FORMALIZED MATHEMATICS
2007, Vol. **15**, No. **4**, Pages 181–187
DOI: 10.2478/v10037-007-0022-7

Linear Congruence Relation and Complete Residue Systems

Xiquan Liang
Qingdao University of Science and Technology
China

Li Yan
Qingdao University of Science and Technology
China

Junjie Zhao
Qingdao University of Science and Technology
China

Summary. In this paper, we defined the congruence relation and proved its fundamental properties on the base of some useful theorems. Then we proved the existence of solution and the number of incongruent solution to a linear congruence and the linear congruent equation class, in particular, we proved the Chinese Remainder Theorem. Finally, we defined the complete residue system and proved its fundamental properties.

MML identifier: `INT_4`, version: `7.8.05 4.87.985`

The papers [21], [25], [2], [20], [1], [22], [3], [24], [14], [17], [16], [23], [26], [7], [5], [27], [9], [18], [13], [19], [28], [8], [10], [4], [15], [11], [6], and [12] provide the terminology and notation for this paper.

For simplicity, we adopt the following convention: a, b, m, x, y, i_1, i_2, i_3, i denote integers, k, p, q, n denote natural numbers, c, c_1, c_2 denote elements of $\mathbb{N}$, and X denotes a set.

Next we state the proposition

(1) For every real-membered set X and for every real number a holds $X \approx a \oplus X$.

Let X be a finite real-membered set and let a be a real number. One can verify that $a \oplus X$ is finite.

One can prove the following propositions:

ISSN 1426–2630

(2) For every finite real-membered set X and for every real number a holds $\operatorname{card} X = \operatorname{card}(a \oplus X)$.

(3) For every real-membered set X and for every real number a such that $a \neq 0$ holds $X \approx a \circ X$.

(4) Let X be a real-membered set and a be a real number. Then

(i) if $a = 0$ and X is non empty, then $a \circ X = \{0\}$, and

(ii) if $a \circ X = \{0\}$, then $a = 0$ or $X = \{0\}$.

Let X be a finite real-membered set and let a be a real number. One can verify that $a \circ X$ is finite.

The following propositions are true:

(5) For every finite real-membered set X and for every real number a such that $a \neq 0$ holds $\operatorname{card} X = \operatorname{card}(a \circ X)$.

(6) If $i \mid i_1$ and $i_1 \neq 0$, then $|i| \leq |i_1|$.

(7) For every i_3 such that $i_3 \neq 0$ holds $i_1 \mid i_2$ iff $i_1 \cdot i_3 \mid i_2 \cdot i_3$.

(8) For all natural numbers a, b, m and for every element n of $\mathbb{N}$ such that $a \bmod m = b \bmod m$ holds $a^n \bmod m = b^n \bmod m$.

(9) If $i_1 \cdot i \equiv i_2 \cdot i (\operatorname{mod} i_3)$ and i and i_3 are relative prime, then $i_1 \equiv i_2 (\operatorname{mod} i_3)$.

(10) If $i_1 \equiv i_2 (\operatorname{mod} i_3)$, then $i_1 \cdot k \equiv i_2 \cdot k (\operatorname{mod} i_3 \cdot k)$.

(11) If $i_1 \equiv i_2 (\operatorname{mod} i)$, then $i_1 \cdot i_3 \equiv i_2 \cdot i_3 (\operatorname{mod} i)$.

(12) For every integer i holds $0 = 0 \bmod i$.

(13) For every b such that $b > 0$ and for every a there exist integers q, r such that $a = b \cdot q + r$ and $r \geq 0$ and $r < b$.

(14) If $i_1 \equiv i_2 (\operatorname{mod} i_3)$, then $i_1 \gcd i_3 = i_2 \gcd i_3$.

(15) If a and m are relative prime, then there exists an integer x such that $(a \cdot x - b) \bmod m = 0$.

(16) If $m > 0$ and a and m are relative prime, then there exists a natural number n such that $(a \cdot n - b) \bmod m = 0$.

(17) If $m \neq 0$ and $a \gcd m \nmid b$, then it is not true that there exists an integer x such that $(a \cdot x - b) \bmod m = 0$.

(18) If $m \neq 0$ and $a \gcd m \mid b$, then there exists an integer x such that $(a \cdot x - b) \bmod m = 0$.

Let x be an integer. Observe that $x^{\mathbf{2}}$ is natural.

We now state several propositions:

(19) If $n > 0$ and $p > 0$, then $p \cdot q \bmod p^n = p \cdot (q \bmod p^{n-'1})$.

(20) $p \cdot q \bmod p \cdot n = p \cdot (q \bmod n)$.

(21) If $n > 0$ and p is prime and p and q are relative prime, then $p \nmid q \bmod p^n$.

(22) For all natural numbers p, q, n such that $n > 0$ holds $(p - q) \bmod n = 0$ iff $p \bmod n = q \bmod n$.

(23) For all natural numbers a, b, m such that $m > 0$ holds $a \bmod m = b \bmod m$ iff $m \mid a - b$.

(24) If $n > 0$ and p is prime and p and q are relative prime, then it is not true that there exists an integer x such that $(p \cdot x^{\mathbf{2}} - q) \bmod p^n = 0$.

(25) If $n > 0$ and p is prime and p and q are relative prime, then it is not true that there exists an integer x such that $(p \cdot x - q) \bmod p^n = 0$.

Let m be an integer. The functor $\operatorname{Cong} m$ yielding a binary relation on $\mathbb{Z}$ is defined as follows:

(Def. 1) $\langle x, y\rangle \in \operatorname{Cong} m$ iff $x \equiv y (\bmod m)$.

Let m be an integer. One can check that $\operatorname{Cong} m$ is total.

Let m be an integer. One can check that $\operatorname{Cong} m$ is reflexive, symmetric, and transitive.

Next we state four propositions:

(26) Suppose $m \neq 0$ and $(a \cdot x - b) \bmod m = 0$. Let y be an integer. Then

(i) if a and m are relative prime and $(a \cdot y - b) \bmod m = 0$, then $y \in [x]_{\operatorname{Cong} m}$, and

(ii) if $y \in [x]_{\operatorname{Cong} m}$, then $(a \cdot y - b) \bmod m = 0$.

(27) Let a, b, m, x be integers. Suppose $m \neq 0$ and a and m are relative prime and $(a \cdot x - b) \bmod m = 0$. Then there exists an integer s such that $\langle x, b \cdot s\rangle \in \operatorname{Cong} m$.

(28) Let a, m be elements of $\mathbb{N}$. Suppose $a \neq 0$ and $m > 1$ and a and m are relative prime. Let b, x be integers. If $(a \cdot x - b) \bmod m = 0$, then $\langle x, b \cdot a^{\operatorname{Euler} m - 1}\rangle \in \operatorname{Cong} m$.

(29) Suppose $m \neq 0$ and $a \gcd m \mid b$. Then there exists a finite sequence f_1 of elements of $\mathbb{Z}$ such that $\operatorname{len} f_1 = a \gcd m$ and for every c such that $c \in \operatorname{dom} f_1$ holds $(a \cdot f_1(c) - b) \bmod m = 0$ and for all c_1, c_2 such that $c_1 \in \operatorname{dom} f_1$ and $c_2 \in \operatorname{dom} f_1$ and $c_1 \neq c_2$ holds $f_1(c_1) \not\equiv f_1(c_2) (\bmod m)$.

We use the following convention: f_1, f_2 denote finite sequences of elements of $\mathbb{N}$ and a, b, c, d, n denote elements of $\mathbb{N}$.

Next we state a number of propositions:

(30) For all b, n such that $b \in \operatorname{dom} f_1$ and $\operatorname{len} f_1 = n + 1$ holds $(f_1 \frown \langle d\rangle)_{\restriction b} = ((f_1)_{\restriction b}) \frown \langle d\rangle$.

(31) Suppose $\operatorname{len} f_1 \geq 2$ and for all b, c such that $b \in \operatorname{dom} f_1$ and $c \in \operatorname{dom} f_1$ and $b \neq c$ holds $\gcd(f_1(b), f_1(c)) = 1$. Let given b. If $b \in \operatorname{dom} f_1$, then $\gcd(\prod((f_1)_{\restriction b}), f_1(b)) = 1$.

(32) For every a such that $a \in \operatorname{dom} f_1$ holds $f_1(a) \mid \prod f_1$.

(33) If $a \in \operatorname{dom} f_1$ and $p \mid f_1(a)$, then $p \mid \prod f_1$.

(34) If $\operatorname{len} f_1 = n + 1$ and $a \geq 1$ and $a \leq n$, then $(f_1)_{\restriction a}(n) = f_1(\operatorname{len} f_1)$.

(35) For all a, b such that $a \in \operatorname{dom} f_1$ and $b \in \operatorname{dom} f_1$ and $a \neq b$ and $\operatorname{len} f_1 \geq 1$ holds $f_1(b) \mid \prod((f_1)_{\restriction a})$.

(36) If for every b such that $b \in \operatorname{dom} f_1$ holds $a \mid f_1(b)$, then $a \mid \sum f_1$.

(37) Suppose $\operatorname{len} f_1 \geq 2$ and for all b, c such that $b \in \operatorname{dom} f_1$ and $c \in \operatorname{dom} f_1$ and $b \neq c$ holds $\gcd(f_1(b), f_1(c)) = 1$ and for every b such that $b \in \operatorname{dom} f_1$ holds $f_1(b) \neq 0$. Let given f_2. Suppose $\operatorname{len} f_2 = \operatorname{len} f_1$. Then there exists an integer x such that for every b such that $b \in \operatorname{dom} f_1$ holds $(x - f_2(b)) \bmod f_1(b) = 0$.

(38) If for all b, c such that $b \in \operatorname{dom} f_1$ and $c \in \operatorname{dom} f_1$ and $b \neq c$ holds $\gcd(f_1(b), f_1(c)) = 1$ and for every b such that $b \in \operatorname{dom} f_1$ holds $f_1(b) \mid a$, then $\prod f_1 \mid a$.

(39) Suppose $\operatorname{len} f_1 \geq 2$ and for all b, c such that $b \in \operatorname{dom} f_1$ and $c \in \operatorname{dom} f_1$ and $b \neq c$ holds $\gcd(f_1(b), f_1(c)) = 1$ and for every b such that $b \in \operatorname{dom} f_1$ holds $f_1(b) > 0$. Let given f_2. Suppose $\operatorname{len} f_2 = \operatorname{len} f_1$ and for every b such that $b \in \operatorname{dom} f_1$ holds $(x - f_2(b)) \bmod f_1(b) = 0$ and $(y - f_2(b)) \bmod f_1(b) = 0$. Then $x \equiv y \pmod{\prod f_1}$.

We follow the rules: m_1, m_2, m_3, r, s, a, b, c, c_1, c_2, x denote integers and n_1, n_2, n_3 denote natural numbers.

The following propositions are true:

(40) Suppose $m_1 \neq 0$ and $m_2 \neq 0$ and m_1 and m_2 are relative prime. Then there exists an integer r such that for every x such that $(x - c_1) \bmod m_1 = 0$ and $(x - c_2) \bmod m_2 = 0$ holds $x \equiv c_1 + m_1 \cdot r \pmod{m_1 \cdot m_2}$ and $(m_1 \cdot r - (c_2 - c_1)) \bmod m_2 = 0$.

(41) If $m_1 \neq 0$ and $m_2 \neq 0$ and $m_1 \gcd m_2 \nmid c_1 - c_2$, then it is not true that there exists x such that $(x - c_1) \bmod m_1 = 0$ and $(x - c_2) \bmod m_2 = 0$.

(42) Suppose $m_1 \neq 0$ and $m_2 \neq 0$ and $m_1 \gcd m_2 \mid c_2 - c_1$. Then there exists r such that for every x such that $(x - c_1) \bmod m_1 = 0$ and $(x - c_2) \bmod m_2 = 0$ holds $x \equiv c_1 + m_1 \cdot r \pmod{\operatorname{lcm}(m_1, m_2)}$ and $((m_1 \div (m_1 \gcd m_2)) \cdot r - ((c_2 - c_1) \div (m_1 \gcd m_2))) \bmod (m_2 \div (m_1 \gcd m_2)) = 0$.

(43) Suppose $m_1 \neq 0$ and $m_2 \neq 0$ and $a \gcd m_1 \mid c_1$ and $b \gcd m_2 \mid c_2$ and m_1 and m_2 are relative prime. Then there exist integers w, r, s such that

(i) for every x such that $(a \cdot x - c_1) \bmod m_1 = 0$ and $(b \cdot x - c_2) \bmod m_2 = 0$ holds $x \equiv r + (m_1 \div (a \gcd m_1)) \cdot w \pmod{(m_1 \div (a \gcd m_1)) \cdot (m_2 \div (b \gcd m_2))}$,

(ii) $((a \div (a \gcd m_1)) \cdot r - (c_1 \div (a \gcd m_1))) \bmod (m_1 \div (a \gcd m_1)) = 0$,

(iii) $((b \div (b \gcd m_2)) \cdot s - (c_2 \div (b \gcd m_2))) \bmod (m_2 \div (b \gcd m_2)) = 0$, and

(iv) $((m_1 \div (a \gcd m_1)) \cdot w - (s - r)) \bmod (m_2 \div (b \gcd m_2)) = 0$.

(44) Suppose that

(i) $m_1 \neq 0$,

(ii) $m_2 \neq 0$,

(iii) $m_3 \neq 0$,

(iv) m_1 and m_2 are relative prime,

(v) m_1 and m_3 are relative prime, and

(vi) m_2 and m_3 are relative prime.

Then there exist r, s such that for every x if $(x - a) \bmod m_1 = 0$ and $(x - b) \bmod m_2 = 0$ and $(x - c) \bmod m_3 = 0$, then $x \equiv a + m_1 \cdot r + m_1 \cdot m_2 \cdot s (\bmod m_1 \cdot m_2 \cdot m_3)$ and $(m_1 \cdot r - (b - a)) \bmod m_2 = 0$ and $(m_1 \cdot m_2 \cdot s - (c - a - m_1 \cdot r)) \bmod m_3 = 0$.

(45) Suppose $m_1 \neq 0$ and $m_2 \neq 0$ and $m_3 \neq 0$ and $m_1 \gcd m_2 \nmid a - b$ or $m_1 \gcd m_3 \nmid a - c$ or $m_2 \gcd m_3 \nmid b - c$. Then it is not true that there exists x such that $(x - a) \bmod m_1 = 0$ and $(x - b) \bmod m_2 = 0$ and $(x - c) \bmod m_3 = 0$.

(46) For all non zero natural numbers n_1, n_2, n_3 holds $\operatorname{lcm}(\gcd(n_1, n_3), \gcd(n_2, n_3)) = \gcd(\operatorname{lcm}(n_1, n_2), n_3)$.

(47) Let n_1, n_2, n_3 be non zero natural numbers. Suppose $\gcd(n_1, n_2) \mid a - b$ and $\gcd(n_1, n_3) \mid a - c$ and $\gcd(n_2, n_3) \mid b - c$. Then there exist r, s such that for every x if $(x - a) \bmod n_1 = 0$ and $(x - b) \bmod n_2 = 0$ and $(x - c) \bmod n_3 = 0$, then $x \equiv a + n_1 \cdot r + \operatorname{lcm}(n_1, n_2) \cdot s (\bmod \operatorname{lcm}(\operatorname{lcm}(n_1, n_2), n_3))$ and $((n_1 \div \gcd(n_1, n_2)) \cdot r - ((b - a) \div \gcd(n_1, n_2))) \bmod (n_2 \div \gcd(n_1, n_2)) = 0$ and $((\operatorname{lcm}(n_1, n_2) \div \gcd(\operatorname{lcm}(n_1, n_2), n_3)) \cdot s - ((c - (a + n_1 \cdot r)) \div \gcd(\operatorname{lcm}(n_1, n_2), n_3))) \bmod (n_3 \div \gcd(\operatorname{lcm}(n_1, n_2), n_3)) = 0$.

In the sequel f_1 denotes a finite sequence of elements of $\mathbb{N}$ and a, b, m denote elements of $\mathbb{N}$.

Let m be an element of $\mathbb{N}$ and let X be a set. We say that X is a complete residue system modulo m if and only if:

(Def. 2) There exists a finite sequence f_1 of elements of $\mathbb{Z}$ such that $X = \operatorname{rng} f_1$ and $\operatorname{len} f_1 = m$ and for every b such that $b \in \operatorname{dom} f_1$ holds $f_1(b) \in [b -' 1]_{\operatorname{Cong} m}$.

One can prove the following propositions:

(48) $\{a : a < m\}$ is a complete residue system modulo m.

(49) Let X be a finite set. Suppose X is a complete residue system modulo m. Then $\operatorname{card} X = m$ and for all integers x, y such that $x \in X$ and $y \in X$ and $x \neq y$ holds $\langle x, y \rangle \notin \operatorname{Cong} m$.

(50) $\emptyset$ is a complete residue system modulo m iff $m = 0$.

(51) Let X be a finite set. Suppose $\operatorname{card} X = m$. Then there exists a finite sequence f_1 such that $\operatorname{len} f_1 = m$ and for every a such that $a \in \operatorname{dom} f_1$ holds $f_1(a) \in X$ and f_1 is one-to-one.

(52) Let X be a finite subset of $\mathbb{Z}$. Suppose $\operatorname{card} X = m$ and for all integers x, y such that $x \in X$ and $y \in X$ and $x \neq y$ holds $\langle x, y \rangle \notin \operatorname{Cong} m$. Then X is a complete residue system modulo m.

In the sequel a is an integer.

The following two propositions are true:

(53) Let X be a finite subset of $\mathbb{Z}$. Suppose X is a complete residue system modulo m. Then $a \oplus X$ is a complete residue system modulo m.

(54) Let X be a finite subset of $\mathbb{Z}$. Suppose a and m are relative prime and X is a complete residue system modulo m. Then $a \circ X$ is a complete residue system modulo m.

References

[1] Grzegorz Bancerek. Arithmetic of non-negative rational numbers. *To appear in Formalized Mathematics*.
[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.
[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[6] Józef Białas. Some properties of the intervals. *Formalized Mathematics*, 5(**1**):21–26, 1996.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.
[12] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Scalar multiple of Riemann definite integral. *Formalized Mathematics*, 9(**1**):191–196, 2001.
[13] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(**4**):549–551, 1997.
[14] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[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] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[20] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[21] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[22] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[23] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[24] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[25] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[26] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[27] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[28] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received August 28, 2007