Defining Exponentiation

Here's a loose end that needs tying up. In proving the incompleteness theorems, we took the language of arithmetic to include exponentiation among its primitive symbols. This was convenient, because it made it easy to encode a finite set of numbers by an single number. It was a convenient extravagance, but an unnecessary one. We can prove all our results in a restricted version of the language of arithmetic that eliminates "E" from among its symbols and that removes (Q7) and (Q8) from the axioms of Robinson's arithmetic.

The proof, which was part of Gödel's original paper, makes use of the following venerable theorem of number theory:

> **Chinese Remainder Theorem (Qin Jiushao).** Given $p_0, p_1, \ldots, p_n$ relatively prime integers > 1 (that is, no two of the p_is have a common divisor other than 1), and given a sequence $a_0, a_1, \ldots, a_n$, with each $a_i < p_i$, we can find a number c such that, for each i, a_i is the remainder on dividing c by p_i.

Proof: We first show that, whenever q and p are relatively prime, we can find c and d with $qc = pd + 1$. To do this, find the least positive integer r such that there exist c and d with $qc = pd + r$, and assume, for *reductio ad absurdum*, that $r > 1$. There are two cases:

Case 1. r doesn't divide q. Then we can find $e > 0$ and s with $0 < s < r$ so that $q + s = re$. Then $qce = pde + re$, and so $q(ce - 1) = pde + s$. This contradicts the leastness of r.

Case 2. r divides q. Then r doesn't divide p, and so we can find $f > 0$ and t with $0 < t < r$ so that $p + t = rf$. Then $qcf = pdf + rf$, and so $qcf = p(df - 1) + t$. This again contradicts the leastness of r.

Now let Q be the product of the p_is, and let q_i be the quotient of Q divided by p_i. Then q_i and p_i are relatively prime, so that we can find c_i and d_i with $q_i c_i = p_i d_i + 1$. Thus the remainder

on dividing $q_i \cdot c_i$ by p_i is equal to 1, and so the remainder on dividing $q_i \cdot c_i \cdot a_i$ by p_i is equal to a_i. Let e be the sum $\Sigma\, q_j \cdot c_j \cdot a_j$. p_i divides each of the q_js other than q_i, and so the remainder on dividing e by p_i is the same as the remainder on dividing $q_i \cdot c_i \cdot a_i$ by p_i, which is a_i,☒

We now define Gödel's β-function. Let $\beta(u,v,w)$ to be the remainder obtained on dividing u by $(v \cdot w) + 1$. β can be defined by a bounded formula in the language of arithmetic. For $x > 0$, we have $(x\mathrm{E}y) = z$ if and only if the following formula is satisfied:

$$(\exists u)(\exists v)((\beta(u,v,0) = 1 \wedge (\forall w < y)\beta(u,v,sw) = (\beta(u,v,w) \cdot x)) \wedge \beta(u,v,y) = z).$$

The right-to-left direction of this characterization is obvious. What is hard is to find u and v that verify the left-to-right direction. Given x, y, and z with $(x\mathrm{E}y) = z$, let $v = z!$, the product of the positive integers $\leq z$. If $s < t \leq z$, then $(s \cdot v) + 1$ and $(t \cdot v) + 1$ are relatively prime, since if p were a prime that divided both of them, p would divide $(t - s)v$, and so, since $(t - s)$ is one of the factors of v, p would divide v. But this enables us to conclude that the remainder on dividing $(t \cdot v) + 1$ by p is one, contrary to our assumption that p divides $(t \cdot v) + 1$. Use the Chinese Remainder Theorem to find u so that, for each $t \leq y$, $x\mathrm{E}t$ is the remainder on dividing u by $(t \cdot v) + 1$.☒

As long as our sole interest is the language of arithmetic, the fact that exponentiation can be treated as defined rather than primitive is a mere technical curiosity. It's practical utility comes when we try to show that theories expressed in languages other than the language of arithmetic are undecidable by interpreting Robinson's arithmetic into those other theories. If, in doing this, we don't have to worry about exponentiation, it makes life a lot easier.

(Q7) and (Q8) are the recursive definition of exponentiation, and we can use Gödel's beta function to convert this recursive definition into an explicit definition. We cannot take the process a step further by converting (Q5) and (Q6), which are the recursive definition of

multiplication, into an explicit definition, thereby eliminating multiplication as one of the primitive operations of the language. This follows from a 1929 theorem of Mojzesz Presburger, who showed that there is a decision procedure for the set of sentences of the language with nonlogical symbols "0", "s," "+," and "<" that are true in the standard model. Adding "·" gives us an undecidable theory, so "·" must not be explicitly definable.[1]

[1]It is perhaps worth pointing out that "0," "<" and "s" can all be defined in terms of "+." "$x = 0$" can be defined as "$(x + x) = x$." "$x < y$" is defined by "$(\sim x = y \wedge (\exists z)(x + z) = y)$." For "$sx = y$," we use "$(\forall z)(x < z \leftrightarrow (y = z \vee y < z))$." Thus, for us, the import of Presburger's theorem is that you can't define multiplication in terms of addition.