6.4. Congruence; Divisibility Tests

Note. In this length section, we introduce the equivalence relation of congruence modulo m on the integers $\mathbb{Z}$. We state and prove some properties of this equivalence relation and use it to establish two number theory "tricks" concerning the divisibility of a number by 9 and by 11. By convention, all numbers in this section are assumed to be integers.

Definition 6.37. Fix $m > 0$. Numbers a and b are *congruent modulo* m if $a - b$ is divisible by m. This is denoted $a \equiv b \pmod{m}$. The number m is the *modulus* of the congruence relation.

Example 6.38. We have the congruences $3 \equiv -5 \pmod{4}$, $0 \equiv 15 \pmod{5}$, $-7 \equiv 5 \pmod{6}$, and $5743 \equiv 43 \pmod{100}$. We show below (in Theorem 6.41) that congruence modulo m really is an equivalence relation on $\mathbb{Z}$.

Note. Congruence modulo m is a central idea in number theory. For example, in Elementary Number Theory (MATH 3120) the idea is covered in Section 4. Congruences, in which the idea of "clock arithmetic" is mentioned (see also Example 6.40(b) below) and some history of congruence is given (congruence modulo m was introduced by Carl Friedrich Gauss (April 30, 1777–February 23, 1855) in his 1801 *Disquisitiones Arithmeticae*). Congruence relations are further explored in this class in Section 5. Linear Congruences, and applications of congruence relations play a role throughout the rest of the Elementary Number Theory course.

Note 6.4.A. Notice that we can translate the congruence $a \equiv b \pmod{m}$ into the equations $a - b = mk$ or $a = b + mk$ for some $k \in \mathbb{Z}$.

Example 6.40(b). This example rather literally illustrates the idea of "clock arithmetic" and its cyclic nature. Suppose it is now 5 AM. We want to know the time 784 hours from now. Since it is now 5 hours past midnight, after the given time interval it will be 789 hours past midnight. Division by 12 yields the equation $789 = 12 \cdot 65 + 9$. This equation tells us that over the span of 789 hours, a clock's hour hand will complete 65 full revolutions (taking the time to noon) and will then mark off nine more hours. The result: in 784 hours from now the time will be 9 PM. Of course, we could use military time (in which a clock marks off 24 hours in a day and does not require the AM/PM distinction of times), in which case we would consider the equation $789 = 24 \cdot 32 + 21$ and the congruence statement $789 \equiv 21 \pmod{24}$. In this case, we conclude that the time will be 21 hours (or, in civilian time, $21 - 12 = 9$ PM, as before).

Theorem 6.41. Fix $m > 0$. Then congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Note. The next result shows that congruence modulo m can, in some cases, behave like equations (i.e., like equality).

Theorem 6.42. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

Note. The next corollary follows form Theorem 6.42 by applying the Principle of Mathematical Induction.

Corollary 6.43. Suppose the congruences $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, $\ldots$, $a_n \equiv b_n \pmod{m}$ hold. Then

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m} \text{ and } \prod_{i=1}^{n} a_i \prod_{i=1}^{n} b_i \pmod{m}.$$

In particular, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for all $n \geq 1$.

Note. In our base 10 number system, we represent a nonnegative integer n in decimal form as $n = a_t a_{t-1} \ldots a_1 a_0$, where $0 \leq a_i \leq 9$, and interpret this as

$$n = a_t \cdot 10^t + a_{t-1} \cdot 10^{t-1} + \cdots + a_1 \cdot 10 + a_0 = \sum_{i=0}^{t} a_i \cdot 10^i.$$

Of course this can also be extended to nonintegers if we allow for series (instead of sums) and infinite decimal representations.

Theorem 6.45. Every nonnegative integer is congruent modulo 9 to the sum of its decimal digits. Symbolically, if $0 \leq a_i \leq 9$ for $0 \leq i \leq t$, then

$$\sum_{i=0}^{t} a_i \cdot 10^i \equiv \sum_{i=0}^{t} a_i \pmod{9}.$$

Corollary 6.46. Test for Divisibility by 9.

An integer is a multiple of 9 if and only if the sum of its decimal digits is a multiple of 9.

Note. The previous two results are ultimately based on the fact that 9 is 1 less than 10 and that we are considering decimal digits. So it is not surprising that there is a related result if we use any base to represent a number. If $b \geq 2$ and n is any positive integer, then to write n in base b is to express n as a sum of the form

$$n = \sum_{i=0}^{t} a_i b^i \text{ with } 0 \leq a_i \leq b - 1.$$

In this case, we represent n as $n = a_t a_{t-1} \cdots a_0$ base b. The congruence in Theorem 6.45 can then be generalized as:

$$\sum_{i=0}^{t} a_i b^i \equiv \sum_{i=0} a_i \pmod{b-1}.$$

Corollary 6.46 then generalizes to the statement: An integer is a multiple of $b - 1$ if and only if the sum of its digits in base b representation is a multiple of $b - 1$. For more on base b representations, see my online notes for Elementary Number Theory (MATH 3120) on Section 13. Numbers in Other Bases.

Theorem 6.48. (Test for Divisibility by 11).

An integer n with decimal representation $n = a_t a_{t-1} \ldots a_0$ is divisible by 11 if and only if the number $a_t - a_{t-1} + a_{t-2} - \cdots \pm a_1 \mp a_0$ is divisible by 11.

Example 6.49. The number 319,245,386,597,518,260 is divisible by 11 by Theorem 6.48, because

$$3-1+9-2+4-5+3-8+6-5+9-7+5-1+8-2+6-0=22$$

is divisible by 11.

Revised: 2/27/2022