On the Congruence of Numbers in General

Art. 1

(Congruences, moduli, residues and nonresidues)

If the difference between numbers b and c is a multiple of a number a, then b and c are said to be congruent modulo a, otherwise they are incongruent; the number a is called the modulus of the congruence. In the former case, each of the numbers b and c is called a residue of the other, and in the latter case, a non-residue.

These notions apply to all integers, both positive and negative[1] but they are not to be extended to fractions. For example, -9 and 16 are congruent modulo 5; -7 and 15 are residues of each other modulo 11, but not modulo 3. Moreover, since zero is divisible by all numbers, every number must be regarded as congruent to itself according to any modulus.

Art. 2

All of the numbers congruent to a modulo m are given by the formula $a+km$ where k denotes an indeterminate integer. The propositions which we shall give hereafter can be derived from this with no difficulty; but indeed their truth is equally easy to demonstrate directly.

We will denote congruences with the sign $\equiv$, and if necessary the modulus will be in parentheses, e.g. [2]

$$\begin{aligned} -16 &\equiv 9 \text{ (mod. 5)} \\ -7 &\equiv 15 \text{ (mod. 11)}. \end{aligned}$$

Art. 3

Theorem 1. *Given m consecutive whole numbers*

$$a, a+1, a+2, \ldots, a+m-1$$

and another A, one and only one of them will be congruent to A modulo m.

If indeed $\frac{a-A}{m}$ is an integer, we have $a \equiv A$. If it is a fraction, let the next largest integer (or the next smallest, if it is negative and sign is not taken into account) be k. Then $A + km$ will be between a and $a + m$, and thus it will be the number sought. It is clear that all of the quotients $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$, etc. lie between $k-1$ and $k+1$, therefore no more than one of them can be a whole number.

Art. 4

(Minimal Residues)

It follows that each number has a residue in the series $0, 1, 2, \ldots, m-1$, and also in the series $0, -1, -2, \ldots, 1-m$. We will call it the minimum residue, and it is clear that unless 0 is the remainder then two will be given, one positive and the other negative. If they are unequal in size then one will be $< \frac{m}{2}$, otherwise both will be $= \frac{m}{2}$, the sign not being considered. From this it is clear that any residue not exceeding half of the modulus can be called an absolute minimum.

For example, -13 modulo 5 has minimum positive residue 2, which is the absolute minimum, and also -3, which is the minimum negative residue. 5 modulo 7 is its own minimum positive residue, -2 is the negative minimum residue, which is also the absolute minimum.

[1] Of course, the modulus is always absolute, i.e. it is to be taken without regard to sign

[2] We have adopted this sign due to the strong analogy between equality and congruence. For the same reason, the illustrious Legendre used the sign of equality for congruity. We hesitated to imitate that convention, lest any ambiguity should arise.

Art. 5

(Elementary propositions about congruences)

Having established these notions, let us collect those properties of congruent numbers which present themselves most immediately.

Proposition 1. *Numbers which are congruent according to a composite modulus, are also congruent according to any divisor of the modulus.*

Proposition 2. *If several numbers are each congruent to the same number according to the same modulus, then they will also be congruent to each other (according to that modulus).*

Proposition 3. *Congruent numbers have the same minimum residues, incongruent ones have different ones.*

Art. 6

Given any number of numbers A, B, C, etc. and as many others a, b, c, etc., and any modulus whatsoever,

Proposition 4. *If* $A \equiv a, B \equiv b$ etc. *then* $A + B + C +$ etc. $\equiv a + b + c +$ etc.

Proposition 5. *If* $A \equiv a, B \equiv b,$ *then* $A - B \equiv a - b$.

Art. 7

Proposition 6. *If* $A \equiv a,$ *then* $kA \equiv ka$.

If k is a positive number, this is just a special case of the preceding proposition, in which $A = B = C$ etc and $a = b = c$ etc. If k is negative, then $-k$ is positive, and $-kA \equiv -ka$ and therefore $kA \equiv ka$.

Proposition 7. *If* $A \equiv a, B \equiv b,$ *then* $AB \equiv ab,$ *since* $AB \equiv Ab \equiv ab$.

Art. 8

Given any number of numbers A, B, C, etc. and as many others a, b, c, etc., which are congruent to each other, $A \equiv a$, $B \equiv b$, etc., the products of both will be congruent, ABC etc.$\equiv abc$ etc.

From the preceding article, $AB \equiv ab$, and for the same reason $ABC \equiv abc$; and any number of factors can be treated in the same way.

If all the numbers A, B, C are assumed to be equal, then so are the corresponding a, b, c, and we obtain the following theorem: *If* $A \equiv a$ *and* k *is a positive integer, then* $A^k \equiv a^k$.

Art. 9

Proposition 8. *Let* X *be a function of a variable* x*, of the form*

$$Ax^a + Bx^b + Cx^c + \cdots$$

where A, B, C *etc. are arbitrary integers and* a, b, c *are non-negative integers. Then if the indeterminate* x *values are congruent according to any modulus, the resulting values of the function* X *will also be congruent.*

Proof. Let f, g be congruent values of x. Then from the preceding article $f^a \equiv g^a$ and $Af^a \equiv Ag^a$, and in the same way $Bf^b \equiv Bg^b$ etc. Thus

$$Af^a + Bf^b + Cf^c + etc. \equiv Ag^a + Bg^b + Cg^c + etc.$$

□

Moreover, it is easy to understand how this theorem can be extended to functions of several variables.

Art. 10

If, therefore, all consecutive integers are substituted for x, and the values of the function X are reduced to their minimum residues, these will constitute a series in which, after an interval of m (where m denotes the modulus), the same terms recur again; the series will be formed from the same terms repeated infinitely with period m. **(??)**

For example, let $X = x^3 - 8x + 6$ and $m = 5$. Then for $x = 0, 1, 2, 3$ etc., the values of X have minimum positive residues $1, 4, 3, 4, 3, 1, 4$ etc., where the first $1, 4, 3, 4, 3$ are infinitely repeated; and if the series is continued backwards, i.e. x is given negative values, then the same period is produced with an inverted order of terms. From this it is clear that terms other than those which constitute the period cannot occur anywhere in the series.

Art. 11

In this example, therefore, X can become neither $\equiv 0$ nor $\equiv 2$, much less $= 0$ or $= 2$. Hence it follows that the equations $x^3 - 8x + 6 = 0$ and $x^3 - 8x + 4 = 0$ cannot be solved by integers, and therefore, as is well known, they cannot be solved by rational numbers. It is generally clear that the equation $X = 0$, when X is a function of the variable x, of the form

$$x^n + Ax^{n-1} + Bx^{n-2} + \text{etc.} + N$$

with A, B, C etc. integers and n a positive integer (to which form it is clear that any algebraic equation can be reduced) can have no rational root, if there is a modulus for which the congruence $X \equiv 0$ is impossible. This criterion, which spontaneously presented itself to us, will be discussed in greater detail in Section VIII. Certainly from this example one obtains a sense of the utility of these investigations.

Art. 12

(Some applications)

Several of the theorems presented in this chapter generalize those usually taught in arithmetic, e.g. rules for exploring the divisibility of a given number by 9, 11, or other numbers. According to the modulus 9, all powers of 10 are congruent to unity: therefore, if the proposed number has the form $a + 10b + 100c+$ etc., then its minimum residue modulo 9 will be the same as $a + b + c+$ etc. From this it is clear that if the decimal digits of any number are added with regard to the place they occupy, the sum will give the same minimum residue as the original number, so that the latter can be divided by 9 if it the former is divisible by 9, and vice versa. The same also applies to divisibility by 3. According to the modulus 11, $100 \equiv 1$, so in general $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, and a number of the form $a + 10b + 100c+$ etc. will have the same minimum residue as $a - b + c$ etc.; from which the well-known rule is directly derived. From the same principle all similar precepts are easily deduced.

Another application of the foregoing is the system of rules which are generally recommended for the verification of arithmetical operations. If a from given numbers others are to be found by addition, subtraction, multiplication or exponentiation, then instead of the given numbers their minimal residues are substituted according to the arbitrary modulus (I mean 9 or 11, since in our decadal system the remainders according to these moduli can be found so easily). The numbers derived from this must be congruent with those which were deduced from the proposed numbers; unless this happens, it is concluded that a defect has crept into the calculation.

But since these and the like are abundantly well known, it would be superfluous to dwell on them any longer.