Special Issue: 25 years of the Mizar Mathematical Library

FORMALIZED MATHEMATICS
Vol. **22**, No. **2**, Pages 105–110, **2014**
DOI: 10.2478/forma-2014-0012

DE GRUYTER OPEN
degruyter.com/view/j/forma

Lagrange's Four-Square Theorem

Yasushige Watase
Suginami-ku Matsunoki 6
3-21 Tokyo, Japan

Summary. This article provides a formalized proof of the so-called "the four-square theorem", namely any natural number can be expressed by a sum of four squares, which was proved by Lagrange in 1770. An informal proof of the theorem can be found in the number theory literature, e.g. in [14], [1] or [23].

This theorem is item `#19` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 11P99 03B35

Keywords: Lagrange's four-square theorem

MML identifier: `LAGRA4SQ`, version: `8.1.03 5.23.1207`

The notation and terminology used in this paper have been introduced in the following articles: [19], [2], [7], [6], [12], [8], [9], [21], [17], [4], [15], [16], [5], [10], [13], [24], [25], [22], and [11].

1. Preliminaries

Let n be a natural number. We say that n is a sum of four squares if and only if

(Def. 1) There exist natural numbers n_1, n_2, n_3, n_4 such that $n = {n_1}^{\mathbf{2}} + {n_2}^{\mathbf{2}} + {n_3}^{\mathbf{2}} + {n_4}^{\mathbf{2}}$.

Note that there exists a natural number which is a sum of four squares.

Let y be an integer object. Let us note that $|y|$ is natural.

Now we state the proposition:

(1) Let us consider natural numbers n_1, n_2, n_3, n_4, m_1, m_2, m_3, m_4. Then $({n_1}^{\mathbf{2}} + {n_2}^{\mathbf{2}} + {n_3}^{\mathbf{2}} + {n_4}^{\mathbf{2}}) \cdot ({m_1}^{\mathbf{2}} + {m_2}^{\mathbf{2}} + {m_3}^{\mathbf{2}} + {m_4}^{\mathbf{2}}) = (n_1 \cdot m_1 - n_2 \cdot m_2 - n_3 \cdot m_3 - n_4 \cdot m_4)^{\mathbf{2}} + (n_1 \cdot m_2 + n_2 \cdot m_1 + n_3 \cdot m_4 - n_4 \cdot m_3)^{\mathbf{2}} + (n_1 \cdot m_3 - n_2 \cdot m_4 + n_3 \cdot m_1 + n_4 \cdot m_2)^{\mathbf{2}} + (n_1 \cdot m_4 + n_2 \cdot m_3 - n_3 \cdot m_2 + n_4 \cdot m_1)^{\mathbf{2}}$.

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

Let m, n be natural numbers. Let us note that $m \cdot n$ is a sum of four squares and there exists a prime natural number which is odd.

From now on i, j, k, v, w denote natural numbers, j_1, j_2, m, n, s, t, x, y denote integers, and p denotes an odd prime natural number.

Let us consider p. The functor ModMap(p) yielding a function from $\mathbb{Z}$ into $\mathbb{Z}_p$ is defined by

(Def. 2) Let us consider an element x of $\mathbb{Z}$. Then $it(x) = x \bmod p$.

Let us consider v. The functor Lag4SqF(v) yielding a finite sequence of elements of $\mathbb{Z}$ is defined by

(Def. 3) (i) $\operatorname{len} it = v$, and

(ii) for every natural number i such that $i \in \operatorname{dom} it$ holds $it(i) = (i-1)^{\mathbf{2}}$.

The functor Lag4SqG(v) yielding a finite sequence of elements of $\mathbb{Z}$ is defined by

(Def. 4) (i) $\operatorname{len} it = v$, and

(ii) for every natural number i such that $i \in \operatorname{dom} it$ holds $it(i) = -1 - (i-1)^{\mathbf{2}}$.

Now we state the propositions:

(2) Lag4SqF(v) is one-to-one.

(3) Lag4SqG(v) is one-to-one.

In the sequel a denotes a real number and b denotes an integer.

Let us consider an odd prime natural number p, a natural number s, j_1, and j_2. Now we state the propositions:

(4) If $2 \cdot s = p + 1$ and $j_1, j_2 \in \operatorname{rng} \text{Lag4SqF}(s)$, then $j_1 = j_2$ or $j_1 \bmod p \neq j_2 \bmod p$. PROOF: Consider s such that $p+1 = 2 \cdot s$. For every integers j_1, j_2 such that $j_1, j_2 \in \operatorname{rng} \text{Lag4SqF}(s)$ and $j_1 \neq j_2$ holds $j_1 \bmod p \neq j_2 \bmod p$ by [21, (3), (55)], [16, (80)], [18, (22)]. □

(5) If $2 \cdot s = p + 1$ and $j_1, j_2 \in \operatorname{rng} \text{Lag4SqG}(s)$, then $j_1 = j_2$ or $j_1 \bmod p \neq j_2 \bmod p$. PROOF: Consider s such that $p + 1 = 2 \cdot s$. For every j_1 and j_2 such that $j_1, j_2 \in \operatorname{rng} \text{Lag4SqG}(s)$ and $j_1 \neq j_2$ holds $j_1 \bmod p \neq j_2 \bmod p$ by [21, (3), (55)], [16, (80)], [20, (7)]. □

2. Any Prime Number can be Expressed as a Sum of Four Squares

Now we state the propositions:

(6) There exist natural numbers x_1, x_2, x_3, x_4, h such that

(i) $0 < h < p$, and

(ii) $h \cdot p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.

PROOF: Consider s such that $2 \cdot s = p + 1$. Set $f = \text{Lag4SqF}(s)$. Set $g = \text{Lag4SqG}(s)$. f is one-to-one. g is one-to-one. $\operatorname{rng} f$ misses $\operatorname{rng} g$. $\overline{\overline{\operatorname{rng}(g \frown f)}} = p + 1$ by [2, (70)], [6, (57), (31)], [3, (35), (36)]. Set $A = \operatorname{dom}(\text{ModMap}(p) \restriction \operatorname{rng}(g \frown f))$. Set $B = \operatorname{rng}(\text{ModMap}(p) \restriction \operatorname{rng}(g \frown f))$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element m_1 of $\mathbb{Z}$ such that $\$_1 \in A$ and $\$_2 = m_1$ and $(\text{ModMap}(p) \restriction \operatorname{rng}(g \frown f))(\$_1) = m_1$. For every object x such that $x \in A$ there exists an object y such that $y \in B$ and $\mathcal{P}[x, y]$ by [8, (3)]. Consider h being a function from A into B such that for every object x such that $x \in A$ holds $\mathcal{P}[x, h(x)]$ from [9, Sch. 1]. Consider m_1, m_2 being objects such that $m_1 \in A$ and $m_2 \in A$ and $m_1 \neq m_2$ and $h(m_1) = h(m_2)$. If $m_1 \in \operatorname{rng} f$, then $m_2 \in \operatorname{rng} g$. If $m_1 \in \operatorname{rng} g$, then $m_2 \in \operatorname{rng} f$. There exist natural numbers x_1, x_2, x_3, x_4, h such that $h > 0$ and $h < p$ and $h \cdot p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$ by [20, (7)], [21, (3)]. □

(7) Let us consider natural numbers x_1, h. Suppose $1 < h$. Then there exists an integer y_1 such that

(i) $x_1 \bmod h = y_1 \bmod h$, and

(ii) $-h < 2 \cdot y_1 \leqslant h$, and

(iii) ${x_1}^{\mathbf{2}} \bmod h = {y_1}^{\mathbf{2}} \bmod h$.

PROOF: Consider q_1, r_1 being integers such that $x_1 = h \cdot q_1 + r_1$ and $0 \leqslant r_1$ and $r_1 < h$. There exists an integer y_1 such that $x_1 \bmod h = y_1 \bmod h$ and $-h < 2 \cdot y_1 \leqslant h$ and ${x_1}^{\mathbf{2}} \bmod h = {y_1}^{\mathbf{2}} \bmod h$ by [21, (3)], [18, (23)]. □

(8) Let us consider natural numbers i_1, i_2, c. If $i_1 \leqslant c$ and $i_2 \leqslant c$, then $i_1 + i_2 < 2 \cdot c$ or $i_1 = c$ and $i_2 = c$.

(9) Let us consider natural numbers i_1, i_2, i_3, i_4, c. Suppose

(i) $i_1 \leqslant c$, and

(ii) $i_2 \leqslant c$, and

(iii) $i_3 \leqslant c$, and

(iv) $i_4 \leqslant c$.

Then

(v) $i_1 + i_2 + i_3 + i_4 < 4 \cdot c$, or

(vi) $i_1 = c$ and $i_2 = c$ and $i_3 = c$ and $i_4 = c$.

The theorem is a consequence of (8).

Let us consider natural numbers x_1, h and an integer y_1. Now we state the propositions:

(10) Suppose $1 < h$ and $x_1 \bmod h = y_1 \bmod h$ and $-h < 2 \cdot y_1$ and $(2 \cdot y_1)^{\mathbf{2}} = h^{\mathbf{2}}$. Then

(i) $2 \cdot y_1 = h$, and

(ii) there exists a natural number m_1 such that $2 \cdot x_1 = (2 \cdot m_1 + 1) \cdot h$.

(11) If $1 < h$ and $x_1 \bmod h = y_1 \bmod h$ and $y_1 = 0$, then there exists an integer m_1 such that $x_1 = h \cdot m_1$.

Now we state the proposition:

(12) Let us consider an odd prime number p and natural numbers x_1, x_2, x_3, x_4, h. Suppose

(i) $1 < h < p$, and

(ii) $h \cdot p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.

Then there exist integers y_1, y_2, y_3, y_4 and there exists a natural number r such that $0 < r < h$ and $r \cdot p = {y_1}^{\mathbf{2}} + {y_2}^{\mathbf{2}} + {y_3}^{\mathbf{2}} + {y_4}^{\mathbf{2}}$. The theorem is a consequence of (7), (9), (10), and (11).

Let us consider a prime number p. Now we state the propositions:

(13) If p is even, then $p = 2$.

(14) There exist natural numbers x_1, x_2, x_3, x_4 such that $p = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.

Now we state the proposition:

(15) Let us consider prime numbers p_1, p_2. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $p_1 \cdot p_2 = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. The theorem is a consequence of (14).

Let p_1, p_2 be prime numbers. Let us observe that $p_1 \cdot p_2$ is a sum of four squares.

Now we state the proposition:

(16) Let us consider a prime number p and a natural number n. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $p^n = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ there exist natural numbers x_1, x_2, x_3, x_4 such that $p^{\$_1} = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (14), [7, (75)], [16, (6)]. $\mathcal{P}[0]$ by [16, (4)]. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. $\square$

Let p be a prime number and n be a natural number. Observe that p^n is a sum of four squares.

3. Proof of Lagrange's theorem

Now we state the proposition:

(17) Let us consider a non zero natural number n. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $\prod \mathrm{PPF}(n) = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every non zero natural number n such that $\overline{\overline{\mathrm{support}\,\mathrm{PPF}(n)}} = \$_1$ there exist natural numbers x_1, x_2, x_3, x_4 such that $\prod \mathrm{PPF}(n) = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. $\mathcal{P}[0]$ by [15, (20)]. For

every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [15, (34), (28), (25)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

Now we state the proposition:

(18) Lagrange's four-square theorem:
Let us consider a natural number n. Then there exist natural numbers x_1, x_2, x_3, x_4 such that $n = {x_1}^{\mathbf{2}} + {x_2}^{\mathbf{2}} + {x_3}^{\mathbf{2}} + {x_4}^{\mathbf{2}}$. The theorem is a consequence of (17).

One can verify that every natural number is a sum of four squares.

References

[1] Alan Baker. *A Concise Introduction to the Theory of Numbers.* Cambridge University Press, 1984.
[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[3] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.
[4] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[5] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[7] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[10] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[11] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[13] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.
[14] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 1980.
[15] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.
[16] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[17] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[18] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.
[19] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[20] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**): 247–252, 2008. doi:10.2478/v10037-008-0029-8.
[21] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[22] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[23] Hideo Wada. *The World of Numbers (in Japanese).* Iwanami Shoten, 1984.

[24] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[25] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received June 4, 2014