Divisibility and Congruence

Definition. Let $a \in \mathbb{Z} - \{0\}$ and $b \in \mathbb{Z}$. We say that a *divides* b and write $a \mid b$ if

$$b = aq \qquad \text{for some } q \in \mathbb{Z}.$$

Properties. Suppose $a, b, c \in \mathbb{Z}$ and $a \neq 0$.
If $a \mid b$ and $a \mid c$, then $a \mid (xb + yc)$ for any $x, y \in \mathbb{Z}$.
We express this in words by saying: *if a divides b and c, then a divides any integer linear combination of b and c.*

Definition. Let $m \in \mathbb{Z} - \{0\}$ and $a, b \in \mathbb{Z}$. We say that *a is congruent to b modulo m* and write $a \equiv b \mod m$ if

$$m \mid (b - a).$$

Properties/Examples.

1. $a \equiv 0 \mod m$ if and only if $m \mid a$.
   Proof. If $a \equiv 0 \mod m$, then $m \mid (0 - a)$. Therefore $-a = mp$ for some $p \in \mathbb{Z}$. Thus $a = m(-p)$ and so $m \mid a$.

   Conversely, if $m \mid a$, then $a = mq$ for some $q \in \mathbb{Z}$. Therefore $(0 - a) = -a = m(-q)$ and so $m \mid (0 - a)$. Thus $a \equiv 0 \mod m$. □

2. $a \equiv 0 \mod 2$ if and only if a is even.

3. $a \equiv 1 \mod 2$ if and only if a is odd.

4. $a \equiv 0 \mod 3$ if and only if a is divisible by 3.

5. $a \equiv 1 \mod 3$ if and only if a has a remainder of 1 on division by 3.

6. $a \equiv 2 \mod 3$ if and only if a has a remainder of 2 on division by 3.

7. $\equiv \mod m$ is *reflexive.* That is, $a \equiv a \mod m$ for all integers a.
   Proof. $(a - a) = 0 = m(0)$ and so $a \equiv a \mod m$. □

8. $\equiv \mod m$ is *symmetric.* That is, for all integers a, b, if $a \equiv b \mod m$, then $b \equiv a \mod m$.
   Proof. By hypothesis $m \mid (b - a)$. Thus $(b - a) = mq$ for some $q \in \mathbb{Z}$. Therefore $(a - b) = -(b - a) = m(-q)$ and so $b \equiv a \mod m$. □

9. $\equiv \mod m$ is *transitive.* That is, for all integers a, b, c, if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.
   Proof. By hypothesis $m \mid (b - a)$ and $m \mid (c - b)$. This means $(b - a) = mp$ and $(c - b) = mq$ for some $p, q \in \mathbb{Z}$. Adding gives $(c - a) = (c - b) + (b - a) = m(p + q)$ and so $m \mid (c - a)$. Therefore $a \equiv c \mod m$. □

10. We say that $\equiv \mod m$ is an *equivalence relation*, because it is reflexive, symmetric and transitive. We will talk about equivalence relations more formally anon. Meanwhile, think about other equivalence relations you know about (between numbers, or between people etc.). For example, equality $=$ is an equivalence relation among numbers, geometric congruence (e.g., resulting from side-side-side or side-angle-side) is an equivalence relation among euclidean triangles, "is the same age as" and "is the same height as" are equivalence relations on the set of all students in your class. Try to think of other examples of equivalence relations.

11. **Cool Property 1.** For all integers a, b, x, y, if $a \equiv x \mod m$ and $b \equiv y \mod m$, then $a + b \equiv x + y \mod m$.
Proof. By hypothesis $m \mid (x - a)$ and $m \mid (y - b)$. This means $(x - a) = mp$ and $(y - b) = mq$ for some $p, q \in \mathbb{Z}$. Adding gives $((x + y) - (a + b)) = (x - a) + (y - b) = m(p + q)$, and so $m \mid (x + y) - (a + b)$. Therefore $(a + b) \equiv (x + y) \mod m$. □

12. **Cool Property 2.** For all integers a, b, x, y, if $a \equiv x \mod m$ and $b \equiv y \mod m$, then $ab \equiv xy \mod m$.
Proof. By hypothesis $m \mid (x - a)$ and $m \mid (y - b)$. This means $(x - a) = mp$ and $(y - b) = mq$ for some $p, q \in \mathbb{Z}$. Solving for x and y gives $x = a + mp$ and $y = b + mq$, and so $xy = (a + mp)(b + mq) = ab + m(mpq + pb + qa)$. Thus $xy - ab = m(mpq + pb + qa)$ and so $m \mid (xy - ab)$. Therefore $ab \equiv xy \mod m$. □

13. We have seen Cool Property 1 in action before without articulating it in this level of generality. Here is one instance that we have seen.

    - If a is even and b is even, then $a + b$ is even.
      This now follows from cool property 1, item 2 above, and the fact that $0 + 0 = 0$.
    - If a is odd and b is even, then $a + b$ is odd.
      This now follows from cool property 1, items 2 and 3 above, and the fact that $1 + 0 = 1$.
    - If a is odd and b is odd, then $a + b$ is even.
      This now follows from cool property 1, items 2 and 3 above, and the fact that $1 + 1 = 2 \equiv 0 \mod 2$.

    So, we can think of Cool Property 1 as a general theorem, and can think about our three previous theorems about sums of odd and even numbers as special instances of (or immediate consequences of (also known as "corollaries of")) Cool Property 1.

    Here is another instance where we encountered Cool Property 1.
    Q: If today is Friday, then on what day does an event occur if it was scheduled 72 days from now, but is to be postponed another 144 days from then, and then postponed an additional 703 days? We figured out that what was critical was the sum $2+4+3 = 9$ and concluded that the event will occur on a Sunday. Here's what is happening with congruences. Two numbers which are congruent modulo 7 will result in postponements which occur on the same week day. We know that $72 \equiv 2 \mod 7$, that $144 \equiv 4 \mod 7$, and $703 \equiv 3 \mod 7$. Therefore the cool property enables us to write $72+144+703 \equiv 2+4+3 \mod 7$, which in turn gives $9 \equiv 2 \mod 7$. So we count two days on from Friday to get a Sunday.

14. We have seen Cool Property 2 in action before without articulating it in this level of generality. Here is one instance that we have seen.

    - If a is even and b is even, then ab is even.
      This now follows from cool property 2, item 2 above, and the fact that $(0)(0) = 0$.
    - If a is odd and b is even, then ab is even.
      This now follows from cool property 2, items 2 and 3 above, and the fact that $(1)(0) = 0$.
    - If a is odd and b is odd, then ab is odd.
      This now follows from cool property 2, item 3 above, and the fact that $(1)(1) = 1$.

15. **Exercise.** Use item 1 and Cool Property 2 to give a proof of the following fact. If an integer a is not divisible by 5, then a^2 is not divisible by 5.

16. **Exercise.** Use the previous exercise to prove that $\sqrt{5}$ is irrational.

17. **Exercise.** Use item 1 and Cool Property 2 to give a proof of the following fact. If an integer a is not divisible by 6, then a^2 is not divisible by 6.

18. **Exercise.** Use the previous exercise to prove that $\sqrt{6}$ is irrational.

19. **Exercise.** Write out the multiplication and addition tables $\mod m$ for $m = 2, 3, 4, 5, 6, 7, \ldots$

20. **Exercise.** Give proofs for *divisibility tests* for divisibility of integers by $2, 3, 4, 5, 6, 7, 8, 9, 11$. In all these tests $a_n \ldots a_0$ is an $(n+1)$–digit number in (usual) base 10 notation. Therefore

$$a_n \ldots a_1 a_0 \;=\; a_n(10)^n + \cdots + a_1(10)^1 + a_0$$

- $2 \mid a_n \ldots a_1 a_0$ if and only if $2 \mid a_0$.
- $4 \mid a_n \ldots a_1 a_0$ if and only if $4 \mid (2a_1 + a_0)$.
- $8 \mid a_n \ldots a_1 a_0$ if and only if $8 \mid (4a_2 + 2a_1 + a_0)$.
- $3 \mid a_n \ldots a_1 a_0$ if and only if $3 \mid (a_n + \cdots + a_0)$.
- $9 \mid a_n \ldots a_1 a_0$ if and only if $9 \mid (a_n + \cdots + a_0)$.
- $5 \mid a_n \ldots a_1 a_0$ if and only if $5 \mid a_0$.
- $6 \mid a_n \ldots a_1 a_0$ if and only if $3 \mid (a_n + \cdots + a_0)$ and $2 \mid a_0$.
- $11 \mid a_n \ldots a_1 a_0$ if and only if $11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^n a_n)$.
- $7 \mid a_n \ldots a_1 a_0$ if and only if $7 \mid a_n \ldots a_1 - 2(a_0)$.

21. Prove that if a is an integer and $11 \nmid a$, then $11 \nmid a^2$ and $11 \nmid a^3$.
Proof. By hypothesis, $11 \nmid a$. This means that $a \not\equiv 0 \mod 11$. There are 10 cases to consider: namely, $a \equiv 1 \mod 11, \ldots, a \equiv 10 \mod 11$. We group these cases in complementary pairs and indicate the squares and cubes below. The latter are found by repeated application of Cool Result 2.

$a \mod 11$		$a^2 \mod 11$	$a^3 \mod 11$
$a \equiv 1$	$a \equiv 10 \equiv -1$	$(\pm 1)^2 \equiv 1$	$(\pm 1)^3 \equiv \pm 1$
$a \equiv 2$	$a \equiv 9 \equiv -2$	$(\pm 2)^2 \equiv 4$	$(\pm 1)^3 \equiv \pm 8$
$a \equiv 3$	$a \equiv 8 \equiv -3$	$(\pm 3)^2 \equiv 9$	$(\pm 1)^3 \equiv \pm 5$
$a \equiv 4$	$a \equiv 7 \equiv -4$	$(\pm 4)^2 \equiv 5$	$(\pm 1)^3 \equiv \pm 9$
$a \equiv 5$	$a \equiv 6 \equiv -5$	$(\pm 5)^2 \equiv 3$	$(\pm 1)^3 \equiv \pm 4$

In all 10 cases $a^2 \not\equiv 0 \mod 11$, and $a^3 \not\equiv 0 \mod 11$. Therefore $11 \nmid a^2$ and $11 \nmid a^3$. □

22. Use the result above to prove that $\sqrt{11}$ and $\sqrt[3]{11}$ are both irrational.