UNIVERSAL THEORIES OF INTEGERS AND THE EXTENDED BLIZNETSOV HYPOTHESIS

É. B. Belyakov and V. I. Mart'yanov UDC 517.11

It has been proved in [2, 4] that the universal theory of the integers $\mathbb{Z}$ in the signature $<+, |, 1>$, where $|$ is the relation of divisibility, is decidable. It has been proved in [3] that the universal theory of the integers in the signature $<+, 1, \mathcal{D}>$ where the predicate $\mathcal{D}(x,y,z)$ is true if $z = \pm \text{НОД}(x,y)$, is decidable. From a letter of Yu. V. Matiyasevich, we have come to know that it is possible to reduce the problem of decidability of the universal theory of $<\mathbb{Z}; +, 1, \mathcal{D}>$ to that of decidability of the universal theory of $<\mathbb{Z}; +, |, 1>$, since

$$\mathcal{D}(x,y,z) \Leftrightarrow z|x \,\&\, z|y \,\&\, \forall u\,(u|x \,\&\, u|y \to u|z),$$

$$\neg\mathcal{D}(x,y,z) \Leftrightarrow \forall u \forall v\,(z \nmid x \vee z \nmid y \vee x \nmid u \vee y \nmid v \vee z \neq u+v).$$

Here we prove the decidability of the universal theory of the integers $\mathbb{Z}$ in the signature $<+, |, P, 1>$, where P is the one-place predicate that selects prime numbers. The decidability of this theory is proved under the assumption of satisfiability of the extended Bliznetsov hypothesis, formulated in the following manner.

Let $g_1(x) = a_1x + b_1, \ldots, g_n = a_nx + b_n$ be polynomials with relatively prime integral coefficients such that all the numbers $g_1(t), \ldots, g_n(t)$ are relatively prime to $n!$ for a certain t Then there exists an infinite sequence of integers $t_1 < \ldots < t_m < \ldots$ such that all the numbers $g_1(t_m), \ldots, g_n(t_m)$ are prime for each m. The Bliznetsov hypothesis is the particular case of the extended Bliznetsov hypothesis for the polynomials x and $x+2$. Let us also observe that the extended Bliznetsov hypothesis is satisfiable for $n=1$ by virtue of the Dirichlet theorem [1]. Therefore, besides a relative strengthening of the theorem, which is obtained under the assumption of satisfiability of the extended Bliznetsov hypothesis, we have the following "absolute" strengthening: The fragment of the universal theory of the integers $\mathbb{Z}$ in the signature $<+, 1, |, P>$, in which each formula contains at most one occurrence of the predicate P, is decidable.

In the present article, we use essentially the methods, definitions, and results of [3].

1. Definitions and Preliminary Information

The conditions

$$\Gamma = [\{P(f_i)\}, \{u_j \mid g_j\}, \{v_\ell = 0\}, \{z_s\}, \{w_m \neq 0\}] \tag{1}$$

where $f_i, u_j, \ldots, w_m$ are polynomials with rational coefficients, are said to be satisfiable if there exists a suite $\omega \in \mathbb{Z}^n$ such that $P(f_i(\omega))$, $u_j(\omega) | g_j(\omega)$, $v_\ell(\omega) = 0$, $w_m(\omega) \neq 0$, and

Translated from Algebra i Logika, Vol. 22, No. 1, pp. 26-34, January-February, 1983. Original article submitted December 8, 1981.

the polynomials from Γ have integral values on the suite ω. Let us denote it, in short, by $\models \Gamma(\omega)$. The conditions $\bar{\Gamma}$ are said to be obtained from the conditions Γ by deleting the equation $U = 0$, if this equation belongs to Γ, from this equation a certain $x_n = \bar{U}(x_1, \ldots, x_{n-1})$ is found, the value of this x_n is substituted in all the polynomials that occur in the expression of the conditions Γ, and the condition that $\bar{U}(x_1, \ldots, x_{n-1})$ takes integral values is added. The conditions Γ and $\bar{\Gamma}$ are said to be equivalent if either these are both satisfiable or both nonsatisfiable.

In the sequel, the expression "the polynomials $W_1, \ldots, W_n$ are linearly independent" will mean that their linear combination $\alpha_1 W_1 + \ldots + \alpha_n W_n \in \mathbb{Z} \Leftrightarrow \alpha_1 = \ldots = \alpha_n = 0$.

Let $W_1, \ldots, W_n$ be linearly independent polynomials. Then there exist polynomials $\xi_1, \ldots, \xi_n$ such that

$$x_1 = \xi_1(W_1, \ldots, W_n), \ldots, x_n = \xi_n(W_1, \ldots, W_n). \tag{2}$$

Let $\mathcal{L}$ denote the set of linear polynomials in the variables $x_1, \ldots, x_n$ with rational coefficients. We will denote the submodule generated by the polynomials $f_1, \ldots, f_k$ in $\mathcal{L}$, as a module over the ring $\mathbb{Q}$ (over the ring of integers $\mathbb{Z}$), by $\mathbb{Q}(f_1, \ldots, f_k)(\mathbb{Z}(f_1, \ldots, f_k))$.

The conditions $\bar{\Gamma}$ are said to be obtained from the conditions Γ by the change of variables (2) if $W_1, \ldots, W_n \in \mathbb{Z}(\{f_i\}, \{u_j\}, \{g_j\}, \{v_e\}, \{\tau_s\}, \{w_m\}, x_1, \ldots, x_n)$ and each polynomial f that occurs in $\bar{\Gamma}$ is replaced by the polynomial $f(\xi_1(x_1, \ldots, x_n), \ldots, \xi_n(x_1, \ldots, x_n))$, and, in addition, in $\bar{\Gamma}$, the conditions that the polynomials $\xi_1, \ldots, \xi_n$ take integral value are added.

LEMMA 1. If the conditions $\bar{\Gamma}$ are obtained from the conditions Γ by deleting equations or by the change of variables (2), then the conditions $\bar{\Gamma}$ and Γ are equivalent.

Remark. In certain cases, the conditions (1) will be extended by expressions of the forms $\{\neg P(t_k)\}$ and $\{q_a \nmid d_a\}$. It is clear that all the preceding definitions and properties can be generalized for this type of condition in a natural manner.

The product of the denominators of all the coefficients of a polynomial f that are written as irreducible fractions is called the denominator $\tau(f)$ of f. The product of all $\tau(f)$ for $f \in \Gamma$ is called the denominator $\tau(\Gamma)$ of the conditions Γ. The smallest natural number that is greater than the greatest modulus of the coefficients of a polynomial f is called the height $U(f)$ of f. The greatest height of the polynomials that occur in the expression of the conditions Γ is called the height $U(\Gamma)$ of Γ.

Let us denote the greatest power of a prime number p that divides a by p^a. Let us also denote the set of the prime divisors of a (of numbers from the suite ω that divide a) and the set of the first k prime numbers by $\pi(a), (\pi(\omega))$ and π_k, respectively. By definition, $\theta_k = \prod_{p \in \pi_k} p^k$ for $k = 1, 2, \ldots$.

Let us define the predicates $+$ and $|$, on the residue ring $\mathbb{Z}(t)$ in the usual manner and let us call the invertible elements prime. We say that a suite $\omega \in \mathbb{Z}$ satisfies the conditions Γ of type (1) modulo a number t if $\langle \mathbb{Z}(t); +, |, P \rangle \models \Gamma(\omega)$, and, in addition,

$f(\omega) \not\equiv 0 (mod_p t)$ for each polynomial f that occurs in the expression of Γ and each $p \in \pi(t)$. In this case, the conditions Γ are said to satisfiable modulo t.

LEMMA 2. For each set of conditions Γ and each number t, it can be effectively determined whether there exists a number $m > t$ such that the conditions Γ are satisfiable modulo θ_m.

Proof. We know that the elementary theory of the class $\mathcal{K}$ of the residue rings of integers in the signature $\langle +, \cdot \rangle$ is decidable. The question whether the number m exists is written down by a formula of signature $\langle +, \cdot \rangle$ of the class $\mathcal{K}$.

2. Properties of the Conditions that Consist of Ratios of Polynomials

Following [3], we introduce a series of definitions and notions. Let the conditions T consist of only ratios of polynomials, i.e., let $\Gamma = [\{f_\alpha \mid g_\alpha\}]$, and suppose that these polynomials belong to the ring $Q[x_1, \ldots, x_n]$. By definition, $F(\Gamma)$ are the minimal conditions with the following properties:

a) $\Gamma \subset F(\Gamma)$ and $f_\alpha \mid f_\alpha \in F(\Gamma)$ for each α;

b) If $f \mid a \cdot u, u \mid g \in \Gamma$, then $f \mid a \cdot g \in F(\Gamma)$, where $a \in \mathbb{Q}$;

c) If $f \mid g_1, f \mid g_2 \in F(\Gamma)$, then $f \mid g_1 \pm g_2 \in F(\Gamma)$.

Let the conditions consist of ratios of polynomials:

$$\Omega = [f_1 \mid g_1, \ldots, f_K \mid g_K]. \tag{3}$$

Let us set

$$\Omega^{(0)} = \Omega,\ \Omega^{(1)} = F(\Omega^{(0)}), \ldots, \Omega^{(i+1)} = F(\Omega^{(i)}), \ldots,$$

$$\bar{\Omega} = \lim_{i \to \infty} \Omega^{(i)},\ a_j^{(0)} = \mathbb{Z}(f_j, g_j),\ a_j^{(i)} = \{g : f_j \mid g \in \Omega^{(i)}\},$$

$$a_j = \{g : f_j \mid g \in \bar{\Omega}\}$$

for $j = 1, \ldots, K$, and $i > 0$.

We will say that the conditions Γ_1 follow from the conditions Γ (in symbols, $\Gamma \Rightarrow \Gamma_1$), if each suite ω that satisfies the conditions Γ satisfies the conditions Γ_1 also. The conditions Γ and Γ_1 are said to be isomorphic if $\Gamma \Rightarrow \Gamma_1$ and $\Gamma_1 \Rightarrow \Gamma$, or, in short, $\Gamma \Leftrightarrow \Gamma_1$.

The number of letters of the set $\{x_1, \ldots, x_n\}$ that occur with nonzero coefficients in the expression of Γ is called the rank of the conditions Γ.

The conditions Γ are said to split into the conditions $\Gamma_1, \ldots, \Gamma_m$ $(\Gamma = \Gamma_1 \vee \ldots \vee \Gamma_m)$, if for each suite ω that satisfies Γ, there exists $i = 1, \ldots, m$ such that ω satisfies Γ_i and $j = 1, \ldots, m$ holds for each $\Gamma_j \Rightarrow \Gamma$.

By definition, the canonical conditions

$$\mathcal{K} = \bigcup_{i=1}^{n-1} \mathcal{K}_i \tag{4}$$

have the following properties:

a) If $\mathcal{K}_i$ is nonempty, then

$$\mathcal{K}_i = [f_{i1}(x_1,\ldots,x_i) | g_{i1}(x_1,\ldots,x_i) + d_{i1}x_{i+1},\ldots,f_{im}(x_1,\ldots,x_i) | g_{im}(x_1,\ldots,x_i) + d_{im}x_{i+1}],$$

where each d_{ij} is nonzero.

b) If $f | g(x_1,\ldots,x_\ell) \in \mathcal{K}$, then $f | g(x_1,\ldots,x_\ell) \in \overline{\mathcal{K}}_{\ell-1}$, where $\mathcal{K}_{(i)} = \mathcal{K}_1 \cup \ldots \cup \mathcal{K}_i$.

The following lemma is a reformulation of Lemmas 7 and 8 of [3] and is stated without proof.

LEMMA 3. Let Ω be conditions of rank ρ of the type (3). Then either linearly independent polynomials $u_1,\ldots,u_\rho$ can be effectively indicated such that $u_1,\ldots,u_\rho \in \mathbb{Z}(f_1,\ldots,f_K,g_1,\ldots,g_K)$ and the conditions $\mathcal{K}$ obtained from the conditions Ω by the change of variables (2) are canonical and, in addition, the representation (4) of $\mathcal{K}$ can be found effectively, or polynomials $v_1,\ldots,v_m$ such that $\Omega = [\Omega, v_1 = 0] \vee \ldots \vee [\Omega, v_m = 0]$ can be indicated.

3. Main Results

The conditions

$$\mathcal{K}^* = \mathcal{K} \cup \mathcal{K}' \tag{5}$$

are said to be P-canonical if $\mathcal{K}$ are canonical conditions of type (4) and $\mathcal{K}' = \bigcup_{i=1}^{n-1} \mathcal{K}'_i$, where $\mathcal{K}'_i = [P(\beta_{i1}),\ldots,P(\beta_{iK})]$, the polynomials $\beta_{i1} = s_{i1}(x_1,\ldots,x_i) + \ell_{i1}x_{i+1},\ldots,\beta_{iK} = s_{iK}(x_1,\ldots,x_i) + \ell_{iK}x_{i+1}$.

As in [2], by definition, we set $\tilde{\Omega} = [\{f|g : f|q\cdot g \in \overline{\Omega}$ for a certain $q \in \mathbb{Q}]$, and $\rho(i) = 2^{2^{i-1}} \cdot a^{2^i}$, and let $\mathcal{L}_{\tau,\ell}$ be the set of the polynomials from $\mathcal{L}$ whose denominators divide the number τ and heights do not exceed ℓ.

A suite $\varepsilon = [\varepsilon_1,\ldots,\varepsilon_m]$ is said to be concordant with respect to denominator τ and height a with a suite $\omega = [\omega_1,\ldots,\omega_n]$ that satisfies the conditions (5) modulo a number t if the following conditions are satisfied:

a) $\varepsilon_i \equiv \omega_i \pmod{t}$ for $i = 1,\ldots,m$.

b) The conditions $\mathcal{K}^*$ are satisfiable on the suite ε.

c) For arbitrary prime $p \notin \pi(t)$ and arbitrary polynomials $g_1, g_2 \in \mathcal{L}_{\tau,a}$ in the variables $x_1,\ldots,x_m$, if $p | g_1(\varepsilon)$ and $p | g_2(\varepsilon)$, then either there exists a polynomial f in the variables $x_1,\ldots,x_m$ such that $f|g_1, f|g_2 \in \tilde{\mathcal{K}}$ and ${}_pf(\varepsilon) = {}_pg_1(\varepsilon) = {}_pg_2(\varepsilon)$, and, in addition, $f(\varepsilon), g_1(\varepsilon), g_2(\varepsilon) \in \mathbb{Z}$ or $g_1 = q\cdot g_2$ for a certain $q \in \mathbb{Q}$.

LEMMA 4. Let $\mathcal{K}^*$ be ρ-canonical conditions of the type (5), all of whose polynomials belong to $\mathcal{L}_{\tau,a}$, and set $b=(2\rho(n))^{n+2}$. Then (it is assumed that the extended Bliznetsov hypothesis is satisfiable) for each suite $\omega=[\omega_1,\ldots,\omega_n]$ that satisfies the conditions $\mathcal{K}^*$ modulo the number θ_b, there exists a suite $[\varepsilon_1,\ldots,\varepsilon_n]$ that is concordant with it with respect to denominator τ and height a.

Proof. It is sufficient to show that for each $i=1,\ldots,n$ there exists a suite $[\varepsilon_1,\ldots,\varepsilon_i]$, that is concordant with respect to denominator τ and height $\rho(n-i)$ with the suite ω, since $\rho(0)=a$. We will prove this statement by induction over i. The statement is obvious for $i=2$. By induction hypothesis, there exists a suite $[\varepsilon_1,\ldots,\varepsilon_i]=\delta$ that is concordant with respect to denominator τ and height $c=\rho(n-i)$ with the suite ω.

Let us consider the system

$$\Sigma=\{f_{i1}(\delta)\mid g_{i1}(\delta)+d_{i1}x_{i+1},\ldots,f_{im}(\delta)\mid g_{im}(\delta)+d_{im}x_{i+1}\}\cup \cup\{P(s_{i1}(\delta)+\ell_{i1}x_{i+1}),\ldots,P(s_{ik}(\delta)+\ell_{ik}x_{i+1})\}. \tag{6}$$

By definition, we set $\mathcal{T}=\{p: p\in\pi_b \text{ or } p\in\pi(f(\delta))\}$ for a certain polynomial $f\in\mathcal{L}_{\tau,c}$ in the variables $x_1,\ldots,x_i$ such that $f(\delta)\in\mathbb{Z}$.

For each $p\in\mathcal{T}\setminus\pi_b$ we let β_p be such that $p^{\beta_p}=pf(\delta)$, where $f\in\mathcal{L}_{\tau,c}$; $f(\delta)\in\mathbb{Z}$, $p\in\pi(f(\delta))$ and $f\in\mathbb{Q}(x_1,\ldots,x_i)$.

The system of divisibilities $\{f_{i1}(\delta)\mid g_{i1}(\delta)+d_{i1}x_{i+1},\ldots,f_{im}(\delta)\mid g_{im}(\delta)+d_{im}x_{i+1}\}$ has a solution since, for each prime number $p\in\mathcal{T}\setminus\pi_b$, if $p^{\ell}\mid f_{i\alpha}(\delta), p^{\ell}\mid f_{i\beta}(\delta)$, then $p^{\ell}\mid g(\delta)$, where $g=d_{i\alpha}g_{i\beta}-d_{i\beta}g_{i\alpha}$. Indeed, by virtue of the induction hypothesis and the condition c) of the definition of concordance of suites, there exists a polynomial f such that $f\mid f_{i\alpha}$, $f\mid f_{i\beta}\in\widetilde{\mathcal{K}}$ and $p^{\ell}\mid g(\delta)$. Then $f\mid g\in\widetilde{\mathcal{K}}$, and, since g is a polynomial in $x_1,\ldots,x_i$, it follows from the condition b) of the definition of canonical conditions that $f\mid g\in\widetilde{\mathcal{K}}_{(i-1)}$, and therefore $p^{\ell}\mid g(\delta)$.

We select a solution ε_{i+1} of this system of divisibilities as follows: The system of divisibilities

$$\{f_{i1}(\delta)\mid g_{i1}(\delta)+d_{i1}x_{i+1},\ldots,f_{im}(\delta)\mid g_{im}(\delta)+d_{im}x_{i+1}\}$$

has a solution [3, Lemma 9].

We select this solution such that the following conditions are satisfied:

A1) $\varepsilon_{i+1}\equiv\omega_{i+1}\,(\mathrm{mod}\,\theta_b)$;

A2) $p^{\beta_p+1}\nmid g(\gamma)$ where $u=\rho(n-i-1)$ and $\gamma=[\varepsilon_1,\ldots,\varepsilon_{i+1}]$, for each $p\in\pi(f_{ij}(\delta))$, $p\notin\pi_b$, each polynomial $g\in\mathcal{L}_{\tau,u}$ in the variables $x_1,\ldots,x_{i+1}$ with occurrence of x_{i+1} with nonzero coefficient and $g(\gamma)\in\mathbb{Z}$.

A3) For each $p\in\mathcal{T}\setminus\pi_b$, if $p\notin(f_{i1}(\delta),\ldots,f_{im}(\delta))$, then $p\notin\pi(g(\gamma))$, where $g\in\mathcal{L}_{\tau,u}$ is a polynomial in the variables $x_1,\ldots,x_{i+1}$, such that x_{i+1} occurs in it with nonzero coefficient.

The existence of ε_{i+1} that satisfies the conditions A2) and A3) follows from the fact that the prime numbers $p \notin \pi_\ell$ are quite large, and, in addition, the following stronger result is proved for testing the solvability of a system of divisibilities: If $p \in \pi_\ell$, $p^\ell | f_{i\alpha}(\delta)$, $p^\ell | g_{i\alpha}(\delta) + d_{i\alpha} x_0$ for a certain x_0, then $f_{i\beta}(\delta) | g_{i\beta}(\delta) + d_{i\beta} \cdot x_0$ for arbitrary β.

We show that the suite γ is concordant with respect to denominator τ and height $u = \rho(n-i-1)$ with the suite ω. To this end, it is necessary to verify the condition c) of the definition of concordance. Indeed, let the polynomials $g_1, g_2 \in \mathcal{L}_{\tau,u}$ in the variables $x_1, \dots, x_{i+1}$ be such that $p \notin \pi_\ell$ and $p | g_1(\gamma), p | g_2(\gamma)$. The following three cases are possible

1) $g_1, g_2 \in \mathbb{Q}[x_1, \dots, x_i]$;
2) $g_1 \in \mathbb{Q}[x_1, \dots, x_i]$, $g_2 \notin \mathbb{Q}[x_1, \dots, x_i]$;
3) $g_1, g_2 \notin \mathbb{Q}[x_1, \dots, x_i]$.

The induction hypothesis comes into force in the case 1).

Let us consider the case 2). Let $g_2 \notin \mathbb{Q}[x_1, \dots, x_i]$ and $g_2 = g_2'(x_1, \dots, x_i) + d x_{i+1}$. If $p | g_2(\gamma)$, then, as a consequence of the condition A3) of the choice of the solution there exists an f_{ij} such that $p | f_{ij}(\delta)$. Then by virtue of the condition c) of the definition of concordance, there exists a polynomial f such that $p | f(\delta)$ and $f | g_1, f | f_{ij}, f | g_{ij} + d_{ij} x_{i+1}$, $f | g \in \widetilde{\mathcal{K}}$, where $g = d g_{ij} - d_{ij} g_2'$. Since $d_{ij} g_2 = d(g_{ij} + d_{ij} x_{i+1}) - g$, it follows that $f | g_2 \in \widetilde{\mathcal{K}}$. The equalities ${}_p f(\gamma) = {}_p g_1(\gamma) = {}_p g_2(\gamma)$ follow from the induction hypothesis and the condition A2) of the choice the solution ε_{i+1}. Consequently, the condition c) of the definition of concordance is fulfilled.

Case 3). Let $g_1 = g_1'(x_1, \dots, x_i) + d_1 x_{i+1}$ and $g_2 = g_2'(x_1, \dots, x_i) + d_2 x_{i+1}$. Then $p | g(\delta)$, where $g = d_2 g_1' - d_1 g_2'$ (we suppose that $g_2 \neq q \cdot g_1$ for any $q \in \mathbb{Q}$, since, otherwise, the condition c) of the definition of concordance would be fulfilled at once). Since $g \in \mathcal{L}_{\tau,c}$, it follows from the condition A3) of the choice of the solution ε_{i+1} that the prime number $p \in \pi(f_{i\alpha}(\delta))$ for a certain $\alpha = 1, \dots, m$. Consequently, by virtue of the induction hypothesis, for a certain polynomial f we have $f | f_{i\alpha}, f | g \in \widetilde{\mathcal{K}}$, $p^\ell = {}_p f(\delta) = {}_p f_{i\alpha}(\delta) = {}_p g(\delta)$, and therefore, $f | g_{i\alpha} + d_{i\alpha} x_{i+1} \in \widetilde{\mathcal{K}}$, and ${}_p(g_{i\alpha}(\delta) + d_{i\alpha} \varepsilon_{i+1}) = p^\ell$.

From the last relations and the induction hypotheses, we get $f | W_1$, $f | W_2 \in \widetilde{\mathcal{K}}$, and $p^\ell = {}_p W_1(\delta) = {}_p W_2(\delta)$ where $W_1 = d_1 g_{i\alpha} - d_{i\alpha} g_1'$ and $W_2 = d_2 g_{i\alpha} - d_{i\alpha} g_2'$. The equations $d_{i\alpha} \cdot g_1 = d_1(g_{i\alpha} + d_{i\alpha} x_{i+1}) - W_1$ and $d_{i\alpha} \cdot g_2 = d_2(g_{i\alpha} + d_{i\alpha} x_{i+1}) - W_2$ complete the proof of the case 3).

It remains to choose a suite γ such that

$$\widetilde{\mathcal{K}}_i = \{P(s_{i1}(\delta) + \ell_{i1} x_{i+1}), \dots, P(s_{iK}(\delta) + \ell_{iK} x_{i+1})\}. \tag{7}$$

Let us set $M = b \cdot \prod_{p \in \tau \setminus \pi_\ell} p^{\nu_p}$, where $\nu_p = \beta_p$, if $p \in \pi(f_{i1}(\delta), \dots, f_{im}(\delta))$, and $\nu_p = 1$ in the contrary case. Then for each integer t the number $\varepsilon_{i+1}(t) = \varepsilon_{i+1} + M \cdot t$ satisfies the conditions A1)-A3), imposed on the solution of the system of divisibilities, and, consequently, the suite $\varepsilon(t) = [\varepsilon_1, \dots, \varepsilon_i, \varepsilon_{i+1}(t)]$ is concordant with the suite $[\omega_1, \dots, \omega_{i+1}]$. Let us substitute the term $\varepsilon_{i+1}(t)$ for x_{i+1} in the polynomials in the conditions (7). The resulting polynomials will satisfy the condition of the extended Bliznetsov hypothesis, since the conditions (7) are satisfiable modulo the number θ_{ℓ} . Consequently, for a certain t_0 (under the extended Bliznetsov hypothesis) the suite $\mathcal{E}(t_0)$ satisfies the conditions (7).

The induction step is proved and, since $\rho(n-n)=\rho(0)=a$, the lemma is also proved.

THEOREM 1. The universal theory of the integers $\mathbb{Z}$ in the signature $<+, 1, |, P>$ is decidable under the assumption of satisfiability of the extended Bliznetsov hypothesis, where P is the predicate that selects prime numbers.

Proof. The problem of decidability of the $\exists$-theory (and, therefore, of the $\forall$-theory also) of the model $<\mathbb{Z};+, 1, |, P>$ is narrower than the problem of satisfiability of conditions of type

$$\Gamma=[\{P(f_i)\},\{u_j | g_j\},\{v_\ell=0\},\{r_1\}]\cup[\neg P(t_k), W_m \nmid a_m]. \tag{8}$$

By virtue of Lemmas 1 and 3, it is sufficient to consider the case where the first positive part of the conditions (8) does not have equalities and is P-canonical. Let us suppose that Γ, with the ratios $\{r_1\}$ removed, coincides with the P-canonical conditions (5). Then, by virtue of Lemma 2, we can effectively find whether there exists a suite $\omega=[\omega_1, \ldots, \omega_n]$, satisfying the conditions Γ modulo a number t such that $\ell | t$ (see Lemma 4 for the definition of ℓ). If no such suite ω exists, then the conditions Γ are nonsatisfiable. But if such a suite ω exists, then, using Lemma 4 (in fact, a modification of it, since here the case $t>\ell$ is possible), we see that the conditions Γ are satisfiable. Thus, an algorithm for testing the satisfiability of the conditions (8) exists, and, consequently, the theorem is proved.

COROLLARY. The theory of the fragment of the universal theory of $<\mathbb{Z};+, 1, |, P>$ that consists of the formulas containing at most one occurrence of the predicate P is decidable.

Proof. If a formula contains the single predicate P , then the P-canonical conditions, comparable with it, contain only one condition of the form $P(f)$ and, consequently, the extended Bliznetsov hypothesis for $n=1$, which is valid by the Dirichlet theorem [1], suffices here. Consequently, an algorithm for testing the truth of these formulas exists.

Let us consider the algorithmic problem of testing for an arbitrary set of polynomials $a_1+b_1x, \ldots, a_n+b_nx$, the existence of at least one value x_0 such that $a_1+b_1x_0, \ldots, a_n+b_nx_0$ are prime numbers.

Let us observe that if the universal theory of $<\mathbb{Z};+, 1, |, P>$ is decidable, then a testing algorithm exists, since $<\mathbb{Z};+, 1, |, P> \models \forall x(P(a_1+b_1x)\&\ldots\&P(a_n+b_nx)\to x\neq x) \Longleftrightarrow$ there exists no x_0 such that all the numbers $a_1+b_1x_0, \ldots, a_n+b_nx_0$ are prime.

The problem whether the existence of a testing algorithm implies the decidability of the universal theory of the model $<\mathbb{Z};+, 1, |, P>$ remains unsolved.

LITERATURE CITED

1. K. Prachar, Distribution of Prime Numbers [Russian translation], Mir, Moscow (1967).

2. A. P. Bel'tyukov, "Decidability of the universal theory of natural numbers with addition and divisibility," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst., 60, No. 7, 15-28 (1976).
3. V. I. Mart'yanov, "Universal extended theories of integers," Algebra Logika, 16, No. 5, 588-602 (1977).
4. L. Lipschitz, The Diophantine Problem for +, |, -, Preprint (1975).

RELATIONS BETWEEN TABLE-TYPE DEGREES

A. N. Degtev

UDC 517.11:518.5

Reducibilities intermediary in strength between m- and tt-reducibilities are called table-type reducibilities. As it was remarked in [1], we can define in a definitive sense on recursively-enumerable (r.e.) sets only six table-type reducibilities: tt-, ℓ-, p-, d-, c-, and m-reducibilities. Beside these, which we call basic, certain other bounded table-type reducibilities are known: btt-, $b\ell$-, bp-, bd- and bc-reducibilities. In this article we shall pay most attention to the class of reducibilities $\mathcal{K}=\{tt, \ell, p, d, c, m, btt\}$. It was proved in [6] that if R-reducibility is strictly weaker than r-reducibility, $r, R \in \mathcal{K}$, then the complete R-degree contains a countable number of r.e. r-degrees. In connection with this, a subtle problem arises: for which r, $R \in \mathcal{K}$, where R is weaker than r, does there exist a nonrecursive R-degree, consisting of one r-degree? Jockusch [9] made the first contribution to its solution, proving that there exists a nonrecursive r.e. p-degree, consisting of one m-degree, but that each nonrecursive tt-degree contains at least two p-degrees and a countable number of m-degrees. It follows from [4, 7] that each nonrecursive tt-degree contains at least two btt-degrees, and there exist nonrecursive tt-degrees (ℓ-degrees), consisting of one ℓ-degree (respectively, one m-degree). Thus, only the following problem remained unsolved — does there exist a nonrecursive btt-degree, consisting of one m-degree? Theorem 1 gives a positive answer to this question.

Another problem connected with the class of reducibilities $\mathcal{K}$ is the following: for which r, $R \in \mathcal{K}$, do we have the inequality $\mathrm{Th}(L_r) \neq \mathrm{Th}(L_R)$? Here L_x, $x \in \mathcal{K}$, denotes the upper semilattice of r.e. x-degrees in the signature $\langle \oplus, 0, 1 \rangle$, and $\mathrm{Th}(L_x)$ is its elementary theory. It was proved in [8] that $\mathrm{Th}(L_{tt}) \neq \mathrm{Th}(L_{btt})$. By virtue of [5, 7], at present only the following problems for $\mathcal{K}$ in this direction remain unsolved: (a) $\mathrm{Th}(L_{tt}) \neq \mathrm{Th}(L_p)$? (b) $\mathrm{Th}(L_\ell) \neq \mathrm{Th}(L_{btt})$? and (c) $\mathrm{Th}(L_p) \neq \mathrm{Th}(L_d)$? Theorems 2 and 3 give positive answers to questions (a) and (b), but as yet the answer to (c) is not known.

In this article we use the following conventions. We denote by N the set $\{0, 1, \ldots\}$; if $X \subseteq N$, then $\overline{X} = N \setminus X$. If X is a finite set, then $|X|$ is the number of its elements. We denote the Cantor number of the n-tuple of numbers $(a_1, \ldots, a_n)$ in N by $\langle a_1, \ldots, a_n \rangle$, and ℓ and r are the Cantor enumerated general recursive functions (g.r.f.). By definition, if $X, Y \subseteq N$, then

Translated from Algebra i Logika, Vol. 22, No. 1, pp. 35-52, January-February, 1983. Original article submitted September 15, 1981.

0002-5232/83/2201-0026$07.50