Modular arithmetic and congruences Theory and notation Our previous exploration of Euclid's algorithm has left us perfectly poised on the precipice of the most important theorem in elementary number theory, the Fundamental Theorem of Arithmetic. However, to increase the suspense, we shall delay our study of this theorem until next term. For now, we settle for another core pillar of number theory: modular arithmetic and congruence.

Think of modular arithmetic as cyclic counting, or a system of doing arithmetic in which numbers "wrap" around at a certain value. For example, when we consider the hour of the day on a twelve-hour clock, 13 is the same as 1, 14 is the same as 2, 15 is the same as 3, and so on. In this case the hours wrap around when they get to the number 12. The power of this lies in how we can take an infinity (the positive integers) and reduce it to a finite set of 12 numbers. To illustrate, suppose we start at midnight and add 147 hours. To find the hour of the day at that time, we only need to know how much bigger 147 is than a multiple of 12, because the hours reset every 12 hours. We see that 147 is 3 more than a multiple of 12, so we are at 3 o'clock. Note how this works for an arbitrarily large hour. By subtracting a multiple of 12, we can always reduce the hour to one between 0 and 11; the 12th hour wraps around to 0. Also note how this is the same as finding the remainder after division by 12. The only possible remainders are the numbers $0, 1, 2, \ldots, 11$.

This idea of "wrapping around" is so useful it has its own notation. Given two integers a and b and a third positive integer greater than unity m called the modulus, we say that a is congruent to b modulo m if b can be obtained by subtracting from a a multiple of m. This relation is denoted a≡b (mod m).$Anotherwayofsayingitisthat$a-b$isamultipleof$m.$Wecallaandbresiduesofeachother.$

The preceding algebraic definition is not intuitive. A more intuitive way to think about it is if a and b are congruent modulo m, then a and b are essentially the same number when viewed from the perspective of divisibility by m; that is, they leave the same remainder when divided by m. That remainder is always a number between 0 and m-1 inclusive, and is called the least residue of a and b. Relative to a modulus m, every number is congruent to one number in the set $\{0, 1, 2, \ldots, m-1\}$.$Thissetiscalledacompletesetofresidues.Anysetofmelementsinwhichal$

The definition of congruence extends naturally to negative integers. For example, 2≡-5 (mod 7)$because$2−(−5)$isdivisibleby$7.$Themainalgebraicpicturetokeepinmindisthatof$a-b$beingdivisiblebymifa≡b (mod m). This relation can be written a-b=mk for some integer k. Rearranging yields a=mk+b. Recognise that this is Euclidean division of a and m; this proves there exists some $b = b'$ such that $0 \leq b' \leq m - 1$, and hence any number a is congruent to a number in that range, as already mentioned.

The true power of congruence reveals itself when we being treating the congruence symbol ≡ like an equals sign. Here are some of the basic properties of congruences. Assuming that $a \equiv a'$ (mod m) and $b \equiv b'$ (mod m), then: itemize

e $a+b \equiv a'+b'$ (mod m); $ab \equiv a'b'$ (mod m); rty).