editor, *Rewriting Techniques and Applications*, volume 202 of *Lecture Notes in Computer Science*, pages 345–364, Dijon, France, 1985. Springer-Verlag.
13. G. Kreisel and J.-L. Krivine. *Elements of mathematical logic: model theory*. Studies in Logic and the Foundations of Mathematics. North-Holland, revised second edition, 1971. First edition 1967. Translation of the French 'Eléments de logique mathématique, théorie des modeles' published by Dunod, Paris in 1964.
14. V. Lifschitz. Semantical completeness theorems in logic and algebra. *Proceedings of the American Mathematical Society*, 79:89–96, 1980.
15. L. Lipshitz. The Diophantine problem for addition and divisibility. *Transactions of the American Mathematical Society*, 235:271–283, 1978.
16. Y. V. Matiyasevich. Enumerable sets are Diophantine. *Soviet Mathematics Doklady*, 11:354–358, 1970.
17. M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Sprawozdanie z I Kongresu metematyków slowiańskich, Warszawa 1929*, pages 92–101, 395. Warsaw, 1930. Annotated English version by [20].
18. J. Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949. Author's PhD thesis.
19. H. Simmons. The solution of a decision problem for several classes of rings. *Pacific Journal of Mathematics*, 34:547–557, 1970.
20. R. Stansifer. Presburger's article on integer arithmetic: Remarks and translation. Technical Report CORNELLCS:TR84-639, Cornell University Computer Science Department, 1984.
21. V. Weispfenning and T. Becker. *Groebner bases: a computational approach to commutative algebra*. Graduate Texts in Mathematics. Springer-Verlag, 1993.