Nonstandard Models of Arithmetic

Angus Macintyre

April 18, 2002

1 Introduction

The existence of nonstandard models of arithmetic was discovered in the 1930's. Though Gödel somehow missed it, their existence follows from the Gödel Completeness Theorem (1930) or the later Compactness Theorem, and more interesting examples follow from Gödel's Incompleteness Theorem of 1931. Skolem (who had serious credentials in number theory) gave an explicit construction in 1934.

Our basic object of study is $\mathbb{N}$ $(= \{0, 1, 2, ...\})$, with the usual $+, \cdot, <$ as primitive notions. I prefer to work in the ring $\mathbb{Z}$. This is a commutative ring with 1, discretely ordered by $<$. [Later we spell out the formal axioms for DOR, the class of discretely ordered rings with 1. Usually R is such a ring, and $N = \{x \in R : x \geq 0\}$.]

Full Induction

This is of course the axiom: $X \subseteq N,\ 0 \in X,\ X$ closed under $t \to t+1 \Rightarrow X = N$.

We all know that $\mathbb{Z}$ is (up to isomorphism) the only DOR satisfying Full Induction. So our nonstandard models never satisfy Full Induction.

If we restrict the X in induction we can get nonstandard models. The most common restriction is to restrict X to be first-order definable from $+, \cdot, <$. Rather than going straight to the jungle of syntax (eventually we must) we define **first-order** thus (for $R \in DOR$) :

i) If $f \in R[x_1, ...x_n]$, $\{\bar{x} \in R^n : f(\bar{x}) = 0\}$ and $\{\bar{x} \in R^n : f(\bar{x}) > 0\}$ are first-order;

ii) Close under $\cap, \cup, \neg$, projection $R^{m+n} \to R^n$ (repeatedly) to get R-definable (or first-order definable) subset of R^n.

[Since $\forall \bar{y} = \neg \exists \bar{y} \neg$, one has closure under $\forall$.]

Peano arithmetic (PA) is (the axiomatization of) the class of DOR with induction for X first-order definable.

THERE ARE NONSTANDARD MODELS of PA (in abundance), and we will for now work in an arbitrary one. Later we discuss particularly striking ones, where one may have $f \in \mathbb{Z}[x_1, ...x_9]$ unsolvable in $\mathbb{Z}$, but solvable in R.

The conventional wisdom is that PA is **weak**, because (Gödel) incomplete. In fact it is extremely strong (for example, Fermat's Last Theorem holds in all models of PA), and one has to work very hard to find perspicuous number-theoretic statements independent of (i.e. unsettled by) PA (the best examples, due to Paris et al in the 1970's, involve subtle variants of Ramsey's Theorem in finite combinatorics).

Philosophical issue (Kreisel): If I know that Φ is true in all models of PA (and not merely in $\mathbb{Z}$), what more do I know about $\mathbb{Z}$ than if I merely know that Φ is true in $\mathbb{Z}$?

In fact there is much more information, and this information grows as we weaken induction (thereby increasing the class of DOR considered). This will be made more precise later.

2 Algebraic preliminaries

Some notions make immediate sense in R, and we can prove for them the basic things one knows for $\mathbb{Z}$.

Division: $x \mid y \Leftrightarrow (\exists t)(y = xt)$.
Unit: $x \mid 1$ (± 1 are only units.)
Irreducible: x irreducible $\Leftrightarrow (x = yz \rightarrow y$ or z a unit$)$

Note that all relations above are first-order. So one easily proves by induction:

x not a unit $\Rightarrow x$ is divisible by an irreducible > 1.

Note: The correct property to induct on is:

$\Phi(x) : (\forall t)(0 < t \leq x \rightarrow t = 1$ or t is divisible by an irreducible $> 1)$.

What one does **not** get is factorization into a **finite** product of irreducibles (more on this later).

Primes x is prime $\Leftrightarrow (x \mid yz \rightarrow x \mid y$ or $x \mid z)$. This is of course first-order definable. In all rings, prime $\Rightarrow$ irreducible.

In models of PA, irreducible $\Rightarrow$ prime, and we give the sketch of the proof. The crucial point is that for $a, b \in R$ there are $\lambda, \mu \in R$ so that $\lambda a + \mu b$ divides both a and b. For them, up to $\pm 1, \lambda a + \mu b$ is the greatest common divisor of a, b.

First we establish Euclidean division in N. Say $m, n > 0$. Then $\exists k, \ell$ $m = k.n + \ell$, $0 \leq \ell < n$. If $m < n$ clear. Otherwise, suppose $m \geq n$. Now $mn \geq n$, so by induction there must be k with $n.k \leq m < n.(k+1)$, so let $\ell = m - kn$. [Later we shall look at how much induction needed here.]

Now return to the $\lambda a + \mu b$ argument. We can assume $a, b \in N$, and we do induction on (a, b). (If $a = b$, result clear.) Then if $a < b$, write $b = ka + \ell$, $0 \leq \ell < a$, and work with (a, ℓ). Then get $\lambda a + \mu\ell$ dividing a, ℓ, so $\lambda a + (b - ka)\ell$ divides a, ℓ (whence a and $ka + \ell = b$), so $(\lambda - k\ell)a + b\ell$ works.

In purely algebraic terms this shows: R a model of PA $\Rightarrow$ all finitely generated ideals are principal. (such rings are called Bezout), and algebra gives: Bezout $\Rightarrow$ (irreducible = prime). [Again, we later analyze how much induction really needed.] Also, p prime $\Rightarrow$ $R/(p)$ a field. The usual primes 2,3,5,... remain prime, and, for them $R/(p)$ is $\mathbb{Z}/(p)$. But (nontrivial fact) if R is nonstandard it has nonstandard primes p, and for these $R/(p)$ is an infinite field. What properties does it have? (Answer later.)

Why are there infinite primes, if R nonstandard?

Overspill Principle (R nonstandard)

If X is first-order definable, and contains arbitrarily large standard elements, it contains a nonstandard element.

Proof Let δ be infinite positive, and let $Y = \{t < \delta : (\exists x \in X)(t < x)\}$. Note $\mathbb{N} \subseteq Y$. If result false, $\mathbb{N} = Y$. But $0 \in \mathbb{N}$, and closed under $u \mapsto u + 1$. So $\mathbb{N} = N$, contradiction. $\square$

Cor: There are infinite primes.

Proof Euclid. $\square$

A more delicate question is: If $x \in N$, $\exists y > x, y$ prime? (i.e. are primes cofinal).

Euclid's proof for $\mathbb{N}$ uses factorial. What meaning in N?

3 Exponentiation. Gödel's Device

In a general DOR, 2^x has no sense for $x \in N$. But Gödel showed that there is a natural definition in PA. The key is coding sequences.

Gödel's idea was to code arbitrary sequences $(a_0, ..., a_k)$ in terms of k and two auxiliary parameters λ, μ.

Define Rem(m, n), for $m, n \in N$ as the (clearly unique) ℓ so that $m = k.n + \ell$ in Euclidean division $(0 \leq \ell < n)$.

Given λ, μ, k we get a sequence $(a_0, ...a_k)$ as

$$a_j = \mathrm{Rem}(\lambda, 1 + (j + 1).\mu) \qquad 0 \leq j \leq k.$$

The main point is that by suitable choice of λ, μ we can get **any** $(a_0, ...a_k)$. For now we work in $\mathbb{N}$, and use Chinese Remainder Theorem, which says:

a) if $n_0....n_k$ are coprime in pairs, and $0 \leq a_i < n_i \quad 0 \leq i \leq k$ then there is a λ with $\text{Rem}(\lambda, n_i) = a_i$;

b) moreover, λ can be chosen with $0 \leq \lambda \leq \prod n_k$.

Now, suppose p is a prime dividing $1 + (j+1).\mu$ and $1 + (\ell+1).\mu \quad 0 \leq j, \ell \leq k$, then $p \mid (j - \ell).\mu$. So $p \mid (j - \ell)$ or $p \mid \mu$. But $p \nmid \mu$ for then $p \mid 1$. So $p \mid (j - \ell)$. If $k! \mid \mu$ this implies that $p \mid \mu$, again a contradiction.

So if $k! \mid \mu$ the $i + (j+1).\mu \quad (0 \leq j \leq k)$ are coprime in pairs, and can be taken as the n_i above provided $a_j \leq 1 + (j+1).\mu$.

Let $A = \max a_j$, and assume $\mu > A$. Then there is λ so that $\text{Rem}(\lambda, 1 + (j+1).\mu) = a_j \quad 0 \leq j \leq k$, and $\lambda \leq \pi(1 + (j+1).\mu)$. So, given $(a_0, ...a_k)$ we can choose $\mu \leq \max(k!, \max a_j)$, and $\lambda \leq \pi(1 + (j+1).\mu) \leq (k+z)!.\mu^{k+1}$. These are rather large bounds, and later we try to bypass them.

Definition of the relation $y = 2^x$

Idea: Code $(2^0, 2^1, ...2^x)$

$$\begin{aligned} y &= 2^x \Leftrightarrow \exists \lambda, \mu[\text{Rem}(\lambda, \mu) = 1 \\ \wedge(\forall_j &< x)(\text{Rem}(\lambda, 1 + (j+2).\mu) \\ &= 2\,\text{Rem}(\lambda, 1 + (j+1).\mu)) \\ \wedge\,\text{Rem}(\lambda, 1 + (x+1).\mu) &= y]. \end{aligned}$$

This is clearly correct in $\mathbb{N}$.

What does the RHS formula $\Phi(x, y)$ give in R, for R a general model of PA?

Theorem 1 For each x in N there is a unique y in N with $\Phi(x, y)$ (i.e. Φ is graph of a function).

Proof Clearly $\exists! y \Phi(0, y)$.

Suppose $\exists! y \Phi(x, y)$.

Suppose first $\Phi(x+1, t)$ and let λ', μ' witness this. By truncating the Rem conditions to $j < x$ we see that $\Phi(x, t/2)$, so $t/2$ unique, so t unique.

The existence is trickier, and needs some

Digressions

i) gcd and lcm. Given m, n we got $km + \ell n$ dividing m, n, and this gives $\gcd(m, n)$, the greatest common divisor of m, n. Then let $\operatorname{lcm}(m, n) = \dfrac{mn}{\gcd(m, n)}$. Obviously $m, n \mid \operatorname{lcm}(m, n)$. Suppose $m, n \mid a$. We have

$$\frac{a}{m}.(km + \ell n) = ak + \ell n.\frac{a}{m}$$

so $n \mid \dfrac{a}{m}.(km + \ell n)$, i.e. $\dfrac{mn}{(km + \ell n)} \mid a$. Thus we have a genuine lcm.

ii) $\operatorname{lcm}(1, ..., n)$. This exists in PA, and is easily proved by induction. Suppose $\operatorname{lcm}(1, ..., n)$ exists, $= \alpha$ say. Then $\operatorname{lcm}(\alpha, n + 1)$ is easily seen to be $\operatorname{lcm}(1, ..., n + 1)$.

iii) Chinese Remainder Theorem

This says that the congruence system

$$\begin{aligned} x &\equiv \alpha \mod m \\ x &\equiv \beta \mod n \end{aligned}$$

has a solution iff and only if $\alpha - \beta \equiv 0 \mod \gcd(m, n)$, (and x can be chosen with $0 \leq x < \operatorname{lcm}(m, n)$.

It holds in PA. The necessity is obvious. Clearly by Euclidean division wlog $0 \leq \alpha < m,\ 0 \leq \beta < n$.

$$\begin{aligned} \alpha - \beta &= \frac{\alpha - \beta}{\gcd(m, n)}.\gcd(m, n) \\ &= \frac{\alpha - \beta}{\gcd(m, n)}.(\lambda m + \mu n) \\ &= am + bn, \end{aligned}$$

so $\alpha - am = \beta + bn$ can be taken to solve the system.

Now use induction to get least nonnegative solution of the congruences, x_0 say. If $x_0 \geq \operatorname{lcm}(m, n)$, write $x_0 = k.\operatorname{lcm}(m, n) + \ell,\ 0 \leq \ell < \operatorname{lcm}(m, n)$, so $\ell \equiv x \mod m$ and $\mod n$, so ℓ is solution too.

iv) A maximum principle

Suppose that a subset I of N is bounded above and definable [NONEXAMPLE, $\mathbb{N}$, if R nonstandard.] Then I has a greatest element. For otherwise

$$J = \{n \in I : (\exists m \in I) n < m\} \cup \{0\}$$

violates induction.

v) **General lcm**

If I is as in (iv), there is an element (written $\mathrm{lcm}\, I$) which is divisible by all $n \in I$, and divides all other elements divisible by all elements of I.

Proof Let α be upper bound. Consider $\delta = \mathrm{lcm}(1, ..., \alpha)$ as before, and let J be the set of all numbers $\leq \delta$ which are divisible by all elements of I. Let $\delta_1 = \sup I$ (from (iv)). If $n \in I \rightarrow n \mid \delta_2$, let $\delta_2 = a\delta_1 + b \quad 0 \leq b < \delta_1$, to get $b = 0$ by minimality.

Cor: The primes are cofinal in N.

Proof Suppose α is a bound for the primes. Let $I =$ set of primes $(\leq \alpha)$.

Let $\delta = \mathrm{lcm}\, I$.

Let $q \mid \delta + 1,\ q$ prime, etc.

vi) **General CRT**

Let I be a bounded set, as in (iv), and in addition distinct members of I are pairwise coprime. Let $f : I \rightarrow N$ have definable graph. Then there is $x \in N,\ 0 \leq x \leq \mathrm{lcm}\, I,\ x \equiv f(n) \mod n$, all $n \in I$.

Proof Show by induction on k the result for $I \cap \{y : y \leq k\}$. If result for k, with solution x' say, get to $k+1$ as follows. Nothing to prove if $k+1 \notin I$, use x'. If $k+1 \in I$, consider $\mathrm{lcm}\, I \cap \{y : y \leq k\}$. Again show by induction this is coprime to $k+1$, so use CRT to get x'' with $x'' \equiv x \mod \mathrm{lcm}\, I \cap \{y : y \leq k\},\ x'' \equiv f(k+1) \mod k+1$, and we are done.

END OF DIGRESSION!

We have $\Phi(x, y)$ from Gödel's definition, witnessed by λ, μ. Let $A = 1 + \max(2y, 1+(x+1).\mu)$. Let $\mu' = \mathrm{lcm}(1, 2, ...(x+1)).A$. Let $I = \{1+(j+1).\mu' : 0 \leq j \leq (x+1)\}$ (which is bounded definable). The elements of I are pairwise coprime. So by general CRT get

$$\begin{aligned} \lambda' &= \mathrm{Rem}(\lambda, 1 + (j+1).\mu) \mod (1 + (j+1).\mu') \;\; 0 \leq j \leq x \\ &= 2y \mod (1 + (x+2).\mu'). \end{aligned}$$

One easily checks $\Phi(x+1, 2y)$. This proves Theorem 1.

Additional information

Define 2^x (uniquely) by $\Phi(x, 2^x)$. We have from above $2^{x+1} = 2.2^x$. But in fact:

a) $2^{x_1+x_2} = 2^{x_1}.2^{x_2}$.

Proof Induction on x_2. □

b) $2^x > x$.

Proof Easy induction.

NOTE: We have not yet defined 3^x etc., but this is easy once has the CRT.

"Uniqueness" of 2^x

Theorem 2 There is a unique function $f : N \to N$ **with definable graph** so that

$$f(0) = 1,\ f(x+1) = 2.f(x).$$

Proof Take two solutions and prove by induction they agree. □

This is what we mean by 2^x in PA.

NOTE: In any countable nonstandard model of PA, there are undefinable solutions f, g, h of

$$\begin{aligned} f(0) &= 1 \\ f(x+1) &= f(x)+1 \\ g(0) &= 0 \\ g(x+1) &= g(x)+2 \\ h(0) &= 1 \\ h(x+1) &= h(x).2 \end{aligned}$$

so that

(i) $f(x) \neq x+1$ in general

(ii) $g(x) \neq 2x$ in general

(iii) $h(x) \neq 2^x$ in general.

4 More general recursions

4.1 Obviously Gödel's device allows us to give "invariant" meaning to many other notions originally defined recursively on $\mathbb{N}$. For example: x^y, x^1.

Here is a fairly general result including the above. It is a metatheorem, and it is convenient to use informally the language of category theory. Definable functions are those with definable graphs, and clearly, with the definable sets make up a category.

Suppose $f : N^k \to N$ is total, $g : N^{k+1} \to N$ also. Consider

$$\begin{aligned} F(0, x_1, \ldots, x_k) &= f(x_1, \ldots, x_k) \\ F(x+1, x_1, ..., x_k) &= g(x, x_1, ..., x_k,\ F(x, x_1, ..., x_k)). \end{aligned}$$

A solution F of this is defined from f, g by primitive recursion.

Theorem 3 (R a model of PA), f, g definable. There is a unique definable F satisfying the above scheme.

Proof Uniqueness clear, by induction. Existence uses Gödel's device, and follows the argument for 2^x, but with some slight complications. I sketch the proof. Fix definitions of (graphs of) f, g. Then define

$$\begin{aligned} G(x, x_2, ...x_k, y) \iff & \exists \lambda, \mu \\ & [\mathrm{Rem}(\lambda, 1+\mu) = f(x_2, ...x_k) \\ \wedge \quad & \mathrm{Rem}(\lambda, 1+(x+1).\mu) = y \\ \wedge \quad & (\forall j < x)\, \mathrm{Rem}(\lambda, 1+(j+2)\mu) \\ & = g(j, x_2, ...x_k, \mathrm{Rem}(\lambda, 1+(j+1).\mu)] \end{aligned}$$

We claim: $\forall x \Psi(x)$, where $\Psi(x)$ is $\forall x_2, ...x_k \exists! y G(x, x_2, ...x_k, y)$.

$\Psi(0)$ clear.

Suppose $\Psi(x)$, and fix $x_2, ...x_k$. Uniqueness of z in $G(x+1, x_2, ...x_k)$ clear by truncation (as for 2^x).

Existence The only complication, over the case 2^x, is to get a bound A for the set of y such that $G(j, x_2, ...x_k, y)$ for some $j \leq x$. [For 2^x this was clear since remainders were increasing and bounded by y.] This needs an important digression, concerning a "**Replacement Axiom**".

Lemma Let I be a bounded definable set, and J a definable subset of $J \times N$. Then there is a bounded definable set K so that for all x, if $\exists t\ (x, t) \in J$ then $\exists t \in K\ (x, t) \in J$.

Proof Clearly K need only be defined as $\{t \;\; 0 \leq t \leq a\}$ some a. Consider: J bounded by $n \to (\exists a)\forall x)((\exists t)(x,t) \in J \to (\exists t)(t \leq a \wedge (x,t) \in J))$. True for $n = 0$, and the inductive step is trivial. $\square$

From this we get the A, and inductive step for Theorem 2.

So we have now unambiguous meaning for $x^y, x!$ etc. That of course still leaves us to prove in PA such things as Fermat's Little Theorem, or Wilson's Theorem, or any of the basic number theory in the book by Hardy and Wright. All this is greatly assisted by systematic use of Theorem 2. This gives us the following notions, which behave well in PA:

$$\sum_{x \in I} f(x) \;,\; \prod_{x \in I} f(x).$$

I a **bounded** definable set, and f a definable function on I.

With $f \equiv 1$, it gives us $card(I)$ = cardinality of I.

It gives us also definable enumerations of definable sets I. Here there are two cases:

<u>Case 1</u> I unbounded. Then $g(x)$ = least element of $I > x$ is a definable function, and we define:

$$\begin{aligned} f(0) &= \text{ least element of } I \\ f(n+1) &= g(f(n)). \end{aligned}$$

So f is a definable order-preserving map $N \leftrightarrow I$.

<u>Case 2</u> I bounded, by a say. This time define $\tilde{g}(x)$ as least element of $I > x$, if one exists, and $= a+1$ otherwise. Define $\mathcal{F}(0)$ = least element of I, if $I \neq \phi$ and $a+1$ otherwise; $\mathcal{F}(n+1) = \tilde{g}(\mathcal{F}(n))$. Clearly $\mathcal{F}$ is increasing until it takes value $a+1$, when it remains constant. Let γ = least n so that $\tilde{f}(\gamma) = a+1$. $\tilde{f}$ on $0 \leq x < \gamma$ is an order preserving map **onto** I. (easy induction).

Now we note: card$(\{x : 0 \leq x \leq n\}) = n+1$. Proof by induction.

Now something basic, and mysterious in weaker systems.

<u>**Theorem 4 (PHP)**</u> If f is a definable bijection of bounded definable sets <u>I and J then card(I)</u> = card(J).

Proof By what we just proved, we have to show that if $n \neq m$ there is no definable bijection

$$f : \{x : 0 \leq x < n-1\} \text{ to } \{x : 0 \leq x < m-1\}.$$

Of course you can define from f a new $\mathcal{F}$ that does this, but then **it** is not covered by the induction.

How to quantify over f? By Gödel coding. Note that any definable f on $\{x : 0 \leq x < n\}$ can be coded by λ, μ so that

$$f(x) = \mathrm{Rem}(\lambda, 1 + (x+1).\mu).$$

This is usual CRT argument.

So to prove Theorem 4 we proved a "coded" version, allowing quantification, over λ, μ.

Theorem 5:

$$\begin{aligned}\forall m \neq n \neg \exists \lambda, \mu . \forall j < n \ \mathrm{Rem}(\lambda, 1 + (j+1).\mu) < n \\ \wedge \forall \ell < m \ \exists j < n \ \mathrm{Rem}(\lambda, 1 + (j+1).\mu = \ell \\ \wedge (\forall j_1, j_2 < n)(j_1 \neq j_2) \\ \to \mathrm{Rem}(\lambda, 1 + (j_1+1).\mu) \neq \mathrm{Rem}(\lambda, 1 + (j_2+1).\mu).\end{aligned}$$

Proof Rather routine induction, using CRT devices. □

So we have a satisfactory invariant theory of counting in the definable category.

One can easily go on to binomial coefficients, binomial theorem, little Fermat, Wilson's Theorem, etc.

5 Binary Lengths. Binary Representation

By the maximum principle, if $x \geq 1$ there is a biggest $2^y \leq x$, so $2^y \leq x < 2^{y+1}$. $y (= |x|)$ is called the length of x. We want to give sense in R to the series

$$2^{|x|}, 2^{|x|} + 2^{|x_1|} + ...$$

where e.g. $x_1 = \left| x - 2^{|x|} \right|$, etc.

For future use in weaker systems we follow a new idea: We want (for $x \geq 1$).

$$x = a_0.2^s + a_1.2^{s-1} + ... + a_s.2^0$$

with $a_i \in \{0,1\},\ s = |x|\,,\ a_0 = 1$. We “get at this” thus:

$$\begin{aligned}
\eta_0 &= a_0.2^0 \\
\eta_1 &= a_0.2^1 + a_1.2^0 \\
&\vdots \\
\eta_s &= a_0.2^s + a_1.2^{s-1} + ... + a_s.
\end{aligned}$$

Note that $\eta_{j+1} - 2\eta_j = a_{j+1},\ \eta_2 = x$.

Of course the issue is (in PA) : given $x \geq 0$ are there λ, μ, s so that $\mathrm{Rem}(\lambda, 1+\mu)$ is 0 or 1, and for $j < s$

$$\mathrm{Rem}(\lambda, 1 + (j+2).\mu) - 2\,\mathrm{Rem}(\lambda, 1 + (j+1).\mu)$$

is 0 or 1, and

$$x = \mathrm{Rem}(\lambda, 1 + (s+1).\mu)?$$

Moreover, is s unique, and are then the remainders independent of λ, μ? Is $s = |x|$ if $x \geq 1$.

Obviously true for $x = 0$ that one has a representation, and $s = 0$, remainder unique. To go up through the induction, consider the separate cases x **even** or **odd.** x **even:** λ, μ, s given for x, with the appropriate uniqueness. Then the difference

$$\mathrm{Rem}(\lambda, 1 + (s+1).\mu) - 2\,\mathrm{Rem}(\lambda, 1 + s.\mu) = 0.$$

So all we have to do to get existence is to get λ', μ' so that

$$\mathrm{Rem}(\lambda', 1 + (j+1)\mu') = \mathrm{Rem}(\lambda, 1 + (j+1).\mu)$$

for $j < s$, but

$$\mathrm{Rem}(\lambda', 1 + (s+1).\mu') = \mathrm{Rem}(\lambda, 1 + (s+1).\mu) + 1.$$

Note that $|x| = |x+1|$ here, for if not $x + 1 = 2^{|x+1|}$, even.

This gives existence. For uniqueness we can do exactly the opposite. That is, from λ', μ', s' working for $x+1$ (odd), use CRT to get λ, μ, s to work for x, by subtracting 1 from last remainder and leaving others unchanged. x **odd**. $x = 2.x' + 1$. Clearly $|x| = |x'| + 1$.

The trick is to use the data for $x'+1$ ($\leq x$) to get data for $2(x'+1) = x + 1$. That is, if the remainders $\eta_0, ..., \eta_s$ work for $x'+1$ then $\eta_0, ..., \eta_s,\ 2\eta$ work for $2(x'+1)$. This is easily checked. Conversely, if $\eta_0, \ldots.\eta_{t-1},\ \eta_t/2$ works for $x'+1$, so by uniqueness for $x'+1,\ t = |x'+1| = |x+1| - 1$, etc.

Definition Let $\varepsilon(u, x)$ be the function, defined for $A \leq |x|$, given by

$$\varepsilon(u, x) = \mathrm{Rem}(\lambda, 1 + (u+2)\mu) - \mathrm{Rem}(\lambda, 1 + (u+1).\mu)$$

where λ, μ, x as above. [So $\varepsilon(u, x) = 0$ or 1.]

The **Theorem 6**

i) $x = \sum_{u \leq |x|} \varepsilon(u, x).2^u$

ii) If ε' is any other definable function on $\{u : u \leq |x|\}$ so $x = \sum_{u \leq |x|} \varepsilon'(u).2^u$ then $\varepsilon'(u) = \varepsilon(u, x)$ all u.

Proof

i) Straightforward induction.

ii) Straightforward induction. □

Definition $u \in x \Leftrightarrow \varepsilon(u, x) = 1$.

Note This will be useful later in fragments.

6 Prime powers. Prime power decomposition.

Definition x is a power of (the prime) p if $p \mid x$ and p is the only prime dividing x.

This is first-order definable.

We define $\nu_p(n)$ by, first, an informal recursion (p a prime $\geq 2,\ n \geq 1$) : $\nu_p(n) = 0$ if $p \nmid n$; if $p \mid n,\ \nu_p(n) = 1 + \nu_p(n/p)$. It is quite easy to show (by CRT coding) that there is a unique definable function of p, n satisfying this recursion. Call it $\nu_p(n)$.

One easily proves: if x is a power of $p,\ x = p^{\nu_p(x)}$. (induction)

Theorem 7

i) $x = \prod_{p|x} p^{\nu_p(x)}$

(ii) If ν is a definable function on $\{p \mid p \mid x\}$ so that

$$x = \prod_{p|x} p^{\nu(p)},$$

then $v(p) = v_p(x)$.

iii) if f is a definable function on a bounded definable set S, taking prime power values (of different primes for different values in S), and

$$x = \prod_{s \in S} f(s),$$

then there is a definable bijection $g : \{p \mid p \mid x\}$ with S, so $f(g(p) = p^{v_p(x)}$.

Proof Easy induction. $\square$

7 A Better Definition of 2^x

7.1 Recall the pattern: $(x \geq 1)$

$$\begin{aligned} x &= a_0 2^s + \dots\dots + a_s 2^0 \\ a_0 &= 1 \ , \ s = |x| \\ \eta_0 &= a_0 2^0 \\ \eta_1 &= a_0 2^1 + a_1 2^0 \\ \eta_{j+1} - 2\eta_j &= a_{j+1} \ , \ \eta_s = x. \end{aligned}$$

The idea is to build up to 2^x via $2^{\eta_0}, 2^{\eta_1}, \dots\dots 2^{\eta_s} = 2^x$

$$2^{\eta_{j+1}} = 2^{2\eta_j + a_{j+1}} = 2^{a_{j+1}}.(2^{\eta_j})^2.$$

Let $\xi_i = 2^{\eta_i}$.

N.B. Length of this "computation" is $|x| = s$.

Because of special features of the powers of 2 we can code this more efficiently than for general Gödel recursion.

We use an auxiliary coding device. Imagine it first in $\mathbb{N}$, and later try to understand it in a general model of PA (and even later in a general model of a weaker set of axioms).

$R(u, v, s)$ is intended to mean:

$$\langle u, v \rangle \text{ codes the first } (s+1) \text{ primes.}$$

Let $R(u, v, s)$ say:

1. (i) $v < u$
   (ii) $\text{Rem}(u, 2) = 0$
   (iii) $\forall p, q < v$ (if p and q are consecutive primes $\text{Rem}(u, q) = \text{Rem}(u, p) + 1$).
   (iv) there is a prime $r < v$ so that $\text{Rem}(u, r) = s$.

Note: All quantifiers in this are polynomially bounded in u, v, s.

One easily proves by induction that if $R(u, v, s)$ and $s' \leq s$ then there is a unique prime $r < u$ with $\text{Rem}(u, r) = s'$, and we call this the s'th prime coded by u, v. Denote it by $p_{s'}^{(u,v)}$. Then prove by induction that if $p_{s'}^{(u,v)}$ and $p_{s'}^{(u',v')}$ exist they are equal (in which case we write $p_{s'}$). One easily shows, for PA, that $s \mapsto p_s$ is total. In fragments of PA this may fail (we believe).

Now back to the computation sequences

$$\eta_i, \xi_i \qquad 0 \leq i \leq s \qquad (s = |x|\,.)$$

Let $y = 2^x$ (work in $\mathbb{N}$, for now). Let w be a number divisible only by the primes

$$p_i \quad i \leq s \quad (p_0 = 2),$$

and let w_i be $p_i^{v_{p_i(w)}}$, so $w = \prod_i w_i$, and the w_i are coprime. We tinker a bit with w to get the w_i to do the essential coding of $\langle \eta_i \rangle, \langle \xi_i \rangle$. We want η, ξ to code these, via

$$\eta_i = \mathrm{Rem}(\eta, w_i),\ \xi_i = \mathrm{Rem}(\xi, w_i),\ 0 \leq i \leq s.$$

We think of p_i as given meaning for $1 \leq s$ by u, v coding the first $s+1$ primes. Suppose we have η, ξ, u, v, w coding the η_i, ξ_i as above. We show that η, ξ, u, v, w can be chosen $< 2y^4$. Note first that by CRT we can always (re)arrange

$$v < u \leq \mathrm{lcm}_{i \leq s}\, p_i \leq \mathrm{lcm}_{i \leq s}\, w_i = w$$

and

$$\eta, \xi < \mathrm{lcm}_{i \leq s}\, w_i = w,$$

so it is enough to get $\omega < 2y^4$.

Note that we may truncate to any $t < s$ to get calculation series for η_t, ξ_t, when $\xi_t = 2^{\eta_t}$. We would truncate to $\prod_{i \leq t} w_i$. Suppose (for induction) we have $\prod_{i \leq t} w_i < 2\xi_t^4$, and the other parameters rearranged to be $\leq \prod_{i \leq t} w_i$.

Basically, we have to locate p_{t+1}, and find a suitable power p_{t+1}^m so that $\xi_{t+1} < p_{t+1}^m$, and also do some tinkering with the (rearranged) u, v, etc.

The basic problem is to locate p_{t+1}, and a power

$$p_{t+1}^{m-1} \leq \xi_{t+1} < p_{t+1}^m$$

and then to show

$$\left(\prod_{j \leq t} w_j \right) .p_{t+1}^m < 2.\xi_{t+1}^4\ .$$

From the inductive hypothesis, that $\prod_{j \leq t} w_j < 2.\xi_t^4$, we need

$$2.\xi_t^4.p_{t+1}^m < 2.\xi_{t+1}^4 ,$$

and since $p_{t+1}^m \leq p_{t+1}.\xi_{t+1}$, we need

$$2.\xi_t^4.p_{t+1}.\xi_{t+1} < 2.\xi_{t+1}^4.$$

Since $\xi_{t+1} \geq \xi_t^2$, we need

$$p_{t+1} < \xi_{t+1}^3/\xi_t^4 ,$$

so we need

$$p_{t+1} < \xi_t^2 . \tag{*}$$

This we now show ......

It is obviously false for $t = 0, 1$, so we suppose it only for $t \geq 2$. Now

$$\begin{aligned} p_0....p_t &= 2.3.5.p_3....p_t \\ &\leq 2.3.5.\xi_2^2....\xi_{t-1}^2 \\ &< 2.3.5.w_2^2....w_{t-1}^2 \\ &< (2.3.5/w_0^2.w_1^2) \cdot (w_0....w_{t-1})^2 \\ &< (2.3.5/w_0^2.w_1^2) \cdot \xi_{t-1}^2 . \end{aligned}$$

By Euclid, $p_{t+1} < p_0....p_t$, so we are done if we show

$$\begin{aligned} 2.3.5/w_0^2.w_1^2 \cdot \xi_{t-1}^2 &< \xi_t^2 \\ \text{i.e. } 2.3.5/w_0^2.w_1^2 \cdot \xi_{t-1}^2 &< \xi_{t-1}^4 , \\ \text{i.e. } 2.3.5/w_0^2.w_1^2 &< \xi_{t-1}^2 \qquad t \geq 2 \\ \text{i.e. } 2.3.5 &< w_0^2.w_1^4 . \end{aligned}$$

But

$$\begin{aligned} \xi_0 &= 2, \text{ so } w_0 \geq 4 \\ \xi_1 &\geq 4, \text{ so } w_1 \geq 9 , \end{aligned}$$

whence result.

It should be clear that all this works in PA. Indeed, as we discuss below, it works in a much weaker system.

Let us just set down in words the new definition of

$$y = 2^x, (x \geq 1) : \exists s, u, v, w, \xi, \eta < 2y^4.$$

[u, v code the first $s+1$ primes, $(p_0, ...p_s)$, and if w_i is highest power of p_i dividing w, then $\mathrm{Rem}(\eta, w_0) = 1$ and $\mathrm{Rem}(\eta, w_s) = x \wedge \mathrm{Rem}(\xi, w_0) = 2$ and $\mathrm{Rem}(\xi, w_s) = y \wedge$ for all $j < s$

$$\mathrm{Rem}(\eta, \omega_{j+1}) - 2\,\mathrm{Rem}(\eta, w_j) = 0 \text{ or } 1$$

and if μ_{j+1} is this remainder then $\mathrm{Rem}(\xi, w_{j+1}) = 2^{\mu_{j+1}}.\,\mathrm{Rem}(\xi, w_j)^2$.]

By the above all quantifiers in this formula $B(x, y)$ are bounded by $2.y^4$. Obviously in $\mathbb{N}$, for $x \geq 1,\ B(x, y) \Leftrightarrow y = 2^x$.

Less obviously, but a routine long exercise,

$$PA \vdash \forall x, y(B(x, y) \leftrightarrow y = 2^x).$$

7.2 Bounded Arithmetic

$I\Delta_0$ is the class of (axioms for) discretely ordered rings in which induction is restricted to sets defined using only **polynomially bounded quantifiers.** Such sets are called Δ_0-sets and are defined recursively as follows (for a DOR R with $N = \{x \in R : x \geq 0\}$).

a) if $f \in R[x_1, ...x_n]$, $\{\bar{x} \in N^n : f(\bar{x}) = 0\}$ is Δ_0, and $\{\bar{x} \in N^n : f(\bar{x}) \geq 0\}$ is Δ_0;

b) closure under Boolean operations;

c) $[|x| = x$ if $x \geq 0$, $= -x$ if $x \leq 0]$.

   If $X \subseteq R^{n+1}$ is Δ_0, and $g \in R[x_2, ...x_{n+1}]$, then $\{(x_2, ...x_{n+1}) \in N^n : (\exists x_1)[\ |x| \leq |g(x_2, ...x_{n+1})| \wedge (x_1, ...x_{n+1}) \in X\ ]$ is in Δ_0. ["proper direct image"].

Obviously if M is a model of PA then M is a model of $I\Delta_0$. The converse is not true, as we shall see.

Parikh's Construction

Let M be a model of DOR, and let M_1 be an **initial segment** of M in the sense that

(i) M_1 is an ordered subring of M;

(ii) if $x \in M_1,\ y \in M,\ |y| \leq |x|$, then $y \in M_1$.

Example: $\mathbb{Z}$ in any M.

In the above situation we write: $M_1 \subseteq_e M$, and say M is **an end extension** of M_1.

The most basic fact here is:

Lemma 8 If $M_1 \subseteq_e M$, and M is a model of $I\Delta_0$, so is M_1.

Proof By induction on the recursive definition of Δ_0-set, we show first:

Lemma 9 If $A(x_1, ...x_n)$ is Δ_0 over M_1, and $b_1, ...b_n \in M_1$ then

$$M_1 \models A(b_1, ...b_n) \Leftrightarrow M \models A(b_1, ...b_n)$$

(clearly A is Δ_0-over M).

If $A(x_1, ...x_n)$ is either

$$\{\bar{x} \in N_1^n : f(\bar{x}) > 0\} \text{ or } \{\bar{x} \in N_1^n : f(\bar{x}) = 0$$

for $f \in M_1[x_1, ...x_n]$, result clearly true.

Result clearly propagates through Boolean combinations.

Crucial case is: $X \subseteq M_1^{n+1}$, Δ_0, and $g \in M_1[x_2, ...x_{n+1}]$, and we want

$$\begin{array}{rcl} M_1 & \models & (b_2...b_{n+1}) \in \{(x_2, ...x_{n+1}) \in N_1^n (\exists x_1)[\, |x_1| \leq |g(x_2, ...x_{n+1})| \wedge (x_1, ...x_{n+1}) \in X\,]\} \\ & \Leftrightarrow & \\ M & \models & (b_1, ...b_{n+1}) \in \{(x_2, ...x_{x+1}) \in N^n : (\exists x_1)[\, |x_1| \leq |g(x_2, ...x_{n+1})| \wedge (x_1, ...x_{n+1}) \in X\,]\}. \end{array}$$

$\Rightarrow$: Suppose $\exists x_1 \in N$,

$$|x_1| \leq |g(b_2, ...b_{n+1})| \wedge (x_1, b_2, ...b_{n+1}) \in X.$$

By induction $(x_1, ...b_{n+1}) \in X$ in sense of M, so

$$M \models |x_1| \leq |g(b_2, ...b_{n+1})| \wedge (x_1, b_2, ...b_{n+1}) \in X.$$

$\Leftarrow$: Suppose $\exists_1' \in N$

$$|x_1'| \leq |g(b_2, ...b_{n+1})| \wedge (x_1' b_2, ...b_{n+1}) \in X \text{ (in sense of } M).$$

Since $M_1 \subseteq_e M$, $x_1' \in N_1$, and then by induction $(x_1', b_2, ...b_{n+1}) \in X$ (in sense of M_1), whence result. □

Now we prove Lemma 8. Let X be a Δ_0-subset of N defined over M_1, and suppose that $0 \in X$ and $(\forall t)(t \in X \to t+1 \in X)$ in sense of M_1. Then $0 \in X$ in sense of M by Lemma 9. Now suppose $X \neq N_1$, and pick $a \in N_1$, so $M_1 \models \neg(a \in X)$. So by Lemma 9, $M \models \neg(a \in X)$. So $M \models (\exists x)(|x| \leq a \wedge a \notin X)$, so since $M \models I\Delta_0$,

$$M \models (\exists y)(|y| \leq a \wedge y \in X \wedge (y+1) \notin X).$$

By Lemma 9,

$$M_1 \models (\exists y)(|y| \leq a \wedge y \in X \wedge (y+1) \notin X),$$

contradicting

$$M_1 \models \forall t(t \in X \to t+1 \in X).$$

□

Corollary If $M \models PA$, and $M_1 \subseteq_e M$ then $M_1 \models IA_0$. This leads to Parikh's construction, inside any $M_1 \models I\Delta_0$. Let $a \in N$, and let

$$M_1 = \{x \in M : \text{ for some } k \in \mathbb{N}, \; |x| \leq (a+1)^k\}.$$

Then easily M_1 is a DOR and $M_1 \subseteq M$. We define $BP[a]$ (rel. to M) as the above M_1. By the above, $BP[a] \models I\Delta_0$.

This can be used to show that $I\Delta_0$ is a very restricted system.