Numbers modulo n. We have previously seen examples of clock arithmetic, an algebraic system with only finitely many "numbers." In this lecture, we make a formal analysis.

DEFINITION: Fix a positive integer n, the *modulus*, and let $a, b \in \mathbb{Z}$. We say *a is equivalent to b modulo n*, in symbols $a \equiv b \pmod{n}$, to mean that $n \mid (a-b)$.

EXAMPLE: A standard clock with $n = 12$ hours has hour marks at $1, 2, \ldots, 11, 12$ o'clock. The time 13 hours after noon is 1 o'clock, which corresponds to $13 \equiv 1 \pmod{12}$. Similarly, 11 hours before noon is also 1 o'clock, since $-11 \equiv 1 \pmod{12}$; and 0 hours (noon itself) is 12 o'clock, since $0 \equiv 12 \pmod{12}$. Note that we consider only *whole number hours*, never fractions of an hour.

For a fixed modulus n, the relation $\equiv$ has the properties of an *equivalence relation* on the set of integers. For any $a, b, c \in \mathbb{Z}$, we can show:

- Reflexive: $a \equiv a$
- Symmetric: If $a \equiv b$, then $b \equiv a$.
- Transitive: If $a \equiv b$ and $b \equiv c$, then $a \equiv c$

Each element $a \in \mathbb{Z}$ has its *equivalence class* $\overline{a}$, the set of all elements equivalent to it:

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a\}.$$

Note: Some authors denote the equivalence class as $[a]$.

In the clock example with $n = 12$, each class consists of all the hours before or after noon which give the same clock-time:

$$\begin{array}{rcl} \overline{0} & = & \{\ldots, -12, 0, 12, 24, \ldots\} \\ \overline{1} & = & \{\ldots, -11, 1, 13, 25, \ldots\} \\ \overline{2} & = & \{\ldots, -10, 2, 14, 26, \ldots\} \\ & \vdots & \\ \overline{11} & = & \{\ldots, -1, 11, 23, 35, \ldots\}. \end{array}$$

Note that the next class $\overline{12} = \{\ldots, -12, 0, 12, 24, 36, \ldots\}$ is actually the same set as $\overline{0}$: that is, $\overline{12} = \overline{0}$, since $12 \equiv 0 \pmod{12}$. Similarly, $\overline{13} = \overline{-11} = \overline{1}$, etc. These classes have no common elements, and form a partition of the set $\mathbb{Z}$:

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \cdots \cup \overline{11}.$$

LEMMA: For fixed n, the following conditions are logically equivalent. For any $a, a' \in \mathbb{Z}$:

(i) The numbers are equivalent modulo n: $a \equiv a' \pmod{n}$.

(ii) The numbers have the same equivalence class modulo n: $\overline{a} = \overline{a'}$.

(iii) The numbers have the same remainder when divided by n:

$$a = qn + r \quad \text{and} \quad a' = q'n + r \quad \text{for} \quad 0 \leq r < n.$$

DEFINITION: We write $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, the set of all equivalence classes modulo n.

Modular operations. We would like to define addtion and multiplication operations on the classes in $\mathbb{Z}_n$ by adding or multiplying the integers in each class. However, there is a danger of ambiguity: we do not know which element in each class to add or multiply.

For the example of $n = 12$, we can try to compute in $\mathbb{Z}_{12}$ as follows:

$$\overline{3} + \overline{11} = \overline{14} = \overline{2}, \qquad \overline{3} \cdot \overline{11} = \overline{33} = \overline{9},$$

since $3 + 11 = 14 \equiv 2$ and $3 \cdot 11 = 33 \equiv 9 \pmod{12}$. Now, we could also take the alternative forms $\overline{3} = \overline{27}$ and $\overline{11} = \overline{-1}$, and do the same computation with these:

$$\overline{27} + \overline{-1} = \overline{26} = \overline{2}, \qquad \overline{27} \cdot \overline{-1} = \overline{-27} = \overline{9},$$

since $27 + (-1) = 26 \equiv 2$ and $27 \cdot (-1) = -27 \equiv 9 \pmod{12}$. The answers came out the same, but why? In fact, this will always happen:

PROPOSITION: Fix a modulus n. For $a, a', b, b' \in \mathbb{Z}$, suppose $a \equiv a'$ and $b \equiv b'$. Then:

$$a + b \equiv a' + b' \quad \text{and} \quad ab \equiv a'b'.$$

Proof. The hypothesis $a \equiv a'$ and $b \equiv b'$ means $n \,|\, (a{-}a')$ and $n \,|\, (b{-}b')$. Then:

$$n \,|\, (a{-}a') + (b{-}b') = (a{+}a') - (b{+}b'),$$

so by definition $a + b \equiv a' + b'$. Also, n divides the integer combination:

$$(a{-}a')b + (b{-}b')a' \;=\; ab - a'b + ba' - b'a' \;=\; ab - a'b'.$$

That is, $n \,|\, (ab - a'b')$, so by definition $ab \equiv a'b'$. Q.E.D.

This means that we can unambiguously add and multiply equivalence classes.

DEFINITON: For $\overline{a}, \overline{b} \in \mathbb{Z}_n$, define the sum $\overline{a} + \overline{b}$ to be $\overline{a{+}b}$, the class of the integer sum $a{+}b$. Define the product $\overline{a} \cdot \overline{b}$ to be $\overline{ab}$, the class of the integer product ab.

The proposition guarantees that if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, then $\overline{a{+}b}$ is the same class as $\overline{a'{+}b'}$, and the same for multiplication. The sum or product is specified as a unique class, and we say the operations are *well-defined*.

Properties of modular arithmetic. The addtion and multiplication on $\mathbb{Z}_n$ satisfy most of the usual group properties familiar from the real numbers. They are easily shown to be closed, associative, commutative, and distributive. Also $\overline{0}$ is the additive identity, and $\overline{-a}$ is the additive inverse of $\overline{a}$. Finally, $\overline{1}$ is the multiplicative identity.

The only group axiom which is not clear for $\mathbb{Z}_n$ is multiplicative inverses: any $\overline{a} \in \mathbb{Z}_n$ with $\overline{a} \neq \overline{0}$ should have some $\overline{b} \in \mathbb{Z}_n$ with $\overline{a} \cdot \overline{b} = \overline{1}$. (We denote such $\overline{b}$ by $\overline{a}^{\,-1}$.) Note that we cannot just take $\overline{b}$ to be $\overline{1/a}$ or $\overline{\frac{1}{a}}$, because we do not allow fractional modular numbers in $\mathbb{Z}_n$. Rather, we must find an *integer* $b \in \mathbb{Z}$ with $\overline{a} \cdot \overline{b} = \overline{1}$, meaning $ab \equiv 1 \pmod{n}$. This means $n \,|\, ab - 1$, or $ab - 1 = nk$ for some $k \in \mathbb{Z}$. If we rewrite this as $a(b) + n(-k) = 1$, we recognize this as a familiar problem: find an integer solution $(x, y) = (b, -k)$ to the equation:

$$ax + ny = 1, \qquad x, y \in \mathbb{Z}.$$

Using the Euclidean Algorithm, we can find a solution provided $\gcd(a,n) = 1$, but not otherwise. In other words, $\overline{b} = \overline{a}^{\,-1}$ exists if and only if a is relatively prime to n.

For the example of $\mathbb{Z}_{12}$, we can find $\overline{5}^{\,-1}$ by solving $5x + 12y = 1$. The Euclidean Algorithm gives $5(5) - 2(12) = 1$, or $5(5) + 12(-2) = 1$, so that $(b,k) = (x,-y) = (5,2)$. That is, $b = 5$, so $\overline{5}^{\,-1} = \overline{b} = \overline{5}$, and indeed: $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$. Thus, $\overline{5} \in \mathbb{Z}_{12}$ is analogous to $a = -1 \in \mathbb{R}$, which has $a^2 = 1$ and hence $a^{-1} = a$.

On the other hand, if we want $\overline{3}^{\,-1} \in \mathbb{Z}_{12}$, we would have to solve $3x + 12y = 1$. This is impossible since the left side is divisible by $\gcd(3,12) = 3$, but the right side 1 is not divisible by 3.

There is one case in which every non-zero element $\overline{a} \in \mathbb{Z}_n$ has an inverse $\overline{a}^{\,-1} = \overline{b} \in \mathbb{Z}_n$:

PROPOSITION: If $n = p$ is prime, then the non-zero classes $\mathbb{Z}_p \setminus \{\overline{0}\}$ with the multiplication operation form a commutative group.

Proof. As noted above, the only non-obvious condition is the existence of inverses. If $\overline{a} \neq \overline{0}$, then $a \not\equiv 0 \pmod{p}$, meaning $p \nmid a$. Since p is prime, this implies $\gcd(a,p) = 1$, and the Euclidean algorithm gives integers $x, y \in \mathbb{Z}$ with $ax + py = 1$. Then $ax - 1 = -py$, so $ax \equiv 1 \pmod{p}$, so $\overline{a} \cdot \overline{x} = \overline{1}$, and $\overline{a}^{\,-1} = \overline{x} \in \mathbb{Z}_p$. Q.E.D.

For example, for the prime modulus $n = p = 11$, we can check that:

$$\overline{1} \;=\; \overline{1} \cdot \overline{1} \;=\; \overline{2} \cdot \overline{6} \;=\; \overline{3} \cdot \overline{4} \;=\; \overline{5} \cdot \overline{9} \;=\; \overline{7} \cdot \overline{8} \;=\; \overline{10} \cdot \overline{10},$$

so every non-zero $\overline{a} \in \mathbb{Z}_{11}$ has a multiplicative inverse.

Modular algebra. Since $\mathbb{Z}_p$ (for p a prime) obeys all the usual axioms of addition and multiplication, almost everything we know about algebra carries over to $\mathbb{Z}_p$, provided we remember that $\overline{p} = \overline{0}$.

For example, the quadratic formula gives the solutions to the equation $ax^2 + bx + c = 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\,.$$

Now, if we want to solve an equation like:

$$x^2 + \overline{2}x + \overline{3} = 0 \quad \text{for} \quad x \in \mathbb{Z}_{11}\,,$$

we apply the quadratic formula to the number system $\mathbb{Z}_{11}$. We need the square root of $b^2 - 4ac = \overline{-8} = \overline{3}$, which by definition is some $y \in \mathbb{Z}_{11}$ with $y^2 = \overline{3}$. By trial and error we find $\overline{5}^2 = \overline{25} = \overline{3}$, so we take $y = \pm\overline{5}$. Also, dividing by $2a = \overline{2}$ means multiplying by $\overline{2}^{\,-1} = \overline{6}$. Thus we get:

$$x = (-b \pm y)(2a)^{-1} = (-\overline{2} \pm \overline{5})(\overline{6}) = \overline{18}, \overline{-42} = \overline{7}, \overline{2}.$$

Check: for $x = \overline{7}$, we have: $(\overline{7})^2 + \overline{2}(\overline{7}) + \overline{3} = \overline{66} = \overline{0}$, and similarly for $x = \overline{2}$.

Public-key cryptography. The coding methods used in internet security have one basic requirement: a *trap-door function*, namely a bijection $f : S \to S$ on some finite set S, such that f is publicly known and efficiently computable, but its inverse function is not practically computable without knowing a secret number, the so-called *private key.* That is, anyone can compute $f(a) = b$, but given only the function f and output b, no one can recover the input a with a reasonable amount of computing power, unless they have access to the private key number.

Public-key cryptography (conceived by Diffie and Hellmann in 1976) is a paradigm for secret communication over insecure channels. Everyone has a personal trap-door function f, which they reveal publicly; but they keep their private key d a secret. The sender puts a message into the form of a number $a \in S$, encodes it as $b = f(a)$ using the recipient's public function f, then transmits the encoded message b along an insecure connection to the recipient, who recovers the message a with her private key d. However, an attacker who intercepts the encoded message b will be unable to recover a, not knowing the private key. (The image is that the message a falls through the trap-door f and becomes $b = f(a)$; then it cannot climb out without the rope d.)

A baby example of a trap-door function is multiplication in $\mathbb{Z}_p$ for some large prime p. Fix some value $\overline{c} \in \mathbb{Z}_p$, and take $f(x) = \overline{c}x$ for $x \in \mathbb{Z}_p$. Given an output $\overline{b} = f(\overline{a}) = \overline{ca}$, to recover $\overline{a}$ we would need to perform the inverse of multiplication by $\overline{c}$, i.e. multiplication by $\overline{d} = \overline{c}^{\,-1}$. If we did not know the Euclidean Algorithm, it would be difficult to find $\overline{d}$, and thus not practical to recover $\overline{a} = \overline{db}$. We could then take $\overline{d}$ as the private key, and have a good trap-door function: no one could undo $f(x)$ unless they knew the secret value $\overline{d} = \overline{c}^{\,-1}$.

However, we do know the Euclidean algorithm, so we need a better trap-door function. The one used by the ubiquitous RSA coding method is not multiplication, but exponentiation in $\mathbb{Z}_n$. For appropriate positive integers n and c, we define the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f(x) = x^c$. The inverse function is very difficult to compute, even though everyone knows n and c. In fact, it is possible to find certain n and pairs (c, d) such that, for any output $\overline{b} = f(\overline{a}) = \overline{a}^{\,c}$, we recover the input as $\overline{a} = \overline{b}^{\,d}$. We then make public the function f, but keep d as the private key.

Such pairs (c, d) are found by analyzing the multiplicative structure of $\mathbb{Z}_n$, where the modulus is a product of two large primes: $n = pq$ with p, q prime. We say $\overline{a} \in \mathbb{Z}_n$ is *invertible* if there exists an inverse $\overline{a}^{\,-1}$, i.e. if $\gcd(a, n) = 1$. The set of invertible classes is denoted $\mathbb{Z}_n^\times$, and it forms a multiplicative group. The size of this group, the number of invertible elements, is $(p-1)(q-1)$. (Try to prove this.) Euler's Theorem says that, for any $\overline{a} \in \mathbb{Z}_n^\times$, we have $\overline{a}^{(p-1)(q-1)} = \overline{1}$. Now we use the Euclidean Algorithm to compute an inverse pair $cd \equiv 1 \pmod{(p-1)(q-1)}$, so that $cd = 1 + k(p-1)(q-1)$. Now we define:

$$f : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times, \qquad f(x) = x^c.$$

We choose our message-numbers to be $\overline{a} \in \mathbb{Z}_n^\times$, and $\overline{b} = f(\overline{a}) = \overline{a}^{\,c}$ can be reversed by:

$$\overline{b}^{\,d} \;=\; \overline{a}^{\,cd} \;=\; \overline{a}^{\,1+k(p-1)(q-1)} \;=\; \overline{a}\,\overline{1}^{\,k} = \overline{a}\,,$$

and we decode the message $\overline{a}$. However, an attacker who knows only $n = pq$ and c would not be able to find d, since that requires knowing $(p-1)(q-1) = n - p - q + 1$, which requires finding the factors p, q. But there is no known practical factoring algorithm for very large n.

Problems

1. Prove that the relation $\equiv$ modulo n has the properties stated on p. 1: reflexive, symmetric, and transitive.

2. The Lemma on p. 1 asserts that the three conditions (i), (ii), (iii) are all logically equivalent. A complete proof requires several independent parts.

a. Prove (i) $\Rightarrow$ (ii). That is, if $a \equiv a' \pmod{n}$, then the equivalence classes $\overline{a}$ and $\overline{a'}$ are the same set. Hint: You do not need to consider the definition of $a \equiv b$ or mess with divisibility: just use the basic properties of $\equiv$ in part (a) to show that $b \in \overline{a} \iff b \in \overline{a'}$.

b. Prove (ii) $\Rightarrow$ (i). That is, if $\overline{a} = \overline{a'}$ are the same set, then $a \equiv a' \pmod{n}$. Hint: Again, this follows immediately from the definiton of $\overline{a}$, without worrying about divisibility.

c. Prove (i) $\Rightarrow$ (iii): that is, if $a \equiv a' \pmod{n}$, then a and a' have the same remainder when divided by n. Hint: By the Division Lemma, we can always write $a = qn + r$ and $a' = q'n + r'$, and you must show that $r = r'$.

d. Prove (iii) $\Rightarrow$ (i): that is, if a and a' have the same remainder mod n, then $a \equiv a'$.

3. Consider the modular number system $\mathbb{Z}_9$

a. Write the complete 9×9 addition and mulitiplication tables. For example, we have $\overline{6} + \overline{7} = \overline{13} = \overline{4}$, so in the addtion table, the entry in the $\overline{6}$ row and $\overline{7}$ column should be $\overline{4}$. Hint: For simplicity, don't write the lines over the numbers in the table: just keep in mind that all the entries are classes in $\mathbb{Z}_9$, so that everything is modulo 9.

b. Looking at the multiplication table, determine which elements $\overline{a} \in \mathbb{Z}_9$ have inverses $\overline{a}^{-1}$. Explain how this matches the general rule for when $\overline{a}^{-1}$ exists at the top of p. 3.

c. Determine which elements have square roots. That is, for which $\overline{a} \in \mathbb{Z}_9$ is there some $\overline{b} \in \mathbb{Z}_9$ with $\overline{b}^2 = \overline{a}$?

d. Use the quadratic formula to solve the equation $x^2 + \overline{3}x + \overline{5} = \overline{0}$ for $x \in \mathbb{Z}_9$.

4. I have encoded a secret message by the following method. Each letter of my message is represented by a number using the obvious code A = 1, B = 2, ..., Z = 26, and also: comma = 27, period = 28, exclamation point = 29, question mark = 30, space = 31.

Next, I encrypt each number by the function $f : \mathbb{Z}_{31} \to \mathbb{Z}_{31}$ with $f(x) = \overline{7}x$. For example, the letter T is the 20th letter of the alphabet, and $f(\overline{20}) = \overline{7} \cdot \overline{20} = \overline{140} = \overline{16}$, so the encrypted number is 16.

The encrypted numbers of my message are:

$$4, 23, 22, 4, 2, 17.$$

Break this code and find the original message. That is, for each encrypted number $b = f(a)$, reverse the function f to find the original a, and look up its letter. Hint: What is the reverse operation of multiplying by $\overline{7}$ in $\mathbb{Z}_{31}$?