FORMALIZED MATHEMATICS
Vol. 16, No. 1, Pages 23–28, 2008
DOI: 10.2478/v10037-008-0004-4

Gauss Lemma and Law of Quadratic Reciprocity

Li Yan
Qingdao University of Science
and Technology
China

Xiquan Liang
Qingdao University of Science
and Technology
China

Junjie Zhao
Qingdao University of Science
and Technology
China

Summary. In this paper, we defined the quadratic residue and proved its fundamental properties on the base of some useful theorems. Then we defined the Legendre symbol and proved its useful theorems [14], [12]. Finally, Gauss Lemma and Law of Quadratic Reciprocity are proven.

MML identifier: `INT_5`, version: `7.8.05 4.89.993`

The papers [20], [10], [9], [11], [4], [1], [2], [17], [8], [19], [7], [16], [13], [21], [22], [5], [18], [3], [15], [6], and [23] provide the terminology and notation for this paper.

For simplicity, we adopt the following convention: i, i_1, i_2, i_3, j, a, b, x denote integers, d, e, n denote natural numbers, f, f' denote finite sequences of elements of $\mathbb{Z}$, g, g_1, g_2 denote finite sequences of elements of $\mathbb{R}$, and p denotes a prime number.

We now state two propositions:

(1) If $i_1 \mid i_2$ and $i_1 \mid i_3$, then $i_1 \mid i_2 - i_3$.

(2) If $i \mid a$ and $i \mid a - b$, then $i \mid b$.

Let us consider f. The functor $\mathcal{P}_{\mathbb{Z}}(f)$ yields a function from $\mathbb{Z}$ into $\mathbb{Z}$ and is defined by the condition (Def. 1).

ISSN 1426–2630(p), 1898-9934(e)

(Def. 1) Let x be an element of $\mathbb{Z}$. Then there exists a finite sequence f' of elements of $\mathbb{Z}$ such that $\operatorname{len} f' = \operatorname{len} f$ and for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = f(d) \cdot x^{d -' 1}$ and $(\mathcal{P}_{\mathbb{Z}}(f))(x) = \sum f'$.

Let f be a finite sequence of elements of $\mathbb{Z}$ and let x be an integer. Observe that $(\mathcal{P}_{\mathbb{Z}}(f))(x)$ is integer.

We now state two propositions:

(3) If $\operatorname{len} f = 1$, then $\mathcal{P}_{\mathbb{Z}}(f) = \mathbb{Z} \longmapsto f(1)$.

(4) If $\operatorname{len} f = 1$, then for every element x of $\mathbb{Z}$ holds $(\mathcal{P}_{\mathbb{Z}}(f))(x) = f(1)$.

In the sequel f' denotes a finite sequence of elements of $\mathbb{R}$.

Next we state three propositions:

(5) Let given g, g_1, g_2. Suppose $\operatorname{len} g = n+1$ and $\operatorname{len} g_1 = \operatorname{len} g$ and $\operatorname{len} g_2 = \operatorname{len} g$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) = g_1(d) - g_2(d)$. Then there exists f' such that $\operatorname{len} f' = \operatorname{len} g - 1$ and for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = g_1(d) - g_2(d+1)$ and $\sum g = ((\sum f') + g_1(n+1)) - g_2(1)$.

(6) Suppose $\operatorname{len} f = n + 2$. Let a be an integer. Then there exists a finite sequence f' of elements of $\mathbb{Z}$ and there exists an integer r such that $\operatorname{len} f' = n+1$ and for every element x of $\mathbb{Z}$ holds $(\mathcal{P}_{\mathbb{Z}}(f))(x) = (x-a) \cdot (\mathcal{P}_{\mathbb{Z}}(f'))(x) + r$ and $f(n+2) = f'(n+1)$.

(7) If $p \mid i \cdot j$, then $p \mid i$ or $p \mid j$.

In the sequel f', g are finite sequences of elements of $\mathbb{Z}$.

The following proposition is true

(8) Let given f. Suppose $\operatorname{len} f = n+1$ and $p > 2$ and $p \nmid f(n+1)$. Let given f'. Suppose for every d such that $d \in \operatorname{dom} f'$ holds $(\mathcal{P}_{\mathbb{Z}}(f))(f'(d)) \bmod p = 0$ and for all d, e such that $d, e \in \operatorname{dom} f'$ and $d \neq e$ holds $f'(d) \not\equiv f'(e) \pmod{p}$. Then $\operatorname{len} f' \leq n$.

Let a be an integer and let m be a natural number. We say that a is quadratic residue mod m if and only if:

(Def. 2) There exists an integer x such that $(x^{\mathbf{2}} - a) \bmod m = 0$.

In the sequel b, m denote natural numbers.

We now state four propositions:

(9) If $a \gcd m = 1$, then $a^{\mathbf{2}}$ is quadratic residue mod m.

(10) 1 is quadratic residue mod 2.

(11) If $i \gcd m = 1$ and i is quadratic residue mod m and $i \equiv j \pmod{m}$, then j is quadratic residue mod m.

(12) If $i \mid j$, then $i \gcd j = |i|$.

Let k be an integer and let a be a natural number. One can verify that k^a is integer.

One can prove the following propositions:

(13) For all integers i, j, m such that $i \bmod m = j \bmod m$ holds $i^n \bmod m = j^n \bmod m$.

(14) If $a \gcd p = 1$ and $(x^{\mathbf{2}} - a) \bmod p = 0$, then x and p are relative prime.

(15) Suppose $p > 2$ and $a \gcd p = 1$ and a is quadratic residue mod p. Then there exist integers x, y such that $(x^{\mathbf{2}} - a) \bmod p = 0$ and $(y^{\mathbf{2}} - a) \bmod p = 0$ and $x \not\equiv y \pmod{p}$.

Let f be a finite sequence of elements of $\mathbb{N}$ and let us consider d. One can check that $f(d)$ is natural.

The following propositions are true:

(16) Suppose $p > 2$. Then there exists a finite sequence f of elements of $\mathbb{N}$ such that

(i) $\operatorname{len} f = (p -' 1) \div 2$,

(ii) for every d such that $d \in \operatorname{dom} f$ holds $\gcd(f(d), p) = 1$,

(iii) for every d such that $d \in \operatorname{dom} f$ holds $f(d)$ is quadratic residue mod p, and

(iv) for all d, e such that $d, e \in \operatorname{dom} f$ and $d \neq e$ holds $f(d) \not\equiv f(e) \pmod{p}$.

(17) If $p > 2$ and $a \gcd p = 1$ and a is quadratic residue mod p, then $a^{(p-'1) \div 2} \bmod p = 1$.

(18) If $p > 2$ and $b \gcd p = 1$ and b is not quadratic residue mod p, then $b^{(p-'1) \div 2} \bmod p = p - 1$.

(19) If $p > 2$ and $a \gcd p = 1$ and a is not quadratic residue mod p, then $a^{(p-'1) \div 2} \bmod p = p - 1$.

(20) If $p > 2$ and $a \gcd p = 1$ and a is quadratic residue mod p, then $(a^{(p-'1) \div 2} - 1) \bmod p = 0$.

(21) If $p > 2$ and $a \gcd p = 1$ and a is not quadratic residue mod p, then $(a^{(p-'1) \div 2} + 1) \bmod p = 0$.

In the sequel b is an integer.

We now state three propositions:

(22) Suppose $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$ and a is quadratic residue mod p and b is quadratic residue mod p. Then $a \cdot b$ is quadratic residue mod p.

(23) Suppose $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$ and a is quadratic residue mod p and b is not quadratic residue mod p. Then $a \cdot b$ is not quadratic residue mod p.

(24) Suppose $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$ and a is not quadratic residue mod p and b is not quadratic residue mod p. Then $a \cdot b$ is quadratic residue mod p.

Let a be an integer and let p be a prime number. The functor $\left(\frac{a}{p}\right)$ yielding an integer is defined by:

(Def. 3) $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is quadratic residue mod } p, \\ -1, & \text{otherwise.} \end{cases}$

One can prove the following propositions:

(25) $\left(\frac{a}{p}\right) = 1$ or $\left(\frac{a}{p}\right) = -1$.

(26) If $a \gcd p = 1$, then $\left(\frac{a^{\mathbf{2}}}{p}\right) = 1$.

(27) $\left(\frac{1}{p}\right) = 1$.

(28) If $p > 2$ and $a \gcd p = 1$, then $\left(\frac{a}{p}\right) \equiv a^{(p-'1)\div 2} \pmod{p}$.

(29) If $p > 2$ and $a \gcd p = 1$ and $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(30) If $p > 2$ and $a \gcd p = 1$ and $b \gcd p = 1$, then $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

(31) If for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = 1$ or $f'(d) = -1$, then $\prod f' = 1$ or $\prod f' = -1$.

In the sequel m denotes an integer.

One can prove the following propositions:

(32) For all g, f' such that $\operatorname{len} g = \operatorname{len} f'$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) \equiv f'(d) \pmod{m}$ holds $\prod g \equiv \prod f' \pmod{m}$.

(33) For all g, f' such that $\operatorname{len} g = \operatorname{len} f'$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) \equiv -f'(d) \pmod{m}$ holds $\prod g \equiv (-1)^{\operatorname{len} g} \cdot \prod f' \pmod{m}$.

In the sequel f denotes a finite sequence of elements of $\mathbb{N}$.

Next we state several propositions:

(34) Suppose $p > 2$ and for every d such that $d \in \operatorname{dom} f$ holds $\gcd(f(d), p) = 1$. Then there exists a finite sequence f' of elements of $\mathbb{Z}$ such that $\operatorname{len} f' = \operatorname{len} f$ and for every d such that $d \in \operatorname{dom} f'$ holds $f'(d) = \left(\frac{f(d)}{p}\right)$ and $\left(\frac{\prod f}{p}\right) = \prod f'$.

(35) If $p > 2$ and $\gcd(d, p) = 1$ and $\gcd(e, p) = 1$, then $\left(\frac{d^{\mathbf{2}} \cdot e}{p}\right) = \left(\frac{e}{p}\right)$.

(36) If $p > 2$, then $\left(\frac{-1}{p}\right) = (-1)^{(p-'1)\div 2}$.

(37) If $p > 2$ and $p \bmod 4 = 1$, then -1 is quadratic residue mod p.

(38) If $p > 2$ and $p \bmod 4 = 3$, then -1 is not quadratic residue mod p.

(39) Let D be a non empty set, g be a finite sequence of elements of D, and i, j be natural numbers. Then g is one-to-one if and only if $\operatorname{Swap}(g, i, j)$ is one-to-one.

(40) Let g be a finite sequence of elements of $\mathbb{N}$. Suppose $\operatorname{len} g = n$ and for every d such that $d \in \operatorname{dom} g$ holds $g(d) > 0$ and $g(d) \leq n$ and g is one-to-one. Then $\operatorname{rng} g = \operatorname{Seg} n$.

In the sequel a, m are natural numbers.

Next we state several propositions:

(41) Let g be a finite sequence of elements of $\mathbb{N}$. Suppose $p > 2$ and $\gcd(a, p) = 1$ and $g = a \cdot \mathrm{idseq}((p -' 1) \div 2)$ and $m = \overline{\overline{\{k \in \mathbb{N}\colon k \in \mathrm{rng}(g \bmod p) \wedge k > \frac{p}{2}\}}}$. Then $\left(\frac{a}{p}\right) = (-1)^m$.

(42) If $p > 2$, then $\left(\frac{2}{p}\right) = (-1)^{(p^2 -' 1) \div 8}$.

(43) If $p > 2$ and if $p \bmod 8 = 1$ or $p \bmod 8 = 7$, then 2 is quadratic residue mod p.

(44) If $p > 2$ and if $p \bmod 8 = 3$ or $p \bmod 8 = 5$, then 2 is not quadratic residue mod p.

(45) For all natural numbers a, b such that $a \bmod 2 = b \bmod 2$ holds $(-1)^a = (-1)^b$.

In the sequel g, g, h, k denote finite sequences of elements of $\mathbb{R}$.

Next we state two propositions:

(46) If $\mathrm{len}\, g = \mathrm{len}\, h$ and $\mathrm{len}\, g = \mathrm{len}\, k$, then $g \frown g - h \frown k = (g - h) \frown (g - k)$.

(47) For every finite sequence g of elements of $\mathbb{R}$ and for every real number m holds $\sum(\mathrm{len}\, g \mapsto m - g) = \mathrm{len}\, g \cdot m - \sum g$.

In the sequel X denotes a finite set and F denotes a finite sequence of elements of 2^X.

Let us consider X, F. Then $\overline{\overline{F}}$ is a cardinal yielding finite sequence of elements of $\mathbb{N}$.

The following proposition is true

(48) Let g be a finite sequence of elements of 2^X. Suppose $\mathrm{len}\, g = n$ and for all d, e such that $d, e \in \mathrm{dom}\, g$ and $d \neq e$ holds $g(d)$ misses $g(e)$. Then $\overline{\overline{\bigcup \mathrm{rng}\, g}} = \sum \overline{\overline{g}}$.

In the sequel q is a prime number.

The following three propositions are true:

(49) If $p > 2$ and $q > 2$ and $p \neq q$, then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{((p -' 1) \div 2) \cdot ((q -' 1) \div 2)}$.

(50) If $p > 2$ and $q > 2$ and $p \neq q$ and $p \bmod 4 = 3$ and $q \bmod 4 = 3$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(51) If $p > 2$ and $q > 2$ and $p \neq q$ and $p \bmod 4 = 1$ or $q \bmod 4 = 1$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[7] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 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. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] Zhang Dexin. *Integer Theory.* Science Publication, China, 1965.
[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] Hua Loo Keng. *Introduction to Number Theory.* Beijing Science Publication, China, 1957.
[15] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[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 relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[18] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[19] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[23] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Set sequences and monotone class. *Formalized Mathematics*, 13(**4**):435–441, 2005.

Received October 9, 2007