PROBLEM 2: NUMBER OF RESIDUES

TEAM BULGARIA

Abstract. In the following paper we study the number of residues of triangular numbers modulo $n \in \mathbb{N}$. Using the Chinese Remainder Theorem and a variety of observations in given modules we present formulas for u_n in the required cases.

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 μ_n be the number of distinct members of the sequence $(T_k \mod n)_{k\geq 1}$.

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

Solution: Our aim will be to prove that, when n is a power of 2, $u_n = n$. Let $n = 2^p$. The different residues modulo n are exactly n, so $u_n \leq n$.

We will focus on the natural numbers between 1 and $n-1$. Let us assume that there are 2 different natural numbers k, l, which satisfy the following conditions:

1) $k > l$;

2) $k, l < n \in \mathbb{Z}$;

3) $\frac{k(k+1)}{2} \equiv \frac{l(l+1)}{2} \pmod{n}$;

From **3)** we have: $\frac{k(k+1)}{2} - \frac{l(l+1)}{2} \equiv 0 (\text{mod n})$.

$\frac{k(k+1)}{2} - \frac{l(l+1)}{2} = \frac{k^2+k-l^2-l}{2} = \frac{(k-l)(k+l+1)}{2}$. And again, using **3)** we come to the conclusion that $\frac{(k-l)(k+l+1)}{2} = nt$ for any number $t \in \mathbb{N}$. Furthermore we have $(k-l)(k+l+1) = 2nt = 2 \times 2^p \times t = 2^{p+1}t$ We see that 2^{p+1} divides the right side of this equation, so it will divide the left one as well. But we know that if $k-l$ is odd then $k+l+1$ is even or vice versa. Therefore both can not be divided by 2 in the same time, so $2^{p+1}|k-l$ or $2^{p+1}|k+l+1$. But we know that neither of these is possible since $k-l < n$ and $k-l < n-1+n-2 < 2n = 2^{p+1}$.

So far, we proved that the natural numbers from 1 until $n-1$ give different residues modulo n.

If $\frac{k(k+1)}{2} \equiv 0 (\text{mod } \text{ n})$, then $k(k+1) = 2 \times 2^p l$ ($l \in \mathbb{N}$). Then $2^{p+1}|k$ or $2^{p+1}|k+1$ (k and $k+1$ are co-prime numbers). Therefore $k \geq 2n-1$. From this statement we know that none of the numbers from 1 to $n-1$ gives residue 0 modulo n. To sum up, we found that all of the numbers from 1 to $n-1$ give different residues modulo n and none of them is 0 and that there is a natural number that satisfies the congruence $\frac{k(k+1)}{2} \equiv 0 (\text{mod } \text{ n})$. Therefore, bearing in mind that $u_n \leq n$, we proved that $u_n = n-1+1 = n$.

Problem 2. *Find a formula for u_n where n is a power of a prime number.*

Solution: First of all , we will mention that $8 \times T_k + 1$ is an exact square ($p^2 = (2n+1)^2$). As $(8, p) = 1$, u_n will be equal to the number of quadratic residues modulo(p^k) in the interval $[1, p^k]$, where p is prime and odd number and $k \in \mathbb{N}$.

We will prove that the number of quadratic residues modulo p^k is exactly $[\frac{p^{k+1}-1}{2(p+1)}]+1$.

1). To begin with, we will look at the numbers that are not divided by p. It is true that a is a quadratic residue modulo p^n, if and only if a is a quadratic residue modulo p. It is a well-known fact that in the interval $[ip+1,(i+1)p]$, exactly half of the numbers are quadratic residues, therefore in each of this intervals, there are exactly $\frac{p-1}{2}$ quadratic residues. Bearing in mind that there are exactly p^{n-1} intervals , there are $p^{n-1}\frac{p-1}{2}$ numbers that are quadratic residues modulo p^n, which are not divided by p.

2). Now we will look at the numbers that are divided by p. One such number is $a=p^k$. Now let $1\leq a<p^k$. We know that $p|a$ and let $a=bp^s$ $(1\leq s<k, b\geq 1, p\nmid b)$. If $x_0^2\equiv bp^s(mod\ p^k)$, then $p|x_0$. Let $x_0=p^xy_0$, $p|y_0$. Then $p^{2x}y_0^2\equiv bp^s\ (mod\ p^k)$, $p^{2x-s}y_0^2\equiv b(mod\ p^{k-2x})$. This leads us to $s=2x$, $y_0^2\equiv b(mod\ p^{k-2x})$. $1\leq x<\frac{k}{2}\Leftrightarrow x=1,2,\ldots,[\frac{k-1}{2}]$. As for fixed number x, the number of the numbers in $[1,p^{k-2x}]$ is $p^{k-2x-1}.\frac{p-1}{2}$, this means that the total number is $\sum_{x=1}^{[\frac{k-1}{2}]}$. We should not forget to add 1 for the number $a=p^k$.

From **1).** and **2.)** we find out that the total number of quadratic residues modulo p^k is $p^{k-1}\frac{p-1}{2}+\frac{p-1}{2}\sum_{x=1}^{[\frac{k-1}{2}]}p^{k-2x-1}+1=1+\frac{p^{k+1}-p^{k-1-2[\frac{k-1}{2}]}}{2(p+1)}=[\frac{p^{n+1}-1}{2(p+1)}]+1$.

Problem 3. *Find a formula for u_n in general case.*

Solution: We just have to mention that using the Chinese Remainder Theorem and Problem 2.2, if $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, then $u_n=u_{p_1^{\alpha_1}}u_{p_2^{\alpha_2}}\ldots u_{p_r^{\alpha_r}}$.

Problem 4. *Let $P(x)$ be a polynomial with rational coefficients such that $P(k)$ is integer for every $k\in\mathbb{Z}$. Find the number of distinct residues modulo n in the sequences $(P(k))_{k\geq 1}$, where n is a positive integer.*

Solution: Let $P(x)=Ax+B$, $A,B\in\mathbb{N}$.

4.1 If $LCD(A,n)=1$. Let there be 2 integers k,l and $k\leq l\leq n$, for which $kA\equiv lA\pmod n\Rightarrow (k-l)A\equiv 0\pmod n$ as $LCD(A,n)=1\Rightarrow k-l\equiv 0\pmod n$ and we come to a contradiction. Therefore the answer is n.

Sofia High School of Mathematics, Iskar 61, 1000 Sofia, Bulgaria