Section 4. Congruences

Note. In this section, we define congruence modulo m on the set of integers. We give some properties and prove results that allow us to solve or simplify some congruence relations. Some of the material in this section is also in my online notes for Mathematical Reasoning (MATH 3000) on Section 6.4. Congruence; Divisibility Tests.

Definition. For $a, b \in \mathbb{Z}$, we say a is *congruent* to b modulo m (where we take $m > 0$) if $m \mid (a - b)$, denoted $a \equiv b \pmod{m}$.

Note. Sometimes arithmetic modulo m is called "clock arithmetic." For example, if $m = 12$ then we have 9 o'clock plus 4 hours equal to 1 o'clock (not 13 o'clock).

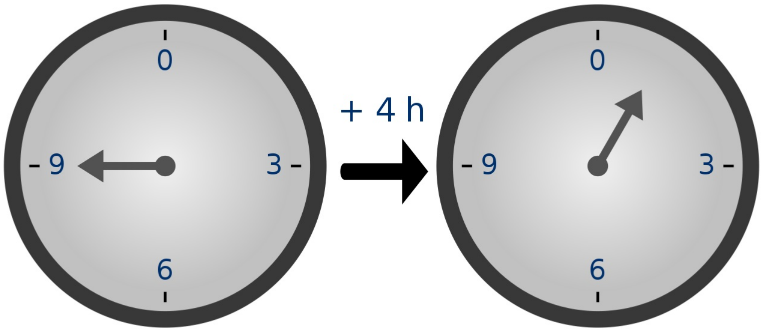

Image from the Wikipedia Modular Arithmetic page (accessed 7/8/2012)

Note. Carl Friedrich Gauss contributed to several fields of mathematics and some areas of physics. He did work in number theory concerning the distribution of prime numbers which is related to one of the most famous unsolved problems today (the location of the zeros of the Riemann Zeta function; Riemann was a student of Gauss). His work on curvature of surfaces was taken up by Riemann who extended them to manifolds and the creation of the area of differential geometry (this area of math was later used by Einstein in his development of general relativity). He also worked in orbital mechanics and introduced statistical analysis of observations in the estimation of orbits (and the normal distribution in statistics is often called the "Gaussian distribution"). He gave a compass and straight edge construction of a regular 17-gon, a construction that was unknown since the time of Euclid. Gauss graduated with degrees from Göttingen University in 1798 and Brunswick Collegium Carolinum in 1799. His dissertation (which he submitted to the University of Helmstedt) discussed the Fundamental Theorem of Algebra (for which he gave numerous proofs throughout his life). In the summer of 1801 he published *Disquisitiones Arithmeticae* which contained seven sections, six of which were on number theory. In other books, he contributed to the areas of series (and introduced the hypergeometric function), approximation of integrals, statistical estimators, and potential theory. Around 1820 he was involved in a geodesic survey of the state of Hanover. Based on this experience, he developed an interest in mapping one surface onto another leading to his work on surfaces. In connection with this work and the use of measurements which contain possible errors, he developed the method of least squares. Gauss took an interest in non-Euclidean geometry around 1800. In connection with this, he communicated with Farkas Bolyai. In 1831, Farkas Bolyai's son János Bolyai sent his work on non-Euclidean geometry to Gauss. When reviewing the work, Gauss commented that "to praise it would mean to praise myself." By this, Gauss meant to imply that he had already reached the conclusions of the work on his own (though he had not published his work). Similarly, upon learning that Nikolai Lobachevsky had worked on the subject, he praised the work while commenting that he had held the same convictions for the past 54 years. This controversy about who deserves the credit for the discovery ("invention"?) of non-Euclidean geometry (between Gauss, Bolyai, and Lobechevsky) exists to this day. But our focus is on his work in number theory. In this direction, we concentrate on his *Disquisitiones Arithmeticae*. It is in this work that Gauss introduces the idea of congruence modulo m (in Sections I and II). A copy of *Disquisitiones Arithmeticae* translated by Arthur A. Clarke is available to read online through JSTOR (you will need our ETSU username and password to access this).

Carl Friedrich Gauss (April 30, 1777–February 23, 1855)

This image and the biographical information is from MacTutor History of Mathematics Archive Gauss biography page.

Theorem 4.1. We have $a \equiv b \pmod{m}$ if and only if there is integer k such that $a = b + km$.

Theorem 4.2. Every integer is congruent modulo m to exactly one of $0, 1, 2, \ldots, m-1$. This number is called the *least residue* of the integer modulo m.

Note. Strictly speaking, congruence modulo m is an "equivalence relation" on the integers $\mathbb{Z}$. In Introduction to Modern Algebra (MATH 4127/5127) and Modern Algebra 1 (MATH 5410) we introduce congruence modulo m as an equivalence relation and then we denote the equivalence classes modulo m as $\bar{i}$ where $i = 0, 1, 2, \ldots, m-1$. So, for example, the equivalence class $\overline{0} = \{z \in \mathbb{Z} \mid z \equiv 0 \pmod{m}\}$. This is dealt with in terms of quotients groups and we have that the integers modulo m is the quotient group $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$. See my online notes for Introduction to Modern Algebra (MATH 4127/5127) on Section III.14. Factor Groups and my online notes for Modern Algebra 1 (MATH 5410) on Section I.5. Normality, Quotient Groups, and Homomorphisms where the integers modulo m, $\mathbb{Z}_m$, is defined as the quotient group $\mathbb{Z}/(m\mathbb{Z})$. Again, the elements of the integers modulo m are equivalence classes modulo m. For example, in the integers modulo m we have $\overline{0} = \{i \in \mathbb{Z} \mid i \equiv 0 \pmod{m}\}$.

Theorem 4.3. We have $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m.

Lemma 4.1. For integers a, b, c, and d we have

(a) $a \equiv a \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

(e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Note. Lemma 4.1 parts (a), (b), and (c) imply that congruence modulo m is an "equivalence relation" on $\mathbb{Z}$. Notice that we do not have a cancellation property (or more appropriately, we may not have multiplicative inverses modulo m). For example, $3 \cdot t \equiv 3 \cdot 8 \pmod{12}$ but $4 \not\equiv 8 \pmod{12}$ (even thought $3 \not\equiv 0 \pmod{12}$). However, under certain conditions we can perform cancellation, as given in the next result.

Theorem 4.4. If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$. That is, we can cancel a factor on both sides of a congruence if the factor is relatively prime to the modulus.

Note. The next result shows how to deal with common factors on both sides of a congruence when the factor and modulus are not relatively prime.

Theorem 4.5. If $ac \equiv bc \pmod{m}$ and $(c, m) = d$, then $a \equiv b \pmod{m/d}$.

Example 4.A. We want to show that no integer of the form $8n + 7$ is the sum of three squares. To establish this, suppose $k = 8n + 7$ so that $k \equiv 7 \pmod{8}$.

Consider $a^2 + b^2 + c^2$ for integers a, b, and c. Now every integer has a residue of 0, 1, 2, 3, 4, 5, 6, or 7 modulo 8 by Theorem 4.2 and:

$$0^2 \equiv 0 \pmod{8},\ \ 1^2 \equiv 1 \pmod{8},\ \ 2^2 \equiv 4 \pmod{8},\ \ 3^2 \equiv 1 \pmod{8},$$

$$4^2 \equiv 0 \pmod{8},\ \ 5^2 \equiv 1 \pmod{8},\ \ 6^2 \equiv 4 \pmod{8},\ \ 7^2 \equiv 1 \pmod{8}.$$

So the square of any integer is congruent to 0, 1, or 4 modulo 8. Hence $a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5,$ or $6 \pmod{8}$ (the possible sums modulo 8 of three of 0, 1, and 4). So $a^2 + b^2 + c^2$ is never congruent to 7 modulo 8 and hence we cannot have $a^2 + b2 + c^2 = 8n + 7$.

Theorem 4.6. Every integer is congruent modulo 9 to the sum of its digits.

Note. The process of "Casting Out Nines" is based on Theorem 4.6 and can be used to check a sum or product. We replace a number with the sum of its digits (repeatedly, if necessary) and see if the product and the alleged result are the same. What we actually do in this procedure, is check if the product and the alleged result are equal modulo 9. If they are not, the the alleged result cannot be correct. Of course, if they are the same modulo 9 then the alleged result could still be incorrect. For example, consider the claim that $(314)(159) = 49826$. Working modulo 9 we have

$$(314)(159) \equiv (3 + 1 + 4)(1 + 5 + 9) \equiv 8 \cdot 15 \equiv 8(1 + 5)$$
$$\equiv 48 \equiv 4 + 8 \equiv 12 \equiv 1 + 2 \equiv 3 \pmod{9},$$

while

$$49826 \equiv 4 + 9 + 8 + 2 + 6 \equiv 29 \equiv 2 + 9 = 11 \equiv 1 + 1 \equiv 2 \pmod{9}.$$

So (314)(159) and 49826 are not congruent modulo 9 and hence the product (314)(159) cannot equal 49826. More detail can be found on the Wikipedia page on "Casting Out Nines".

Revised: 3/4/2022