FORMALIZED MATHEMATICS
Vol. 29, No. 4, Pages 221–228, 2021
DOI: 10.2478/forma-2021-0020

sciendo
https://sciendo.com/journal/forma

Prime Representing Polynomial

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Summary. The main purpose of formalization is to prove that the set of prime numbers is diophantine, i.e., is representable by a polynomial formula. We formalize this problem, using the Mizar system [1], [2], in two independent ways, proving the existence of a polynomial without formulating it explicitly as well as with its indication.

First, we reuse nearly all the techniques invented to prove the MRDP-theorem [11]. Applying a trick with Mizar schemes that go beyond first-order logic we give a short sophisticated proof for the existence of such a polynomial but without formulating it explicitly. Then we formulate the polynomial proposed in [6] that has 26 variables in the Mizar language as follows

$$(w\cdot z+h+j-q)^{\mathbf{2}}+((g\cdot k+g+k)\cdot(h+j)+h-z)^{\mathbf{2}}+(2\cdot k^3\cdot(2\cdot k+2)\cdot(n+1)^2+1-f^{\mathbf{2}})^{\mathbf{2}}+ (p+q+z+2\cdot n-e)^{\mathbf{2}}+(e^3\cdot(e+2)\cdot(a+1)^2+1-o^{\mathbf{2}})^{\mathbf{2}}+(x^{\mathbf{2}}-(a^{\mathbf{2}}-'1)\cdot y^{\mathbf{2}}-1)^{\mathbf{2}}+ (16\cdot(a^{\mathbf{2}}-1)\cdot r^{\mathbf{2}}\cdot y^{\mathbf{2}}\cdot y^{\mathbf{2}}+1-u^{\mathbf{2}})^{\mathbf{2}}+(((a+u^{\mathbf{2}}\cdot(u^{\mathbf{2}}-a))^{\mathbf{2}}-1)\cdot(n+4\cdot d\cdot y)^{\mathbf{2}}+ 1-(x+c\cdot u)^{\mathbf{2}})^{\mathbf{2}}+ (m^{\mathbf{2}}-(a^{\mathbf{2}}-'1)\cdot l^{\mathbf{2}}-1)^{\mathbf{2}}+(k+i\cdot(a-1)-l)^{\mathbf{2}}+(n+l+v-y)^{\mathbf{2}}+ (p+l\cdot(a-n-1)+b\cdot(2\cdot a\cdot(n+1)-(n+1)^{\mathbf{2}}-1)-m)^{\mathbf{2}}+ (q+y\cdot(a-p-1)+s\cdot(2\cdot a\cdot(p+1)-(p+1)^{\mathbf{2}}-1)-x)^{\mathbf{2}}+(z+p\cdot l\cdot(a-p)+ t\cdot(2\cdot a\cdot p-p^{\mathbf{2}}-1)-p\cdot m)^{\mathbf{2}}$$

and we prove that that for any positive integer k so that $k+1$ is prime it is necessary and sufficient that there exist other natural variables a-z for which the polynomial equals zero. 26 variables is not the best known result in relation to the set of prime numbers, since any diophantine equation over ℕ can be reduced to one in 13 unknowns [8] or even less [5], [13]. The best currently known result for all prime numbers, where the polynomial is explicitly constructed is 10 [7] or even 7 in the case of Fermat as well as Mersenne prime number [4]. We are currently focusing our formalization efforts in this direction.

MSC: 11D45 68V20

Keywords: prime number; polynomial reduction; diophantine equation

MML identifier: HILB10_6, version: 8.1.11 5.68.1412

ISSN 1426–2630(Print), 1898-9934(Online)

1. The Prime Number Set as a Diophantine Set

From now on n denotes a natural number, i, j, i_1, i_2, i_3, i_4, i_5, i_6 denote elements of n, and p, q, r denote n-element finite 0-sequences of $\mathbb{N}$.

Now we state the propositions:

(1) $\{p : p(i) > 1\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

PROOF: Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(i) > 0 \cdot \$_1(i) + 1$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i) > 1$. $\{q : \mathcal{Q}[q]\} = \{r : \mathcal{R}[r]\}$. □

(2) $\{p : p(i) = (p(j) -' 1)! + 1\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

PROOF: For every n, i_1, and i_2, $\{p : p(i_1) = p(i_2) -' 1\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. For every n, i_1, and i_2, $\{p : p(i_1) = (p(i_2) -' 1)!\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$ by [10, (32)]. Define $\mathcal{P}$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv \$_4 = 1 \cdot \$_3 + 1$. Define $\mathcal{F}$(natural number, natural number, natural number) $= (\$_2 -' 1)!$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_1) = 1 \cdot ((\$_1(i_2) -' 1)!) + 1$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_1) = (\$_1(i_2) -' 1)! + 1$. $\{q : \mathcal{Q}[q]\} = \{r : \mathcal{R}[r]\}$. □

(3) $\{p : (p(i) -' 1)! + 1 \bmod p(i) = 0$ and $p(i) > 1\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

PROOF: Define $\mathcal{P}$[natural number, natural number, natural object, natural number, natural number, natural number] $\equiv 1 \cdot \$_3 \equiv 0 \cdot \$_4 \pmod{1 \cdot \$_4}$. Define $\mathcal{F}$(natural number, natural number, natural number) $= (\$_2 -' 1)! + 1$. For every n, i_1, i_2, i_3, and i_4, $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = p(i_4)\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{Q}_1$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot ((\$_1(i) -' 1)! + 1) \equiv 0 \cdot \$_1(i) \pmod{1 \cdot \$_1(i)}$.

Define $\mathcal{Q}_2$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i) > 1$. Define $\mathcal{Q}_{12}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{Q}_1[\$_1]$ and $\mathcal{Q}_2[\$_1]$. $\{q : \mathcal{Q}_2[q]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. $\{q : \mathcal{Q}_1[q]$ and $\mathcal{Q}_2[q]\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv (\$_1(i) -' 1)! + 1 \bmod \$_1(i) = 0$ and $\$_1(i) > 1$ by [12, (11)]. $\mathcal{Q}_{12}[q]$ iff $\mathcal{R}[q]$. $\{q : \mathcal{Q}_{12}[q]\} = \{r : \mathcal{R}[r]\}$. □

(4) Let us consider a natural number n, and an element i of n. Then $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N} : p(i)$ is prime$\}$ is a Diophantine subset of the n-xtuples of $\mathbb{N}$.

PROOF: Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i)$ is prime. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv (\$_1(i) -' 1)! + 1 \bmod \$_1(i) = 0$ and $\$_1(i) > 1$. $\{q : \mathcal{Q}[q]\} = \{r : \mathcal{R}[r]\}$. □

2. Special Case of Pell's Equation - Selected Properties

In the sequel i, j, n, n_1, n_2, m, k, l, u, e, p, t denote natural numbers, a, b denote non trivial natural numbers, x, y denote integers, and r, q denote real numbers.

Now we state the propositions:

(5) If $2 \leqslant e$ and there exists i such that $e^{\mathbf{2}} \cdot e \cdot (e+2) \cdot (n+1)^{\mathbf{2}} + 1 = i^{\mathbf{2}}$, then $e - 1 + e^{e-'2} \leqslant n$.
Proof: Set $a = e+1$. Set $n_1 = n+1$. Reconsider $e_2 = e-2$ as a natural number. Consider j such that $i = \mathtt{x}_a(j)$ and $e \cdot n_1 = \mathtt{y}_a(j)$. $(a-2) \cdot e + e^{e_2+1} < (2 \cdot a - 1)^{e_2+1}$ by [14, (103)]. $\square$

(6) If $2 \leqslant e$ and $0 < t$, then there exists n and there exists i such that $t \mid n+1$ and $e^{\mathbf{2}} \cdot e \cdot (e+2) \cdot (n+1)^{\mathbf{2}} + 1 = i^{\mathbf{2}}$.

(7) If $n \geqslant k$, then $\binom{n}{k} \geqslant \frac{(n+1-k)^k}{k!}$.
Proof: Set $n_1 = n+1$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant n$, then $\binom{n}{\$_1} \geqslant \frac{(n_1-\$_1)^{\$_1}}{\$_1!}$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. $\square$

(8) If $n \geqslant k$, then $\binom{n}{k} \leqslant \frac{n^k}{k!}$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant n$, then $\binom{n}{\$_1} \leqslant \frac{n^{\$_1}}{\$_1!}$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. $\square$

(9) If $i \leqslant j$ and $2 \cdot j \leqslant n+1$, then $\binom{n}{i} \leqslant \binom{n}{j}$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ if $i \leqslant \$_1$ and $2 \cdot \$_1 \leqslant n+1$, then $\binom{n}{i} \leqslant \binom{n}{\$_1}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(10) If $k \leqslant n$, then $n! \leqslant k! \cdot (n^{n-'k})$.
Proof: Define $\mathcal{P}$[natural number] $\equiv (k+\$_1)! \leqslant k! \cdot (k+\$_1)^{\$_1}$. If $\mathcal{P}[i]$, then $\mathcal{P}[i+1]$. $\mathcal{P}[i]$. $\square$

(11) Suppose $0 < k$ and $2 \cdot k^k \leqslant n$ and $n^k < p$. Then

(i) $(p+1)^n \bmod p^{k+1} > 0$, and

(ii) $k! < \frac{(n+1)^k \cdot (p^k)}{(p+1)^n \bmod p^{k+1}} < k! + 1$.

Proof: Set $k_1 = k+1$. Set $n_1 = n+1$. Reconsider $K = k-1$, $n_3 = n-k$ as a natural number. Set $P = \langle \binom{n}{0} 1^0 p^n, \ldots, \binom{n}{n} 1^n p^0 \rangle$. $\sum(P \restriction k_1) \equiv \sum P \pmod{p^{k_1}}$. $\sum(P \restriction k_1) \neq 0$. $\sum(P \restriction k_1) < p^{k_1}$. $\binom{n}{k} \leqslant \frac{n^k}{k!}$. $\sum(P \restriction k) \leqslant \frac{n^k}{k!} \cdot (p^K) \cdot k$. $\binom{n}{k} \geqslant \frac{(n_1-k)^k}{k!}$. $k \cdot k \leqslant n$ and $2 \cdot k \cdot k \leqslant n_1$. $1 \cdot (2 \cdot k^k) \geqslant 2 \cdot k^{\mathbf{2}} \cdot (k!)$. $\square$

(12) (i) $\mathtt{x}_a(n+2) = 2 \cdot a \cdot \mathtt{x}_a(n+1) - \mathtt{x}_a(n)$, and

(ii) $\mathtt{y}_a(n+2) = 2 \cdot a \cdot \mathtt{y}_a(n+1) - \mathtt{y}_a(n)$.

(13) $\mathtt{x}_a(n) \equiv p^n + \mathtt{y}_a(n) \cdot (a - p) \pmod{2 \cdot a \cdot p - p^{\mathbf{2}} - 1}$.

PROOF: Set $P = 2 \cdot a \cdot p - p^{\mathbf{2}} - 1$. Define $\mathcal{T}$[natural number] $\equiv \mathtt{x}_a(\$_1) - \mathtt{y}_a(\$_1) \cdot (a - p) \equiv p^{\$_1} \pmod{P}$. Define $\mathcal{P}$[natural number] $\equiv \mathcal{T}[\$_1]$ and $\mathcal{T}[\$_1 + 1]$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(14) If $0 < p^n < a$, then $p^n + \mathtt{y}_a(n) \cdot (a - p) \leqslant \mathtt{x}_a(n)$.

(15) If $a \leqslant b$, then $\mathtt{x}_a(n) \leqslant \mathtt{x}_b(n)$ and $\mathtt{y}_a(n) \leqslant \mathtt{y}_b(n)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathtt{x}_a(\$_1) \leqslant \mathtt{x}_b(\$_1)$ and $\mathtt{y}_a(\$_1) \leqslant \mathtt{y}_b(\$_1)$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(16) If $a \equiv b \pmod{k}$, then $\mathtt{x}_a(n) \equiv \mathtt{x}_b(n) \pmod{k}$.

(17) $\mathtt{x}_a(|2 \cdot x + y|) \equiv -\mathtt{x}_a(|y|) \pmod{\mathtt{x}_a(|x|)}$.

PROOF: Set $i = x$. Set $j = y$. Set $A = a^{\mathbf{2}} -' 1$. $A \cdot \operatorname{sgn}(i) \cdot \mathtt{y}_a(|i|) \cdot (\operatorname{sgn}(i) \cdot \mathtt{y}_a(|i|) \cdot \mathtt{x}_a(|j|)) = (A \cdot (\mathtt{y}_a(|i|) \cdot \mathtt{y}_a(|i|))) \cdot \mathtt{x}_a(|j|)$. □

(18) $\mathtt{x}_a(|4 \cdot x + y|) \equiv \mathtt{x}_a(|y|) \pmod{\mathtt{x}_a(|x|)}$. The theorem is a consequence of (17).

(19) If $k < n$, then $\mathtt{x}_a(k) < \mathtt{x}_a(n)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 > 0$, then $\mathtt{x}_a(k) < \mathtt{x}_a(k + \$_1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. $\mathcal{P}[n_1]$. □

(20) If $\mathtt{x}_a(k) = \mathtt{x}_a(n)$, then $k = n$. The theorem is a consequence of (19).

(21) If $i \leqslant j \leqslant 2 \cdot n$ and $\mathtt{x}_a(i) \equiv \mathtt{x}_a(j) \pmod{\mathtt{x}_a(n)}$, then $i = 0$ and $j = 2$ and $a = 2$ and $n = 1$ or $i = j$. The theorem is a consequence of (19), (17), and (20).

(22) If $0 < i \leqslant n$ and $0 \leqslant j < 4 \cdot n$ and $\mathtt{x}_a(i) \equiv \mathtt{x}_a(j) \pmod{\mathtt{x}_a(n)}$, then $j = i$ or $j + i = 4 \cdot n$. The theorem is a consequence of (18) and (21).

(23) $\mathtt{x}_a(|4 \cdot x \cdot n + y|) \equiv \mathtt{x}_a(|y|) \pmod{\mathtt{x}_a(|x|)}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathtt{x}_a(|4 \cdot x \cdot \$_1 + y|) \equiv \mathtt{x}_a(|y|) \pmod{\mathtt{x}_a(|x|)}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

(24) Suppose $0 < i \leqslant n$ and $\mathtt{x}_a(i) \equiv \mathtt{x}_a(j) \pmod{\mathtt{x}_a(n)}$. Then

(i) $j \equiv i \pmod{4 \cdot n}$, or

(ii) $j \equiv -i \pmod{4 \cdot n}$.

The theorem is a consequence of (23) and (22).

(25) $\mathtt{y}_a(2 \cdot n) = 2 \cdot \mathtt{y}_a(n) \cdot \mathtt{x}_a(n)$.

3. Special Case of Pell's Equation - Diophantine Polynomial with 8 Variables

Now we state the propositions:

(26) Let us consider a non trivial natural number a, and natural numbers y, n, b, c, d, r, s, t, u, v, x. Suppose $1 \leqslant n$ and $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $\langle u, v \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $\langle s, t \rangle$ is a Pell's solution of $b^{\mathbf{2}} -' 1$ and $v = 4 \cdot r \cdot y^{\mathbf{2}}$ and $b = a + u^{\mathbf{2}} \cdot (u^{\mathbf{2}} - a)$ and $s = x + c \cdot u$ and $t = n + 4 \cdot d \cdot y$ and $n \leqslant y$. Then

(i) b is not trivial, and

(ii) $u^{\mathbf{2}} > a$, and

(iii) $y = \mathtt{y}_a(n)$.

Proof: Consider i being a natural number such that $x = \mathtt{x}_a(i)$ and $y = \mathtt{y}_a(i)$. Consider n_1 being a natural number such that $u = \mathtt{x}_a(n_1)$ and $v = \mathtt{y}_a(n_1)$. $v \neq 0$ by [3, (1)]. Reconsider $B = b$ as a non trivial natural number. Consider j being a natural number such that $s = \mathtt{x}_B(j)$ and $t = \mathtt{y}_B(j)$. $\mathtt{x}_B(j) \equiv \mathtt{x}_a(j) \pmod{\mathtt{x}_a(n_1)}$. $j \equiv i \pmod{4 \cdot n_1}$ or $j \equiv -i \pmod{4 \cdot n_1}$. Consider d_1 being a natural number such that $\mathtt{y}_a(i) \cdot d_1 = n_1$. $n = i$ by [9, (13)]. □

(27) Let us consider a non trivial natural number a, and natural numbers y, n. Suppose $1 \leqslant n$. Suppose $y = \mathtt{y}_a(n)$. Then there exist natural numbers b, c, d, r, s, t, u, v, x such that

(i) $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$, and

(ii) $\langle u, v \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$, and

(iii) $\langle s, t \rangle$ is a Pell's solution of $b^{\mathbf{2}} -' 1$, and

(iv) $v = 4 \cdot r \cdot y^{\mathbf{2}}$, and

(v) $b = a + u^{\mathbf{2}} \cdot (u^{\mathbf{2}} - a)$, and

(vi) $s = x + c \cdot u$, and

(vii) $t = n + 4 \cdot d \cdot y$, and

(viii) $n \leqslant y$.

The theorem is a consequence of (25), (16), and (15).

(28) Let us consider natural numbers y, n. Suppose $1 \leqslant n$. Then $y = \mathtt{y}_a(n)$ if and only if there exist natural numbers c, d, r, u, x such that $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $u^{\mathbf{2}} = 16 \cdot (a^{\mathbf{2}} - 1) \cdot r^{\mathbf{2}} \cdot y^{\mathbf{2}} \cdot y^{\mathbf{2}} + 1$ and $(x + c \cdot u)^{\mathbf{2}} = ((a + u^{\mathbf{2}} \cdot (u^{\mathbf{2}} - a))^{\mathbf{2}} - 1) \cdot (n + 4 \cdot d \cdot y)^{\mathbf{2}} + 1$ and $n \leqslant y$.

Proof: If $y = \mathtt{y}_a(n)$, then there exist natural numbers c, d, r, u, x such that $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $u^{\mathbf{2}} = 16 \cdot (a^{\mathbf{2}} - 1) \cdot r^{\mathbf{2}} \cdot y^{\mathbf{2}} \cdot y^{\mathbf{2}} + 1$

and $(x + c \cdot u)^{\mathbf{2}} = ((a + u^{\mathbf{2}} \cdot (u^{\mathbf{2}} - a))^{\mathbf{2}} - 1) \cdot (n + 4 \cdot d \cdot y)^{\mathbf{2}} + 1$ and $n \leqslant y$. Consider k such that $x = \mathtt{x}_a(k)$ and $y = \mathtt{y}_a(k)$. $r \neq 0$. □

(29) Let us consider positive natural numbers f, k. Then $f = k!$ if and only if there exist natural numbers j, h, w and there exist positive natural numbers n, p, q, z such that $q = w \cdot z + h + j$ and $z = f \cdot (h + j) + h$ and $2 \cdot k^3 \cdot (2 \cdot k + 2) \cdot (n + 1)^2 + 1$ is a square and $p = (n + 1)^k$ and $q = (p + 1)^n$ and $z = p^{k+1}$.

Proof: Set $k_2 = 2 \cdot k$. If $f = k!$, then there exist natural numbers j, h, w and there exist positive natural numbers n, p, q, z such that $q = w \cdot z + h + j$ and $z = f \cdot (h + j) + h$ and $2 \cdot k^3 \cdot (k_2 + 2) \cdot (n + 1)^2 + 1$ is a square and $p = (n + 1)^k$ and $q = (p + 1)^n$ and $z = p^{k+1}$. ${k_2}^k \leqslant n$. $h + j \neq z$. $k! < \frac{z}{h+j} < k! + 1$. □

(30) Let us consider a positive natural number k. Then $k + 1$ is prime if and only if there exist natural numbers a, b, c, d, e, f, g, h, i, j, l, m, n, o, p, q, r, s, t, u, w, v, x, y, z such that $q = w \cdot z + h + j$ and $z = (g \cdot k + g + k) \cdot (h + j) + h$ and $2 \cdot k^3 \cdot (2 \cdot k + 2) \cdot (n + 1)^2 + 1 = f^{\mathbf{2}}$ and $e = p + q + z + 2 \cdot n$ and $e^3 \cdot (e + 2) \cdot (a + 1)^2 + 1 = o^{\mathbf{2}}$ and $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $u^{\mathbf{2}} = 16 \cdot (a^{\mathbf{2}} - 1) \cdot r^{\mathbf{2}} \cdot y^{\mathbf{2}} \cdot y^{\mathbf{2}} + 1$ and $(x + c \cdot u)^{\mathbf{2}} = ((a + u^{\mathbf{2}} \cdot (u^{\mathbf{2}} - a))^{\mathbf{2}} - 1) \cdot (n + 4 \cdot d \cdot y)^{\mathbf{2}} + 1$ and $\langle m, l \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $l = k + i \cdot (a - 1)$ and $n + l + v = y$ and $m = p + l \cdot (a - n - 1) + b \cdot (2 \cdot a \cdot (n + 1) - (n + 1)^{\mathbf{2}} - 1)$ and $x = q + y \cdot (a - p - 1) + s \cdot (2 \cdot a \cdot (p + 1) - (p + 1)^{\mathbf{2}} - 1)$ and $p \cdot m = z + p \cdot l \cdot (a - p) + t \cdot (2 \cdot a \cdot p - p^{\mathbf{2}} - 1)$.

Proof: If $k + 1$ is prime, then there exist natural numbers a, b, c, d, e, f, g, h, i, j, l, m, n, o, p, q, r, s, t, u, w, v, x, y, z such that $q = w \cdot z + h + j$ and $z = (g \cdot k + g + k) \cdot (h + j) + h$ and $2 \cdot k^3 \cdot (2 \cdot k + 2) \cdot (n + 1)^2 + 1 = f^{\mathbf{2}}$ and $e = p + q + z + 2 \cdot n$ and $e^3 \cdot (e + 2) \cdot (a + 1)^2 + 1 = o^{\mathbf{2}}$ and $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $u^{\mathbf{2}} = 16 \cdot (a^{\mathbf{2}} - 1) \cdot r^{\mathbf{2}} \cdot y^{\mathbf{2}} \cdot y^{\mathbf{2}} + 1$ and $(x + c \cdot u)^{\mathbf{2}} = ((a + u^{\mathbf{2}} \cdot (u^{\mathbf{2}} - a))^{\mathbf{2}} - 1) \cdot (n + 4 \cdot d \cdot y)^{\mathbf{2}} + 1$ and $\langle m, l \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $l = k + i \cdot (a - 1)$ and $n + l + v = y$ and $m = p + l \cdot (a - n - 1) + b \cdot (2 \cdot a \cdot (n + 1) - (n + 1)^{\mathbf{2}} - 1)$ and $x = q + y \cdot (a - p - 1) + s \cdot (2 \cdot a \cdot (p + 1) - (p + 1)^{\mathbf{2}} - 1)$ and $p \cdot m = z + p \cdot l \cdot (a - p) + t \cdot (2 \cdot a \cdot p - p^{\mathbf{2}} - 1)$. $2 \cdot k - 1 + 2 \cdot k^{2 \cdot k -' 2} \leqslant n$. $e - 1 + e^{e -' 2} \leqslant a$. $e - 1 + e^{e -' 2} \leqslant a$. $y = \mathtt{y}_a(n)$.

Consider n_2 being a natural number such that $x = \mathtt{x}_a(n_2)$ and $y = \mathtt{y}_a(n_2)$. Consider k_1 being a natural number such that $m = \mathtt{x}_a(k_1)$ and $l = \mathtt{y}_a(k_1)$. $(n + 1)^k < a$. $(n + 1)^k + (\mathtt{y}_a(k)) \cdot (a - (n + 1)) \equiv \mathtt{x}_a(k) \pmod{2 \cdot a \cdot (n + 1) - (n + 1)^{\mathbf{2}} - 1}$. $(p + 1)^n < a$. $(p + 1)^n + (\mathtt{y}_a(n)) \cdot (a - (p + 1)) \equiv \mathtt{x}_a(n) \pmod{2 \cdot a \cdot (p + 1) - (p + 1)^{\mathbf{2}} - 1}$. $p^{k+1} < a$. $p^k + (\mathtt{y}_a(k)) \cdot (a - p) \equiv \mathtt{x}_a(k) \pmod{2 \cdot a \cdot p - p^{\mathbf{2}} - 1}$. $g \cdot k + g + k = k!$. □

4. Prime Representing Polynomial with 26 Variables

Now we state the proposition:

(31) Prime Representing Polynomial:

Let us consider a positive natural number k. Then $k+1$ is prime if and only if there exist natural numbers a, b, c, d, e, f, g, h, i, j, l, m, n, o, p, q, r, s, t, u, w, v, x, y, z such that:

$0 = (w \cdot z + h + j - q)^{\mathbf{2}} + ((g \cdot k + g + k) \cdot (h + j) + h - z)^{\mathbf{2}} + (2 \cdot k^3 \cdot (2 \cdot k + 2) \cdot (n+1)^2 + 1 - f^{\mathbf{2}})^{\mathbf{2}} + (p+q+z+2 \cdot n - e)^{\mathbf{2}} + (e^3 \cdot (e+2) \cdot (a+1)^2 + 1 - o^{\mathbf{2}})^{\mathbf{2}} + (x^{\mathbf{2}} - (a^{\mathbf{2}} -' 1) \cdot y^{\mathbf{2}} - 1)^{\mathbf{2}} + (16 \cdot (a^{\mathbf{2}} - 1) \cdot r^{\mathbf{2}} \cdot y^{\mathbf{2}} \cdot y^{\mathbf{2}} + 1 - u^{\mathbf{2}})^{\mathbf{2}} + (((a + u^{\mathbf{2}} \cdot (u^{\mathbf{2}} - a))^{\mathbf{2}} - 1) \cdot (n + 4 \cdot d \cdot y)^{\mathbf{2}} + 1 - (x + c \cdot u)^{\mathbf{2}})^{\mathbf{2}} + (m^{\mathbf{2}} - (a^{\mathbf{2}} -' 1) \cdot l^{\mathbf{2}} - 1)^{\mathbf{2}} + (k + i \cdot (a-1) - l)^{\mathbf{2}} + (n + l + v - y)^{\mathbf{2}} + (p + l \cdot (a - n - 1) + b \cdot (2 \cdot a \cdot (n+1) - (n+1)^{\mathbf{2}} - 1) - m)^{\mathbf{2}} + (q + y \cdot (a - p - 1) + s \cdot (2 \cdot a \cdot (p+1) - (p+1)^{\mathbf{2}} - 1) - x)^{\mathbf{2}} + (z + p \cdot l \cdot (a - p) + t \cdot (2 \cdot a \cdot p - p^{\mathbf{2}} - 1) - p \cdot m)^{\mathbf{2}}$. The theorem is a consequence of (30).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, 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.

[2] 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.

[3] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Gaussian integers. *Formalized Mathematics*, 21(**2**):115–125, 2013. doi:10.2478/forma-2013-0013.

[4] James P. Jones. Diophantine representation of Mersenne and Fermat primes. *Acta Arithmetica*, 35:209–221, 1979. doi:10.4064/AA-35-3-209-221.

[5] James P. Jones. Universal diophantine equation. *Journal of Symbolic Logic*, 47(4):549–571, 1982.

[6] 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.

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

[8] Yuri Matiyasevich and Julia Robinson. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, 27:521–553, 1975.

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

[10] Karol Pąk. Diophantine sets. Part II. *Formalized Mathematics*, 27(**2**):197–208, 2019. doi:10.2478/forma-2019-0019.

[11] Karol Pąk. Formalization of the MRDP theorem in the Mizar system. *Formalized Mathematics*, 27(**2**):209–221, 2019. doi:10.2478/forma-2019-0020.

[12] Christoph Schwarzweller. Proth numbers. *Formalized Mathematics*, 22(**2**):111–118, 2014. doi:10.2478/forma-2014-0013.

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

[14] Rafał Ziobro. Prime factorization of sums and differences of two like powers. *Formalized Mathematics*, 24(**3**):187–198, 2016. doi:10.1515/forma-2016-0015.

Accepted November 30, 2021