# Automating elementary number-theoretic proofs using Gröbner bases

John Harrison

Intel Corporation

CADE, Bremen

Tue 17th July 2007 (12:00–12:30)

## Divisibility properties over the integers

Often want to prove tedious lemmas like

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

## Expanding divisibility properties

Eliminate divisibility notions in terms of existentials:

- $s \mid t$ to $\exists d.\, t = sd$
- $s \equiv t \pmod{u}$ to $\exists d.\, t - s = ud$
- coprime$(s, t)$ to $\exists x\ y.\, sx + ty = 1$.

## Applied to the example

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

Pull out the quantifiers in the antecedent:

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

## Solving a more general problem

We are already well into the realm of ‘undecidable in general’ thanks to the unsolvability of Hilbert’s $10^{th}$ problem.

## Solving a more general problem

We are already well into the realm of ‘undecidable in general’ thanks to the unsolvability of Hilbert’s $10^{th}$ problem.

Instead, attempt to prove the property holds *in all rings*.

It turns out that this problem *is* decidable using well-known methods.

## Word problem for rings

$$\forall \overline{x}.\, p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0$$

holds in all rings iff

$$q \in \mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$$

i.e. there exist ‘cofactor’ polynomials with integer coefficients such that

$$p_1 \cdot q_1 + \cdots + p_n \cdot q_n = q$$

## Generalizes to linear existential theorems

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

holds in all rings iff (Horn-Herbrand) there are terms in the language of rings s.t.

$$\mathsf{Ring} \vdash \forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow\ \ p_1(\overline{x})t_1(\overline{x}) + \cdots + p_n(\overline{x})t_n(\overline{x}) = a(\overline{x})$$

iff (previous theorem)

$$a \in \mathsf{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_m, p_1, \ldots, p_n \rangle$$

## . . . and simultaneous linear existentials

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

holds in all rings iff

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

where the $u_i$ are fresh variables.

## Solving ideal membership problems

The most natural approach to solving ideal membership problem is Gröbner bases.

Strictly, should use an integer version. However, can use the rational version speculatively and see if we get integer cofactors.

With an instrumented version of Buchberger's algorithm, can generate cofactors and hence easily generate a rigorous formal proof.

## In our example

We want to prove

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

## In our example

We want to prove

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

This is true because

$$y - x = \quad (ay - ax - nd) \cdot u + (au + nv - 1) \cdot (x - y) + n \cdot (ud + vy - vx)$$

## Extensions

- Use linear equations $x + a = b$ to substitute directly
- Add greatest common divisors by characterizing theorem
  $g \mid a \wedge g \mid b \wedge (\exists u\ v.\ au + bv = g)$
- Solve for existential witnesses sequentially to defer nonlinear ones.

## Implementation in HOL Light

A prototype of the procedure is available in the latest release of HOL Light, 2.20:

```
# INTEGER_RULE
   ‘!a1 a2 n1 n2:int.
          (a1 == a2) (mod (gcd(n1,n2)))
          ==> ?x. (x == a1) (mod n1) /\ (x == a2) (mod n2)‘;;
```

## Implementation in HOL Light

A prototype of the procedure is available in the latest release of HOL Light, 2.20:

```
# 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))
```

## Various successful examples

$d|a \wedge d|b \Rightarrow d|(a - b)$

$\mathsf{coprime}(d, a) \wedge \mathsf{coprime}(d, b) \Rightarrow \mathsf{coprime}(d, ab)$

$\mathsf{coprime}(d, ab) \Rightarrow \mathsf{coprime}(d, a)$

$\mathsf{coprime}(a, b) \wedge x \equiv y \pmod{a} \wedge x \equiv y \pmod{b} \Rightarrow x \equiv y \pmod{(ab)}$

$m|r \wedge n|r \wedge \mathsf{coprime}(m, n) \Rightarrow (mn)|r$

$\mathsf{coprime}(xy, x^2 + y^2) \Leftrightarrow \mathsf{coprime}(x, y)$

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

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

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

## Failures

Can’t solve problems where special properties of the integers are used

$$2|x^2 + x$$

This fails over some rings, e.g. $\mathbb{R}[x]$.

However, such examples very seldom appear in typical routine lemmas.

## Conclusions

- Simple but surprisingly powerful idea; very useful for routine lemmas
- Another indication of the surprising versatility of ideal membership
- Hints at a general strategy for new decision methods:

## Conclusions

- Simple but surprisingly powerful idea; very useful for routine lemmas
- Another indication of the surprising versatility of ideal membership
- Hints at a general strategy for new decision methods:
  **solve a more general problem**