

MATH 110: Class 11

August 31: Modular arithmetic; Divisibility tests

Modular arithmetic

1. **Equivalence modulo n .** We say that two integers a and b are **equivalent modulo n** or that a and b are in the same **residue class** modulo n if they have the same remainder after division by n . Put another way, a and b are equivalent modulo n if

$$a - b = mn$$

for some integer m .

- By definition an integer a is divisible by a nonzero integer m (equivalently, m divides a) if $a = km$ for some integer k . Thus, a is divisible by b if and only if $b \equiv 0 \pmod{a}$.

2. **Additional modulo n .** Suppose

$$a \equiv b \pmod{n} \quad \text{and} \quad a' \equiv b' \pmod{n},$$

so that $a - b = mn$ and $a' - b' = m'n$ for some m, m' . Then, adding gives

$$a + a' = (mn + b) + (m'n + b') = (m + m')n + (b + b'),$$

or equivalently

$$a + a' \equiv b + b' \pmod{n}.$$

So, if a and b have the same residue class and a' and b' have the same residue class, so do $a + a'$ and $b + b'$. This defines an operation on the set \mathbb{Z}_n of residue classes modulo n ; we usually denote the operation by $+$ but here we'll use $+_n$ to help distinguish it from the usual addition of integers. Let \bar{a} and \bar{b} denote residue classes modulo n , and pick numbers a, b such that

$$\bar{a} = a \pmod{n} \quad \text{and} \quad \bar{b} = b \pmod{n}.$$

Then,

$$\bar{a} +_n \bar{b} = a + b \pmod{n} = \overline{a + b}.$$

We often denote the residue classes modulo n by $\bar{0}, \dots, \overline{n-1}$. Notice that $\bar{n} = \bar{0}$.

EXAMPLE (Addition modulo 2). Consider the special case $n = 2$. By definition, an integer a is even if $a \equiv 0 \pmod{2}$ and odd if $a \equiv 1 \pmod{2}$. Then the addition operation $+_2 : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ has multiplication table

$+_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

In other words, the rule for $+_2$ says just that adding two even numbers or two odd numbers gives an even number, and adding an even number and an odd number gives an odd number.

Notice that if we erase the bars, our multiplication table is the same as the one for the propositional logical operation we called exclusive disjunction or XOR (\vee).

- **The cyclic group of order n .** Notice that $+_n$ defines a group structure on \mathbb{Z}_n : It has identity $\bar{0}$, the inverse of \bar{a} is $-\bar{a} := \overline{-a}$, and $+_n$ is associative because $+$ is. It has n elements, and for any nonnegative integer a , $\bar{a} = \underbrace{\bar{1} + \dots + \bar{1}}_a$, so it is cyclic, that is, \mathbb{Z}_n can be identified with the group C_n of rotations of a regular n -gon.

3. **Multiplication modulo n .** If $a = b \pmod{n}$ and $a' = b' \pmod{n}$, so that $a = mn + b$ and $a' = m'n + b'$ for some integers m, m' , then

$$aa' = (mn + b)(m'n + b') = (mm'n + mb' + m'b)n + bb',$$

so the products aa' and bb' have the same residue class modulo n . Thus, multiplication determines another binary operation on \mathbb{Z}_n , namely multiplication modulo n : For any residue classes \bar{a}, \bar{a}' modulo n , pick numbers such that $\bar{a} = a \pmod{n}$ and $\bar{a}' = a' \pmod{n}$. Then, $\bar{a} \cdot_n \bar{a}' = aa' \pmod{n} = \overline{a \cdot a'}$.

- **The algebraic structure of \cdot_n .** Note that \cdot_n does *not* define a group structure (at least, not for $n > 1$): For any $\bar{a} \in \mathbb{Z}_n$, $\bar{0} \cdot \bar{a} = \overline{0 \cdot a} = \bar{0}$, so \cdot_n has no inverse map. Still, it is a perfectly good binary operation. The multiplication table is:

\cdot_2	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

If we erase the bars, what logical operation is this?

4. **Multiplicative subgroup modulo n .** First, notice that $\bar{1}$ is a multiplicative identity of \cdot_n and so is its own multiplicative inverse. Also notice that if n factors into smaller positive integers as $n = qr$, then $\bar{q} \cdot \bar{r} = \bar{qr} = \bar{n} = \bar{0}$. So, neither \bar{q} nor \bar{r} can have a multiplicative inverse in \mathbb{Z}_n (if, say, \bar{q} did, then $\bar{r} = \bar{q}^{-1}\bar{q}\bar{r} = \bar{q}^{-1}\bar{0} = \bar{0}$, a contradiction).

More generally, if n and $q < n$ have a common factor > 1 , say, $n = \ell s, q = ms$ for some $\ell, m > 1$, then $\ell q = \ell ms = mn$, so $\ell \bar{q} = \bar{0}$, hence \bar{q} does not have a multiplicative inverse.

On the other hand, if n and q have no common factors > 1 (that is, if n and q are **coprime**), a similar argument shows that \bar{q} does have a multiplicative inverse.

ACTIVITY (Elements of \mathbb{Z}_{12} with multiplicative inverses) The numbers < 12 coprime to 12 are 1, 5, 7, 11, so the elements of \mathbb{Z}_{12} with multiplicative inverses are $\bar{1}, \bar{5}, \bar{7}, \bar{11}$; we denote $\mathbb{Z}_{12}^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$. Computing gives $\bar{1}^2 = \bar{5}^2 = \bar{7}^2 = \bar{11}^2 = 1$, so all four of those elements are their own inverses. Notice that $(\mathbb{Z}_{12}^\times, \cdot_{12})$ is a group isomorphic to the Klein 4-group, $C_2 \times C_2$ (i.e., the group of symmetries of a nonsquare rectangle).

ACTIVITY (Inverses of elements of \mathbb{Z}_n^\times for small n)

- For each value $2 \leq n \leq 10$ find the elements of \mathbb{Z}_n that have a multiplicative inverse, and compute their respective inverses. The set \mathbb{Z}_n^\times of elements of \mathbb{Z}_n that have a multiplicative inverse is denoted \mathbb{Z}_n^\times .
- Show that (for every n) \mathbb{Z}_n^\times is a group under multiplication, \cdot_n .
- Determine which groups we've previously seen the groups $\mathbb{Z}_2^\times, \dots, \mathbb{Z}_{10}^\times$ are isomorphic to.
- Is \cdot_n commutative (i.e., is \mathbb{Z}_n^\times Abelian) for every n ?

5. **Euler's totient function.** We denote the number of numbers in $\{1, \dots, n\}$ coprime to n by $\phi(n)$; in particular, $|\mathbb{Z}_n^\times| = \phi(n)$. In particular, ϕ is a function $\mathbb{Z}_+ \rightarrow \mathbb{Z}_+$, where $\mathbb{Z}_+ = \mathbb{N} \setminus \{0\}$ denotes the set of positive integers. By definition p is prime if and only if $\phi(p) = p - 1$. Euler's totient function is *multiplicative*: If a and b are coprime, then $\phi(ab) = \phi(a)\phi(b)$.
6. **Euler's Theorem** Lagrange's Theorem (a result from group theory) implies that the order of an element of a group divides the order of the group, so for any element $\bar{a} \in \mathbb{Z}_n$, $\bar{a}^{\phi(n)} = 1$, that is,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

- In the special case that $n = p$ is prime, we get **Fermat's Little Theorem**: $a^{p-1} \equiv 1 \pmod{p}$, or just as well, $a^p \equiv a \pmod{p}$.
- This theorem will be especially useful tomorrow, when we use the properties of prime numbers and Euler's Theorem to encode and decode secret messages using the RSA algorithm from cryptography.

Divisibility tests

1. **(Divisibility tests for small integers)** We can use modular arithmetic to devise tests for divisibility of integers by various (usually small) integers.

EXAMPLE. **(Divisibility tests for 2, 3, 4, 6, 7, 10)**

- (a) **(Divisibility by 10).** We can write any integer as $10a + b$ for some integers a, b , and $10a + b \pmod{10} = b \pmod{10}$, so an integer is divisible by 10 if and only if its last digit is 0.
- (b) **(Divisibility by 2).** We can write any integer as $10a + b$ for some integers a, b , and $10a + b \pmod{2} = b \pmod{2}$, so a number is divisible by 2 (even) if and only if its last digit is even.
- (c) **(Divisibility by 4).** We can write any integer as $100a + 10b + c$, and $100a + 10b + c \pmod{4} = 10b + c \pmod{4}$, so a number is divisible by 4 if and only if its last two digits are. Furthermore, $100a + 10b + c \pmod{4} = 2b + c$, so a number is divisible by 4 if and only if its penultimate digit is even and its last digit is divisible by 4, or if its penultimate digit is odd and last digit is even but not divisible by 4.
- (d) **(Divisibility by 3).** We can write any integer as $\underline{a_n \cdots a_0} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$. Since $10 = 1 \pmod{3}$, $10^k = 1 \pmod{3}$ for all k , and so $\underline{a_n \cdots a_0} = a_n + \cdots + a_0 \pmod{3}$, that is, an integer is a multiple of 3 if and only if the sum of its digits is.
- (e) **(Divisibility by 6.)** Since 6 is the product of the numbers 2 and 3, which share no common factors, a number is divisible by 6 if and only if it is divisible by both 2 and 3, and we can use the above tests.
- (f) **(Divisibility by 7.)** This case is famously tricky. Proceeding as with divisibility by 3, we see that We can write any integer as $\underline{a_n \cdots a_0} \pmod{7} = a_n \cdot 3^n + a_{n-1} \cdot 3^{n-1} + \cdots + a_1 \cdot 3 + a_0 \pmod{7}$, so it's enough to compute the powers of 3 modulo 7, and we get $3, 2, -1, -3, -2, 1 \pmod{7}$, so a number is divisible by 7 if $3a_0 + 2a_1 - a_2 - 3a_3 - 2a_4 + a_5 + 3a_6 + 2a_7 + \cdots$ is. This is not so practical for mental computation! Instead notice that

$$\underline{a_n \cdots a_0} \pmod{7} = (a_n \cdot 3^n + a_{n-1} \cdot 3^{n-1} + \cdots + a_1 \cdot 3 + a_0) \pmod{7} \quad (1)$$

$$= 3(a_n \cdot 3^{n-1} + \cdots + a_2 \cdot 3 + a_1 - 2a_0) \pmod{7} \quad (2)$$

$$= 3(\underline{a_n \cdots a_1} - 2a_0) \pmod{7}. \quad (3)$$

So, $\underline{a_n \cdots a_0}$ is divisible by 7 if and only if $\underline{a_n \cdots a_1} - 2a_0$ is. For example, consider $\underline{a_2 a_1 a_0} = 854$: Then, $\underline{a_2 a_1} = 85$ and $a_0 = 4$, so $\underline{a_2 a_1} - 2a_0 = 85 - 2 \cdot 4 = 77 = 11 \cdot 7$, so 854 is divisible by 7.

ACTIVITY. **(More divisibility tests.)** In small groups, devise divisibility tests for 5, 8, 9, 11, 12, 14, and 15. (For a challenge, devise a test for divisibility by 13. *Hint: Modify our method for computing divisibility by 13.*)