MAST-332 / COMP-367
Techniques in Symbolic Computation
Lecture 3 Notes:

Congruences (Ch. 5):

Congruence Modulo m (Ch. 5A)

Definition: two integers a and b are said to be ***congruent modulo m*** ,

$$a \equiv b \pmod{m} :$$

if m divides $a - b$, or equivalently, if $a = b + k \cdot m$, with some $k \in \mathbb{Z}$.

Note that $\boldsymbol{a \equiv 0 \pmod{m}}$ means that m divides a.
The number m is called ***modulus*** .

Examples:
$143 \equiv 3 \pmod{14}$
$143 \equiv 0 \pmod{13}$
$-5 \equiv 5 \pmod{10}$
$16 \equiv 31 \pmod{5}$

In Maple,

```
> 143 mod 14, 143 mod 13, -5 mod 10;
                                3, 0, 5                              (1.1.1)
> evalb(16 mod 5 = 31 mod 5);
                                 true                                (1.1.2)
>
```

All integers are congruent to each other modulo 1 (!). Therefore normally the modulus m should be a natural number larger than 1, i.e. $m \geq 2$:

A **congruence ('≡') modulo *m*** is an ***equivalence relation*** (~) on the set $\mathbb{Z}$, since it is

(1) ***Reflexive***: $a \equiv a \mod m$ for $\forall a \in$ (as $m \mid (a - a)$).

(2) ***Symmetric***: if $a \equiv b \pmod{m}$ **then** $b \equiv a \pmod{m}$:
(since if m divides (a-b) then m divides (b-a) as well).

(3) ***Transitive***: if $a \equiv b$ **and** $b \equiv c$ **then** $a \equiv c$
Proof: if $a \equiv b$ **and** $b \equiv c \pmod{m}$ **then** $a = b + k \cdot m$ **and** $b = c + n \cdot m$:
therefore $a = c + n \cdot m + k \cdot m = c + (n + k) \cdot m$ **and** $(n + k) \in \mathbb{Z}$

$\Rightarrow\ a \equiv c \ \mathbf{mod}\ m :$

Thus, a congruence modulo m divides the set $\mathbb{Z}$ of integers into *equivalence* classes (or ***Congruence classes*** in this case, studied in detail in the next chapter of this Lecture). The most commonly used representation of the equivalence classes is given by the set of the least residues modulo m, i.e. $R_m = \{0, 1, ..., m-1\}$:

Proposition 1: Let $m \geq 2$. Every integer number a is congruent modulo m to one and only one number in the set R_m :

The numbers in this set represent the residuals of the division of a on m , and are called the *least non-negative residues of a* (**mod** m).

These resudues have a notation 'a **mod** m'. So
13 mod 6 = 1,
-5 mod 9 = 4.

Using this notation, we can formulate the following proposition:

Proposition 2: $a \equiv b \ (\mathbf{mod}\ m)$ if and only if $a\ \mathbf{mod}\ m = b\ \mathbf{mod}\ m$.

Proof:
Let us denote
$a\ \mathbf{mod}\ m = r1$, **and**
$b\ \mathbf{mod}\ m = r2$:

$$\Rightarrow\ a = q1 \cdot m + r1 :$$
$$b = q2 \cdot m + r2 :$$
$$q1, q2 \in \mathbb{Z} :$$

(i) If $r1 = r2$ **then**

$$a - q1 \cdot m = b - q2 \cdot m \ \Rightarrow$$
$$(a-b) = q1 \cdot m - q2 \cdot m = m \cdot (q1 - q2)$$

Therefore $a \equiv b \ (\mathbf{mod}\ m)$:

(ii) If $a \equiv b \ (\mathbf{mod}\ m)$ **then**

$$a - b = m \cdot k \ (k \in \mathbb{Z}) :$$
$$\Rightarrow r1 - r2 - q1 \cdot m + q2 \cdot m = k \cdot m$$
$$\Rightarrow r1 = r2 + m \cdot (k + q1 - q2) :$$

......

(Continue: why then r1 = r2 ?)

Exercise (*class exercise*): New Year Day in the year 2006 fell on Sunday. On what day of the week
did New Year Day fall on in the year 2007 ?

Solution (class) **:**

Linear Congruencies and Bezout's Identity (Ch. 5E)

Solving congruences for unknowns:

Proposition 18: The congruence $a \cdot x \equiv b \pmod{m}$ is solvable iff (a,m) divides b.

Proof:
We need to find a solution to the equation $a \cdot x = b - y \cdot m$ with some integers x and y. This can be rewritten as $a \cdot x + m \cdot y = b$.
By Proposition 10 (p. 44), this Diophantine equation has a solution if and only if (a, m) divides b.

Exercise (# 47)**:**
Find a solution for the congruence $9\,x \equiv 24 \pmod{21}$:

Solution:

The GCD (9,21)=3, which divides 24. Therefore this congruence, equivalent to the Diophantine equation $9\,x + 21\,y = 24$, has a solution. Cancel this equation by 3. Then we have to solve $3\,x + 7\,y = 8$. Set up the Extended Euclid's Algorithm:

1. [0, 1, 7]
2. [1, 0, 3] (multiply by irem(7,3)=2 and subtract from the firts line)
3. [-2, 1, 1]

we can stop here since we have 1 in the last position of the last list, which corresponds to the equation
$-2 \cdot 3 + 7 \cdot 1 = 1$. Therefore $3 \cdot (-2 \cdot 8) + 7 \cdot 8 = 8$, which implies $x = -16$ is a solution for the initial congruence $9\,x \equiv 24 \pmod{21}$. Check:

```
> (9·(−16) −24) mod 21 = 0;
                                  0 = 0                                  (1.2.1)
```

To find all solutions of the given congruence, we have to add to this solution all the solutions of the congruence
$9\,x \equiv 0 \pmod{21}$
$\Rightarrow 3\,x - 7\,y = 0$
$\Rightarrow x0 = 7\,k,\ \ y = y0 = 3\,k.$

So the general solution is $\{x = -16 + 7\,k \mid k \in \mathbb{Z}\}$.
Note that this solution set can be also represented (equivalently) as
$\{x = -16 + 21 + 7\,k = 5 + 7\,k \mid k \in \mathbb{Z}\}$
which corresponds to the shift of k in those sets by 3.

Exercise (*class*):
Solve 10x≡ 14 (mod 15)

Solution:
....

Proposition 19

Proposition 19 (p. 86)**:** If $(a, m) = 1$ then the congruence $a \cdot x \equiv 1 \pmod{m}$ has a unique solution modulo *m*.

Proof:
The given congruence is equivalent to the Bezout's Indentity $a \cdot x + m \cdot y = 1$, which has a solution $x = r$ **and** $y = s$ because $(a, m) = 1$.
Assume now that there is another solution, x_1 **and** y_1 , so that $a \cdot x_1 + m \cdot y_1 = 1$. Then $a(r - x_1) + m(s - y_1) = 0$. Because $(a, m) = 1$, the only possibility is $(x_1 - r) = k \cdot m,\ k \in \mathbb{Z}$.
$\Rightarrow x_1 = r + k \cdot m \ \Rightarrow x_1 \equiv r \pmod{m}$:

NOTE: the solution $x{=}r$ to this congruence in the list R_m of the least non-negative residues represents the **inverse of *a* modulo *m***.

Exercise: Find a solution of $18\,x \equiv 12 \pmod{20}$ in the list R_{20}:
(Hint: cancel by 2, and use that 9 is the inverse of 9 (mod 10)).

Solution:

....

Systems of Congruences (*simple case*):

Let us now consider a specific problem:

Problem: Find a number *a* such that $a = s1 \pmod{m1}$ **and** $a = s2 \pmod{m2}$:

This problem is reduced to the following system of Diphantine equations:
$a = s1 + m1 \cdot k$, **and**
$a = s2 + m2 \cdot p$
where *k* and *p* are the integers that should be found.
This system corresponds to the Diophantine equation
$s1 + m1 \cdot k = s2 + m2 \cdot p$

which can be written in the 'standard' form
$m1 \cdot X + m2 \cdot Y = (s2 - s1)$
after denoting $k = X$ **and** $p = -Y$:
This equation will be consistent iff $d = (m1, m2)$ divides $(s2 - s1)$. After finding X and Y, a solution for *a* can be found from the first or the second of the initial equations of the system.

Example:
Find a number a such that $a = 1\ (\mathbf{mod}\ 3)$ **and** $a = 4\ (\mathbf{mod}\ 6)$

Solution:
The system of equations to solve is:
$a = 3\cdot k + 1$ **and**
$a = 6\cdot p + 4$:
This is reduced to $6\cdot p - 3\,k = 1 - 4$
After cancelling by 3, we find:
$2\,p - k = -1$:

We don't need to use here Euclid's algorithm because the equation is too simple to solve.
Say $\{p = 0, k = 2\,p + 1 = 1\}$ will be one possible solution. Another can be, say
$\{p = 1, k = 3\}$, etc.
In the first case the number $a = 3\cdot 1 + 1 = 6\cdot 0 + 4 = 4$.
For the second solution we will have $a = 3\cdot 3 + 1 = 6\cdot 1 + 4 = 10$.
Obviously, there will be infinitely many solutions for this problem.

Basic properties of congruences (Ch. 5B)

Proposition 4: Let $a, b, c, d, k\,, n \in \mathbb{Z}$ and m be a natural number .

(A) ***Multiplication by a scalar***:

If $a \equiv b\ (\mathbf{mod}\ m)$ **then** *also* $ka \equiv kb\ (\mathbf{mod}\ m)$:
Proof: since m divides $a - b$ **then** *also* m divides $ka - kb = k\cdot(a - b)$:

(B) ***Addition:***

If $a \equiv b\ (\mathbf{mod}\ m)$ **and** $c \equiv d\ (\mathbf{mod}\ m)$ **then** *also* $a + c \equiv b + d\ (\mathbf{mod}\ m)$:

(C) ***Multiplication of congruences:***

If $a \equiv b\ (\mathbf{mod}\ m)$ **and** $c \equiv d\ (\mathbf{mod}\ m)$ **then** *also* $a\cdot c \equiv b\cdot d\ (\mathbf{mod}\ m)$:

Proof: If $a \equiv b\ (\mathbf{mod}\ m)$ **and** $c \equiv d\ (\mathbf{mod}\ m)$ **then** $a = b + k\cdot m$ **and** $c = d + n\cdot m$:
Therefore
$a\cdot c = (b + k\cdot m)\cdot(d + n\cdot m) = b\cdot d + (b\cdot n + d\cdot k + k\cdot n\cdot m)\cdot m \equiv b\cdot d\ (\mathbf{mod}\ m)$:

Examples of congruences:

114 mod 11 $\equiv$ 26 mod 11 (= 4)
18 (mod 11) $\equiv$ 62 (mod 11) (=7)
Check the product .

> $114\cdot 18\ \mathbf{mod}\ 11 = 26\cdot 62\ \mathbf{mod}\ 11;$

$$6 = 6 \qquad \textbf{(1.3.1)}$$

>

Example: ***using properties of congruences*** (*simple case*):

Given $x + a \equiv d \ (\mathbf{mod}\ m)$, find x.

Solution:

Since $-a \equiv -a \ (\mathbf{mod}\ m)$, using addition property for congruences we find

$(x + a) - a \equiv d - a \ (\mathbf{mod}\ m) : \Rightarrow \ x \equiv d - a \ (\mathbf{mod}\ m) :$

Important:
The property of ordinary equality '=' that does not generally hold for congruences is the cancellation:
In general, if $k \cdot a \equiv k \cdot b$ (**mod** m), it is not generally true that also $a \equiv b \ (\mathbf{mod}\ m) :$

For example,
$(3 \cdot 1 \ \mathbf{mod}\ 9) \equiv (3 \cdot 4 \ \mathbf{mod}\ 9);$

$$3 \equiv 3 \tag{1.3.2}$$

However, 1 (mod 9) $\not\equiv$ 4 (mod 9) (!!).

Proposition 5: If $a \equiv b \ (\mathbf{mod}\ m)$ and d divides m, then $a \equiv b \ (\mathbf{mod}\ d) :$

Proof: ***i***f $\boldsymbol{m} = k \cdot d$ divides (a - b) (by the definition of congruences) then also d divides $(a - b)$:

Proposition 6: For all natural numbers k and integers a and b, if $a \equiv b \ (\mathbf{mod}\ m)$ **then**:

$a^k \equiv b^k \ (\mathbf{mod}\ m) :$

Proof: (*follows from the congruence multiplication property by ordinary induction*) .

Application of the exponentiation,

Property 6: residuals of large powers.

Examples:
(1) $12^{31} \ (\mathbf{mod}\ 13) \equiv ?$

Solution:
12 (mod 13) ≡ - 1 (mod 13). ⇒
$12^{31} \equiv (-1)^{31} \equiv -1 \ (\mathbf{mod}\ 13) \equiv 12 :$

(2) $6^{37}\ \mathbf{mod}\ 13 = ?$

Solution:

$$6^2 = 36 \equiv -3 \pmod{13}$$

$$\Rightarrow 6^6 = \left(6^2\right)^3 \equiv (-3)^3 = -27 \equiv -1 \pmod{13}:$$

$$\Rightarrow 6^{36} = \left(6^6\right)^6 \equiv (-1)^6 \equiv 1 \pmod{13}:$$

$$\Rightarrow 6^{37} = 6^{36+1} \equiv 1 \cdot 6 \pmod{13} \equiv 6 \pmod{13} = 6:$$

Exercise (*class*)**:**
Find 68^{105} **mod** 7;

***Solution*:**

....

(*Cases of cancellation*)

Proposition 16: If $ra \equiv rb \pmod{rm}$ **then** $a \equiv b \pmod{m}$:

Proof:

$$ra = rb + k \cdot rm = r \cdot (b + k \cdot m)$$

$$\Rightarrow a = b + k \cdot m$$

$$\Rightarrow a \equiv b \pmod{m}:$$

Proposition 17: If $ra \equiv rb \pmod{m}$ **and** $(r, m) = 1$ **then** $a \equiv b \pmod{m}$:

Proof:
Since $ra - rb = r \cdot (a - b)$ **and** m and r are coprime , the only possibility for m to divide $r(a - b)$ is that m must divide $(a - b)$, that is $(a - b) \equiv 0 \pmod{m} \Rightarrow a \equiv b \pmod{m}$:

Exercise (*class*)**:**
True or False? Justify

For any integer k>1, if $ka \equiv kb \pmod{7}$ **then** $a \equiv b \pmod{7}$:

***Solution*:**

Congruence Classes (Ch. 6):

Congruence Classes $\mathbb{Z}/\mathbf{m}\mathbb{Z}$ (Ch.6-B,C) :

Reminder:
Congruence modulo m , $a \equiv b \ (\mathbf{mod}\ m)$, satisfies all 3 equivalence relations, namely, it is:
reflexive $(a \equiv a)$:
symmetric (if $a \equiv b$ **then** $b \equiv a$):
transitive (if $a \equiv b$ **and** $b \equiv c$ **then** $a \equiv c$:).

Therefore, as any equivalence relation on a set, it ***partitions*** the set of integers $\mathbb{Z}$ onto distinct sets of equivalence classes, called ***congruence classes modulo m***, and denoted $[\boldsymbol{a}]_{\boldsymbol{m}}$.
Thus, $[a]_m = \{a + k \cdot m \mid k \in \mathbb{Z}\}$.

Examples:

$[1]_2 = \{ \ldots\ldots -5, -3, -1, \mathbf{1}, 3, 5, 7 \ldots\} \quad (\boldsymbol{odd})$:

$[0]_2 = \{ \ldots -4, -2, \mathbf{0}, 2, 4 \ldots\} \quad (\boldsymbol{even})$:

$[2]_2 = \{ \ldots -4, -2, 0, \mathbf{2}, 4, 6 \ldots\} \quad (\boldsymbol{even})$:

$[5]_4 = \{ \ldots -7, -3, 1, \mathbf{5}, 9, 13, 17 \ldots\}$:

$[-5]_3 = \{ \mathbf{-5}, -2, -8, 1, -11, 4, \ldots\}$

Note that in the congruence classes may look different but in fact be the same. In the examples above it is clear that $[0]_2 = [2]_2$: are both sets of even integers. More generally, congruence classes $[a]_m$ and $[a + p \cdot m]_m \ (p \in \mathbb{Z})$ represent the same set, so $[a]_m = [a + p \cdot m]_m$.

Proposition 1: For a **and** b **in** $\mathbb{Z}$, $a \equiv b \ (\mathbf{mod}\ m)$ if and only if $[a]_m = [b]_m$
(i.e. iff they are in the same congruence class modulo m).

Any number in $\mathbb{Z}$ is in ***one*** and ***only one*** congruence class modulo m. If we know that some integer $c \in [a]_m$ **and** $c \in [b]_m$, because of the *transitivity* property of congruence classes this means that $[a]_m = [b]_m$:
The set $\mathbb{Z}$ is partitioned by **mod** m into m disjoint subsets $[a]_m$, $(a = 1, \ldots m)$

Definition: $\boldsymbol{\mathbb{Z}/m\mathbb{Z}} = \{ [a]_m \mid a = 1, \ldots m \}$ is the set of all congruence classes modulo m.

For example, we can write

$\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$, **or** $= \{[1]_3, [2]_3, [3]_3\}$, **or** $= \{[-1]_3, [4]_3, [0]_3\}$,

because
$[0]_3 = [3]_3$:
$[1]_3 = [4]_3$:
$[-1]_3 = [2]_3$:

Introduction of congruence classes and partition of $\mathbb{Z}$ into $[a]_m$ allows us to define arithmetic operations on $\mathbb{Z}/\mathrm{m}\mathbb{Z}$ very similar to ordinary integer numbers where instead of writing congruence notation ' $\equiv$ (mod m) ' we can use just the equation sign '=' .

From Chapter 5 we know that congruence modulo m respects addition and multiplication operations. In the language of sets representing congruence classes this corresponds to the following properties of arithmetic operations on congruence classes:

$(\mathbf{1})$ $\boldsymbol{[a]_m + [b]_m = [a+b]_m}$ **:**
$(\mathbf{2})$ $\boldsymbol{[a]_m \cdot [b]_m = [a \cdot b]_m}$ **:**
$(\mathbf{3})$ $\boldsymbol{k \cdot [a]_m = [k \cdot a]_m}$ **:**

The last operation (multiplication by a scalar, an integer *k*), when applied with $k = -1$, results in the definition of negative of the congruence $[a]_m$:
$\boldsymbol{-\ [a]_m = [-a]_m}$ **:**

Arithmetics on Congruence Classes: ***Examples***

$[7]_{12} + [9]_{12} = [16]_{12} \left(= [4]_{12} \right)$:

$[7]_{12} \cdot [9]_{12} = [63]_{12} \left(= [3]_{12} \right)$:

$3 \cdot [5]_9 - [4]_9 \cdot [6]_9 = [3 \cdot 5 - 4 \cdot 6]_9 = [-9]_9 = [0]_9$:

Note that the congruence classes $[0]_m$ **and** $[1]_m$ are special, because for any congruence class $[a]_m$ we have the following properties:
(A) $\boldsymbol{[a]_m + [0]_m = [a]_m}$ **:**
(B) $\boldsymbol{[a]_m \cdot [0]_m = [0]_m \cdot [a]_m = [0]_m}$ **:**
(C) $\boldsymbol{[a]_m \cdot [1]_m = [1]_m \cdot [a]_m = [a]_m}$ **:**

With this definition of arithmetic operations we can introduce addition and multiplication tables which will be restricted to only *m* classes of $\mathbb{Z}/m\mathbb{Z}$. For example the addition table for m=5 arithmetic on congruence classes $\mathbb{Z}/5\mathbb{Z}$ looks like this:

(**mod** 5)	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Example: '*casting out nines*'.

Using the properties of addition we can derive a test for divisibility of an integer by 9.
First, let us represent an (n+1)-digit number a in the base 10 as

$$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \ldots + r_1 \cdot 10 + r_0 = \sum_{k=0}^{n} r_k \cdot 10^k$$

Then we use the properties (1)-(3) and the fact that $[10^k]_9 = \left([10]_9\right)^k = [1]_9^k = [1]_9$ to derive

$$[a]_9 = \sum_{k=0}^{n} \left[r_k \cdot 10^k\right]_9 = \sum_{k=0}^{n} \left[r_k\right]_9 \cdot [10^k]_9 = \sum_{k=0}^{n} \left[r_k\right]_9 \cdot [1]_9 = \sum_{k=0}^{n} \left[r_k\right]_9$$

Thus, the congruence class of any natural number a $(\mathbf{mod}\ 9)$ is equal to the sum of the digits of a $(\mathbf{mod}\ 9)$: In particular, a number is divisible by 9 iff the sum of its digits is divisible by 9.

Solving congruence equations by choosing a 'convenient' representation for $[a]_m$:

Although the set of congruence classes $\left\{[0]_m, [1]_m, \ldots., [m-1]_m\right\}$ represents completely $\mathbb{Z}$/m$\mathbb{Z}$ (as discussed below), it is sometimes useful to use different forms of representing congruence classes for solving different problems.

Examples:

(A)

Solve the equation $[x]_{31}^2 = [2]_{31}$:

Solution:

We can try to find a solution by looking at different representations of the class $[2]_{31}$ trying to find a number that is a square of some integer:

```
> class2mod31:=[seq(2+31*k,k=0...10)];
```

$$class2mod31 := [2, 33, 64, 95, 126, 157, 188, 219, 250, 281, 312] \qquad \textbf{(2.1.1)}$$

```
> map(sqrt, class2mod31);
```

$$\left[\sqrt{2}, \sqrt{33}, 8, \sqrt{95}, 3\sqrt{14}, \sqrt{157}, 2\sqrt{47}, \sqrt{219}, 5\sqrt{10}, \sqrt{281}, 2\sqrt{78}\right] \qquad \textbf{(2.1.2)}$$

We can see from this output that there is such representation, namely $[2]_{31} = [64]_{31}$:
Because the equation $[x]_{31}^2 = [2]_{31}$ is equivalent to $[x]_{31}^2 = [64]_{31} = [8]_{31}^2$, $x = 8$ solves the given equation.
We cannot, however, claim whether there are other solutions to this equation or not (to answer that question, we will need a more consistent theory based on polynomial algebra).

Note that in modular algebra we can find a real-value solution to quadratic equations with formally negative right-hand side, like $[x]_{31}^2 =- [29]_{31}$, since

$-[29]_{31}=[-29]_{31}=[2]_{31}=[64\ ]_{31}:$

(B)

Solve $[3]_5 \cdot [x]_5=[2]_5:$

Solution:
We can try to find a representative of $[2]_5$ in the form of a number divisible by 3.
Observe that $[2]_5=[12]_5=[3]_5\cdot[4]_5:$ Therefore $x=4$ solves the given equation.

Another way is to write $[3]_5=[-2]_5=-[2]_5$. Therefore,
$[2]_5=[3]_5\cdot[x]_5=-[2]_5\cdot[x]_5=[2]_5\cdot[-x]_5$, implying $x=-1$.
Does it, however, represent a different solution? The answer is negative since $[-1]_5=[4]_5:$

Exercise (*class)*: Solve the equation $[a]_m\ [x]_m=[b]_m$ by finding convenient representatives for $[a]$ **and** $[b]$.
Is the solution unique?

(A) $[6]_{10}\cdot[x]_{10}=[4]_{10}$.

***Solution*:**

(B) $[11]_{13}\cdot[x]_{13}^2=[7]_{13}:$
(HINT: first try to bring the equation to the form $[x]_{13}^2=[a]_{13}$).

***Solution*:**

>

Complete sets of Representatives (C6.D)

Definition: A set $R=\{r_1, r_2, \ldots, r_m\}$ such that every integer in $\mathbb{Z}$ is congruent modulo ***m*** to one and only one of the numbers r_i in the set is called a complete set of representtatives for $\mathbb{Z}$/m$\mathbb{Z}$.

In other words, if R is a complete set of representatives then $\mathbb{Z}/\mathrm{m}\mathbb{Z} = \left\{ [r_1]_m, [r_2]_m, \ldots, [r_m]_m \right\}$:

The set of least non-negative residues $\{0, 1, \ldots, m-1\}$ is one of such complete sets of representatives.

Another set often used is $\{1, 2, \ldots., m\}$; obviously $[m]_m = [0]_m$.

More genral, any set of m consecutive numbers is a complete set of representatives since modulo m such set is reduced to the set of least non-negative residues.

Theorem 3: If m is a prime number then there exists some integer b, called *primitive root modulo m*, such that $\left\{0, b, b^2, \ldots, b^{m-1}\right\}$ is a complete set of representatives for $\mathbb{Z}/m\mathbb{Z}$.

Examples:

(A) For m=5, the numbers 2 and 3 are primitive roots. Check:

```
> R:= [0,seq(2^i,i=1..4)];
                              R := [0, 2, 4, 8, 16]                          (2.2.1)
> R mod 5;
                                 [0, 2, 4, 3, 1]                             (2.2.2)
> R2 := [0, seq(3^i, i = 1 ..4)] mod 5;
                              R2 := [0, 3, 4, 2, 1]                          (2.2.3)
```

(B) For m=17, the numbers b=3, 5, 6 are (some of) the primitive roots. For example, for the 16 first powers of b=3 we have:

```
> residues := [seq(3^i, i = 1 ..16)] mod 17;
  powers   := [seq(i, i = 1 ..16)]
              residues := [3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]
              powers := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]   (2.2.4)
> nops(convert(residues, set));
                                      16                                     (2.2.5)
>
```

The list 'powers' actually represents the *log to base 3* of $(n = 3^r)$ the congruence class of which is given in the list 'residues'. The table produced by these two lists can be used for effective modular calculations on polynomials.

Example: Let $f(x) = x^4 + 5 \cdot x^3 + 8 \cdot x^2 + x + 15$, and we want to compute $f(12)$ modulo 17.

Solution: From the *log to base 3* conversion table we have $[12]_{17} = [3^{13}]_{17}$.

Using also the properties

$[a \cdot b]_m = [a]_m \cdot [b]_m$,

$[a^n]_m = [a]_m^n$ **and**

$\left([a]_m^n\right)^k = [a]_m^{n \cdot k}$:

we find in $\mathbb{Z}/17\mathbb{Z}$

$$[f(12)]_{17} = 12^4 + 5\cdot 12^3 + 8\cdot 12^2 + 12 + 15 \ (\textbf{mod}\ 17)$$
$$= 3^{13\cdot 4} + 3^5\cdot 3^{13\cdot 3} + 3^{10}\cdot 3^{13\cdot 2} + 12 + 15 \ (\textbf{mod}\ 17)$$
$$= 3^{3\cdot 16+4} + 3^{2\cdot 16+12} + 3^{2\cdot 16+4} + 27 \ (\textbf{mod}\ 17)$$
$$= 3^4 + 3^{12} + 3^4 + 27 \ \ (\textbf{mod}\ 17)$$

In the last transformation we used that $3^{16} \equiv 1$ **mod** 17. Using again the numbers in the log conversion table, we find
$[f(12)]_{17} = 13 + 4 + 13 + 27 = 57 = 6 \ (\textbf{mod}\ 17)$.

Question: (class) How can we compute $f(158)$ **mod** 17 ? (The argument is larger than 17).

Solution:

Units

For any rational number $a \in \mathbb{Q}$ except 0 we can find $b \in \mathbb{Q}$ such that $a\cdot b = 1$.
The numbers *a* and *b* are called (*multiplicative*) *inverse*s of each other.

For integers, however, only two numbers have inverse. Namely, the equation $b\cdot a = 1$ has a solution for only a=1 ($b = 1$) and $a = -1$ ($b = -1$). For all other integers the solution is not an integer but a fraction.

What is the case with modular arithmetic? Let us try to find a solution to $a\cdot b = 1 \ (\textbf{mod}\ m)$.

Definition: The congruence classes $[a]_m$ that have inverses are called ***units.***

Note first that $[1]_m$ is the ***multiplicative identity*** of $\mathbb{Z}$/m$\mathbb{Z}$ very similar to the number 1 for integer numbers: $[a]_m\cdot[1]_m = [a]_m$.
There cannot be any other congruence class in $\mathbb{Z}$/m$\mathbb{Z}$ that plays a similar role. Indeed, if there is some class $[e]_m \in \mathbb{Z}$/m$\mathbb{Z}$ such that $[e]_m\cdot[a]_m = [a]_m$, then we would have
$[e]_m\cdot[1]_m = [1]_m = [e]_m$.

What are the units of $\mathbb{Z}$/m$\mathbb{Z}$? Or else, which classes do have inverses and which do not?

The answer comes from the analysis of the congruence $b\cdot a \equiv 1 \ (\textbf{mod}\ m)$:
This is equivalent to equation $\boldsymbol{b\cdot a + k\cdot m = 1}$**,** which is the Bezout identity for the given a and m in terms of unknowns b and k. The Bezout Identity theorem states that solution exists if and only if $(a, m) = 1$!

Therefore,
Theorem 5: In $\mathbb{Z}/\text{m}\mathbb{Z}$, $[a]_m$ is a unit if and only if the numbers a and m are coprime.

Corollary 6: The number of units in $\mathbb{Z}/\text{m}\mathbb{Z}$ is equal to number of least positive residues coprime to m.

Definition: The set of all congruence classes representing units in $\mathbb{Z}/\text{m}\mathbb{Z}$ is called ***complete set of units*** U_m.

Example:
in $\mathbb{Z}/5\,\mathbb{Z}$, $U_5 = \{[1], [2], [3], [4]\}$:
in $\mathbb{Z}/9\,\mathbb{Z}$, $U_9 = \{[1], [2], [4], [5], [7], [8]\}$:

Definition: The number of elements in U_m is a function called ***Euler's phi function*** φ(m).

Note that if $[a]$ **and** $[b]$ are units in $\mathbb{Z}/\text{m}\mathbb{Z}$, then also $[ab]$ is a unit (i.e. is invertible). Indeed, if $[a][a'] = [1]$ **and** $[b][b'] = [1]$ **then** $[a\cdot b]\cdot[a'\cdot b'] = [ab\cdot a'b'] = [aa']\cdot[bb'] = [1][1] = [1]$.

From this observation follows that the converse of the Primitive Root Theorem is also true:

Theorem: If there exists a primitive root for a modulus m, then m is prime.

Proof: Assume that b is a primitive root of $\mathbb{Z}/\text{m}\mathbb{Z}$, i.e. that $R = \{0, b, b^2,..., b^{m-1}\}$ is a complete set of representatives. Then b is a unit because $[b^k]_m = [1]_m$ for some $1 \le k \le m-1$, which implies that b and m are coprime. Note that product of units is also a unit. Therefore also each of the powers of b is a unit. The number of such powes in the set R is (m-1), and they represent different congruence classes from 1 to (m-1) coprime to m. This is only possible if m is prime.

Using inverses of inits, it is easy to solve equations in $\mathbb{Z}/m\mathbb{Z}$ involving units as coefficients. Say, the equation $[3]_{17}X = [11]_{17}$ can be immediately solved if we note that $[6]_{17}$ is the congruence class inverse to $[3]_{17}$. Therefore by multiplying the equation by the inverse of [3], we find in $\mathbb{Z}/17\,\mathbb{Z}$

$$[6]\cdot[3]\cdot X = [6]\cdot[11] \;\Rightarrow\; [1]\cdot X = [66]$$
$$\Rightarrow\; X = [15]_{17}$$

Question: Is the found solution unique?
Answer: Yes.
(*Class*: Explain why...)

Proposition: Every unit has one and only one inverse in $\mathbb{Z}_m$.
Proof: ... (class)

Exercise 1 (class)**:**
Decide which elements in $\mathbb{Z}/12\mathbb{Z}$ have inverses, and for each such element find its inverse.

Solution:

Exercise 2 (class)**:**
Use the results found in Exercise 1 above to solve the equation
$[11]_{12}X = [6]_{12}$

Solving (linear) equations in $\mathbb{Z}_m$

Example 1: Consider the following equation in $\mathbb{Z}_{16}(= \mathbb{Z}/16\,\mathbb{Z})$:
$[6]_{16}X = [14]_{16}$

In $\mathbb{Z}/16\mathbb{Z}$ the class $[6]_{16}$ is not a unit (why ?), therefore we cannot solve this equation by finding its inverse. Still, we can find a solution by observing that [14]=[30]=[6][5], so $X = [5]$ is one solution.

There also is another solution that is found by observing that
$[14]_{16} = [14 - 2\cdot 16]_{16} = [-18]_{16} = [6]_{16}\cdot[-3]_{16} = [6]_{16}[13]_{16}$.
So X=[13] is another solution.

This implies that in the equation $aX = b$ in $\mathbb{Z}/\mathrm{m}\mathbb{Z}$, if a is not a unit then the solution may not be unique.

Proposition: Let $X = x_0$ be a solution of *inhmogeneous* equation $aX = b$ in $\mathbb{Z}/\mathrm{m}\mathbb{Z}$. Let N be the set of all solutions t of the *homogeneous* equation $aX = 0$. Then every solution z of the equation $aX = b$ has the form $z = x_0 + t$ where $t \in N$.

Proof: If z is a solution of $aX = b$, then $az = b$. Also $a\cdot x_0 = b$. Because addition and distribution properties hold in $\mathbb{Z}/\mathrm{m}\mathbb{Z}$, by subtracting the two equations we find
$a\cdot z - a\cdot x_0 = b - b = 0 \;\Rightarrow\; a\cdot\left(z - x_0\right) = 0 \;\Rightarrow\; \left(z - x_0\right) = t \in N$
Thus, any solution of nonhomogeneous equation (with b) is in the form $z = x_0 + t$.

Example 1 (continued).
Consider again the equation in $\mathbb{Z}/16\mathbb{Z}$:

$[6]X=[14]$

x_0=[5] is a solution of this equation. To find all solutions, we solve the homogeneous equation [6] X = [0]. In $\mathbb{Z}/16\mathbb{Z}$ this implies an equation
$\mathbf{6 \cdot x = 16 \cdot y}$
with integers x and y. We can cancel the GCD factor (6,16)=2 from this equation to arrive at

$\mathbf{3 \cdot x = 8 \cdot y}$

Because (3,8)=1, this equation implies that x is a multiple of 8 and y is a similar multiple of 3:
$x=8\ k$ **and** $y=3\ k$: so that $3 \cdot 8\ k = 8 \cdot 3\ k$ *where* $k \in \mathbb{Z}$:

In terms of $X=[x]_{16}=[8\ k]_{16}$ we have two congruence classes solving the homogeneous equation,
$N=\{[0], [8]\}_{16}$:
Thus, we have only two solutions for the inhomogeneous equation,
$x_0=[5]+[0]=[5]$:
$x_1=[5]+[8]=[13]$:

Note that the total number of solutions of the inhomogeneous equation is equal to GCD (*a,m*) = 2.

Proposition: If d=(a,m) then the general solution of $[a]X=[0]$ in $\mathbb{Z}$/m$\mathbb{Z}$ is $X=\left[\frac{m}{d} \cdot k\right]$ where $k=0, 1, ..., d-1$.

Proof: the equation to solve in $\mathbb{Z}$/m$\mathbb{Z}$ can be written in $\mathbb{Z}$ as $a \cdot x = m \cdot y$.
Given $d=(a, m)$, we can represent a and m as $a=d \cdot a_0$ **and** $m=d \cdot m_0$ with a_0 **and** m_0 coprime.
Thus, we come to
$a_0 \cdot x = m_0 \cdot y$
the general solution of which is $x=m_0 k, y=a_0 k$. Thus, the solution is
$x=m_0 \cdot k=\frac{m}{d} \cdot k$, $k \in \mathbb{Z}$
In terms of congruence classes we have therefore exactly d solutions coresponding to
$k=0, 1,..., d-1$. The set N is
$N=\left\{[0]_m, \left[\frac{m}{d}\right]_m, \left[\frac{m}{d}2\right]_m, ..., \left[\frac{m}{d}(d-1)\right]_m\right\}$

Example 3: In $\mathbb{Z}/90\mathbb{Z}$, the equation
[36] X = [54]

has a solution u=[4]. The set of all solutions can be found by solving the homogeneous equation
[36] X = [0]

Because (36, 90) = 18, we are looking for 18 solution classes for the latter equation in $\mathbb{Z}/90\mathbb{Z}$.
Since the 90/18 = 5, we have the following congruences in the set N:
$N=\{[0], [5], [10], ..., [80], [85]\}$.

This results in 18 following solutions for the inhomogeneous equation:
X= [4]+N= {[4], [9], ..., [89]}.

Example 4: Find all solutions of the equation in $\mathbb{Z}/90\mathbb{Z}$:

$$[7]\ X = [54].$$

Solution: Since GCD (7,90) = 1, [7] is invertible. The inverse b can be found from the equation $b\cdot 7 = 1\ (\textbf{mod}\ 90)$, which corresponds to $7\ b + 90\ k = 1$. In general, the Euclid's algorithm can be applied to find b. In this case, however, we can see that $7\cdot 13 = 91$, so (k=-1, b= 13) solves this Bezout
equation. Thus , $[13]_{90}$ is the inverse of $[7]_{90}$. Using this inverse, we find the solution X for the given
inhomogeneous equation:
$[13][7]$ X = [1] X = X = [13][54] = [702] = [72]. (mod 90).

The homogeneous equation [7]X=[0] has only one solution in $\mathbb{Z}/90\mathbb{Z}$, namely X= $[0]_{90}[13]_{90} = [0]_{90}$:
Therefore the congruence class $[72]_{90}$ represents the only solution of the given inhomogeneous equation.

Exercise: (*class*)
Find all solutions of the following equations:

(A) $[25]X = [36]$ in $\mathbb{Z}_{15}$.

(B) $[36]X = [6]$ in $\mathbb{Z}_{45}$

Solution:

(A) The congruence class $[36]_{15} = [6]_{15}$, therefore the given equation is equivalent to
$25\cdot X + 15\cdot Y = 6$:
The GCD (25,15) = 5; it does not divide 6, so the equation does not have a solution.

(B).