Notes prepared by
Stanley Burris
February 10, 1997

1 Arithmetic I

1.1 First-order Arithmetic

Let $\boldsymbol{\omega}$ be the structure $(\omega, +, \times, 0, 1)$, where ω is the set of non-negative integers. *First-order Arithmetic* is $\mathrm{Th}(\boldsymbol{\omega})$, the set of first-order statements in the language $\{+, \times, 0, 1\}$ which are true in $\boldsymbol{\omega}$. Much of the fascination of working with first-order number theory comes from the simple fact that there are so many assertions P, including unsolved problems, in number theory for which one can routinely exhibit a specific first-order φ such that the assertion P is true iff $\boldsymbol{\omega} \models \varphi$. We say that such assertions can be *expressed* in first-order arithmetic.

This contrasts sharply with Presburger Arithmetic, i.e., the first-order theory of $(Z, +, 0, 1, <)$, or the first-order theory for the calculus of classes, i.e., the first-order theory of all structures $(P(U), \cup, \cap, ', 0, 1)$. For these two examples there are *no* known unsettled assertions in mathematics for which one can find such a corresponding first-order φ.

In this section we look at the basic ideas for translating number-theoretic assertions into first-order arithmetic. The starting point is to express some well known relations by first-order formulas.

DEFINITION 1 For $n \in \omega$ we define the term $\bar{n}$ by: $\bar{0} = 0$, $\overline{n+1} = \bar{n} + 1$.

$\bar{n}$ is an obvious choice for a term to represent the number n.

DEFINITION 2 A relation $r \subseteq \omega^n$ is *definable* on $\boldsymbol{\omega}$ if there is a formula $\varphi(x_1, \ldots, x_n)$ such that $r = \varphi^{\boldsymbol{\omega}}$, i.e.,

$$(k_1, \ldots, k_n) \in r \qquad \text{iff} \qquad \boldsymbol{\omega} \models \varphi(\bar{k}_1, \ldots, \bar{k}_n).$$

Now we look at a few definable relations:

Relation	Defining Formula
$x \leq y$	$\exists z\,(x+z \approx y)$
$x < y$	$x \not\approx y \ \wedge x \leq y$
$x \mid y$	$\exists z\,(xz \approx y)$
$x \equiv y \bmod z$	$\exists u\,[(u+x \approx y \ \vee \ y+u \approx x) \ \wedge \ z \mid u]$
$\mathrm{prime}(x)$	$(x \not\approx 1) \wedge \forall y\,(y \mid x \ \rightarrow \ y \approx 1 \vee y \approx x)$
$\mathrm{coprime}(x,y)$	$\forall u\,(u \mid x \wedge u \mid y \ \rightarrow u \approx 1)$

With just these formulas we can express important results, for Euclid's theorem on the infinitude of primes is given by

$$\forall x \exists y \ x < y \wedge \mathrm{prime}\,(y);$$

and Dirichlet's theorem about the infinitude of primes in an arithmetical progression $an+b$, when a and b are relatively prime, is expressed by

$$\forall u \forall v \ \mathrm{coprime}(u,v) \ \rightarrow \ \forall x \exists y \ [x < y \wedge \mathrm{prime}\,(uy+v)].$$

And one can express Goldbach's Twin Prime conjecture by

$$\forall x \exists y \ x < y \wedge \mathrm{prime}(y) \wedge \mathrm{prime}(y+\bar{2}).$$

Many of the results and problems in number theory deal with the *exponential function* x^y. If we had given ourselves this function as a fundamental operation of $\boldsymbol{\omega}$ then we could easily express Fermat's Last Theorem by

$$\forall x \forall y \forall z \forall w\,[x^w + y^w \approx z^w \ \rightarrow \ w < \bar{3} \vee xy \approx 0].$$

However we do not have this simple situation. Nonetheless we are able to work with a wide class of functions in first-order number theory by defining their graphs.

DEFINITION 3 A function $f : \omega^n \rightarrow \omega$ is *definable* in first-order arithmetic if there is a formula $\varphi(x_1,\ldots,x_n,y)$ such that $f(\vec{k}) = m$ iff $\varphi^{\boldsymbol{\omega}}(\bar{k}_1,\ldots,\bar{k}_n,\bar{m})$ holds in $\boldsymbol{\omega}$.

Now, if we could define the exponential function, say by $\varphi_{\uparrow}(x,y,z)$, then we could express Fermat's Last Theorem by

$$\forall x \forall y \forall z \forall w \forall u \forall v \ \varphi_{\uparrow}(x,w,u) \wedge \varphi_{\uparrow}(y,w,v) \wedge \varphi_{\uparrow}(z,w,u+v) \ \rightarrow \ w < \bar{3} \vee xy \approx 0.$$

So let us find a way to define exponentiation. The obvious approach is to use recursion (as Dedekind did): $a^0 = 1$ and $a^{n+1} = a^n a$. To compute a^n

directly from such a definition we would compute the sequence $a^0, a^1, \ldots, a^n$. However this does not appear to be expressible in first-order form.

For the moment suppose there is a definable function $s : \omega^2 \rightarrow \omega$, defined by $\varphi_s(x,y,z)$, such that for each finite sequence $a_0, \ldots, a_n$ there is a b such that $s(b,0) = a_0, \ldots, s(b,n) = a_n$. Then we could use φ_s to define exponentiation in first-order arithmetic using the following formula $\varphi_\uparrow(x,y,z)$:

$$\exists u\ [\varphi_s(u,\bar{0},\bar{1}) \wedge \forall v \forall w\,(v < y \wedge \varphi_s(u,v,w)\ \rightarrow\ \varphi_s(u, v+\bar{1}, wx))\ \wedge\ \varphi_s(u,y,z)].$$

A beautiful observation of Gödel in his 1931 paper was the fact that one could find such a formula — however it was simpler to define a certain function of three variables, called Gödel's beta function, given by

$$\beta(x,y,z) = rem\,(1 + (z+1)y,\ x),$$

where $rem\,(x,y)$ is the remainder after dividing y by x. Clearly β is defined by the following formula $\varphi_\beta(x,y,z,w)$:

$$\exists w\,[w \equiv x \bmod 1 + (z+1)y\ \wedge\ w < 1 + (z+1)y].$$

The following lemma says that for any finite sequence $a_0, \ldots, a_n$ from ω there are numbers b and c from ω such that a_i is the result of reducing b modulo $1 + (i+1)c$.

LEMMA 4 Given any finite sequence $a_0, \ldots, a_n \in \omega$ there are $b, c \in \omega$ such that $\beta(b,c,i) = a_i$ for $0 \leq i \leq n$.

Proof. Let $c = \max(n, a_0, \ldots, a_n)!$ and let $u_i = 1 + (i+1)c$ for $0 \leq i \leq n$. Then for p a prime we have $p|u_i \Longrightarrow p \not| c$, and thus for $0 \leq i < j \leq n$ we have

$$\begin{aligned} p|u_i\ \&\ p|u_j &\Longrightarrow p|u_i - u_j \\ &\Longrightarrow p|(i-j)c \\ &\Longrightarrow p|i-j. \end{aligned}$$

But $i - j|c$, so $p|c$, which is impossible. Thus the u_i are pairwise coprime. Consequently by the Chinese remainder theorem one can find an integer b ($< u_0 \cdots u_n$) such that $b \equiv a_i \bmod u_i$; and since $a_i < u_i$ we have $rem\,(u_i, b) = a_i$. ■

So now a slight modification of our attempt (using φ_s) at defining exponentiation succeeds, and we can write a a simple sentence φ_{FLT} which holds in $\boldsymbol{\omega}$ iff Fermat's Last Theorem is true.

Exercises Let DEF be the class of functions definable on $\boldsymbol{\omega}$ (we include the constants as nullary functions).

Problem 1 Show that DEF is closed under *composition*, i.e., if $f : \omega^n \to \omega$ and $g_i : \omega^k \to \omega$ are in DEF, $1 \leq i \leq n$, then $f(g_1, \ldots, g_n) : \omega^k \to \omega$ is in DEF.

Problem 2 Show that DEF is closed under *primitive recursion*, i.e., suppose $n > 0$ and $g : \omega^{n-1} \to \omega$ and $h : \omega^{n+1} \to \omega$ are in DEF. Then $f : \omega^n \to \omega$ given by

$$\begin{aligned} f(x_1, \ldots, x_{n-1}, 0) &= g(x_1, \ldots, x_{n-1}) \\ f(x_1, \ldots, x_{n-1}, x_n + 1) &= h(x_1, \ldots, x_n, f(x_1, \ldots, x_n)) \end{aligned}$$

is also in DEF[1].

1.2 Peano Arithmetic

Based on the work of Dedekind and Peano one can give a relatively simple set of first-order axioms, called PA, for the natural numbers[2] from which one can prove all standard theorems of number theory which can be formulated as first-order statements.

[1]Note that we obtain exponentiation by using $g = 1$ and $h(x_1, x_2) = x_1 \cdot x_2$.

[2]Although Dedekind, Peano, and Landau were interested in axiomatizing *positive* integers (natural numbers), the standard now is to work with the *nonnegative* integers.

Peano Arithmetic

- The language is $\{+, \times, 0, 1\}$
- The AXIOMS are

$$
\begin{array}{ll}
\forall x & x+1 \not\approx 0 \\
\forall x \forall y & x+1 \approx y+1 \rightarrow x \approx y \\
\forall x & x+0 \approx x \\
\forall x \forall y & x+(y+1) \approx (x+y)+1 \\
\forall x & x \times 0 \approx 0 \\
\forall x \forall y & x \times (y+1) \approx (x \times y)+x
\end{array}
$$

and for each first-order formula $\varphi(x, \vec{y})$
the first-order induction axiom

$$\forall \vec{y}\,([\varphi(0, \vec{y}) \wedge \forall z(\varphi(z, \vec{y}) \rightarrow \varphi(z+1, \vec{y})] \rightarrow \ \forall x \varphi(x, \vec{y}))$$

The standard model of PA is $(\omega, +, \times, 0, 1)$, where the operations are the usual ones. In Example V.14.3 of **LMCS** we saw that there are *other* countable models of PA. And once we have developed a derivation calculus then it is possible to return to the sentences φ in §1 which expressed important assertions and *try* to prove them by seeing if we can show PA $\vdash \varphi$. This method cannot work all the time by Gödel's incompleteness theorem – and indeed we do not know if PA is strong enough to prove any interesting open problems in number theory.