Math 3 (VE3020) — Exercises, week 3

1. Write a complete residue system modulo 11 composed entirely of multiples of 3.

Recall the definition that the set $\{x_1, \dots, x_m\}$ is called a complete residue system modulo m if for every integer y there is one and only one x_j such that x_j is the residue in $y \equiv x_j \mod m$.

We now want to construct a set of $m = 11$ integers that are divisible by 3, but not congruent with each other mod 11.

$3 \equiv 3 \mod 11$	$15 \equiv 4 \mod 11$	$27 \equiv 5 \mod 11$
$6 \equiv 6 \mod 11$	$18 \equiv 7 \mod 11$	$30 \equiv 8 \mod 11$
$9 \equiv 9 \mod 11$	$21 \equiv 10 \mod 11$	$0 \equiv 0 \mod 11$
$12 \equiv 1 \mod 11$	$24 \equiv 2 \mod 11$	

We see that every element in the set
$S = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}$
is divisible by three.

S contains 11 elements s_i and $s_i \not\equiv s_j \bmod 11$,
when $i \neq j$. Thus for every integer y,
there is only one element in S that
satisfies $y \equiv s_i \bmod 11$,

2. Write any reduced residue system for modulus 12.

Recall that a reduced residue system mod m can be obtained from a complete residue system mod m by removing elements that are not relatively prime to m, i.e. for which hold $(x, m) \neq 1$.

Let us choose our complete residue system mod 12 to be $\{1, 2, 3, \ldots, 12\}$

Now $(1,12) = (5,12) = (7,12) = (11,12) = 1$

but $(2,12) = 2$, $(3,12) = 3$, $(4,12) = 4$,
$(6,12) = 6$, $(8,12) = 4$, $(9,12) = 3$,
$(10,12) = 2$, $(12,12) = 12$

Our reduced residue system mod 12 is thus $\{1, 5, 7, 11\}$.

3. Evaluate the Euler's ϕ- function $\phi(m)$ for $m = 1, 2, \ldots, 11$

$\phi(m)$ is the number of elements in a reduced residue system mod m, i.e. $\phi(m)$ is the number $0 < a \leq m$ for which $(a, m) = 1$.

Let us write some reduced residue classes for $m = 1, \ldots, 11$ and deduce $\phi(m)$

$m = 1$: $\{1\}$ $\Rightarrow \phi(1) = 1$

$m = 2$ $\{1\}$ $\Rightarrow \phi(2) = 1$

$m = 3$ $\{1, 2\}$ $\Rightarrow \phi(3) = 2$

$m = 4$ $\{1, 3\}$ $\Rightarrow \phi(4) = 2$

$m = 5$ $\{1, 2, 3, 4\}$ $\Rightarrow \phi(5) = 4$

$m = 6$ $\{1, 5\}$ $\Rightarrow \phi(6) = 2$

$m = 7$ $\{1, 2, 3, 4, 5, 6\}$ $\Rightarrow \phi(7) = 6$

$m = 8$ $\{1, 3, 5, 7\}$ $\Rightarrow \phi(8) = 4$

$m = 9$ $\{1, 2, 4, 5, 7, 8\}$ $\Rightarrow \phi(9) = 6$

$m = 10$ $\{1, 3, 7, 9\}$ $\Rightarrow \phi(10) = 4$

$m = 11$ $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $\Rightarrow \phi(11) = 10$

Note that since we are dealing with small integers m here, it is easy to check their prime decomposition $m = \prod_p p^{\alpha(p)}$ and use the Theorem from the lectures that allows you to write $\phi(m) = \prod_{p|m} (p^{\alpha(p)} - p^{\alpha(p)-1})$.

For example

$m = 6 = 2^1 \cdot 3^1 \Longrightarrow \phi(6) = (2^1 - 2^0)(3^1 - 3^0) = 2$

$m = 8 = 2^3 \Longrightarrow \phi(8) = (2^3 - 2^2) = 4$.

(4.) Claim: If p is a prime number and $a^2 \equiv b^2 \mod p$, then $p \mid (a+b)$ or $p \mid (a-b)$.

Proof:

Now $a^2 \equiv b^2 \mod p$ means by definition that $p \mid (a^2 - b^2)$. This means that $a^2 - b^2 = px$ for some $x \in \mathbb{Z}$.

Note that $a^2 - b^2 = (a+b)(a-b)$.

Let us write a proof by contradiction by imposing $p \nmid (a+b)$ and $p \nmid (a-b)$. Because the prime factoring of an integer is unique p is not a part of $(a+b) = \prod_{p'} p'^{\alpha(p')}$ and $(a-b) = \prod_{p''} p''^{\beta(p'')}$, i.e. $\alpha(p'=p) = \beta(p''=p) = 0$.

However $px = a^2 - b^2 = \prod_{p'} p'^{\alpha(p')} \prod_{p''} p''^{\beta(p'')}$, meaning at least one of $\alpha(p)$ or $\beta(p)$ is not 0, which is a contradiction. $\square$

5. Find all integers that satisfy simultaneously $x \equiv 2 \bmod 3$, $x \equiv 1 \bmod 5$, and $x \equiv 5 \bmod 2$.

Let's use the same notation as in the lecture notes for the Chinese remainder theorem:

$a_1 = 2, \quad a_2 = 1, \quad a_3 = 5,$

$m_1 = 3, \quad m_2 = 5, \quad m_3 = 2, \quad m = m_1 m_2 m_3 = 30$

It is important to check that all m_i are relatively prime in pairs for the Chinese remainder theorem to hold:

$(3,5) = (3,2) = (5,2) = 1.$ OK!

Now $(m_2 m_3, m_1) = (10, 3) = 1$, so we use the Euclidean algorithm to find b and c that satisfy $b(m_2 m_3) + c m_1 = 1$

Let's tabulate the results. (These numbers are easy enough that the Euclidean algorithm is not necessary but it is still good practice.)

$$m_2 m_3 = q_1 \, m_1 + r_1$$
$$10 = 3 \cdot 3 + 1$$

This is already actually the form that we want, but we could construct this by using the Euclidean algorithm:

$$m_1 = q_2 \, r_1 + r_2$$
$$3 = 3 \cdot 1$$

We could also work backwards by choosing $r_{-1} = m_2 m_3 = 10$, in which case

$$m_2 m_3 = q_{-1} \, m_1 + r_{-1}$$
$$10 = 0 \cdot 3 + 10$$

Similarly, we could write $r_0 = m_1 = 3$

$$0 \cdot m_1 m_2 = q_0 \, m_1 + r_0$$
$$0 \cdot m_1 m_2 = -1 \cdot 3 + 3$$

We can multiply the equation

$$0 \cdot m_1 m_2 = q_0 m_1 + r_0$$
$$0 \cdot m_1 m_2 = -1 \cdot 3 + 3$$

by $q_1 = 3$ and substract it from

$$m_2 m_3 = q_{-1} m_1 + r_{-1}$$
$$10 = 0 \cdot 3 + 10$$

to obtain

$$10 - 3 \cdot 0 = 0 - 3 \cdot (-1 \cdot 3) + 10 - 3 \cdot 3$$
$$\Rightarrow \quad 10 = 3 \cdot 3 + 1$$

So we have constructed our

$$b\, m_2 m_3 + c\, m_1 = 1$$

with $b = 1$ and $c = -3$

For the Chinese remainder theorem, we now choose $b_1 = 1$

Similarly $(m_1 m_3, m_2) = (3 \cdot 2, 5) = (6, 5) = 1$ and we want to solve $b_2 m_1 m_3 + c_2 m_2 = 1$, i.e. $b_2 \cdot 6 + c_2 \cdot 5 = 1$.

We see that (you can also use the Euclidean algorithm) $1 \cdot 6 - 1 \cdot 5 = 1$ is a solution so we choose $b_2 = 1$

Finally $(m_1 m_2, m_3) = (3 \cdot 5, 2) = (15, 2) = 1$ so we're after solutions $b_3 m_1 m_2 + c_3 m_3 = 1$, i.e. $b_3 \cdot 15 + c_3 \cdot 2 = 1$.
Here $1 \cdot 15 - 7 \cdot 2 = 1$ is a solution so we choose $b_3 = 1$

To recap, we have obtained
$a_1 = 2, \quad a_2 = 1, \quad a_3 = 5,$
$m_1 = 3, \quad m_2 = 5, \quad m_3 = 2, \quad m = m_1 m_2 m_3 = 30$
$b_1 = b_2 = b_3 = 1$

The Chinese remainder theorem tells us that the solutions of the simultaneous congruences is of the form

$$x_0 = \sum_{j=1}^{3} \frac{m}{m_j} b_j a_j = \frac{30}{3} \cdot 1 \cdot 2 + \frac{30}{5} \cdot 1 \cdot 1 + \frac{30}{2} \cdot 1 \cdot 5$$
$$= 20 + 6 + 75 = 101$$

Let us confirm that 101 is a solution

$101 \equiv 2 \mod 3$ OK

$101 \equiv 1 \mod 5$ OK

$101 \equiv 5 \mod 2$ OK

All solutions have to be congruent to $x_0 = 101$ modulus $m = 30$, i.e. the full solutions are

$x \equiv 101 \mod 30$ or alternatively

$x = 11 \mod 30$.