TEAM France 3

Problem 2 **A number of residues**

We study here the different residues of the triangular numbers modulo an integer. To simplify the task, we often use periocity properties. The answer is rather easy for the powers of 2, and all residues are obtained. It is a particular case of prime powers. And, we can suppose that the function giving the number of different residues as a function of n is multiplicative (that is, if a and b are coprime, $f(ab) = f(a)f(b)$.

General remarks and properties

First of all, one remark easily that for all natural n, $u_n \leq n$.

Now, we establish a property on the periodicity of the sequence (T_k) modulo n. Let $n \in \mathbb{N}$ and k and k' two positive integers such that $k \equiv k' \mod n$. Let b an integer such that $k = k' + nb$, we have :

$$\begin{aligned} T_k - T'_k &= \frac{k(k+1) - k'(k'+1)}{2} \\ T_k - T'_k &= \frac{(k'+nb)(k'+nb+1) - k'(k'+1)}{2} \\ T_k - T'_k &= \frac{k'^2 + k' + 2k'nb + (nb)^2 + nb - k'^2 - k'}{2} \\ T_k - T'_k &= k'nb + \frac{nb(nb+1)}{2} \end{aligned}$$

If n and 2 are coprime (that is, n is odd) then by Euclid's lemma, $\frac{b(nb+1)}{2}$ is an integer, so that

$$T_k \equiv T'_k mod[n]$$

Thus, it suffices to consider T_k with $1 \leq k \leq n$ to determinate u_n.
If n is even, the proof above doesn't work. However, if $k \equiv k' \mod 2n$ with $k = k' + 2cn$, we have as before :

$$T_k - T'_k = 2nk'c + \frac{2nc(nc+1)}{2}$$

which is divisible by n, so that it suffices to consider T_k with $1 \leq k \leq 2n$. We call this property the periodicity property.

Powers of 2

Let n and N be two integers such that $n = 2^N$. Consider $k, k' \in \mathbb{N}$ two distinct integers such that $0 \leq k' < k \leq 2^N - 1$. We have :

$$T_k - T_{k'} = \frac{(k-k')(k+k'+1)}{2}.$$

- If $k - k'$ is even, then $k + k' + 1$ is odd and $0 < k - k' < 2^N$ so that $T_k - T_{k'} \not\equiv 0 \mod 2^N$.
- If $k - k'$ is odd, then $k + k' + 1$ is even. Furthermore $k \leq 2^N - 1$, $k' \leq 2^N - 2$, so $k + k' + 1 \leq 2^{N+1} - 3$ and $\frac{k+k'+1}{2} \not\equiv 0 \mod 2^N$, therefore $T_k - T_{k'} \not\equiv 0 \mod 2^N$.

Thus for all $k, k' \in \mathbb{N}$ such that $0 \leq k' < k \leq 2^N - 1$, T_k and $T_{k'}$ do not have the same residue modulo n, so that we obtain n different residues modulo n. Hence $u_n = n$.

Powers of a prime number.

Suppose now that $n = p^N$, where p is an odd prime number and $N \in \mathbb{N}^*$. First, we establish two important lemmas.

Lemma 1 *The sequence (T_k) is periodic modulo n, and its period is p^N.*

This is a corollary of the peridicity property, since p^N is odd.

Lemma 2 *The numbers T_k, $k \in \mathbb{N}$ verify the following symetry property :*

$$T_k \equiv T_{p^N-k-1} \mod p^N, \ \forall k \in \mathbb{N} \text{ so that } 0 \leq k \leq p^N - 1. \tag{1}$$

Proof : Let $k \in \mathbb{N}$ tel que $0 \leq k \leq p^N - 1$. Then

$$T_{p^N-1-k} = \frac{(p^N - k - 1)(p^N - k)}{2} = \frac{p^{2N} - kp^N - kp^N + k^2 - p^N + k}{2}$$
$$T_{p^N-1-k} = \frac{p^N(p^N - 2k - 1)}{2} + \frac{k(k+1)}{2} = \frac{p^N(p^N - 2k - 1)}{2} + T_k$$

Since $p^N - 2k - 1$ is even, $\dfrac{p^N - 2k - 1}{2}$ is an integer. Thus,

$$T_{p^N-1-k} \equiv T_k \mod p^N$$

□

Using the Lemma 1, we can consider T_k for $0 \leq k \leq p^N - 1$, that is p^N integers. Using the Lemma 2, there are at most $\frac{p^N-1}{2}$ different residues modulo n for the triangular numbers from T_0 to T_{p^N-1}, since each residue has an even number of occurences. Therefore, we have

$$u_n \leq \frac{p^N - 1}{2} + 1 = \frac{p^N + 1}{2}$$

Remark 1 *The sequence (T_k) modulo n with $0 \leq k \leq p^N - 1$ is a "palindrome" (this comes directly from the symetrey property).*

Now, let's show that $u_p = \dfrac{p-1}{2} + 1$.

Let k and k' be two distinct integers, such that $0 \leq k' < k \leq \dfrac{p-1}{2}$. Notice that $0 \leq k' < k \leq \dfrac{p-1}{2}$, so that we have $k - k' < k + k' + 1 < p$, so

$$T_k - T_{k'} = \frac{(k - k')(k + k' + 1)}{2} \not\equiv 0 \mod p.$$

Therefore, the residues of T_k for $0 \leq k \leq \dfrac{p-1}{2}$ are all distincts, so the upper bound we established is also a lower bound here :

$$u_p = \frac{p-1}{2} + 1.$$

Let's now look at the more general case. Suppose $N \geq 2$ and consider u_{p^N}.

Consider the palindrome of the rests modulo p^N with the center $T_{\frac{p^N-1}{2}}$. Inside we find another palindrome with the center $T_{\frac{p^{N-1}-1}{2}}$.

Now let's show that

$$T_{\frac{p^{N-1}-1}{2}+kp} \equiv T_{\frac{p^{N-1}-1}{2}-kp} \mod p^N, \quad \forall k \in \mathbb{N}.$$

We have

$$\begin{aligned}
T_{\frac{p^{N-1}-1}{2}+kp} &= \frac{1}{2}\left(\frac{p^{N-1}-1}{2} + kp\right)\left(\frac{p^{N-1}+1}{2} + kp\right) \\
&= \frac{1}{2}\left(\frac{p^{2N-2}-1}{4} + kp\frac{p^{N-1}-1}{2} + kp\frac{p^{N-1}+1}{2} + k^2p^2\right) \\
&= T_{\frac{p^{N-1}-1}{2}-kp} + \frac{1}{2}(kp(p^{N-1}-1) + kp(p^{N-1}+1)) \\
&= T_{\frac{p^{N-1}-1}{2}-kp} + \frac{1}{2}kp2p^{N-1} \\
&= T_{\frac{p^{N-1}-1}{2}-kp} + kp^N,
\end{aligned}$$

that is exactly what we wanted to prove.

It means that the rest modulo p^N of the triangular number of rank $\frac{p^{N-1}-1}{2} + kp$ is the same as the rest modulo p^N of the triangular number of rank $\frac{p^{N-1}-1}{2} - kp$ for any k. Thus those numbers contribute as one for u_{p^N}.

Between the triangular numbers $T_{\frac{p^{N-1}-1}{2}}$ and $T_{\frac{p^N-1}{2}}$ there are exactly $\dfrac{p^N-1}{2} - \dfrac{p^{N-1}-1}{2} = \dfrac{p^{N-1}(p-1)}{2}$ triangular numbers.

Starting from $\dfrac{p^{N-1}-1}{2}$ every p-th triangular number has the same rest that was met before. Thus

$$u_{p^N} \leq \frac{p^N-1}{2} + 1 - \frac{(p-1)p^{N-2}}{2},$$

where the last term represents the number of rest that we have counted twice : between $T_{\frac{p^{N-1}-1}{2}}$ and $T_{\frac{p^N-1}{2}}$ one of every p numbers has the same residue as another one.

Now, we can still find another palindrome inside the palindrome of the rests modulo p^N with the center $T_{\frac{p^N-1}{2}}$. If $N \geq 4$, it is the palindrome with the center $T_{\frac{p^{N-2}-1}{2}}$.

Let's show that

$$T_{\frac{p^{N-2}-1}{2}+kp^2} \equiv T_{\frac{p^{N-2}-1}{2}-kp^2} \mod p^N, \quad \forall k \in \mathbb{N}.$$

We have

$$\begin{aligned}
T_{\frac{p^{N-2}-1}{2}+kp^2} &= \frac{1}{2}\left(\frac{p^{N-2}-1}{2}+kp^2\right)\left(\frac{p^{N-2}+1}{2}+kp^2\right) \\
&= \frac{1}{2}\left(\frac{p^{2N-4}-1}{4}+kp^2\frac{p^{N-2}-1}{2}+kp^2\frac{p^{N-2}+1}{2}+k^2p^4\right) \\
&= T_{\frac{p^{N-2}-1}{2}-kp^2}+\frac{1}{2}(kp^2(p^{N-2}-1)+kp^2(p^{N-2}+1)) \\
&= T_{\frac{p^{N-2}-1}{2}-kp^2}+\frac{1}{2}kp^2*2p^{N-2} \\
&= T_{\frac{p^{N-2}-1}{2}-kp^2}+kp^N,
\end{aligned}$$

that is exactly what we wanted to prove.

It means that the rest modulo p^N of the triangular number of rank $\frac{p^{N-2}-1}{2}+kp^2$ is the same as the rest modulo p^N of the triangular number of rank $\frac{p^{N-2}-1}{2}-kp^2$ for any k. Thus those numbers contribute as one for u_{p^N}.

Between the triangular numbers $T_{\frac{p^{N-2}-1}{2}}$ and $T_{\frac{p^{N-1}-1}{2}}$ there are exactly $\frac{p^{N-1}-1}{2}-\frac{p^{N-2}-1}{2}=\frac{p^{N-2}(p-1)}{2}$ triangular numbers.

Starting from $\frac{p^{N-2}-1}{2}$ every p^2-th triangular number has the same rest that was met before. Thus, for $N \geq 4$

$$u_{p^N} \leq \frac{p^N-1}{2}+1-\frac{(p-1)p^{N-2}}{2}-\frac{(p-1)p^{N-4}}{2},$$

where the last term represents the number of rest that we have counted twice : between $T_{\frac{p^{N-2}-1}{2}}$ and $T_{\frac{p^{N-1}-1}{2}}$ one of every p^2 numbers has the same residue as another one.

The same resasoning gives us, if $N \geq 6$,

$$u_{p^N} \leq \frac{p^N-1}{2}+1-\frac{(p-1)p^{N-2}}{2}-\frac{(p-1)p^{N-4}}{2}-\frac{(p-1)p^{N-6}}{2},$$

And more generally, if $N \geq 2k$, where $k \in \mathbb{N}$ is maximal such that $N \geq 2k$, we have

$$u_{p^N} \leq \frac{p^N-1}{2}+1-\frac{(p-1)p^{N-2}}{2}-\frac{(p-1)p^{N-4}}{2}-\frac{(p-1)p^{N-6}}{2}-\cdots-\frac{(p-1)p^{N-2k}}{2},$$

Next we will prove that among the numbers with rank greater than $\frac{p^{N-1}-1}{2}$, only the numbers whose rank is of the type $\frac{p^{N-1}-1}{2}+kp$ have rests equals to the rest of some triangular number of smaller rank.
Let R and x be integers such that $R = \frac{p^N-1}{2}+kp+n$ with $0 \leq n \leq p$ and with k an integer such that $0 \leq x \leq R \leq \frac{p^N-1}{2}$
We have to prove that $T_R - T_x \not\equiv 0 \mod p^N$, for any $0 < x < R$.
That is to say that p^N cannot divide $\frac{(R-x)(R+x+1)}{2}$
For k set, the only way for $R - x \equiv 0 \mod p^A$, with A an integer such that $1 \leq A \leq N-1$, and k prominenetly such that $R > p^A$, is that $x \equiv R \mod p^A$, so
$x = \frac{p^N-1}{2}+kp+n-Qp^A = p\frac{p^{N-2}-1}{2}+\frac{p-1}{2}+kp+n-Qp^A$
And $x \equiv \frac{p-1}{2}+n \mod p$
So, if $R - x \equiv 0 \mod p^A$, we have
$R+x+1 \equiv \frac{p^N-1}{2}+kp+n+x+1 \equiv p-1+2n+1 \equiv 2n \mod p$.

But $n \not\equiv 0 \mod p$, so $pgcd(R+x+1, p^N) = 1$, and $pgcd(R-x, p^N) * pgcd(R+x+1, p^N) < p^N$.

Therefore, p^N cannot divide $T_R - T_x$, and among the numbers with rank greater than $\frac{p^{N-1}-1}{2}$, only the numbers whose rank is of the type $\frac{p^{N-1}-1}{2}+kp$ have rests equals to the rest of some triangular number of smaller rank.

Likewise, among the numbers with rank greater than $\frac{p^{N-2}-1}{2}$ and inferior or equal than $\frac{p^{N-1}-1}{2}$, only the numbers whose rank is of the type $\frac{p^{N-2}-1}{2}+kp^2$ have rests equals to the rest of some triangular number of smaller rank. It goes the same for the numbers whose rank is of the type $\frac{p^{N-3}-1}{2}+kp^3$ and is greater than $\frac{p^{N-3}-1}{2}$ and inferior or equal than $\frac{p^{N-2}-1}{2}$, and etc.

So, we have $u_{p^N} = \frac{p^N-1}{2}+1-\frac{(p-1)p^{N-2}}{2}-\frac{(p-1)p^{N-4}}{2}-\frac{(p-1)p^{N-6}}{2}-\cdots-\frac{(p-1)p^{N-2k}}{2}$

Therefore

$$\text{If } N \text{ is even, then} \quad u_{p^N} = \frac{p^N-1}{2} - \frac{p^{N-1}}{2} + \frac{p^{N-2}}{2} - \cdots - \frac{p}{2} + \frac{1}{2} + 1.$$
$$\text{If } N \text{ is odd, then} \quad u_{p^N} = \frac{p^N-1}{2} - \frac{p^{N-1}}{2} + \frac{p^{N-2}}{2} - \cdots + \frac{p}{2} + 1.$$

Continuing this way, we obtain :

$$\text{If } N \text{ is even, then} \quad u_{p^N} = \frac{p^N-1}{2} - \frac{p^{N-1}-1}{2} + \frac{p^{N-2}-1}{2} - \cdots - \frac{p-1}{2} + 1.$$
$$\text{If } N \text{ is odd, then} \quad u_{p^N} = \frac{p^N-1}{2} - \frac{p^{N-1}-1}{2} + \frac{p^{N-2}-1}{2} - \cdots + \frac{p-1}{2} + 1.$$

So

$$\text{If } N \text{ is even, then} \quad u_{p^N} = \sum_{k=1}^{N} (-1)^k \frac{p^k-1}{2} + 1.$$
$$\text{If } N \text{ is odd, then} \quad u_{p^N} = \sum_{k=1}^{N} (-1)^{k-1} \frac{p^k-1}{2} + 1.$$

Then for even N we have

$$\begin{aligned} u_{p^N} &= \frac{1}{2}\sum_{k=1}^{N}(-1)^k(p^k-1)+1 = \frac{1}{2}\sum_{k=1}^{N}(-1)^k p^k - \frac{1}{2}\sum_{k=1}^{N}(-1)^k + 1 \\ &= \frac{1}{2}\sum_{k=1}^{N}(-1)^k p^k + 1, \end{aligned}$$

since N is even and $\sum_{k=1} N(-1)^k = 0$. Therefore, if N is even, we have

$$\begin{aligned} u_{p^N} &= \frac{1}{2}\sum_{k=1}^{N}(-1)^k p^k + 1 = \frac{1}{2}(-p)\frac{1-(-p)^N}{1-(-p)} + 1 \\ &= \frac{1}{2}(-p)\frac{1-p^N}{1+p} + 1 = \frac{-p(1-p^N)+2+2p}{2+2p} \\ &= \frac{p+p^{N+1}+2}{2+2p}. \end{aligned}$$

The similar computations for N odd yelds

$$u_{p^N} = \frac{2p+p^{N+1}+1}{2+2p}.$$

1 General case.

Let $n = \prod_{i=1}^{m} {p_i}^{a_i}$ be the decomposition of n into prime factors. It seems that : $u_n = u_{\prod_{i=1}^{m} {p_i}^{a_i}} = \prod_{i=1}^{m} u_{{p_i}^{a_i}}$