Problem 2 : *A Number of Residues*

Descartes High School
Team TS6-Descartes

Abstract

1^{st} part

We denote by $T_k = \frac{k(k+1)}{2}$ the k^{th} triangular number, where $k \in \mathbb{N}$. For each positive integer n, let u_n be the number of distinct members of the sequence $(T_k \bmod n)_{k\geqslant 1}$. We want to establish a formula for (u_n) in particular cases, in order to find a formula in a general case.

Thanks to values tables, we conjecture and then we prove the frequency of number sequences.
Next, we prove that :

- for $n = 2^k$: $u_{2^k} = 2^k$
- for $n = p^k$ with p an odd prime number.
  $u_{p^0} = u_1 = 1$
  $u_p = \dfrac{1}{2}(p+1)$

We prove that if $n = p^k$ is a power of an odd prime number : $u_{p^k} = u_{p^{k-2}} + \dfrac{1}{2}(p^k - p^{k-1})$.

Then, we conclude that :

If n is an even power of prime
$$u_{p^k} = \frac{1}{2}\left[\frac{1-(-p)^{k+1}}{1+p} + 1\right]$$

If n is an odd power of prime
$$u_{p^k} = \frac{1}{2}\left[-\frac{1-(-p)^{k+1}}{1+p} + 2\right]$$

Finally, in general case, we prove that : $u_n = u_{p_1^{k_1}}.u_{p_2^{k_2}}...u_{p_r^{k_r}}$
with $n = p_1^{k_1}.p_2^{k_2}...p_r^{k_r}$ the prime factorization of n

2^{nd} part

Let $P(x)$ be a polynomial with rational coefficients such as $P(k)$ is integer for every $k \in \mathbb{Z}$. We try to find the number of distinct residues modulo n in the sequence $(P(k))_{k\geqslant 1}$.

We prove that the only polynomials with rational coefficients, such as $P(k)$ is an integer for every integer k, are with integer coefficients, hence of the form :

$$P(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x)$$

with $(\lambda_0, \lambda_1, ...\lambda_n) \in \mathbb{Z}^{n+1}$
and $T_n(x) = \dfrac{x(x-1)(x-2)...(x-(n-1))}{n!}$

Then, we study two particular cases :
for $P(x) = a$, the number of residues is 1 ;
for $P(x) = ax + b$, the number of residues is $\dfrac{n}{a \wedge n}$.

Preliminaries

0.1 Notations.

$\mathbb{N}$:	the set of all positive integers with 0.
$\mathbb{Z}$:	the set of all integers with 0.
$\mathbb{R}$:	the set of all real numbers
$\mathcal{P}$:	the set of all prime numbers with 2.
$[[X;Y]]$:	the set of all integers between X and Y.
$\mathbb{Z}/p\mathbb{Z}^*$:	the set of classes of integers modulo p (except 0).
$\sharp$:	cardinality
$\equiv$:	congrued to
$X[Y]$:	X modulo Y
gcd or $\wedge$:	greatest common divisor
$\begin{pmatrix} a \\ b \end{pmatrix}$	binomial coefficient

0.2 Definition of a triangular number

A triangular number is a particular set of figurate numbers.

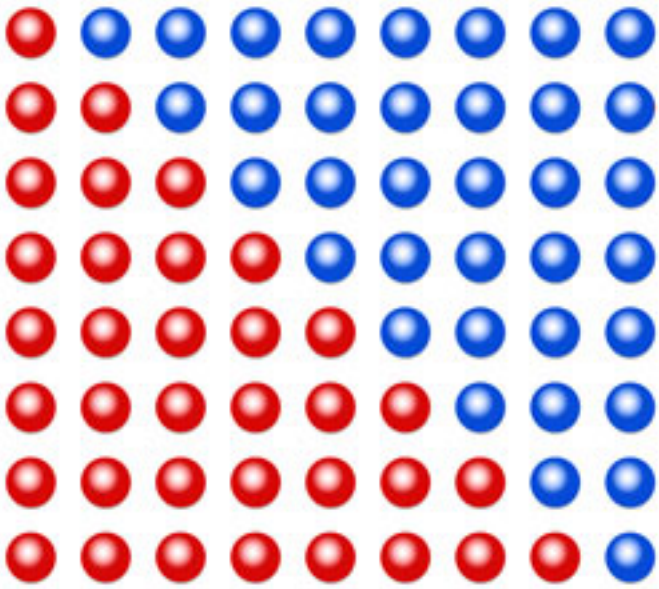

FIGURE 1 – Triangular numbers

We can see that two k^{th} triangular number build a rectangle of area $k(k+1)$.

The k^{th} triangular number is equal to the sum of all integers from 1 to k, which is Gauss sum :

$$T_k = \sum_{n=1}^{k} n = \frac{k(k+1)}{2}$$

0.3 Frame of (u_n)

The number of different residues is necessarily at least 1.
Moreover, they are such as $0 \leqslant r < n$, therefore they are at most n different. So, we can assert that :

$$1 \leqslant u_n \leqslant n$$

0.4 Values Table of (u_n)

The values tables are in appendixes.

1 Find a formula for u_n when n is a power of 2

With values tables (in appendixes), we can conjecture in this case that for $n = 2^k$:

$$u_{2^k} = 2^k$$

First, we can prove two preliminary properties

1.1 Property 1 : *If $a \equiv b[n]$, $a \equiv b[2n]$ or $a \equiv b + n[2n]$.*

Let a be an integer such as $a \equiv b[n]$ with $0 \leqslant b < a$. We obtain $a - b = q \cdot n$.
q is odd or even.

- If q is even, we can write $q = 2k$.
  $a - b = 2k \cdot n = k \cdot 2n$
  So, $a \equiv b[2n]$
- If q is odd, we can write $q = 2k + 1$
  $a - b = (2k + 1) \cdot n = k \cdot 2n + n \iff a - (b + n) = k \cdot 2n$
  So, $a \equiv b + n[2n]$

Finally, $a \equiv b[n] \Rightarrow a \equiv b[2n]$ or $a \equiv b + n[2n]$

1.2 Property 2 : *If $T_k \equiv a[n]$ so $T_{k+2n} \equiv a[n]$*

We can conjecture with values table that the sequences of residues are $2n$-periodic
Let $T_k = \dfrac{k(k+1)}{a} \equiv a[n]$.
Let us show that $T_{k+2n} = \dfrac{(k+2n)(k+1+2n)}{2} \equiv a[n]$

$$\frac{(k+2n)(k+1+2n)}{2} = \frac{k(k+1)}{2} + \frac{k \cdot 2n + 2n(k+2n+1)}{2} = T_k + n(2k+2n+1)$$

But, $n(2k + 2n + 1) \equiv 0[n]$ and $T_k \equiv a[n]$

So, $T_{k+2n} = \dfrac{(k+2n)(k+1+2n)}{2} \equiv a[n]$

We obtain : $T_k \equiv T_{k+2n} \equiv a[n]$. The sequence is 2n-periodic.

1.3 Corollary of those properties

According to the first property, if $T_k \equiv a[n]$, so :

- If $T_k \equiv a[2n]$
  According to the second property : $T_{k+2n} = \frac{k(k+1)}{2} + 2kn + 2n^2 + n$
  But $2kn + 2n^2 + n \equiv n[2n]$
  So, $T_{k+2n} \equiv a + n[2n]$

- If $T_k \equiv a + n[2n]$
  Similarly, we obtain : $T_{k+2n} \equiv a + n + n \equiv a + 2n[2n]$
  So, $T_{k+2n} \equiv a[2n]$

1.4 Proof by induction of the conjecture : $\forall n \in \mathbb{N}, u_{2^n} = 2^n$

We have obviously an only residue modulo n, whatever T_k.
So $u_1 = 1$, which matches with the conjecture.

Basis step : For $n = 1$

We have $T_2 = 3$. But, $3 \equiv 1[2]$ So, the residue is 1.
Similarly, $T_3 = 6$. But, $6 \equiv 0[2]$. So, the residue is 0.
The residues are sush as $0 \leqslant r < 2$
So, $u_2 = 2$. The property is checked.

Inductive step

We assume that for some n : $\forall a \in [[0, 2^n - 1]]$, $\exists T_{k_a} \equiv a[2^n]$
Let us show that : $\forall b \in [[0, 2^{n+1} - 1]]$, $\exists T_{k_b} \equiv b[2^{n+1}]$

Take $b \in [0; 2^{n+1} - 1]$

- If $b \in [0; 2^n - 1]$
  According to the hypothesis, there is $T_{k_b} \equiv b[2^n]$

- If $b \in [2^n; 2^{n+1} - 1]$
  So $b - 2^n \in [0; 2^n - 1]$.
  According to the hypothesis, there is $T_{k_b} \equiv b - 2^n[2^n] \equiv b[2^n]$.
  In both cases, $T_{k_b} \equiv b[2^n]$.
  According to the property 1. , we split in two cases :
  – If $T_{k_b} \equiv b[2^{n+1}]$ the property is checked.
  – If $T_{k_b} \equiv b + 2^n[2^{n+1}]$, $T_{k_b+2^{n+1}} \equiv b[2^{n+1}]$. The property is checked.

Conclusion

$$\forall n = 2^k \text{ with } k \in \mathbb{N}, \text{ we have } u_{2^k} = 2^k$$

2 Find a formula when n is a power of prime number

2.1 Property 3 : p is an odd prime number, so $T_k \equiv T_{k+p} \equiv b[p]$

Let $T_k = \dfrac{k(k+1)}{2} \equiv b[p]$

Let us show that $T_{k+p} = \dfrac{(k+p)(k+p+1)}{2} \equiv b[p]$

$$\frac{(k+p)(k+p+1)}{2} = \frac{k(k+1)}{2} + \frac{2kp+p^2+p}{2} = \frac{k(k+1)}{2} + p\frac{(2k+p+1)}{2}$$

But, $p \cdot \dfrac{2k+p+1}{2} \equiv 0[p]$ and $\dfrac{k(k+1)}{2} \equiv b[p]$

We obtain : $T_k \equiv T_{k+p} \equiv b[p]$. For the prime numbers, the sequence is p-periodic.

2.2 Conjectures

Let be $p \in \mathcal{P} \setminus \{2\}$
With the values table, we can conjecture :

$$u_p = \frac{1}{2}(p+1)$$

$$u_{p^2} = \frac{1}{2}((p^2-p+1)+1)$$

$$u_{p^3} = \frac{1}{2}((p^3-p^2+p-1)+2)$$

$$u_{p^4} = \frac{1}{2}((p^4-p^3+p^2-p+1)+1)$$

The conjecture can be written as follows :

- If k is even

$$u_{p^k} = \frac{1}{2}\left[\left(\sum_{i=0}^{k}(-p)^i\right)+1\right]$$

- If k is odd

$$u_{p^k} = \frac{1}{2}\left[-\left(\sum_{j=0}^{k}(-p)^j\right)+2\right]$$

But, $\sum_{i=0}^{k}(-p)^i = \frac{1-(-p)^{k+1}}{1+p}$

So, we can write :

- If k is even

$$u_{p^k} = \frac{1}{2}\left[\frac{1-(-p)^{k+1}}{1+p} + 1\right]$$

- If k is odd

$$u_{p^k} = \frac{1}{2}\left[-\frac{1-(-p)^{k+1}}{1+p} + 2\right]$$

We remark also that :

$$u_{p^k} = u_{p^{k-2}} + \frac{1}{2}(p^k - p^{k-1})$$

If we prove that conjecture and that :

– $u_{p^0} = 1$

– $u_p = \frac{1}{2}(p+1)$

The property will be checked.

2.3 Theorem 1

"In $\mathbb{Z}/p\mathbb{Z}^*$ with p an odd prime number, there are $\frac{p-1}{2}$ squares with two different square roots and $\frac{p-1}{2}$ non-square"

We prove this theorem :

Consider the map $g : \begin{cases} \mathbb{Z}/p\mathbb{Z}^* \to \mathbb{Z}/p\mathbb{Z}^* \\ x \to x^2 \end{cases}$ with $\sharp\mathbb{Z}/p\mathbb{Z}^* = p-1$

Denote A the subset of squares in $\mathbb{Z}/p\mathbb{Z}^*$ and $\overline{A}$ his complementary. Let $a \in \mathbb{Z}/p\mathbb{Z}^*$

- If $a \in \overline{A} \Longrightarrow \nexists x \in \mathbb{Z}/p\mathbb{Z}^*$ such as $g(x) = a$
- If $a \in \overline{A} \Longrightarrow \exists x \in \mathbb{Z}/p\mathbb{Z}^*$ such as $g(x) = a$

$$g(y) = a \Longleftrightarrow y^2 = x^2 \Longleftrightarrow y = \pm x$$

a has two square roots : x and $-x$ with $-x = -x + p$ in $\mathbb{Z}/p\mathbb{Z}^*$
But $x = -x + p \Longleftrightarrow p = 2x$ which is impossible because p is a prime number.

So, x and $-x$ are two different roots in $\mathbb{Z}/p\mathbb{Z}^*$

We obtain :

$$\begin{cases} 0 \times \sharp A + 2 \times \sharp A = \sharp\mathbb{Z}/p\mathbb{Z}^* = p-1 \\ \sharp\overline{A} + \sharp A = \sharp\mathbb{Z}/p\mathbb{Z}^* = p-1 \end{cases} \Longleftrightarrow \sharp A = \sharp\overline{A} = \frac{(p-1)}{2}$$

2.4 Proof of the conjecture for an odd prime number : $u_p = \frac{1}{2}(p+1)$

We denote $T_k = \dfrac{k(k+1)}{2} \equiv a[p]$ with $p \in \mathcal{P} \setminus \{2\}$

We search the number of different values a

We can study the problem only in $\mathbb{Z}/p\mathbb{Z}^*$ because the sequence is p-periodic.

We can solve : $\frac{k(k+1)}{2} = a \iff k^2 + k - 2a = 0$

This is a second degree equation with $\Delta = 1 + 8a$

This equation has integer solution if $\Delta = 1 + 8a$ is a perfect square.

But, $a \to 1 + 8a$ is obviously a bijection in $\mathbb{Z}/p\mathbb{Z}^*$.

$a = 0$ is an evident solution. So, now we have to search the number of strictly positive perfect square. Thus, we can use the theorem 1.

We obtain : $\dfrac{p-1}{2} + 1 = \dfrac{p+1}{2}$ different residues.

So, we have : $u_p = \frac{1}{2}(p+1)$

2.5 Property 4 : $u_{p^n} = \sharp\{k^2[p^n]/k \in \mathbb{Z}\}$

Let p be an odd prime number.

We can remark that : $\sharp\left\{\dfrac{k(k+1)}{2}[p^n]/k \in \mathbb{Z}\right\} = \sharp\left\{4k(k+1)[p^n]/k \in \mathbb{Z}\right\}$.

Indeed $\begin{cases} \mathbb{Z}/p^n\mathbb{Z} & \to & \mathbb{Z}/p^n\mathbb{Z} \\ k & \to & 8k \end{cases}$ is a bijection because $\gcd(8; p^n) = 1$.

So $\sharp\left\{\dfrac{k(k+1)}{2}[p^n]/k \in \mathbb{Z}\right\} = \sharp\left\{(2k+1)^2 - 1[p^n]/k \in \mathbb{Z}\right\}$.

But, substract 1 doesn't change the cardinality of this set.

$\sharp\left\{\dfrac{k(k+1)}{2}[p^n]/k \in \mathbb{Z}\right\} = \sharp\left\{(2k+1)^2[p^n]/k \in \mathbb{Z}\right\}$

For all k', there exists k such as $2k + 1 \equiv k'[p^n]$.

So, $\sharp\left\{\dfrac{k(k+1)}{2}[p^n]/k \in \mathbb{Z}\right\} = \sharp\left\{k'^2[p^n]/k \in \mathbb{Z}\right\}$

Finally, we have : $u_{p^n} = \sharp\{k^2[p^n]/k \in \mathbb{Z}\}$

2.6 Property 5 : $u_{p^n} = u_{p^{n-2}} + \frac{1}{2}(p^n - p^{n-1})$

We can write that :

$$u_{p^n} = \sharp\{k^2[p^n]/k \in \mathbb{Z}\} = \sharp\left(\left\{k^2[p^n]/k \in \mathbb{Z}, p|k\right\} \cup \left\{l^2[p^n]/l \in \mathbb{Z}, p \nmid l\right\}\right)$$

We denote by $A = \left\{k^2[p^n]/k \in \mathbb{Z}, p|k\right\}$ and by $B = \left\{l^2[p^n]/l \in \mathbb{Z}, p \nmid l\right\}$
So, we obtain :

$$u_{p^n} = \sharp(A \cup B) = \sharp A + \sharp B - \sharp(A \cap B)$$

Let us prove now that :
– $\sharp(A \cap B) = 0$
– $\sharp A = u_{p^{n-2}}$
– $\sharp B = \frac{1}{2}(p^n - p^{n-1})$

2.6.1 Let us prove that : $\sharp(A \cap B) = 0$

We suppose that : $k^2 \equiv l^2[p^n]$ with $p \mid k$ and $p \nmid l$.
So :

$$p^n \mid k^2 - l^2$$
$$p^n \mid (k-l)(k+l)$$
$$p \mid (k-l)(k+l)$$

But, $\gcd(p; k+l) = 1$ and $\gcd(p; k-l) = 1$.
So $p \mid (k-l)(k+l)$ is absurd.
We conclude :

$$A \cap B = \emptyset$$

2.6.2 Let us prove that : $\sharp A = u_{p^{n-2}}$

We can write that : $A = \{k^2[p^n]/k \in \mathbb{Z}, p \mid k\} = \{(ip)^2[p^n]/i \in \mathbb{Z}\} = \{p^2 \cdot i^2[p^n]/i \in \mathbb{Z}\}$

We obtain : $p^2 \cdot i^2 \equiv p^2 \cdot j^2[p^n]$
So, $p^n \mid p^2(i^2 j^2)$
We can write : $p^2(i^2 - j^2)q = p^n$ with $q \in \mathbb{Z}$
And then : $(i^2 - j^2)q = p^{n-2}$
So we obtain : $i^2 \equiv j^2[p^{n-2}]$
We conclude that : $A = \{i^2[p^{n-2}]/i \in \mathbb{Z}\}$.
According to property 4., we obtain :

$$\sharp A = u_{p^{n-2}}$$

2.6.3 Let us prove that : $\sharp B = \frac{1}{2}(p^n - p^{n-1})$

We denote by : $A' = \{k'[p^n]/k' \in \mathbb{Z}, p \mid k'\}$ and $B' = \{l'[p^n]/l' \in \mathbb{Z}, p \nmid l\}$.
We obtain : $\sharp B' = \sharp(A' \cup B') - \sharp A' = p^n - p^{n-1}$.

Now, we solve : $k^2 \equiv l^2[p^n]$ with $k \in A$ and $l \in B$.
So we can write : $p^n \mid k^2 - l^2$ $p \mid (k-l)(k+l)$
But, p divides neither $(k-l)$ nor $(k+l)$ according to subsection 2.5.2.

So, $\begin{array}{lll} p^n \mid k-l & or & p^n \mid k+l \\ k \equiv l[p^n] & or & k \equiv -l[p^n] \end{array}$
But, $l \neq -l$.

Finally, $\sharp B = \frac{1}{2}\sharp B'$.

So, we have : $\sharp B = \frac{1}{2}(p^n - p^{n-1})$

2.6.4 Conclusion

Let p be an odd prime number and $k \geq 2$ an integer.
Now, we have :

$$u_{p^k} = u_{p^{k-2}} + \frac{1}{2}(p^k - p^{k-1})$$

2.7 Proof of the conjectures 2.2.

We prove the conjecture 2.2. by a second degree inclusion.

Basis step : For $n = 0$ and $n = 1$

We have $u_{p^0} = u_1 = 1$ and $u_p = \frac{1}{2}(p+1)$ according to part 2.4.
On the other hand, we have with our conjectures :

$$u_{p^0} = \frac{1}{2}\left[\frac{1-(-p)^{0+1}}{1+p} + 1\right] = \frac{1}{2}\left[\frac{1+p}{1+p} + 1\right] = 1$$

And :

$$u_p = \frac{1}{2}\left[-\frac{1-(-p)^{1+1}}{1+p} + 2\right] = \frac{1}{2}\left[-\frac{1-p^2}{1+p} + 2\right] = \frac{1}{2}\left[-\frac{(1-p)(1+p)}{1+p} + 2\right] = \frac{1}{2}(p-1+2) = \frac{1}{2}(p+1)$$

So, the properties are checked for $n = 0$ and $n = 1$.

Inductive step

- **If n is even**

  We assume that for one even n : $u_{p^n} = \frac{1}{2}\left[\frac{1-(-p)^{n+1}}{1+p} + 1\right]$

  We show that : $u_{p^{n+2}} = \frac{1}{2}\left[\frac{1-(-p)^{n+3}}{1+p} + 1\right]$

  According to Property 5., we have :

$$u_{p^{n+2}} = u_p + \frac{1}{2}(p^{n+2} - p^{n+1}) = \frac{1}{2}\left[\frac{1-(-p)^{n+1}}{1+p} + p^{n+2} - p^{n+1} + 1\right]$$

$$u_{p^{n+2}} = \frac{1}{2}(p^{n+2} - p^{n+1} + p^n - p^{n-1} + p^{n-2} - \cdots + 1 + 1)$$

$$u_{p^{n+2}} = \frac{1}{2}\left[\frac{1-(-p)^{n+3}}{1+p} + 1\right]$$

  So, the property is checked if n is even.

- **If n is odd**

  We assume that for one even n : $u_{p^n} = \frac{1}{2}\left[-\frac{1-(-p)^{n+1}}{1+p} + 2\right]$

  We show that : $u_{p^{n+2}} = \frac{1}{2}\left[-\frac{1-(-p)^{n+3}}{1+p} + 2\right]$

  According to Property 5., we have :

$$u_{p^{n+2}} = u_p + \frac{1}{2}(p^{n+2} - p^{n+1}) = \frac{1}{2}\left[-\frac{1-(-p)^{n+1}}{1+p} + p^{n+2} - p^{n+1} + 2\right]$$

$$u_{p^{n+2}} = \frac{1}{2}(p^{n+2} - p^{n+1} + p^n - p^{n-1} + p^{n-2} - \cdots - 1 + 2)$$

$$u_{p^{n+2}} = \frac{1}{2}\left[-\frac{1-(-p)^{n+3}}{1+p} + 2\right]$$

So, the property is checked if n is odd.

Conclusion
We obtain, for p an odd prime number :

- If k is even

$$u_{p^k} = \frac{1}{2}\left[\frac{1-(-p)^{k+1}}{1+p} + 1\right]$$

- If k is odd

$$u_{p^k} = \frac{1}{2}\left[-\frac{1-(-p)^{k+1}}{1+p} + 2\right]$$

3 Find a general formula for u_n

3.1 Conjecture

We know that for all $n \geqslant 2$, there is an unique decomposition as : $n = p_1^{k_1} \cdot p_2^{k_2} \dots p_r^{k_r}$ with $p_1, p_2 \dots p_r$ different prime numbers and $(k_1, k_2 \dots k_r) \in \mathbb{N}^r$

With values tables, we can conjecture :

$$u_n = u_{p_1^{k_1}} \cdot u_{p_2^{k_2}} \dots u_{p_r^{k_r}}$$

So, for example : $u_{350} = 88$
But $u_7 \cdot u_{5^2} \cdot u_2 = 4 \times 11 \times 2 = 88$
So, we have $u_{350} = u_7 \cdot u_{5^2} \cdot u_2$

3.2 Proof of the conjecture

3.2.1 Notations

We can write that : $u_n = \sharp A_n = \sharp\{T_k[n]/k \in \mathbb{Z}\} = \sharp\{k^2[n]/k \in \mathbb{Z}\}$ thanks to property 4.

We denote for all i such as $1 \leqslant i \leqslant r$:

$$u_{p_i}^{k_i} = \sharp A_i = \sharp\{k^2[p_i^{k_i}]/k \in \mathbb{Z}\}$$

We denote by Φ the map :

$$\Phi : \left\{ \begin{array}{ccc} A_n & \to & A_1 \times A_2 \times \dots \times A_r \\ k^2[n] & \mapsto & k^2[p_i^{k_i}]; k^2[p_2^{k_2}]; \dots; k^2[p_r^{k_r}] \end{array} \right.$$

3.2.2 Let us prove that Φ is an injective function

Denote by k and l two integers such as : $\Phi(k^2) = \Phi(l^2)$
We obtain : $\forall i \in [1; r], k^2 \equiv l^2[p_i^{k_i}]$
So, $\forall i \in [1; r], p_i^{k_i} \mid k^2 - l^2$.
But, $\gcd(p_1^{k_1}, p_2^{k_2}, \dots, p_r^{k_r}) = 1$.

$$\prod_{i=1}^{r} p_i^{k_i} \mid k^2 - l^2$$

$$n \mid k^2 - l^2$$

We conclude that : If $\Phi(k) = \Phi(l)$, so $k \equiv l[n]$.

Φ is injective.

3.2.3 Let us prove that Φ is a surjective function

Let $(l_1, l_2, \cdots, l_r) \in A_1 \times A_2 \times \cdots \times A_r$
As $\gcd(p_1^{k_1}, p_2^{k_2}, \cdots, p_r^{k_r}) = 1$, thanks to the "Chinese remainder theorem" :

$\exists k / \forall i \in [1; r], k \equiv l_i [p_i^{k_i}]$
$\exists k / \forall i \in [1; r], k^2 \equiv l_i^2 [p_i^{k_i}]$

We obtain : $\Phi(k) = (l_1; l_2; \cdots; l_r)$

Φ is surjective.

3.2.4 Conclusion

We proved that Φ is injective and surjective.
So, we can conclude that Φ is bijective.
We have :

$$u_n = \prod_{i=1}^{r} u_{p_i}^{k_i} = \sharp A_n = \sharp(A_1 \times A_2 \times \cdots \times A_r) = \prod_{i=1}^{r} \sharp A_i$$

We can conclude that, in a general case :

$$u_n = u_{p_1^{k_1}} \cdot u_{p_2^{k_2}} \ldots u_{p_r^{k_r}}$$

4 Study of $P(x)$ a polynomial with rational coefficients

4.1 Polynomial with integer coefficients

First, a polynomial $P(x)$ with integer coefficients is obviously defined by : $\forall x \in \mathbb{Z}, P(x) \in \mathbb{Z}$
Let us study these polynomials for the degrees 0 and 1

4.1.1 Degree 0

Let be $P(x) = a$
This function is constant. But, according to the Euclid's theorem, we have : $a = qn + r$ such as $0 \leqslant r < a$ with an unique r for every n.

So, there is only one residue modulo n.

4.1.2 Degree 1

Let $P(x) = ax + b$
With values tables, we can conjecture that the number of different residues modulo n for a polynomial of degree 1 is :

$$\frac{n}{a \wedge n}$$

- Influence of b on the number of different residues
  For all $x \in \mathbb{Z}$, we set out the euclidean division of $P(x)$ by n :
  $ax + b = nq + r$ with $0 \leqslant r < n$
  So, $ax = nq + (r - b)$
  But, it may be that $(r - b)$ is no longer between 0 and n.
  So, $r - b = kn + r'$ with $0 \leqslant r' < n$
  For each b, we can study $ax \equiv r'[n]$

  b has no influence on the number of residues of $P(x)$ modulo n. We shall study the cases where $P(x) = ax$

- Proof of the conjecture

  – $a \wedge n = 1$
  According to Bezout's theorem, there is $x, y \in \mathbb{Z}$ such as $ax + ny = 1$
  $\forall k \in \mathbb{Z}$, $\exists (x; y) \in \mathbb{Z}^2 \mid ax + ny = k$
  We obtain : $ax = -ny + k \iff ax \equiv k[n]$
  But, this congruence is valid for all integer k, therefore for $k \in [\![0, n - 1]\!]$

  The number of residues is n, it satisfies the conjecture

– $a \wedge n = d$ with $d \in \mathbb{N}^*$
We can write : $a = da'$ and $n = dn'$ with $a' \wedge n' = 1$

According to the Bezout's theorem, there are integers x and y such as :

$ax + ny = d \iff da'x + dn'y = kd \iff a'x + n'y = k$

But $a' \wedge n' = 1$

So, the number of different residues of $a'x$ modulo n' is $n' = \frac{n}{d}$: all the integers from 0 to $n' - 1$.

Consequently, the number of different residues of $P(x) = ax$ modulo n is also $\frac{n}{d} = \frac{n}{a \wedge n}$: all the multiples of d from 0 to $n - 1$

Finally, the number of different residues of $P(x) = ax + b$ modulo n is :
$$\frac{n}{a \wedge n}$$

4.2 Polynomial with rational coefficients

4.2.1 Shape of functions to study

We search if the polynomials with integer coefficient are the only to satisfy $\forall x \in \mathbb{Z} \mid P(x) \in \mathbb{Z}$

For example, the functionnal $T(x) = \frac{x(x-1)}{2}$ inspired to the formula of the triangular numbers is with rational coefficients and non-integer, but checks $T(x) \in \mathbb{Z}$

Finally, we can wonder if the same is true for all functions of the form of :

$$T_n(x) = \frac{x(x-1)(x-2)...(x-(n-1))}{n!}$$

For $n = 0$, we have $T_0(x) = 1 \in \mathbb{Z}$

Let be three different cases.

- If $0 \leqslant k < n$

$$T_n(k) = \frac{k(k-1)(k-2)...(k-k)...(k-(n-1))}{n!} = \frac{k(k-1)(k-2)...0...(k-(n-1))}{n!} = 0$$

Therefore, we have : $T_n(x) \in \mathbb{Z}$.

- If $k \geqslant n$

$$T_n(k) = \frac{k(k-1)(k-2)...(k-(n-1))}{n!} = \frac{k!}{(k-n)!n!} = \begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{Z}$$

- If $k < 0$

$$T_n(k) = \frac{k(k-1)(k-2)...(k-k)...(k-(n-1))}{n!} = (-1)^n.\frac{(-k)(-k+1)...(-k+n-1)}{n!}$$

$$T_n(k) = (-1)^n.\frac{(-k+n-1)!}{(-k-1)!n!} = (-1)^n \begin{pmatrix} n-k-1 \\ n \end{pmatrix} \in \mathbb{Z}$$

Finally, all the functions $T_n(x) \in \mathbb{Z}$.
Furthermore, the functions on the form of
$P(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x) \in \mathbb{Z}$ with λ_0, λ_1 ... $\lambda_n \in \mathbb{Z}^{n+1}$

4.2.2 Reciprocal

We can wonder if these functions are the only functions with rational coefficients checking this condition.

Let be $P(x)$ a nonzero polynomial. Denote n the degree of $P(x)$ and a_n his dominant coefficient.

- Let us prove that $P(x) - n!a_n T_n(x)$ is a polynomial of degree less than or equal to $n-1$.

  We can write : $P(x) = a_n x^n + Q(x)$ with $Q(x)$ a polynomial of degree less than or equal to $n-1$
  But, T_n is a product of n term of degree from 1 to n and consequently of degree n. So, his dominant coefficient is $\frac{1}{n!}$ and his dominant term is $\frac{x^n}{n!}$. We can write that $Tn(x) = \frac{x^n}{n!} + R(x)$ with $R(x)$ a polynomial of degree less than or equal to $n-1$

  We deduce that :

$$P(x) - n!a_n T_n(x) = a_n x^n + Q(x) - n!a_n \left(\frac{x^n}{n!} + R(x) \right) = a_n x^n + Q(x) - a_n x^n - n!a_n R(x)$$

$$= Q(x) - n!a_n R(x)$$

  $P(x) - n!a_n T_n(x)$ is the difference between two polynomials of degree less than or equal to $n-1$. His degree is less than or equal to $n-1$.

- Existence of λ_0, λ_1 ... $\lambda_n \in \mathbb{R}^{n+1}$.

  Let us prove by induction that there are λ_0, λ_1 ... $\lambda_n \in \mathbb{R}^{n+1}$ such as $P(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x)$

  Basis step
  If $P(x)$ is of degree 0, we have : $P(x) = a \in \mathbb{R}$.
  But, $T_0(x) = 1$.
  So, $P(x) = a.T_0(x)$. The property is checked.

  Inductive step
  Suppose that for one n the property is checked.
  Show that it is also checked for $n+1$

  If the degree of $P(x)$ is lower or equal to n, so there is $(\lambda_0, \lambda_1 ... \lambda_n) \in \mathbb{Z}^{n+1}$ such as $P(x) = \lambda_0 T_0 + \lambda_1 T_1 + ... + \lambda_n T_n$ according to our conjecture.

  If the degree of $P(x)$ is $n+1$, we denote a_{n+1} nonzero his dominant coefficient.
  But, according to the previous demonstration, $P(x) - (n+1)a_{n+1}T_{n+1}(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x)$.

We deduce that : $P(x) == \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x) + (n+1)! a_{n+1} T_{n+1}(x)$.
The property is checked for $n+1$

Conclusion

For all integer n, there are $(\lambda_0, \lambda_1 \ ... \ \lambda_n) \in \mathbb{R}^{n+1}$ such as :
$P(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x)$

- Let us prove by high induction that $\lambda_0, \lambda_1 \ ... \ \lambda_n \in \mathbb{Z}^{n+1}$

Let be $\forall k \in \mathbb{Z}$, $P(k) \in \mathbb{Z}$
We can notice that $T_n(n) = \dfrac{n!}{n!} = 1$
According to the previous demonstration, we know that there are $\lambda_0, \lambda_1 \ ... \ \lambda_n \in \mathbb{R}^{n+1}$ such as :
$P(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x)$.

Basis step
We have $P(0) = \lambda_0 T_0(0) = \lambda_0$ according to the previous remark
But, if $P(0) \in \mathbb{Z}$, so $\lambda_0 \in \mathbb{Z}$.

Similarly, we have $P(1) = \lambda_0 T_0(1) + \lambda_1 T_1(1) = \lambda_1 T_1(1) + \lambda_1$
That is to say : $\lambda_1 = P(1) - \lambda_0 T_0(1)$.
But, if $P(1) \in \mathbb{Z}$, and $\lambda_0 T_0(1) \in \mathbb{Z}$, so $\lambda_1 \in \mathbb{Z}$

Inductive step
Suppose that $\lambda_0, (\lambda_1 \ ... \ \lambda_k) \in \mathbb{R}^{n+1}$ for $0 \leqslant k < n$
Show also that $\lambda_{k+1} \in \mathbb{Z}$

We have : $P(k+1) = \lambda_0 T_0(k+1) + \lambda_1 T_1(k+1) + ... + \lambda_k T_k(k+1) + \lambda_{k+1} T_{k+1}(k+1) = \lambda_0 T_0(k+1) + \lambda_1 T_1(k+1) + ... + \lambda_k T_k(k+1) + \lambda_{k+1}$.

Thus, $\lambda_{k+1} = P(k+1) - (\lambda_0 T_0(k+1) + \lambda_1 T_1(k+1) + ... + \lambda_k T_k(k+1))$

But, $\lambda_0 T_0(k+1) + \lambda_1 T_1(k+1) + ... + \lambda_k T_k(k+1) \in \mathbb{Z}$ and we want $P(k+1) \in \mathbb{Z}$

So, $\lambda_{k+1} \in \mathbb{Z}$.

Conclusion

If $P(x) \in \mathbb{Z}$, there are $(\lambda_0, \lambda_1 \ ... \ \lambda_k) \in \mathbb{Z}^{n+1}$ such as :
$P(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x)$

Finally, we demonstrated the following double implication :
Denote : $T_n(x) = \dfrac{x(x-1)(x-2)...(x-(n-1))}{n!}$

$$P(x) \in \mathbb{Z} \iff \exists (\lambda_0, \lambda_1 \ ... \ \lambda_n) \in \mathbb{Z}^{n+1} \mid P(x) = \lambda_0 T_0(x) + \lambda_1 T_1(x) + ... + \lambda_n T_n(x)$$

The functionnals we will study in this question are necessarily of this form.
First, we have to study all the functions T_n.
We can conjecture that for all n, T_n admits 2^m differents residues modulo 2^m.
We can denote that :

$$T_{n+1}(x) = \frac{x(x-1)(x-2)...(x-(n-1))(x-n)}{(n+1)!} = T_n(x).\frac{x-n}{n+1}$$

We should be able to use this relation to demonstrate the property for any integer.

APPENDIXES

We can check that the sequences are periodic.

Values table of U_n

Triangular numbers	U_2=2	U_3=2	U_4=4	U_5=3	U_6=4	U_7=4	U_8=8	U_9=4	U_{10}=6	U_{11}=6	U_{12}=6	U_{13}=7	U_{14}=8	U_{15}=6
T_1=1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
T_2=3	1	0	3	3	3	3	3	3	3	3	3	3	3	3
T_3=6	0	0	2	1	0	6	6	6	6	6	6	6	6	6
T_4=10	0	1	2	0	4	3	2	1	0	10	10	10	10	10
T_5=15	1	0	3	0	3	1	7	6	5	4	3	2	1	0
T_6=21	1	0	1	1	3	0	5	3	1	10	9	8	7	6
T_7=28	0	1	0	3	4	0	4	1	8	6	4	2	0	13
T_8=36	0	0	0	1	0	1	4	0	6	3	0	10	8	6
T_9=45	1	0	1	0	3	3	5	0	5	1	9	6	3	0
T_{10}=55	1	1	3	0	1	6	7	1	5	0	7	3	13	10
T_{11}=66	0	0	2	1	0	3	2	3	6	0	6	1	10	6
T_{12}=78	0	0	2	3	0	1	6	6	8	1	6	0	8	3
T_{13}=91	1	1	3	1	1	0	3	1	1	3	7	0	7	1
T_{14}=105	1	0	1	0	3	0	1	6	5	6	9	1	7	0
T_{15}=120	0	0	0	0	0	1	0	3	0	10	0	3	8	0
T_{16}=136	0	1	0	1	4	3	0	1	6	4	4	6	10	1
T_{17}=153	1	0	1	3	3	6	1	0	3	10	9	10	13	3
T_{18}=171	1	0	3	1	3	3	3	0	1	6	3	2	3	6
T_{19}=190	0	1	2	0	4	1	6	1	0	3	10	8	8	10
T_{20}=210	0	0	2	0	0	0	2	3	0	1	6	2	0	0
T_{21}=231	1	0	3	1	3	0	7	6	1	0	3	10	7	6
T_{22}=253	1	1	1	3	1	1	5	1	3	0	1	6	1	13
T_{23}=276	0	0	0	1	0	3	4	6	6	1	0	3	10	6
T_{24}=300	0	0	0	0	0	6	4	3	0	3	0	1	6	0
T_{25}=325	1	1	1	0	1	3	5	1	5	6	1	0	3	10
T_{26}=351	1	0	3	1	3	1	7	0	1	10	3	0	1	6
T_{27}=378	0	0	2	3	0	0	2	0	8	4	6	1	0	3
T_{28}=406	0	1	2	1	4	0	6	1	6	10	10	3	0	1
T_{29}=435	1	0	3	0	3	1	3	3	5	6	3	6	1	0
T_{30}=465	1	0	1	0	3	3	1	6	5	3	9	10	3	0
T_{31}=496	0	1	0	1	4	6	0	1	6	1	4	2	6	1
T_{32}=528	0	0	0	3	0	3	0	6	8	0	0	8	10	3
T_{33}=561	1	0	1	1	3	1	1	3	1	0	9	2	1	6
T_{34}=595	1	1	3	0	1	0	3	1	5	1	7	10	7	10
T_{35}=630	0	0	2	0	0	0	6	0	0	3	6	6	0	0
T_{36}=666	0	0	2	1	0	1	2	0	6	6	6	3	8	6
T_{37}=703	1	1	3	3	1	3	7	1	3	10	7	1	3	13
T_{38}=741	1	0	1	1	3	6	5	3	1	4	9	0	13	6
T_{39}=780	0	0	0	0	0	3	4	6	0	10	0	0	10	0
T_{40}=820	0	1	0	0	4	1	4	1	0	6	4	1	8	10
T_{41}=861	1	0	1	1	3	0	5	6	1	3	9	3	7	6
T_{42}=903	1	0	3	3	3	0	7	3	3	1	3	6	7	3
T_{43}=946	0	1	2	1	4	1	2	1	6	0	10	10	8	1
T_{44}=990	0	0	2	0	0	3	6	0	0	0	6	2	10	0
T_{45}=1035	1	0	3	0	3	6	3	0	5	1	3	8	13	0
T_{46}=1081	1	1	1	1	1	3	1	1	1	3	1	2	3	1
T_{47}=1128	0	0	0	3	0	1	0	3	8	6	0	10	8	3
T_{48}=1176	0	0	0	1	0	0	0	6	6	10	0	6	0	6
T_{49}=1225	1	1	1	0	1	0	1	1	5	4	1	3	7	10
T_{50}=1275	1	0	3	0	3	1	3	6	5	10	3	1	1	0
T_{51}=1326	0	0	2	1	0	3	6	3	6	6	6	0	10	6
T_{52}=1378	0	1	2	3	4	6	2	1	8	3	10	0	6	13
T_{53}=1431	1	0	3	1	3	3	7	0	1	1	3	1	3	6
T_{54}=1485	1	0	1	0	3	1	5	0	5	0	9	3	1	0
T_{55}=1540	0	1	0	0	4	0	4	1	0	0	4	6	0	10
T_{56}=1596	0	0	0	1	0	0	4	3	6	1	0	10	0	6

We can check that our formulas are right from u_1 to u_{400}.

n	Un	n	Un	n	Un	n	Un	n	Un	n	Un	n	Un	n	Un	n	Un	n	Un
1	1	41	21	81	31	121	56	161	48	201	68	241	121	281	141	321	108	361	172
2	2	42	16	82	42	122	62	162	62	202	102	242	112	282	96	322	96	362	182
3	2	43	22	83	42	123	42	163	82	203	60	243	92	283	142	323	90	363	112
4	4	44	24	84	32	124	64	164	84	204	72	244	124	284	144	324	124	364	112
5	3	45	12	85	27	125	53	165	36	205	63	245	66	285	60	325	77	365	111
6	4	46	24	86	44	126	32	166	84	206	104	246	84	286	84	326	164	366	124
7	4	47	24	87	30	127	64	167	84	207	48	247	70	287	84	327	110	367	184
8	8	48	32	88	48	128	128	168	64	208	112	248	128	288	128	328	168	368	192
9	4	49	22	89	45	129	44	169	79	209	60	249	84	289	137	329	96	369	84
10	6	50	22	90	24	130	42	170	54	210	48	250	106	290	90	330	72	370	114
11	6	51	18	91	28	131	66	171	40	211	106	251	126	291	98	331	166	371	108
12	8	52	28	92	48	132	48	172	88	212	108	252	64	292	148	332	168	372	128
13	7	53	27	93	32	133	40	173	87	213	72	253	72	293	147	333	76	373	187
14	8	54	22	94	48	134	68	174	60	214	108	254	128	294	88	334	168	374	108
15	6	55	18	95	30	135	33	175	44	215	66	255	54	295	90	335	102	375	106
16	16	56	32	96	64	136	72	176	96	216	88	256	256	296	152	336	128	376	192
17	9	57	20	97	49	137	69	177	60	217	64	257	129	297	66	337	169	377	105
18	8	58	30	98	44	138	48	178	90	218	110	258	88	298	150	338	158	378	88
19	10	59	30	99	24	139	70	179	90	219	74	259	76	299	84	339	114	379	190
20	12	60	24	100	44	140	48	180	48	220	72	260	84	300	88	340	108	380	120
21	8	61	31	101	51	141	48	181	91	221	63	261	60	301	88	341	96	381	128
22	12	62	32	102	36	142	72	182	56	222	76	262	132	302	152	342	80	382	192
23	12	63	16	103	52	143	42	183	62	223	112	263	132	303	102	343	151	383	192
24	16	64	64	104	56	144	64	184	96	224	128	264	96	304	160	344	176	384	256
25	11	65	21	105	24	145	45	185	57	225	44	265	81	305	93	345	72	385	72
26	14	66	24	106	54	146	74	186	64	226	114	266	80	306	72	346	174	386	194
27	11	67	34	107	54	147	44	187	54	227	114	267	90	307	154	347	174	387	88
28	16	68	36	108	44	148	76	188	96	228	80	268	136	308	96	348	120	388	196
29	15	69	24	109	55	149	75	189	44	229	115	269	135	309	104	349	175	389	195
30	12	70	24	110	36	150	44	190	60	230	72	270	66	310	96	350	88	390	84
31	16	71	36	111	38	151	76	191	96	231	48	271	136	311	156	351	77	391	108
32	32	72	32	112	64	152	80	192	128	232	120	272	144	312	112	352	192	392	176
33	12	73	37	113	57	153	36	193	97	233	117	273	56	313	157	353	177	393	132
34	18	74	38	114	40	154	48	194	98	234	56	274	138	314	158	354	120	394	198
35	12	75	22	115	36	155	48	195	42	235	72	275	66	315	48	355	108	395	120
36	16	76	40	116	60	156	56	196	88	236	120	276	96	316	160	356	180	396	96
37	19	77	24	117	28	157	79	197	99	237	80	277	139	317	159	357	72	397	199
38	20	78	28	118	60	158	80	198	48	238	72	278	140	318	108	358	180	398	200
39	14	79	40	119	36	159	54	199	100	239	120	279	64	319	90	359	180	399	80
40	24	80	48	120	48	160	96	200	88	240	96	280	96	320	192	360	96	400	176