FORMALIZED MATHEMATICS
Vol. 30, No. 4, Pages 245–253, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0020

sciendo
sciendo.com/journal/forma

Prime Representing Polynomial with 10 Unknowns – Introduction. Part II

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Summary. In our previous work [7] we prove that the set of prime numbers is diophantine using the 26-variable polynomial proposed in [4]. In this paper, we focus on the reduction of the number of variables to 10 and it is the smallest variables number known today [5], [10]. Using the Mizar [3], [2] system, we formalize the first step in this direction by proving Theorem 1 [5] formulated as follows: Let $k \in \mathbb{N}$. Then k is prime if and only if there exists $f, i, j, m, u \in \mathbb{N}^+$, $r, s, t \in \mathbb{N}$ unknowns such that

$$\begin{gathered} DFI \texttt{ is square } \wedge (M^2-1)S^2+1 \texttt{ is square } \wedge \\ ((MU)^2-1)T^2+1 \texttt{ is square } \wedge \\ (4f^2-1)(r-mSTU)^2+4u^2S^2T^2 < 8fuST(r-mSTU) \\ FL \mid (H-C)Z+F(f+1)Q+F(k+1)((W^2-1)Su-W^2u^2+1) \end{gathered} \tag{0.1}$$

where auxiliary variables $A-I, L, M, S-W, Q \in \mathbb{Z}$ are simply abbreviations defined as follows $W = 100fk(k+1)$, $U = 100u^3W^3+1$, $M = 100mUW+1$, $S = (M-1)s+k+1$, $T = (MU-1)t+W-k+1$, $Q = 2MW-W^2-1$, $L = (k+1)Q$, $A = M(U+1)$, $B = W+1$, $C = r+W+1$, $D = (A^2-1)C^2+1$, $E = 2iC^2LD$, $F = (A^2-1)E^2+1$, $G = A+F(F-A)$, $H = B+2(j-1)C$, $I = (G^2-1)H^2+1$. It is easily see that (0.1) uses 8 unknowns explicitly along with five implicit one for each diophantine relationship: `is square`, inequality, and divisibility. Together with k this gives a total of 14 variables. This work has been partially presented in [8].

MSC: 11D45 68V20

Keywords: polynomial reduction; diophantine equation

MML identifier: `HILB10_8`, version: `8.1.12 5.72.1435`

1. Theta Notation

From now on A denotes a non trivial natural number, B, C, n, m, k denote natural numbers, and e denotes a natural number.

Let θ be a real number. We say that θ is theta if and only if

(Def. 1) $-1 \leqslant \theta \leqslant 1$.

Let us observe that 0 is theta and there exists a real number which is theta.

A Theta is a theta real number. Let θ be a Theta. Let us observe that $-\theta$ is theta.

Let u be a Theta. Let us note that $\theta \cdot u$ is theta. Now we state the propositions:

(1) Let us consider a Theta θ. Then $|\theta| \leqslant 1$.

(2) Let us consider a Theta θ, and real numbers λ, ε_1, ε_2. Suppose $\lambda = \theta \cdot \varepsilon_1$ and $|\varepsilon_1| \leqslant |\varepsilon_2|$. Then there exists a Theta θ_1 such that $\lambda = \theta_1 \cdot \varepsilon_2$.

(3) Let us consider Theta's θ_1, θ_2, and real numbers λ, ε_1, ε_2. Suppose $\lambda = (1 + \theta_1 \cdot \varepsilon_1) \cdot (1 + \theta_2 \cdot \varepsilon_2)$ and $0 \leqslant \varepsilon_1 \leqslant 1$ and $0 \leqslant \varepsilon_2$. Then there exists a Theta θ such that $\lambda = 1 + \theta \cdot (\varepsilon_1 + 2 \cdot \varepsilon_2)$.

(4) Let us consider Theta's θ_1, θ_2, and real numbers ε_1, ε_2. Suppose $\theta_1 \cdot \varepsilon_1 \leqslant \varepsilon_2 \leqslant \theta_2 \cdot \varepsilon_1$. Then there exists a Theta θ such that $\varepsilon_2 = \theta \cdot \varepsilon_1$.

(5) Let us consider a Theta θ, and real numbers λ, ε_1, ε_2. Suppose $\lambda = \theta \cdot \varepsilon_1$ and $\varepsilon_1 \leqslant \varepsilon_2$ and $0 \leqslant \varepsilon_1$. Then there exists a Theta θ_1 such that $\lambda = \theta_1 \cdot \varepsilon_2$. The theorem is a consequence of (2).

(6) Let us consider Theta's θ_1, θ_2, and real numbers ε_1, ε_2. Suppose $0 \leqslant \varepsilon_1$ and $0 \leqslant \varepsilon_2$. Then there exists a Theta θ such that $\theta_1 \cdot \varepsilon_1 + \theta_2 \cdot \varepsilon_2 = \theta \cdot (\varepsilon_1 + \varepsilon_2)$. The theorem is a consequence of (4).

(7) Let us consider a Theta θ_1, and a real number ε. Suppose $0 \leqslant \varepsilon \leqslant \frac{1}{2}$. Then there exists a Theta θ_2 such that $\frac{1}{1+\theta_1 \cdot \varepsilon} = 1 + \theta_2 \cdot 2 \cdot \varepsilon$. The theorem is a consequence of (2).

(8) If $m^{\mathbf{2}} \leqslant n$, then there exists a Theta θ such that $\binom{n}{m} = \frac{n^m}{m!} \cdot (1 + \theta \cdot \frac{m^{\mathbf{2}}}{n})$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1^{\mathbf{2}} \leqslant n$, then there exists a Theta θ such that $\binom{n}{\$_1} = \frac{n^{\$_1}}{\$_1!} \cdot (1 + \theta \cdot \frac{\$_1^{\mathbf{2}}}{n})$. For every m such that $\mathcal{P}[m]$ holds $\mathcal{P}[m+1]$. For every m, $\mathcal{P}[m]$. $\square$

(9) Let us consider a Theta θ, and real numbers α, ε. Suppose $\alpha = (1 + \theta \cdot \varepsilon)^n$ and $0 \leqslant \varepsilon \leqslant \frac{1}{2 \cdot n}$. Then there exists a Theta θ_1 such that $\alpha = 1 + \theta_1 \cdot 2 \cdot n \cdot \varepsilon$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every Theta θ for every real numbers α, ε such that $\alpha = (1 + \theta \cdot \varepsilon)^{\$_1}$ and $0 \leqslant \varepsilon \leqslant \frac{1}{2 \cdot \$_1}$ there exists a Theta θ_1 such that $\alpha = 1 + \theta_1 \cdot 2 \cdot \$_1 \cdot \varepsilon$. $\mathcal{P}[0]$. If $\mathcal{P}[m]$, then $\mathcal{P}[m+1]$. $\mathcal{P}[m]$. $\square$

2. More on Solutions to Pell's Equation

In the sequel a denotes a non trivial natural number. Now we state the propositions:

(10) If $n \leqslant a$, then there exists a Theta θ such that $\mathrm{y}_a(n+1) = (2 \cdot a)^n \cdot (1 + \theta \cdot \frac{n}{a})$. The theorem is a consequence of (9) and (4).

(11) Let us consider a non trivial natural number a, and natural numbers y, n. Suppose $y > 0$ and $n > 0$ and $(a^{\mathbf{2}} - 1) \cdot y^{\mathbf{2}} + 1$ is a square and $y \equiv n \pmod{a-1}$ and $y \leqslant \mathrm{y}_a(a-1)$ and $n \leqslant a - 1$. Then $y = \mathrm{y}_a(n)$.

(12) Let us consider a non trivial natural number a, and natural numbers s, n. Then $s^{\mathbf{2}} \cdot (s^n)^{\mathbf{2}} - (s^{\mathbf{2}} - 1) \cdot \mathrm{y}_a(n+1) \cdot s^n - 1 \equiv 0 \pmod{2 \cdot a \cdot s - s^{\mathbf{2}} - 1}$.
Proof: Set $S = s^{\mathbf{2}}$. Define $\mathcal{P}[\text{natural number}] \equiv S \cdot (s^{\$_1})^{\mathbf{2}} - (S-1) \cdot \mathrm{y}_a(\$_1 + 1) \cdot s^{\$_1} - 1 \equiv 0 \pmod{2 \cdot a \cdot s - s^{\mathbf{2}} - 1}$. For every natural number k such that for every n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$. $\mathcal{P}[n]$. $\square$

(13) Let us consider a non trivial natural number a, and natural numbers s, n, r. Suppose $s > 0$ and $r > 0$ and $s^{\mathbf{2}} \cdot r^{\mathbf{2}} - (s^{\mathbf{2}} - 1) \cdot \mathrm{y}_a(n+1) \cdot r - 1 \equiv 0 \pmod{2 \cdot a \cdot s - s^{\mathbf{2}} - 1}$ and $s \cdot (s^n)^{\mathbf{2}} \cdot s^n < a$ and $s \cdot r^{\mathbf{2}} \cdot r < a$. Then $r = s^n$. The theorem is a consequence of (12).

(14) Let us consider natural numbers a, b, c, d. Suppose $a \leqslant b \leqslant c$ and $2 \cdot c \leqslant d$ and $c > 0$. Let us consider a finite sequence f of elements of $\mathbb{R}$. Suppose $\operatorname{len} f = b - a + 1$ and for every natural number i such that $i + 1 \in \operatorname{dom} f$ holds $f(i+1) = \binom{c}{a+i} \cdot d^{c -' (a+i)}$. Then $0 < \sum f < 2 \cdot c^a \cdot d^{c -' a}$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every natural numbers a, b, c, d such that $a \leqslant b \leqslant c$ and $2 \cdot c \leqslant d$ and $c > 0$ and $b - a = \$_1$ for every finite sequence f of elements of $\mathbb{R}$ such that $\operatorname{len} f = b - a + 1$ and for every natural number i such that $i + 1 \in \operatorname{dom} f$ holds $f(i+1) = \binom{c}{a+i} \cdot d^{c -' (a+i)}$ holds $0 \leqslant 1 - (\frac{c}{d})^{b+1-'a}$ and $0 < \sum f \leqslant \frac{1 - (\frac{c}{d})^{b+1-'a}}{1 - \frac{c}{d}} \cdot c^a \cdot d^{c -' a}$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. $\square$

(15) Let us consider natural numbers f, k, m, r, s, t, u, and integers W, M, U, S, T, Q. Suppose $f > 0$ and $k > 0$ and $m > 0$ and $u > 0$ and $(M^{\mathbf{2}} - 1) \cdot S^{\mathbf{2}} + 1$ is a square and $((M \cdot U)^{\mathbf{2}} - 1) \cdot T^{\mathbf{2}} + 1$ is a square and $W^{\mathbf{2}} \cdot u^{\mathbf{2}} - (W^{\mathbf{2}} - 1) \cdot S \cdot u - 1 \equiv 0 \pmod{Q}$ and $(4 \cdot f^{\mathbf{2}} - 1) \cdot (r - m \cdot S \cdot T \cdot U)^{\mathbf{2}} + 4 \cdot u^{\mathbf{2}} \cdot S^{\mathbf{2}} \cdot T^{\mathbf{2}} < 8 \cdot f \cdot u \cdot S \cdot T \cdot (r - m \cdot S \cdot T \cdot U)$ and $W = 100 \cdot f \cdot k \cdot (k+1)$ and $U = 100 \cdot u^3 \cdot W^3 + 1$ and $M = 100 \cdot m \cdot U \cdot W + 1$ and $S = (M-1) \cdot s + k + 1$ and $T = (M \cdot U - 1) \cdot t + W - k + 1$ and $Q = 2 \cdot M \cdot W - W^{\mathbf{2}} - 1$. Then

(i) $M \cdot (U + 1)$ is a non trivial natural number, and

(ii) W is a natural number, and

(iii) for every non trivial natural number m_1 and for every natural number w such that $m_1 = M \cdot (U+1)$ and $w = W$ and $r+W+1 = \mathtt{y}_{m_1}(w+1)$ holds $f = k!$.

Proof: Reconsider $W_2 = W - k$ as a natural number. Reconsider $M_3 = M \cdot U$ as a non trivial natural number. Reconsider $M_1 = M - 1$ as a natural number. Set $R = r - m \cdot S \cdot T \cdot U$. $(\frac{u}{\frac{r}{S \cdot T} - m \cdot U} - f) \cdot (\frac{u}{\frac{r}{S \cdot T} - m \cdot U} - f) < \frac{1}{4}$. $r < \mathtt{y}_M(M_1)$ and $r < \mathtt{y}_M(M_3 - 1)$. $S = \mathtt{y}_M(k+1)$. $T = \mathtt{y}_{M_3}(W_2 + 1)$. $R < 3 \cdot u \cdot S \cdot T$. $m \cdot U + 3 \cdot u > \frac{r}{S \cdot T}$. Consider θ_1 being a Theta such that $\mathtt{y}_{m_1}(w+1) = (2 \cdot m_1)^w \cdot (1+\theta_1 \cdot \frac{w}{m_1})$. Reconsider $I = 1$ as a Theta. Consider θ_2 being a Theta such that $\theta_1 \cdot \frac{w}{m_1} - \frac{W+1}{(2 \cdot m_1)^W} = \theta_2 \cdot \frac{1}{M}$. $u = W^k$. Consider θ_3 being a Theta such that $\mathtt{y}_M(k+1) = (2 \cdot M)^k \cdot (1 + \theta_3 \cdot \frac{k}{M})$. Consider θ_4 being a Theta such that $\mathtt{y}_{M_3}(W_2+1) = (2 \cdot M_3)^{W_2} \cdot (1 + \theta_4 \cdot \frac{W_2}{M_3})$. Consider θ'_3 being a Theta such that $\frac{1}{1+\theta_3 \cdot \frac{k}{M}} = 1 + \theta'_3 \cdot 2 \cdot \frac{k}{M}$. Consider θ'_4 being a Theta such that $\frac{1}{1+\theta_4 \cdot \frac{W_2}{M_3}} = 1 + \theta'_4 \cdot 2 \cdot \frac{W_2}{M_3}$. Consider θ_5 being a Theta such that $(1 + \theta'_3 \cdot (2 \cdot \frac{k}{M})) \cdot (1 + \theta_2 \cdot \frac{1}{M}) = 1 + \theta_5 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M})$.

Consider θ_6 being a Theta such that $(1+\theta_5 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M})) \cdot (1 + \theta'_4 \cdot (2 \cdot \frac{W_2}{M_3})) = 1 + \theta_6 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M} + 2 \cdot (2 \cdot \frac{W_2}{M_3}))$. Consider θ_7 being a Theta such that $\theta_6 \cdot (2 \cdot \frac{k}{M} + 2 \cdot \frac{1}{M} + 2 \cdot (2 \cdot \frac{W_2}{M_3})) = \theta_7 \cdot \frac{5 \cdot k}{M}$. Set $I_1 = \langle \binom{W}{0} U^0 1^W, \ldots, \binom{W}{W} U^W 1^0 \rangle$. Set $I_3 = I_1 \restriction k$. Consider I_2 being a finite sequence such that $I_1 = I_3 \frown I_2$. For every natural number i such that $i+1 \in \operatorname{dom} I_3$ holds $I_3(i+1) = \binom{W}{0+i} \cdot U^{W -' (0+i)}$. $0 < \sum I_3 < 2 \cdot W^0 \cdot U^{W -' 0}$. Set $U_2 = \frac{1}{U^{W_2+1}} \cdot I_3$. $\operatorname{rng} U_2 \subseteq \mathbb{N}$. Reconsider $Z = \sum U_2$ as an element of $\mathbb{N}$. For every natural number i such that $i+1 \in \operatorname{dom} I_2$ holds $I_2(i+1) = \binom{W}{k+i} \cdot U^{W -' (k+i)}$. $0 < \sum I_2 < 2 \cdot W^k \cdot U^{W -' k}$. $|\theta_7| \leqslant 1$ and $|\frac{5 \cdot k}{M}| \leqslant 1$. $|\theta_7 \cdot (Z \cdot \frac{5 \cdot k}{M})| \leqslant 1 \cdot |Z \cdot \frac{5 \cdot k}{M}|$. Consider θ_8 being a Theta such that $(1 + I \cdot \frac{1}{U})^W = 1 + \theta_8 \cdot 2 \cdot W \cdot \frac{1}{U}$. Consider θ_9 being a Theta such that $\theta_7 \cdot (1 + \theta_8 \cdot 2 \cdot W \cdot \frac{1}{U}) = \theta_9 \cdot 2$.

Consider i_3 being a finite sequence of elements of $\mathbb{R}$, x being an element of $\mathbb{R}$ such that $I_2 = \langle x \rangle \frown i_3$. For every natural number i such that $i+1 \in \operatorname{dom} i_3$ holds $i_3(i+1) = \binom{W}{k+1+i} \cdot U^{W -' (k+1+i)}$. $0 < \sum i_3 < 2 \cdot W^{k+1} \cdot U^{W -' (k+1)}$. Consider θ_{10} being a Theta such that $I \cdot (\frac{1}{U^{W_2}} \cdot (\sum i_3)) = \theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U})$. Reconsider $\theta_{12} = \frac{1}{\binom{W}{k}}$ as a Theta. Consider θ_{11} being a Theta such that $\theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U}) + \theta_9 \cdot \frac{U^k \cdot 10 \cdot k}{M} = \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$. Consider θ'_{13} being a Theta such that $\binom{W}{k} = \frac{W^k}{k!} \cdot (1 + \theta'_{13} \cdot \frac{k^{\mathbf{2}}}{W})$. Consider θ_{13} being a Theta such that $\frac{1}{1+\theta'_{13} \cdot \frac{k^{\mathbf{2}}}{W}} = 1 + \theta_{13} \cdot 2 \cdot \frac{k^{\mathbf{2}}}{W}$. Consider θ_{14} being a Theta such that $\frac{1}{1+\theta_{12} \cdot \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})} = 1 + \theta_{14} \cdot 2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$.

Consider θ_{15} being a Theta such that $(1+\theta_{14}\cdot(2\cdot(2\cdot W^{k+1}\cdot\frac{1}{U}+\frac{U^k\cdot 10\cdot k}{M})))\cdot(1+\theta_{13}\cdot(2\cdot\frac{k^2}{W}))=1+\theta_{15}\cdot(2\cdot(2\cdot W^{k+1}\cdot\frac{1}{U}+\frac{U^k\cdot 10\cdot k}{M})+2\cdot(2\cdot\frac{k^2}{W}))$. $\square$

(16) Let us consider natural numbers f, k. Suppose $f=k!$ and $k>0$. Then there exist natural numbers m, r, s, t, u and there exist natural numbers W, U, S, T, Q and there exists a non trivial natural number M such that $m>0$ and $u>0$ and $r+W+1=\mathtt{y}_{M\cdot(U+1)}(W+1)$ and $(M^2-1)\cdot S^2+1$ is a square and $((M\cdot U)^2-1)\cdot T^2+1$ is a square and $W^2\cdot u^2-(W^2-1)\cdot S\cdot u-1\equiv 0\ (\mathrm{mod}\,Q)$ and $(4\cdot f^2-1)\cdot(r-m\cdot S\cdot T\cdot U)^2+4\cdot u^2\cdot S^2\cdot T^2<8\cdot f\cdot u\cdot S\cdot T\cdot(r-m\cdot S\cdot T\cdot U)$ and $W=100\cdot f\cdot k\cdot(k+1)$ and $U=100\cdot u^3\cdot W^3+1$ and $M=100\cdot m\cdot U\cdot W+1$ and $S=(M-1)\cdot s+k+1$ and $T=(M\cdot U-1)\cdot t+W-k+1$ and $Q=2\cdot M\cdot W-W^2-1$.

PROOF: Set $W=100\cdot f\cdot k\cdot(k+1)$. Set $u=W^k$. Set $U=100\cdot u^3\cdot W^3+1$. Set $I_1=\langle\binom{W}{0}U^0 1^W,\ldots,\binom{W}{W}U^W 1^0\rangle$. Set $I_3=I_1{\restriction}k$. Reconsider $W_2=W-k$ as a natural number. Consider I_2 being a finite sequence such that $I_1=I_3\frown I_2$. For every natural number i such that $i+1\in\operatorname{dom}I_3$ holds $I_3(i+1)=\binom{W}{0+i}\cdot U^{W-'(0+i)}$. $0<\sum I_3<2\cdot W^0\cdot U^{W-'0}$. Set $U_2=\frac{1}{U^{W_2+1}}\cdot I_3$. $\operatorname{rng}U_2\subseteq\mathbb{N}$. Reconsider $Z=\sum U_2$ as an element of $\mathbb{N}$. Set $m=Z$. Set $M=100\cdot m\cdot U\cdot W+1$. Set $m_1=M\cdot(U+1)$. Reconsider $M_3=M\cdot U$ as a non trivial natural number. Set $S=\mathtt{y}_M(k+1)$. Set $T=\mathtt{y}_{M_3}(W_2+1)$. Reconsider $r=\mathtt{y}_{m_1}(W+1)-(W+1)$ as a natural number. Consider s being an integer such that $(M-1)\cdot s=S-(k+1)$.

Consider t being an integer such that $(M_3-1)\cdot t=T-(W_2+1)$. For every natural number i such that $i+1\in\operatorname{dom}I_2$ holds $I_2(i+1)=\binom{W}{k+i}\cdot U^{W-'(k+i)}$. $0<\sum I_2<2\cdot W^k\cdot U^{W-'k}$. Consider θ_1 being a Theta such that $\mathtt{y}_{m_1}(W+1)=(2\cdot m_1)^W\cdot(1+\theta_1\cdot\frac{W}{m_1})$. Reconsider $I=1$ as a Theta. Consider θ_3 being a Theta such that $\mathtt{y}_M(k+1)=(2\cdot M)^k\cdot(1+\theta_3\cdot\frac{k}{M})$. Consider θ_4 being a Theta such that $\mathtt{y}_{M_3}(W_2+1)=(2\cdot M_3)^{W_2}\cdot(1+\theta_4\cdot\frac{W_2}{M_3})$. Consider θ'_3 being a Theta such that $\frac{1}{1+\theta_3\cdot\frac{k}{M}}=1+\theta'_3\cdot 2\cdot\frac{k}{M}$. Consider θ'_4 being a Theta such that $\frac{1}{1+\theta_4\cdot\frac{W_2}{M_3}}=1+\theta'_4\cdot 2\cdot\frac{W_2}{M_3}$. Consider θ_2 being a Theta such that $\theta_1\cdot\frac{W}{m_1}-\frac{W+1}{(2\cdot m_1)^W}=\theta_2\cdot\frac{1}{M}$. Consider θ_5 being a Theta such that $(1+\theta'_3\cdot(2\cdot\frac{k}{M}))\cdot(1+\theta_2\cdot\frac{1}{M})=1+\theta_5\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M})$. Consider θ_6 being a Theta such that $(1+\theta_5\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M}))\cdot(1+\theta'_4\cdot(2\cdot\frac{W_2}{M_3}))=1+\theta_6\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M}+2\cdot(2\cdot\frac{W_2}{M_3}))$. Consider θ_7 being a Theta such that $\theta_6\cdot(2\cdot\frac{k}{M}+2\cdot\frac{1}{M}+2\cdot(2\cdot\frac{W_2}{M_3}))=\theta_7\cdot\frac{5\cdot k}{M}$.

Consider u_1 being a finite sequence of elements of $\mathbb{N}$, y being an element of $\mathbb{N}$ such that $U_2=\langle y\rangle\frown u_1$. Consider θ_8 being a Theta such that $(1+I\cdot\frac{1}{U})^W=1+\theta_8\cdot 2\cdot W\cdot\frac{1}{U}$. Consider θ_9 being a Theta such that

$\theta_7 \cdot (1+\theta_8 \cdot 2 \cdot W \cdot \frac{1}{U}) = \theta_9 \cdot 2$. Consider i_3 being a finite sequence of elements of $\mathbb{R}$, x being an element of $\mathbb{R}$ such that $I_2 = \langle x \rangle \frown i_3$. For every natural number i such that $i+1 \in \operatorname{dom} i_3$ holds $i_3(i+1) = \binom{W}{k+1+i} \cdot U^{W-'(k+1+i)}$. $0 < \sum i_3 < 2 \cdot W^{k+1} \cdot U^{W-'(k+1)}$. Consider θ_{10} being a Theta such that $I \cdot (\frac{1}{U^{W_2}} \cdot (\sum i_3)) = \theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U})$. Reconsider $\theta_{12} = \frac{1}{\binom{W}{k}}$ as a Theta.

Consider θ_{11} being a Theta such that $\theta_{10} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U}) + \theta_9 \cdot \frac{U^k \cdot 10 \cdot k}{M} = \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$. Consider θ'_{13} being a Theta such that $\binom{W}{k} = \frac{W^k}{k!} \cdot (1+\theta'_{13} \cdot \frac{k^2}{W})$. Consider θ_{13} being a Theta such that $\frac{1}{1+\theta'_{13} \cdot \frac{k^2}{W}} = 1+\theta_{13} \cdot 2 \cdot \frac{k^2}{W}$. Consider θ_{14} being a Theta such that $\frac{1}{1+\theta_{12} \cdot \theta_{11} \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})} = 1+\theta_{14} \cdot 2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M})$. Consider θ_{15} being a Theta such that $(1+\theta_{14} \cdot (2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M}))) \cdot (1+\theta_{13} \cdot (2 \cdot \frac{k^2}{W})) = 1+\theta_{15} \cdot (2 \cdot (2 \cdot W^{k+1} \cdot \frac{1}{U} + \frac{U^k \cdot 10 \cdot k}{M}) + 2 \cdot (2 \cdot \frac{k^2}{W}))$. Set $R = r - m \cdot S \cdot T \cdot U$. $R \neq 0$. $\square$

(17) Let us consider a non trivial natural number A, natural numbers C, B, and e. Suppose $0 < B$. Suppose $C = \mathtt{y}_A(B)$. Then there exist natural numbers i, j and there exist natural numbers D, E, F, G, H, I such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^2 - 1) \cdot C^2 + 1$ and $E = 2 \cdot (i+1) \cdot D \cdot (e+1) \cdot C^2$ and $F = (A^2 - 1) \cdot E^2 + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot j \cdot C$ and $I = (G^2 - 1) \cdot H^2 + 1$.

Proof: Set $x = \mathtt{x}_A(B)$. Set $D = x^2$. There exist natural numbers q, i such that $2 \cdot D \cdot (e+1) \cdot C^2 \cdot (i+1) = \mathtt{y}_A(q)$ by [1, (14)], [6, (4)]. Consider q, i being natural numbers such that $2 \cdot D \cdot (e+1) \cdot C^2 \cdot (i+1) = \mathtt{y}_A(q)$. Set $F = (\mathtt{x}_A(q))^2$. Reconsider $G = A + F \cdot (F - A)$ as a non trivial natural number. Set $H = \mathtt{y}_G(B)$. $H \equiv B \pmod{2 \cdot C}$. Consider j being an integer such that $H - B = 2 \cdot C \cdot j$. $\square$

(18) Let us consider a non trivial natural number A, natural numbers C, B, and a natural number e. Suppose $0 < B$. Let us consider natural numbers i, j, and integers D, E, F, G, H, I. Suppose $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^2 - 1) \cdot C^2 + 1$ and $E = 2 \cdot (i+1) \cdot D \cdot (e+1) \cdot C^2$ and $F = (A^2 - 1) \cdot E^2 + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot j \cdot C$ and $I = (G^2 - 1) \cdot H^2 + 1$. Then $C = \mathtt{y}_A(B)$.

Proof: Consider d being a natural number such that $d^2 = D$. Consider f being a natural number such that $f^2 = F$. Consider i_2 being a natural number such that ${i_2}^2 = I$. Consider i_1 being a natural number such that $d = \mathtt{x}_A(i_1)$ and $C = \mathtt{y}_A(i_1)$. Consider n_1 being a natural number such that $f = \mathtt{x}_A(n_1)$ and $E = \mathtt{y}_A(n_1)$. Consider j_1 being a natural number such that $i_2 = \mathtt{x}_G(j_1)$ and $H = \mathtt{y}_G(j_1)$. $\mathtt{y}_G(j_1) \equiv j_1 \pmod{2 \cdot C}$. $\square$

(19) DIOPHANTINE REPRESENTATION OF SOLUTIONS TO PELL'S EQUATION: Let us consider a non trivial natural number A, natural numbers C, B, and e. Suppose $0 < B$. Then $C = \mathtt{y}_A(B)$ if and only if there exist natural numbers i, j and there exist integers D, E, F, G, H, I such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot (i+1) \cdot D \cdot (e+1) \cdot C^{\mathbf{2}}$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot j \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$. The theorem is a consequence of (17) and (18).

(20) Let us consider a non trivial natural number A, a natural number C, and positive natural numbers B, L. Then $C = \mathtt{y}_A(B)$ if and only if there exist positive natural numbers i, j and there exist integers D, E, F, G, H, I such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $B \leqslant C$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot i \cdot C^{\mathbf{2}} \cdot L \cdot D$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot (j - 1) \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$. The theorem is a consequence of (17) and (18).

3. PRIME DIOPHANTINE REPRESENTATION

Now we state the propositions:

(21) Let us consider a natural number k, and a positive natural number L. Suppose $k > 0$. Then $k + 1$ is prime if and only if there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, W, U, M, S, T, Q such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $(M^{\mathbf{2}} - 1) \cdot S^{\mathbf{2}} + 1$ is a square and $((M \cdot U)^{\mathbf{2}} - 1) \cdot T^{\mathbf{2}} + 1$ is a square and $W^{\mathbf{2}} \cdot u^{\mathbf{2}} - (W^{\mathbf{2}} - 1) \cdot S \cdot u - 1 \equiv 0 \pmod{Q}$ and $(4 \cdot f^{\mathbf{2}} - 1) \cdot (r - m \cdot S \cdot T \cdot U)^{\mathbf{2}} + 4 \cdot u^{\mathbf{2}} \cdot S^{\mathbf{2}} \cdot T^{\mathbf{2}} < 8 \cdot f \cdot u \cdot S \cdot T \cdot (r - m \cdot S \cdot T \cdot U)$ and $k+1 \mid f+1$ and $A = M \cdot (U+1)$ and $B = W+1$ and $C = r+W+1$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot i \cdot C^{\mathbf{2}} \cdot L \cdot D$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and $G = A + F \cdot (F - A)$ and $H = B + 2 \cdot (j - 1) \cdot C$ and $I = (G^{\mathbf{2}} - 1) \cdot H^{\mathbf{2}} + 1$ and $W = 100 \cdot f \cdot k \cdot (k+1)$ and $U = 100 \cdot u^3 \cdot W^3 + 1$ and $M = 100 \cdot m \cdot U \cdot W + 1$ and $S = (M - 1) \cdot s + k + 1$ and $T = (M \cdot U - 1) \cdot t + W - k + 1$ and $Q = 2 \cdot M \cdot W - W^{\mathbf{2}} - 1$.

PROOF: If $k + 1$ is prime, then there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, W, U, M, S, T, Q such that $D \cdot F \cdot I$ is a square and $F \mid H - C$ and $(M^{\mathbf{2}} - 1) \cdot S^{\mathbf{2}} + 1$ is a square and $((M \cdot U)^{\mathbf{2}} - 1) \cdot T^{\mathbf{2}} + 1$ is a square and $W^{\mathbf{2}} \cdot u^{\mathbf{2}} - (W^{\mathbf{2}} - 1) \cdot S \cdot u - 1 \equiv 0 \pmod{Q}$ and $(4 \cdot f^{\mathbf{2}} - 1) \cdot (r - m \cdot S \cdot T \cdot U)^{\mathbf{2}} + 4 \cdot u^{\mathbf{2}} \cdot S^{\mathbf{2}} \cdot T^{\mathbf{2}} < 8 \cdot f \cdot u \cdot S \cdot T \cdot (r - m \cdot S \cdot T \cdot U)$ and $k + 1 \mid f + 1$ and $A = M \cdot (U + 1)$ and $B = W + 1$ and $C = r + W + 1$ and $D = (A^{\mathbf{2}} - 1) \cdot C^{\mathbf{2}} + 1$ and $E = 2 \cdot i \cdot C^{\mathbf{2}} \cdot L \cdot D$ and $F = (A^{\mathbf{2}} - 1) \cdot E^{\mathbf{2}} + 1$ and

$G = A+F\cdot(F-A)$ and $H = B+2\cdot(j-1)\cdot C$ and $I = (G^{\mathbf{2}}-1)\cdot H^{\mathbf{2}}+1$ and $W = 100\cdot f\cdot k\cdot(k+1)$ and $U = 100\cdot u^3\cdot W^3+1$ and $M = 100\cdot m\cdot U\cdot W+1$ and $S = (M-1)\cdot s+k+1$ and $T = (M\cdot U-1)\cdot t+W-k+1$ and $Q = 2\cdot M\cdot W-W^{\mathbf{2}}-1$. $C = \mathtt{y}_A(B)$. $f = k!$. □

(22) Let us consider integers a, b, A, B. Suppose a and b are relatively prime. Then $a \mid A$ and $b \mid B$ if and only if $a\cdot b \mid a\cdot B+b\cdot A$.

(23) Diophantine Representation of Prime Numbers with 8 Explicite Unknowns:
Let us consider a natural number k. Suppose $k > 0$. Then $k+1$ is prime if and only if there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, L, W, U, M, S, T, Q such that $D\cdot F\cdot I$ is a square and $(M^{\mathbf{2}}-1)\cdot S^{\mathbf{2}}+1$ is a square and $((M\cdot U)^{\mathbf{2}}-1)\cdot T^{\mathbf{2}}+1$ is a square and $(4\cdot f^{\mathbf{2}}-1)\cdot(r-m\cdot S\cdot T\cdot U)^{\mathbf{2}}+4\cdot u^{\mathbf{2}}\cdot S^{\mathbf{2}}\cdot T^{\mathbf{2}} < 8\cdot f\cdot u\cdot S\cdot T\cdot(r-m\cdot S\cdot T\cdot U)$ and $F\cdot L \mid (H-C)\cdot L+F\cdot(f+1)\cdot Q+F\cdot(k+1)\cdot((W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1)$ and $A = M\cdot(U+1)$ and $B = W+1$ and $C = r+W+1$ and $D = (A^{\mathbf{2}}-1)\cdot C^{\mathbf{2}}+1$ and $E = 2\cdot i\cdot C^{\mathbf{2}}\cdot L\cdot D$ and $F = (A^{\mathbf{2}}-1)\cdot E^{\mathbf{2}}+1$ and $G = A+F\cdot(F-A)$ and $H = B+2\cdot(j-1)\cdot C$ and $I = (G^{\mathbf{2}}-1)\cdot H^{\mathbf{2}}+1$ and $L = (k+1)\cdot Q$ and $W = 100\cdot f\cdot k\cdot(k+1)$ and $U = 100\cdot u^3\cdot W^3+1$ and $M = 100\cdot m\cdot U\cdot W+1$ and $S = (M-1)\cdot s+k+1$ and $T = (M\cdot U-1)\cdot t+W-k+1$ and $Q = 2\cdot M\cdot W-W^{\mathbf{2}}-1$.

Proof: If $k+1$ is prime, then there exist positive natural numbers f, i, j, m, u and there exist natural numbers r, s, t and there exist integers A, B, C, D, E, F, G, H, I, L, W, U, M, S, T, Q such that $D\cdot F\cdot I$ is a square and $(M^{\mathbf{2}}-1)\cdot S^{\mathbf{2}}+1$ is a square and $((M\cdot U)^{\mathbf{2}}-1)\cdot T^{\mathbf{2}}+1$ is a square and $(4\cdot f^{\mathbf{2}}-1)\cdot(r-m\cdot S\cdot T\cdot U)^{\mathbf{2}}+4\cdot u^{\mathbf{2}}\cdot S^{\mathbf{2}}\cdot T^{\mathbf{2}} < 8\cdot f\cdot u\cdot S\cdot T\cdot(r-m\cdot S\cdot T\cdot U)$ and $F\cdot L \mid (H-C)\cdot L+F\cdot(f+1)\cdot Q+F\cdot(k+1)\cdot((W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1)$ and $A = M\cdot(U+1)$ and $B = W+1$ and $C = r+W+1$ and $D = (A^{\mathbf{2}}-1)\cdot C^{\mathbf{2}}+1$ and $E = 2\cdot i\cdot C^{\mathbf{2}}\cdot L\cdot D$ and $F = (A^{\mathbf{2}}-1)\cdot E^{\mathbf{2}}+1$ and $G = A+F\cdot(F-A)$ and $H = B+2\cdot(j-1)\cdot C$ and $I = (G^{\mathbf{2}}-1)\cdot H^{\mathbf{2}}+1$ and $L = (k+1)\cdot Q$ and $W = 100\cdot f\cdot k\cdot(k+1)$ and $U = 100\cdot u^3\cdot W^3+1$ and $M = 100\cdot m\cdot U\cdot W+1$ and $S = (M-1)\cdot s+k+1$ and $T = (M\cdot U-1)\cdot t+W-k+1$ and $Q = 2\cdot M\cdot W-W^{\mathbf{2}}-1$ by [9, (22)], (16).

$F \mid H-C$ and $Q\cdot(k+1) \mid (f+1)\cdot Q+(k+1)\cdot((W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1)$. $Q \mid (W^{\mathbf{2}}-1)\cdot S\cdot u-W^{\mathbf{2}}\cdot u^{\mathbf{2}}+1$ and $k+1 \mid f+1$. $C = \mathtt{y}_A(B)$. $f = k!$. □

References

[1] Marcin Acewicz and Karol Pąk. Pell's equation. *Formalized Mathematics*, 25(**3**):197–204, 2017. doi:10.1515/forma-2017-0019.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Ma-

tuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[4] James P. Jones, Sato Daihachiro, Hideo Wada, and Douglas Wiens. Diophantine representation of the set of prime numbers. *The American Mathematical Monthly*, 83(6):449–464, 1976.

[5] Yuri Matiyasevich. Primes are nonnegative values of a polynomial in 10 variables. *Journal of Soviet Mathematics*, 15:33–44, 1981. doi:10.1007/BF01404106.

[6] Karol Pąk. The Matiyasevich theorem. Preliminaries. *Formalized Mathematics*, 25(**4**):315–322, 2017. doi:10.1515/forma-2017-0029.

[7] Karol Pąk. Prime representing polynomial. *Formalized Mathematics*, 29(**4**):221–228, 2021. doi:10.2478/forma-2021-0020.

[8] Karol Pąk and Cezary Kaliszyk. Formalizing a diophantine representation of the set of prime numbers. In June Andronick and Leonardo de Moura, editors, *13th International Conference on Interactive Theorem Proving, ITP 2022, August 7-10, 2022, Haifa, Israel*, volume 237 of *LIPIcs*, pages 26:1–26:8. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.ITP.2022.26.

[9] Marco Riccardi. The perfect number theorem and Wilson's theorem. *Formalized Mathematics*, 17(**2**):123–128, 2009. doi:10.2478/v10037-009-0013-y.

[10] Zhi-Wei Sun. Further results on Hilbert's Tenth Problem. *Science China Mathematics*, 64:281–306, 2021. doi:10.1007/s11425-020-1813-5.

Accepted December 27, 2022