Chapter 5

Integer numbers

Decomposition of integers

We will deal with sets of natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

and integer numbers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

An integer number can be decomposed into a product of other (smaller) integers. Example:

$$24 = 6 \times 4 = 3 \times 2^3 \times 1$$

How can we do it in a general case?

Divisibility of integers

Theorem (division algorithm): Let $a, b \in \mathbb{N}$, $b \neq 0$. Then $\exists! q, r \in \mathbb{N}$ such that

$$a = bq + r, \quad 0 \leq r < b$$

Def.: We say that $b \in \mathbb{N} \backslash \{0\}$ divides $a \in \mathbb{N}$ if $\exists q \in \mathbb{N}$ such that $a = qb$. We will denote it as $b|a$.

Def.: We say that $p \in \mathbb{N} \backslash \{0, 1\}$ is a prime number if p is divisible by 1 and p only.

Def.: We will call the greatest common divisor of $a, b \in \mathbb{N} \backslash \{0\}$ the number

$$d = \gcd(a, b) \quad \text{if} \quad d|a, \quad d|b$$

and if c divides a and b, then $c \leq d$.

Def.: We will call the minimal common multiple of $a, b \in \mathbb{N}\backslash\{0\}$ the number

$$m = \mathrm{lcm}(a, b) \quad \text{if} \quad a|m, \quad b|m$$

and if n is divided by a and b, then $n \geq m$.

Theorem: $\forall n \in \mathbb{N}\backslash\{0, 1\}$ there exists a prime number p, s.t. $p|n$.

Lema of Bezout: $\forall a, b \in \mathbb{N}\backslash\{0\}$ there exists another couple $u, v \in \mathbb{Z}$, s.t.

$$\mathrm{gcd}(a, b) = ua + vb$$

Theorem (fundamental of arithmetics): Any number $a \in \mathbb{N} \setminus \{0, 1\}$ can be represented as a product of prime numbers.

Any $a, b \in \mathbb{N} \setminus \{0\}$ can be represented in the form

$$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}, \qquad b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$$

Then

$$\gcd(a, b) = p_1^{\min\{r_1, s_1\}} p_2^{\min\{r_2, s_2\}} \cdots p_n^{\min\{r_n, s_n\}}$$

$$\mathrm{lcm}(a, b) = p_1^{\max\{r_1, s_1\}} p_2^{\max\{r_2, s_2\}} \cdots p_n^{\max\{r_n, s_n\}}$$

Corollary:

$$ab = \gcd(a, b)\,\mathrm{lcm}(a, b)$$

Euclides' algorithm

Lema: Let $a, b \in \mathbb{N} \backslash \{0\}$, s.t. $a = qb + r$, $0 < r < b$. Then

$$\gcd(a, b) = \gcd(b, r)$$

Poof: Let $d \in \mathbb{N}$ s.t. $d|a$ and $d|b$. Then

$$a = md = qb + r = qnd + r \quad \Rightarrow \quad r = (m - qn)d \quad \Rightarrow \quad d|r$$

Thus, the common divisors of a and b are also divisors of b and r and hence maximal of them is the gcd.

Theorem: Given $a, b \in \mathbb{N} \backslash \{0\}$ we define the sequence

$$b = r_1 > r_2 > r_3 > \cdots > r_n > r_{n+1} = 0$$

obtained by $r_{i-1} = q_i r_i + r_{i+1}$, with $r_0 = a$ (e.g. $a = q_1 b + r_2$). Then $\gcd(a, b) = r_n$.

Problem 5.1a: Find gcd for 10672 and 4147.

i	0	1	2	3	4	5	6	7	8
r_i	10672	4147	2378	1769	609	551	58	29	0
q_i	–	2	1	1	2	1	9	2	

Thus, $\gcd(10672, 4147) = 29$

Let's find the Bezout's identity. We use $r_{i-1} = q_i r_i + r_{i+1}$ and go backwards to get $\gcd(a, b) = ua + vb$.

$$\gcd(a, b) = 29 = r_7 = r_5 - 9r_6 = r_5 - 9(r_4 - r_5) = 10(r_3 - 2r_4) - 9r_4 =$$

$$= 10r_3 - 29(r_2 - r_3) = 39(r_1 - r_2) - 29r_2 = -68(r_0 - 2r_1) + 39r_1 =$$

$$= -68a + 175b = -68 * 10672 + 175 * 4147 = 29$$

To find the minimal common multiple: $ab = \mathrm{lcm}(a, b)\gcd(a, b)$. Thus

$$\mathrm{lcm}(a, b) = 10672\frac{4147}{29} = 1526096$$

Extended Euclides' algorithm

As before we will use rows r and q, but we will add two new rows α and β

$$r_i = r_{i-2} - q_{i-1} r_{i-1}$$
$$\alpha_i = \alpha_{i-2} - q_{i-1} \alpha_{i-1}$$
$$\beta_i = \beta_{i-2} - q_{i-1} \beta_{i-1}$$

with $\alpha_0 = 1$, $\alpha_1 = 0$, $\beta_0 = 0$, $\beta_1 = 1$.

Problem 5.1e: 322 and 406

r_i	406	322	84	70	14	0
q_i		1	3	1	5	
α_i	1	0	1	-3	4	
β_i	0	1	-1	4	-5	

Thus, $\gcd(406, 322) = 14$. Besides we get immediately the Bezout's identity (using the last values of α and β):

$$\gcd(406, 322) = 14 = 4 \times 406 - 5 \times 322$$

The minimal common multiple:

$$\operatorname{lcm}(406, 322) = \frac{406}{14} 322 = 9338$$

Problem 5.2 Let $a, b \in \mathbb{N} \backslash \{0\}$ and $d = \gcd(a, b)$. Prove that $d | (na + mb)$, $\forall n, m \in \mathbb{Z}$.

Since $d = \gcd(a, b)$ then $d|a$ and $d|b$ and hence $a = dq_a$ and $b = dq_b$. Now

$$na + mb = nq_a d + mq_b d = (nq_a + mq_b)d$$

Thus, $d | (na + mb)$.

Problem 5.3 Prove that $\forall n \in \mathbb{Z}$ $\gcd(n, n+1) = 1$.

Let $n > 0$ and $d = \gcd(n, n+1)$ then $n = q_1 d$. We thus have

$$n + 1 = q_1 d + 1 = q_2 d \quad \Rightarrow \quad (q_2 - q_1)d = 1, \quad q_2 - q_1 \geq 1$$

Therefore $d|1$ and we conclude that $d = 1$.

2. What are the possible values of $\gcd(n, n+2)$?

Let $d = \gcd(n, n+2)$. Then $n = q_1 d$, $n + 2 = q_2 d$

$$n + 2 = q_2 d = q_1 d + 2, \quad \Rightarrow \quad (q_2 - q_1)d = 2 \quad (q_2 > q_1)$$

Thus $d \in \{1, 2\}$.

Congruences

Let's remind: given $m \in \mathbb{N}\backslash\{0\}$, $\forall a \in \mathbb{Z}$ there exist a unique $r \in \mathbb{N}$ s.t.

$$a = qm + r, \quad 0 \leq r < m$$

Thus, there exist m classes of numbers or m classes of congruences.

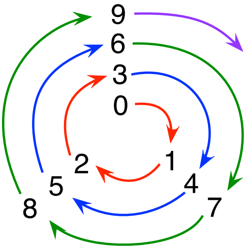
Example: $m = 2$. Then we have

a	equation	class
0	$0 = 0 \times 2 + 0$	0
1	$1 = 0 \times 2 + 1$	1
2	$2 = 1 \times 2 + 0$	0
3	$3 = 1 \times 2 + 1$	1
$\vdots$	$\vdots$	$\vdots$

Thus, we get classes of even $(r = 0)$ and odd $(r = 1)$ numbers.

Def.: We say that $a, b \in \mathbb{Z}$ are congruent by module m if $\exists q_1, q_2 \in \mathbb{Z}$ s.t.

$$a = q_1 m + r, \quad b = q_2 m + r \qquad (0 \leq r < m)$$



We then write

$$a \equiv b \mod m$$

$$a \equiv b \mod m \quad \text{iff} \quad m | (a - b)$$

Problem 5.5 Given that $a \equiv b \bmod m$ and $a \equiv b \bmod n$, prove $a \equiv b \bmod \mathrm{lcm}(n, m)$.

Let's assume that n and m are coprimes. Then from the one side $\mathrm{lcm}(n, m) = nm$ and $\gcd(n, m) = 1 = t_1 n + t_2 m$. From the other side we have

$$\begin{aligned} a \equiv b \mod n \quad &\Rightarrow \quad a - b = q_1 n \\ a \equiv b \mod m \quad &\Rightarrow \quad a - b = q_2 m \end{aligned}$$

Thus $q_1 n = q_2 m$ by multiplying by t_2 we get

$$q_1 t_2 n = q_2 t_2 m = q_2(1 - t_1 n) \;\Rightarrow\; q_2 = (q_1 t_2 + q_2 t_1) n \;\Rightarrow\; n | q_2$$

Therefore, $a - b = q_2 m = q_3 nm$ and hence $a \equiv b \mod nm$.

The rule $b \equiv a \bmod m$ defines the equivalence classes on $\mathbb{Z}$. For example, the numbers

$$1, 4, 7, 10, \ldots$$

form a class for $m = 3$, i.e. they are related ($4 \equiv 1 \bmod 3$; $7 \equiv 1 \bmod 3$, etc.)
Every integer congruent with $x \bmod m$ enters to its equivalence class $x + \mathbb{Z}_m$

Def.: Let $m \in \mathbb{N}\backslash\{0\}$ and $a \in \mathbb{Z}$. We will denote

$$[a]_m = \{x \in \mathbb{Z} : \; x = qm + a, \; q \in \mathbb{Z}\}$$

the equivalence class of a (this is a set of numbers).

Def.: We denote by $\mathbb{Z}_m$ the set generated by the equivalence classes

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Operations on $\mathbb{Z}_m$

Example : $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ where

$$[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}, \quad [1]_2 = \{\ldots, -3, -1, 1, 3, \ldots\}$$

define the classes of odd and even numbers.

Note: $[0]_2 \cap [1]_2 = \emptyset, \quad [0]_2 \cup [1]_2 = \mathbb{Z}$

Def.: We define the addition of congruences as the following map:

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m \\ ([a]_m, [b]_m) &\to [a]_m + [b]_m = [a+b]_m \end{aligned}$$

Def.: We define the multiplication of congruences by:

$$\begin{aligned} \times : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m \\ ([a]_m, [b]_m) &\to [a]_m[b]_m = [ab]_m \end{aligned}$$

Addition and multiplication tables

Let's consider $\mathbb{Z}_4$, i.e. $m = 4$. Then we have the tables

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[0]

$\times$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Example of addition: Evaluate $233 - 350$ in $\mathbb{Z}_4$.

1: $233 = 58 \times 4 + 1$, hence $233 \equiv 1 \bmod 4$. $-350 \equiv 2 \bmod 4$.

$$233 + (-350) \equiv 1 + 2 \equiv 3 \mod 4$$

2: Another way: $233 - 350 = -117 = -30 \times 4 + 3 \equiv 3 \bmod 4$

From the tables we note that [0] and [1] are neutral elements for addition and multiplication, respectively.

Def.: We call the inverse of $[n] \in \mathbb{Z}_m$ in respect to addition, a congruence $[k] \in \mathbb{Z}_m$ s.t. $[n] + [k] = [0]$. Example: $[2]_3 + [1]_3 = [0]_3$, thus, $[2]_3$ is the inverse of $[1]_3$ and vice versa.

Def.: We call the inverse of $[n] \in \mathbb{Z}_m$ in resect to multiplication a congruence $[k] \in \mathbb{Z}_m$ s.t. $[n][k] = 1$. We then denote the inverse by $[n]^{-1}$.

Problem 5.6: Prove that $[n]^{-1} \in \mathbb{Z}_m$ exists iff $\gcd(n, m) = 1$.

1. If $\gcd(n, m) = 1$ then by the Bezout's lemma

$$1 = um + vn \quad \Rightarrow \quad vn = -um + 1 \quad \Rightarrow \quad [v][n] = 1$$

Thus $\exists v \in \mathbb{Z}_m$ s.t. $[v][n] = 1$

2. If $\gcd(n, m) = r > 1$ then $n = q_1 r$ and $m = q_2 r$ $(1 \leq q_{1,2} \leq m)$. Then

$$[nq_2] = [q_1 q_2 r] = [q_1 m] = 0 \tag{1}$$

Now assume that there exists $[n]^{-1}$, i.e. $[n]^{-1}[n] = 1$. Then multiplying (1) by $[n]^{-1}$ we get

$$[n]^{-1}[n][q_2] = q_2 = [n]^{-1}[q_1][m] = [n]^{-1} \times 0 = 0$$

Thus $q_2 = 0$ that contradicts the initial assumption.

If m is a prime number then $\forall [a]_m \in \mathbb{Z}_m \backslash \{[0]_m\}$ there exists its inverse. This property will be important for theory of groups.

Problem 5.7: Find the inverse of the following congruences
(a) 6 in $\mathbb{Z}_{17}$.

17 is a prime, hence the inverse exists. We apply the Euclides' algorithm

r_i	17	6	5	1	0
q_i		2	1	5	
α_i	1	0	1	-1	
β_i	0	1	-2	3	

Using r_3, α_3 and β_3 we can write the Bezout's identity

$$\gcd(17,6) = 1 = -1\times 17 + 3\times 6 \;\Rightarrow\; [1]_{17} = [-17]_{17} + [3]_{17}\times[6]_{17} \;\Rightarrow$$

$$\Rightarrow \quad [1]_{17} = [3]_{17} \times [6]_{17}$$

Thus, $[6]^{-1} = [3]$.

Problem 5.10d $35x \equiv 119 \bmod 139$

To solve, we find $[35]^{-1}$ and multiply both sides of the equation:

$$x = [35]_{139}^{-1} \times [119]_{139}$$

r_i	139	35	34	1	0
q_i		3	1	34	
α_i	1	0	1	-1	
β_i	0	1	-3	4	

Thus, $[1]_{139} = [-139]_{139} + [4 \times 35]_{139}$ and hence $[35]_{139}^{-1} = [4]_{139}$

Now

$$x = [4]_{139} \times [119]_{139} = [476]_{139} = [59]_{139}$$

Chinese remainder theorem

Consider the following k equations in congruences

$$x \equiv a_i \mod n_i, \quad i = 1, 2, \ldots, k$$

where $a_i \in \mathbb{Z}$, $n_i \in \mathbb{N}\backslash\{0\}$. If n_i are pairwise co-primes ($\gcd(n_i, n_j) = 1$, $\forall i \neq j$), then the system has a solution. Moreover, if x and y are two solutions then

$$x \equiv y \mod \mathrm{lcm}(n1, \ldots, n_k) = n_1 n_2 \cdots n_k$$

Proof: The idea is to search for a solution in the form

$$x = c_1 a_1 + c_2 a_2 + \cdots + c_k a_k$$

Then the constants $\{c_i\}$ must satisfy the condition

$$c_i \equiv \begin{cases} 1 \mod n_j & j = i \\ 0 \mod n_j & j \neq i \end{cases}$$

Then when substituting to the i-th equation we get:

$$\sum (c_j a_j \mod n_i) \equiv a_i = a_i$$

Now we select c_i in the appropriate way.
Let $n = n_1 n_2 \cdots n_k$ and

$$q_i = \frac{n}{n_i}, \quad i = 1, \ldots, k$$

Since $\gcd(q_i, n_i) = 1$, there exists the inverse of q_i in $\mathbb{Z}_{n_i}$:

$$c_i = q_i r_i \equiv 1 \mod n_i, \qquad (q_i r_i \equiv 0 \mod n_j)$$

Now we define

$$x = \sum_{i=1}^{k} q_i r_i a_i$$

Let us now check that x is a solution. Since $n_i | q_j$ for $i \neq j$ we have

$$x = \sum_{m \neq j} a_m q_m r_m \mod n_i + a_i q_i r_i \mod n_i = a_i q_i r_i \mod n_i$$

Since $q_i r_i = 1 \mod n_i$ we get $x = a_i \bmod n_i$.
Now let $y = a_i \bmod n_i$ be another solution. Since $[x]_{n_i} = [y]_{n_i}$.
Then $n_i | (x - y)$ for $i = 1, \ldots, k$, which implies
$x = y \bmod \mathrm{lcm}(n1, \ldots, n_k) = n_1 n_2 \cdots n_k$.

Problem 5.11a: Solve the system $x \equiv 2 \bmod 4$, $x \equiv 4 \bmod 5$.

$\mathrm{lcm}(4,5) = 20$, $q_1 = 5$, $q_2 = 4$. Now we find $r_{1,2}$

$$r_1 = [q_1]_{n_1}^{-1} = [5]_4^{-1} = [1]_4^{-1} = 1$$

$$r_2 = [4]_5^{-1} \;\Rightarrow\; 4 \times 4 - 3 \times 5 = 1 \quad \Rightarrow \; r_2 = 4$$

Thus $x = (2 \times 1 \times 5 + 4 \times 4 \times 4) \bmod 20 = [14]_{20}$

Problem 5.11f

$$\begin{aligned} 2x &\equiv 3 \mod 7 \\ 5x &\equiv 4 \mod 9 \\ 3x &\equiv 1 \mod 10 \end{aligned}$$

7,9, and 10 are coprimes, thus there exists a solution.

1: Rewrite in the standard form (multiplying by the corresponding inverses). $[2]_7^{-1} = [4]_7$; $[5]_9^{-1} = [2]_9$; and $[3]_{10}^{-1} = [7]_{10}$. Therefore

$$\begin{aligned} x &\equiv 12 \mod 7 = 5 \mod 7 \\ x &\equiv 8 \mod 9 \\ x &\equiv 7 \mod 10 \end{aligned}$$

Now $n = 7 \times 9 \times 10 = 630$, $q_1 = 90$, $q_2 = 70$, $q_3 = 63$. Let's find the inverses (construct the corresponding Euclides' tables)

$$r_1 = [q_1]_{n_1}^{-1} = [90]_7^{-1} = [6]_7^{-1} = 6; \;\; r_2 = [70]_9^{-1} = 4; \;\; r_3 = [63]_{10}^{-1} = 7.$$

Thus the solution is:

$$x = (5 \times 90 \times 6 + 8 \times 70 \times 4 + 7 \times 63 \times 7) \mod 630 = [467]_{630}$$

Linear Diophantine equations

The equation of the form:

$$ax + by = c, \quad a, b, c, x, y \in \mathbb{Z}$$

in respect to unknown x and y is called Diophantine equation.

The diophantine equation has a solution iff c is a multiple of $\gcd(a, b)$.

To solve it we note that $c = ax + by$ is equivalent to represent c as

$$[c]_b = [ax + by]_b \;\Rightarrow\; c \equiv ax \mod b$$

Then we can solve such an equation for x and use it to find y.

Problem 5.12b Find solutions $54x + 21y = 906$, $x, y \in \mathbb{Z}$.

First we note that $\gcd(54, 21) = 3$ and 906 is a multiple of 3. Thus, we reduce the equation (divide by 3):

$$18x + 7y = 302$$

We then rewrite it

$$18x \equiv 302 \mod 7$$

and observe $[18]_7^{-1} = [2]_7$. We now obtain x

$$x = 2 \times 302 \mod 7 = [2]_7 \quad \Rightarrow \quad x_k = 2 + 7k$$

$$y_k = \frac{302 - 18(2 + 7k)}{7} = 38 - 18k, \quad \forall k \in \mathbb{Z}$$

Problem 5.13 Find natural numbers satisfying

$$84x + 990y = c, \quad 10 < c < 20$$

First we find $\gcd(84, 990) = 6$. Thus c must be multiple of 6. There are two possibilities $c = 12$ and $c = 18$. Then we can use the standard procedure for these cases separately.

Problem 5.14: Let x and y be the amount in dollars and cents of the check. He received $r = 100y + x$ then spent 68 cents and get double amount:

$$100y + x - 68 = 2(100x + y)$$

Thus, we have to solve

$$98y - 199x = 68, \quad x, y \in \mathbb{N}$$

Problem 5.16: Calculate i) $(a+b)^2$ in $\mathbb{Z}_2$; ii) $(a+b)^3$ in $\mathbb{Z}_3$

	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Besides $(a+b)^2 \bmod 2 = a^2 + 2ab + b^2 \bmod 2 = a^2 + b^2$.

$(a+b)^3 \mod 3 = a^3 + 3a^2 b + 3ab^2 + b^3 \mod 3 = a^3 + b^3 \mod 3$

iii)

$$\left(\begin{array}{c} p \\ k \end{array} \right) = \frac{p!}{k!(p-k)!} = \frac{(p-1)!}{k!(p-k)!} p$$

Since p is prime, it is not divisible by the denominator and hence the binomial coefficient is divisible by p. Thus

$$(a+b)^p \mod p = \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} b^k \mod p = a^p + b^p \mod p$$

Problem 5.17: Find the multiples of 28, s.t. the last two digits would be equal to 16.

$$x = 28q, \quad x = 16 \mod 100$$

Thus, we have the following diophantine equation:

$$28q = 16 + 100n, \quad n \in \mathbb{N}$$

We then have $\gcd(28, 100) = 4$ and reduce the diophantine equation:

$$7q = 4 + 25n \;\Rightarrow\; [7]_{25}[q]_{25} = [4]_{25}$$

Multiplying it by $[7]_{25}^{-1} = [18]_{25}$ we get

$$q = [18 \times 4]_{25} = [22]_{25} \;\Rightarrow\; x = 28(22 + 25n) = 616 + 700n$$

Examples: $x = 616$, 1316, 2016, etc.

Problem 5.18: Show that $n^3 - 7n + 7$ and $n - 1$ are comprimes.

We divide $n^3 - 7n + 7$ by $n - 1$ we get

$$\frac{n^3 - 7n + 7}{n - 1} = n^2 + n - 6 + \frac{1}{n - 1}$$

Thus

$$(n^3 - 7n + 7) - (n^2 + n - 6)(n - 1) = 1$$

therefore these numbers have gcd $= 1$

Fast operations

The idea: Instead of working in high dimensions, i.e. in $\mathbb{Z}_m$ when m is high. We can introduce its decomposition into a cartesian product $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cdots \mathbb{Z}_{m_k}$ and apply operations in this new space and then do the inverse transformation.

Let us illustrate it in the following problem:

Problem 5.19: a) Let define the map

$$f : \mathbb{Z}_{140} \to \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$
$$[n]_{140} \mapsto ([n]_4, [n]_5, [n]_7)$$

Prove that f is bijective.

1. f is injective (if $[n] \neq [m]$ then $f([n]) \neq f([m])$).

Assume that $([n]_4, [n]_5, [n]_7) = ([m]_4, [m]_5, [m]_7)$. Then n and m satisfy to

$$\begin{aligned} n &\equiv m \mod 4 \\ n &\equiv m \mod 5 \\ n &\equiv m \mod 7 \end{aligned}$$

Since 4, 5, and 7 are coprimes, then by Problem 5.5 $n \equiv m \mod \operatorname{lcm}(4,5,7)$, i.e., $n \equiv m \mod 140$ and hence $[n]_{140} = [m]_{140}$, which is a contradiction.

2. *f* is surjective $(\forall y \ \exists [n] \text{ s.t. } f([n]) = y)$. Let consider

$$([a_1]_4, [a_2]_5, [a_3]_7) \in \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

We should prove that there exists its pre-image $x \in \mathbb{Z}_{140}$. This is equivalent to

$$x \equiv a_1 \mod 4; \quad x \equiv a_2 \mod 5; \quad x \equiv a_3 \mod 7$$

Since 4, 5, and 7 are coprimes, then by the Chinese theorem there exists a solution.

Thus f is bijective on finite sets. This means that there is its inverse f^{-1} and $f^{-1}(f(y)) = y$.

Evaluate: $f^{-1}(f(35) + f(56))$
By the previous part we know that this is $[35]_{140} + [56]_{140}$ $= [91]_{140}$. But let's see how it works in lower dimensions.

1. Mapping to the cartesian product:

$$[35]_{140} \mapsto ([35]_4, [35]_5, [35]_7) = ([3]_4, [0]_5, [0]_7)$$
$$[56]_{140} \mapsto ([56]_4, [56]_5, [56]_7) = ([0]_4, [1]_5, [0]_7)$$

2. Addition in the cartesian space:

$$f([35]) + f([56]) = ([3]_4, [1]_5, [0]_7)$$

3. Inverse operation:

$$\begin{aligned} x &\equiv 3 \mod 4 \\ x &\equiv 1 \mod 5 \\ x &\equiv 0 \mod 7 \end{aligned}$$

By the Chinese theorem: $n = 140$, $q_1 = 35$, $q_2 = 28$. Then

$$\begin{aligned} -35 + 9 \times 4 = 0 \quad &\Rightarrow \quad r_1 = -1 \\ 2 \times 28 + 11 \times 5 = 0 \quad &\Rightarrow \quad r_2 = 2 \end{aligned}$$

Finally

$$x = [3 \times (-35) + 2 \times 28]_{140} = [-49]_{140} = [91]_{140}$$

Euler function

Def.: We define the Euler function by

$$\begin{aligned} \phi: &\ \mathbb{N}\backslash\{0\} \to \mathbb{N}\backslash\{0\} \\ n \mapsto &\ \mathrm{card}\{k \in \mathbb{N}\backslash\{0\}: \ k < n, \ \gcd(k, n) = 1\} \end{aligned}$$

In other words, $\phi(n)$ is the number of natural numbers $k < n$ coprimes with n.

Property: If p is a prime, then $\phi(p) = p - 1$

Problem 5.20a: Let $\mathbb{Z}_m^*$ be the set of elements of $\mathbb{Z}_m$ that have an inverse. Prove that $\phi(m) = \mathrm{card}\,\mathbb{Z}_m^*$

For a given k $(k = 1, 2, \ldots, m-1)$ let $\gcd(m, k) = 1$ then $[k]_m \in \mathbb{Z}_m^*$. Besides, if $\gcd(m, k) > 1$, then $[k]_m \notin \mathbb{Z}_m^*$. Thus, $\phi(m) = \mathrm{card}\,\mathbb{Z}_m^*$

Problem 5.20b: Evaluate:

1. $\phi(11)$. $\phi(11) = \mathrm{card}\,\mathbb{Z}_{11}^*$. Since 11 is a prime, then $\mathbb{Z}_{11}^* = \mathbb{Z}_{11} \backslash [0]_{11}$. Thus $\phi(11) = 10$.

2. $\phi(16)$. $\gcd(16, k) = 1$, then:

$$\{1, 3, 5, 7, 9, 11, 13, 15\}$$

Thus $\phi(16) = 8$.

3. $\phi(17)$. 17 is prime. $\phi(17) = 16$.

4. $\phi(25)$. $\phi(25) = \phi(5^2)$. 5 is a prime number.

General property: $\gcd(p^2, m) \in \{1, p, p^2\}$. This can be seen from (Fund. Th. Arithmetics) $m = p_1 p_2 \cdots p_k$. Thus $m | p^2$ iff m contains p. Now $m < p^2$ thus the only way (bad case) $\gcd(p^2, m) = p$. Then $m = kp$ with $k = 1, 2, \ldots, p-1$.

Thus there exist $p-1$ numbers s.t. $\gcd(p^2, m) > 1$. To compute $\phi(p^2)$: we have p^2 numbers, we exclude $p-1$ with $\gcd > 1$ and also 0. Thus

$$\phi(p^2) = p^2 - (p-1) - 1 = p^2\left(1 - \frac{1}{p}\right)$$

In general:

$$\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$$

$\phi(25) = \phi(5^2) = 25 - 5 = 20.$

By using fast operations we can show that if $\gcd(n, m) = 1$:

$$\phi(nm) = \phi(n)\phi(m)$$

5. $\phi(100) = \phi(4 \times 25) = \phi(2^2)\phi(5^2) = (4-2) + (25-5) = 22.$

Fermat's little theorem

If $\gcd(a, n) = 1$ then

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

Problem 21: Find the last digit of 2^{333}.

The last digit is the remainder after dividing 2^{333} by 10. Thus

$$x = 2^{333} \mod 10 \text{ or } x = [2^{233}]_{10}$$

Since $\gcd(2, 10) = 2$ we cannot do it directly. From the fast calculations we can use

$$f : \mathbb{Z}_{10} \to \mathbb{Z}_5 \times \mathbb{Z}_2$$

Thus we find $([2^{333}]_5, [2^{333}]_2)$

Since $\gcd(2,5)=1$ we have $[2^{\phi(5)}]_5=[1]_5$. $\phi(5)=4$, i.e. $[2^4]_5=1$. Thus we get

$$[2^{333}]_5=[2^{4\times 83}\times 2]_5=[2^{4\times 83}]_5\times[2]_5=[2]_5$$

Then we note $[2^{333}]_2=[2]_2\times[2]_2\times\cdots\times[2]_2=[0]_2$. Therefore

$$([2^{333}]_5,[2^{333}]_2)=([2]_5,[0]_2)$$

We now apply the inverse transform

$$x\equiv 2 \mod 5,\quad x\equiv 0 \mod 2$$

$n=10$, $q_1=2$, $q_2=5$. Inverse $r_1=[2]_5^{-1}=[3]_5$, $r_2=[5]_2^{-1}=[1]_2$. Finally

$$x=[2\times 2\times 3+0]_{10}=[12]_{10}=[2]_{10}$$

Problem 22a (Worksheet 5)

Cesar's code

```
L = 'abcdefghijklmnñopqrstuvwxyz'; % alphabet
key = 6;                           % codding key
Mess = 'gqqeuaskkjñyqubk';         % codded message

disp('******* Codded message *********')
disp(Mess)

% decoding
for n = 1:length(Mess)
    l = strfind(L, Mess(n))-1;  % charqcter number
    l = mod(l-key,27);          % l - k mod 27
    Mess(n) = L(l+1);
end

disp('******* Decodded message *******')
disp(Mess)
disp('********************************')
```

```
******* Codded message *********
gqqeuaskkjñyqubk
******* Decodded message *******
allyouneedislove
********************************
```