3. Number theoretic theorems

By a <u>number theoretic theorem</u>[4] we shall mean a theorem of the

---

[4] I believe there is no generally accepted meaning for this term, but it should be noticed that we are using it in a rather restricted sense. The most generally accepted meaning is probably this: suppose we take an arbitrary formula of the function calculus of first order and replace the function variables by primitive recursive relations. The resulting formula represents a typical number theoretic theorem in this (more general) sense.

---

form ' $\theta(x)$ vanishes for infinitely many natural numbers x ', where $\theta(x)$ is a primitive recursive[5] function.

---

[5] Primitive recursive functions of natural numbers are defined inductively as follows. Suppose $f(x_1,\dots,x_{n-1})$, $g(x_1,\dots,x_n)$, $h(x_1,\dots,x_{n+1})$ are primitive recursive then $\varphi(x_1,\dots,x_n)$ is primitive recursive if it is defined by one of the sets of equations (a) - (e).

(a) $\varphi(x_1,\dots,x_n) = h(x_1,\dots,x_{m-1}, g(x_1,\dots,x_n), x_{m+1},\dots,x_{n-1},x_n)$, $(1 \leq m \leq n)$

(b) $\varphi(x_1,\dots,x_n) = f(x_1,\dots,x_{n-1})$

(c) $\varphi(x_1) = a$, where $n = 1$ and a is some particular natural number.

(d) $\varphi(x_1) = x_1 + 1 \qquad (n = 1)$

(e) $\varphi(x_1,\dots,x_{n-1},0) = f(x_1,\dots,x_{n-1})$
$\varphi(x_1,\dots,x_{n-1},x_n+1) = h(x_1,\dots,x_n,\varphi(x_1,\dots,x_n))$

The class of primitive recursive function is more restricted than the computable functions, but has the advantage that there is a process whereby one can tell of a set of equations whether if defines a primitive recursive function in the manner described above.

If $\varphi(x_1,\dots,x_n)$ is primitive recursive then $\varphi(x_1,\dots,x_n) = 0$ is described as a primitive recursive relation between $x_1,\dots,x_n$.

We shall say that a problem is number theoretic if it has been shown that any solution of the problem may be put in the form of a proof of one or more number theoretic theorems. More accurately we may we shall have

$$\left|\zeta\left(\frac{\ell+\vartheta}{M} + i\,\frac{m+\vartheta'}{M}\right)\right| \geqslant \frac{X(\ell, m, M) - 122T}{M}$$

$$\frac{1}{2} + \frac{1}{T} \leq \frac{\ell-1}{M} < \frac{\ell+1}{M} < 2 - \frac{1}{M},\ 2 < \frac{m-1}{M} < \frac{m+1}{M} < T,\quad -1<\vartheta<1,\ -1<\vartheta'<1$$

if we define $B(M,T)$ to be the smallest value of $X(\ell, m, M)$ for which $\frac{1}{2} + \frac{1}{T} + \frac{1}{M} \leq \frac{\ell}{M} < 2 - \frac{1}{M},\ 2 + \frac{1}{M} < \frac{m}{M} < T - \frac{1}{M}$, then the Riemann hypothesis is true if for each T there is M satisfying $B(M,T) > 122T$. If on the other hand there is T such that for all M, $B(M,T) \leq 122T$, the Riemann hypothesis is false; for let ℓ_M, m_M be such that $X(\ell_M, m_M, M) \leq 122T$ then $\left|\zeta\left(\frac{\ell_M + i m_M}{M}\right)\right| \leq \frac{244T}{M}$

Now if a is a condensation point of the sequence $\frac{\ell_M + i m_M}{M}$ then since $\zeta(s)$ is continuous except at $s = 1$ we must have $\zeta(a) = 0$ implying the falsity of the Riemann hypothesis. Thus we have reduced the problem to the question as to whether for each T there is M for which $B(M,T) > 122T$. $B(M,T)$

is primitive recursive, and the problem is therefore number theoretic.

validity of C implies the validity of C', and let there be a valid system C_o in W. Finally suppose that given any computable sequence $C_1, C_2, \ldots$ of systems in W the 'limit system' in which a formula is provable if and only if it is provable in one of the systems C_j also belongs to W. These limit systems are to be regarded, not as functions of the sequence given in extension, but as functions of the rules of formation of their terms. A sequence given in extension may be described by various rules of formation, and there will be several corresponding limit systems. Each of these may be described as <u>a</u> limit system of the sequence.

Under these circumstances we may construct an ordinal logic. Let us associate positive integers with the systems, in such a way that to each C corresponds a positive integer m_C, and m_C completely describes the rules of procedure of C. Then there is a W.F.F. $\underline{K}$, such that $\underline{K}(\underline{m}_C)$ conv $\underline{m}_{C'}$ for each C in W, and there is a W.F.F. $\underline{\Theta}$ such that if $\underline{D}(\underline{r})$ conv $\underline{m}_{C_r}$ for each positive integer r then $\underline{\Theta}(\underline{D})$ conv $\underline{m}_C$ where C is a limit system of $C_1, C_2, \ldots$. With each system C of W it is possible to associate a logic formula $\underline{L}_C$: the relation between them is that if G is a formula of W and the number theoretic theorem corresponding to G (assumed expressed in the conversion calculus form) asserts that $\underline{B}$ is dual, then $\underline{L}_C(\underline{B})$ conv 2 if and only if G is provable in C. There will be a W.F.F. $\underline{G}$ such that $\underline{G}(\underline{m}_C)$ conv $\underline{L}_C$ for each C of W. Put

$$\underline{N} \to \lambda a . \underline{G}(a(\underline{\Theta}, \underline{K}, \underline{m}_{C_o}))$$

9. Completeness questions.

The purpose of introducing ordinal logics was to avoid as far as possible the effects of Gödel's theorem. It is a consequence of this theorem, suitably modified, that it is impossible to obtain a complete logic formula, or (roughly speaking now) a complete system of logic. We were able, however, from a given system to obtain a more complete one by the adjunction as axioms of formulae, seen intuitively to be correct, but which the Gödel theorem shows are unprovable[21] in the original system; from this we obtained a yet more complete system by a repetition of the process, and so on. We found that the repetition of the process gave us a new system for each C-K ordinal formula. We should like to know whether this process suffices, or whether the system should be extended in other ways as well. If it were possible to tell of a W.F.F. in normal form whether it was an ordinal formula we should know for certain that it was necessary to extend in other ways. In fact for any ordinal formula Λ it would then be possible to find a single logic formula L such that if $\Lambda(\Omega, A)$ conv 2 for some ordinal formula Ω then $L(A)$ conv 2. Since L must be incomplete there must be formulae A for which $\Lambda(\Omega, A)$ is not convertible to 2 for any ordinal formula Ω. However, in view of the fact, proved in § 7, that there is no method of determining of a formula in normal form whether it is an ordinal formula, the case does not arise, and there is still a possibility that some

---

[21] In the case of P we adjoin all of the axioms $(\exists x_0)\,\mathrm{Proof}_P[x_0, f^{(m)}0]$, where m is the G.R. of $\mathfrak{F}$, some of which the Gödel theorem shows to be unprovable in P.

already required of them, only that it is so with the more natural definitions.

I shall prove the completeness theorem in the following form. If $\mathfrak{B}[x_0]$ is a recursion formula and $\mathfrak{B}[0]$, $\mathfrak{B}[f0]$, . . . are all provable in P, then there is a C-K ordinal formula $\underline{A}$ such that $(x_0)\mathfrak{B}[x_0]$ is provable in the system $P_{\underline{A}}$ of logic obtained from P by adjoining as axioms all formulae whose G.R's are of the form

$$\underline{A}(\lambda mn.\, m(\varpi(2,n), \varpi(3,n)), K, M_P, \underline{r})$$

(provided they represent propositions)

First let us define the formula $\underline{A}$. Suppose $\underline{D}$ is a W.F.F. with the property that $\underline{D}(n)$ conv 2 if $\mathfrak{B}[f^{(n-1)}0]$ is provable in P, but $\underline{D}(n)$ conv 1 if $\sim\mathfrak{B}[f^{(n-1)}0]$ is provable in P (P is being assumed consistent). Let Θ be defined by

$$\Theta \rightarrow \{\lambda vu.\, v(v(v,u))\}(\lambda vu.\, v(v(v,u)))$$

and let V be a formula with the properties

$$V(2) \text{ conv } \lambda u.\, u(Suc, U)$$

$$V(1) \text{ conv } \lambda u.\, u(\underline{I}, \Theta(Suc))$$

The existence of such a formula is established in Kleene 1, corollary on p 220. Now put

$$\underline{A}^{*} \rightarrow \lambda ufx.\, u(\lambda y.\, V(\underline{D}(y), y, u, f, x)$$

$$A \rightarrow Suc(\underline{A}^{*})$$