Udiviteljnoje riadom

Yurij Bazlov gave me to solve the following problem:

For natural number N consider the set $\{1, 2, 3, \ldots, N\}$. Calculate the number of subsets of this set such that the sum of elements of this subset is divisible on p.

Thinking about this problem I fomrulated the following identity:

$$(1+x)(1+x^2)\ldots(1+x^{p-1}) = 1 + C_p(1+x+\ldots+x^{p-1})\,,\,, C_p = \frac{2^{p-1}-1}{p}$$

which is obeyed if p is prime number and $x^p = 1$.

This identity leads to the fact that number of subsets where sum of the elements has given remainder if we divide on p is equal to $2C_p - 1$. This is for prime p.

I came to this identity experimentally, and I was totally confused trying to prove rigorously this identity: On one hand I "see" that this is true identity for the free ring with constraint $x^p = 1$, and on the other hand if x is primitive root, then left hand side is equal to 1.

Now I realise what happened: Consider examples: Denote by

$$P_N(x) = (1+x)(1+x^2\ldots(1+x^{N-1})$$

and denote by

$$T_N(x) = 1 + x + x^2 + \ldots + x^{N-1}$$

We have that if $N = p$ is a prime then T_N is irreducible polynomial of $\varepsilon_p = e^{\frac{2\pi\sqrt{-1}}{p}}$.

We have

$$P_3(x) = 1 + T_3(x)\,, \quad \text{and } P_3(\varepsilon_3) = 1\,,$$

$$P_5(x) = 1 + 3T_5(x)\,, \quad \text{and } P_5(\varepsilon_5) = 1\,,$$