Trans. Nat. Acad. Science & Tech. (Phils.)
1988: 10: 45-49

CONGRUENCE IN THE FIELD OF RATIONAL NUMBERS

Severino V. Gervacio
MSU-Iligan Institute of Technology
Tibanga, Iligan City

ABSTRACT

If m, a, b are integers and m>0, we say that a is congruent to b;modulo m, if and only if m is a divisor of a – b. In symbols, this is written as $a \equiv b \pmod{m}$. It is well known, and easy to prove, that this relation is an equivalence relation in the integral domain Z of all integers. Furthermore, this equivalence relation induces extactly m equivalence classes, i.e., it provides an m-partition of Z.

In this paper,we extend the concept of congruence of the field Q of rational numbers, the smallest field containing Z. Let m be a positive integer and let r, $s \in Q$. We can always write r=a/b, s=c/d as fractions in lowest terms. We definer $r \equiv s \pmod{m}$ if and only if m is a divisor of ad-bc. It is clear that the restriction of this relation to Z is the usual congruence relation, and hence it is an extension of the usual concept of congruence. This study shows that this extended concept of congruence is an equivalence relation and that for a given modulus m>0, the corresponding number of equivalence classes is equal to $m\Pi(1+p^{-1})$, where the product ranges over all prime divisors p of m.

Introduction

Consider the set $Q = (\langle a, b\rangle : b \neq 0$ and a, b are relatively prime integers). Each element $\langle a, b\rangle \in Q$ may be associated with the rational number a/b. Conversely, if r is any rational number, then r = a/b for some $\langle a, b\rangle \in Q$. We may then look at Q as the field of real numbers by thinking of $\langle a, b\rangle$ as the rational number a/b.

For convenience, we shall use consistently the following notations:

Z : The set of all integers.
Q : The set of rational numbers.
a|b : Ta divides b, exactly.
(a, b) : The greatest common divisor of a and b.
[a, b] : The least common multiple of a and b.

Let us recall one equivalence relation in Z. For each positive integer m, we say that *a is congruent to b modulo m,* if and only if m|(a-b). In symbols, we write $a \equiv b \pmod{m}$ if a is congruent to b modulo m, and $a \not\equiv b \pmod{m}$, otherwise. The following definition extends this concept to the set Q.

Definition 1. Let m be a positive integer. In Q, we say that $\langle a, b\rangle$ *is congruent to* $\langle c, d\rangle$ *modulo m* if and onoy if $m|(adbc)$, i.e., $ad \equiv bc \pmod m$.

In symbols, we shall write $\langle a, b\rangle \equiv \langle c, d\rangle \pmod m$ if $\langle a, b\rangle$ is congruent to $\langle b, c\rangle$ modulo m. We shall also use the symbol $\not\equiv$ to denote non-congruence. This concept of congruence in Q will be of no general importance if it is not an equivalence relation. Our first task is to show that it is indeed an equivalence relation in Q. We omit the proof of the following lemmas which we shall use in proving our assertion.

Lemma 1. **If a, b** $\in Z$ are not both zero, then $(na, nb) = |n|(a, b)$ for all non-zero $n \in Z$.

Lemma 2. If $a, b \in Z$ are not both zero, then $[a, b] = |ab|/(a, b)$.

Lemma 3. If $a, b \in Z$, then $(a, b) = (a+nb, b)$ for all $n \in Z$.

Lemma 4. If $ax \equiv ay \pmod m$, then $x \equiv y \pmod{m/(a, m)}$.

Lemma 5. If $a \equiv b \pmod m$ and $a \equiv b \pmod n$, then $a \equiv b \pmod{[m, n]}$.

Lemma 6. If $a \equiv b \pmod m$, then $(am, m) = (b, m)$.

Lemma 7. The congruence $ax \equiv b \pmod m$ has a solution if and only if $(a, m) = 1$.

It is useful to note that the greatest common divisor of three integers, a, b, c, not all zero, is $(a, b, c) = ((a, b), c) = (a, (b, c))$.

Theorem 1. The relation $\langle a, b\rangle \equiv \langle c, d\rangle \pmod m$ is an equivalence relation in Q.

Proof: The reflexive and symmetric properties of the relation are trivial. To prove the transitivity, let $\langle a, b\rangle \equiv \langle c, d\rangle \pmod m$ and $\langle c, d\rangle \equiv \langle e, f\rangle \pmod m$. Then by definition.

$$ad \equiv bc \pmod m \tag{1}$$
$$cf \equiv de \pmod m \tag{2}$$

Multiply (1) by a, (2) by b, and add the results to get $adf \equiv bde \pmod m$. By Lemma 4, this implies that $af \equiv be \pmod{m/(d, m)}$. Similarly, we can get from (1) and (2) the result that $af \equiv be \pmod{m/(C, m)}$. Hence, $af \equiv be \pmod{[m/(d, m), m/(c, m)]}$ in view of Lemma 5. Using Lemmas 1 and 2, it is not difficult to verify that $[m/(d, m), m/(c, m)] = m$. Therefore, $\langle a, b\rangle \equiv \langle e, f\rangle \pmod m$.

An upper Bound for the Number of Equivalence Classes

For a fixed positive integer m, the congruence relation in Q partitions Q into mutually disjoint equivalence classes. The equivalence class containing $\langle a, b\rangle$, denoted by $cl\langle a, b\rangle$ is the set of all $\langle x, y\rangle \in Q$ such that $\langle x, y\rangle \equiv \langle a, b\rangle \pmod m$. We shall show that there are only a finite number of equivalence classes induced by the relation congruence modulo m.

Let m be a positive integer and $\langle a, b\rangle \in Q$. Let us divide each of a, b by m and express the results of division in the forms $a = ma' + u$, $b = mb' + v$, where

$0 \leq u, v < m$. Then $a \equiv u \pmod m$ and $b \equiv v \pmod m$ and we immediately get $av \equiv bu \pmod m$. Let $g = (u, v)$ and $U' = u/g$, $v' = v/g$. Then $\langle u', v' \rangle \in Q$ and by Lemma 4, $av' \equiv bu' \pmod{m/(g, m)}$. Now, $(g, m) = (u, v, m) = (u, (v, m)) = (u, (b-mb', m)) = (u, (b, m)) = (u, (m, b)) = ((u, m), v) = ((a-ma', m), b) = ((a, m), b) = (a, m, b) = 1$. Here, we used Lemma 3. Therefore, $\langle a, b \rangle \equiv \langle u', v' \rangle \pmod m$. We have thus shown that for each $\langle a, b \rangle \in Q$, there exists $\langle u', v' \rangle \in Q$ such that $0 \leq u', v' < m$ and $\langle a, b \rangle \equiv \langle u', v' \rangle \pmod m$. The next theorem is a direct consequence of this result.

Theorem 2. The number of equivalence classes induced by the relation congruence modulo m is finite and not greater than m^2.

The Exact Number of Equivalence Classes

We shall denote by $\theta(m)$ the number of equivalence classes of the relation congruence modulo m. Theorem 2 states that $\theta(m) \leq m^2$. Here, we shall derive an exact expression for $\theta(m)$. We shall prove some lemmas first.

Lemma 8. If $(a, b, c) = 1$ and $c \neq 0$, then there exists an integer n such that $(a+bn, c) = 1$.

Proof: Take $n = c/(a, c)$. Then it is not so difficult to check that $(a+bn, c) = 1$.

Lemma 9. Let m be a positive integer and $\langle a, b \rangle \in Q$. Then there exists $\langle u, v \rangle \in Q$ such that $\langle a, b \rangle \equiv \langle u, v \rangle \pmod m$ and v is a positive divisor of m.

Proof: Set $v = (b, m)$. Obviously, v is a positive divisor of m. Let $b' = b/v$ and $m' = m/v$. By Lemma 7, the congruence $b' x \equiv a \pmod m$ has a solution since $(b', m') = 1$. If u' is any solution, then $u = u' + nm'$ is also a solution for any integer n. Let $g = (u', m', v)$. From the congruence $b' u' \equiv a \pmod{m'}$ and Lemma 6 it follows that $(b' u', m') = (a, m')$. Since $g|(u', m')$, then $g|(a, m')$ and consequently, $g|a$. But $g|v$ and $v = (b, m)$. Therefore, $g|b$ also. Hence $g = 1$ since $(a, b) = 1$. By Lemma 7, there exists an integer n such that $(u' + nm', v) = 1$. Take $u = u' + nm'$. Then $\langle u, v \rangle \in Q$ and $b' u \equiv a \pmod{m'}$. If we multiply this congruence by v, we get $bu \equiv av \pmod m$, and hence $\langle a, b \rangle \equiv \langle u, v \rangle \pmod m$.

The next lemma is easy and its proof is omitted.

Lemma 10. If $\langle a_1, d_1 \rangle, \langle a_2, d_2 \rangle \in Q$ and d_1, d_2 are positive divisors of m such that $\langle a_1, d_1 \rangle \equiv \langle a_2, d_2 \rangle \pmod m$, thn $d_1 = d_2$.

In view of Lemma 10, if $d_1, d_2, \ldots, d_t$ are all the positive divisors of m and if n_i denotes the maximum number of elements $\langle a, d_i \rangle \in Q$ which are mutually incongruent modulo m, then $\theta(m) = n_1 + n_2 + \ldots + n_t$. This is one way of computing for $\theta(m)$. Another method is suggested by the next theorem.

Theorem 3. If $m, n \in Z$ are positive and $(m, n) = 1$, then $\theta(mn) = \theta(m)\theta(n)$, i.e., θ is a multiplicative function.

Proof: Let us first show that $\theta(mn) \geq \theta(m)\theta(n)$. Let $C_m \leq Q$ such that the elements of C_m are mutually incongruent modulo m and every element of Q is congruent to some element of C_m modulo m. Then C_m has exactly $\theta(m)$ elements. In

Proof: If = 1, the product Π is empty and hence equal to 1. If $m > 1$, then $\theta(m) = \Pi\theta(p^e)$ where $m = \Pi p^e$. By the theorem, $\theta(p^e) = p^e + p^{e-1} = p^e(1+p^{-1})$. Therefore, $\theta(m) = \Pi[p^e(1+p^{-1})] = \Pi p^e \Pi(1+p^{-1}) = m\Pi(1+p^{-1})$.

It should be noted that the construction of the set of all equivalence classes of the congruence relation in Q has been given implicitly in the proof of the last theorem. Note also the striking similarity between the formula for $\theta(m)$ and that of Euler's totient $\theta(m) = m\Pi(1-p^{-1})$.

Literature Cited

Dickson, L.E., *History of the Theory of Numbers.* Chelsea Publishing Co., New York, vol. 1, 1952.

Niven, I. and Zuckerman, H., *An Introduction to the Theory of Numbers.* John Wiley and Sons, Inc., 1965.

Gervacio, S.V. *An Extension of Congruence.* Master's Thesis, U.P., 1971.