Problem 2. Recall that the smallest integer greater or equal than a given real number x is denoted by $\lceil x \rceil$ and called the *ceiling* of x. Let p be a prime number and $1 \leq a < p$ an integer. Prove that the number

$$\left\lceil \left(a^{p-1} - 1\right)^{\frac{p}{p-1}} \right\rceil$$

is divisible by p. What can you say when $a = p$?

Solution. Despite its number-theoretical apperance, this problem is mainly about estimates (inequalities).

We will prove the following more general result.

Theorem. *If $a \geq 1$, $k > 1$ are integers then*

$$\left\lceil \left(a^{k-1} - 1\right)^{\frac{k}{k-1}} \right\rceil = a^k - a - \left\lceil \frac{a}{k-1} \right\rceil + 1.$$

Let us first see that this result gives us a solution to the problem. Indeed, if $1 \leq a \leq p-1$ then $\left\lceil \frac{a}{p-1} \right\rceil = 1$ and therefore the number in question is equal to $a^p - a$, which is divisible by p by Fermat's Little Theorem. If $a = p$ then the number in question is $p^p - p - 1$ which is never divisible by p.

It remains to prove the Theorem. When $a = 1$ the result is clear. In what follows, we will assume that $a \geq 2$. We will use the simple remark that in order to find $\lceil x \rceil$ it is sufficient to write x in the form $k - r$ with k an integer and $0 \leq r < 1$. Then $\lceil x \rceil = k$.

The main tool of our proof is the following general and incredibly useful theorem from caclulus:

Taylor's Theorem with Lagrange reminder. *Let f be a function $(n+1)$-differentiable on an open interval (a, b). Then, for any $x, u \in (a, b)$ there exists ζ strictly between x and u such that*

$$f(x) = f(u) + f'(u)(x-u) + \frac{f''(u)}{2!}(x-u)^2 + \cdots + \frac{f^{(n)}(u)}{n!}(x-u)^n + \frac{f^{(n+1)}(\zeta)}{(n+1)!}(x-u)^{n+1}.$$

Here $f^{(k)}(x)$ denotes the k-th derivative of f. Note that when $n = 0$ this is just the Mean Value theorem.

We will apply this theorem to the function $f(x) = (1-x)^{\frac{k}{k-1}}$ with $n = 1$ and $u = 0$:

$$(1-x)^{\frac{k}{k-1}} = 1 - \frac{k}{k-1}x + \frac{\frac{k}{k-1}\frac{1}{k-1}(1-\zeta)^{\frac{k}{k-1}-2}}{2}x^2 = 1 - \frac{k}{k-1}x + \frac{k}{2(k-1)^2(1-\zeta)^{\frac{k-2}{k-1}}}x^2,$$

where ζ is some number between 0 and x. Substituting $x = 1/a^{k-1}$ and multiplying by a^k we get

$$\left(a^{k-1}-1\right)^{\frac{k}{k-1}} = a^k\left(1-\frac{1}{a^{k-1}}\right)^{\frac{k}{k-1}} = a^k - \frac{k}{k-1}a + \frac{k}{2(k-1)^2(1-\zeta)^{\frac{k-2}{k-1}}a^{k-2}},$$

where ζ is some number in the interval $(0, 1/a^{k-1})$. Let us denote the quantity $\frac{k}{2(k-1)^2(1-\zeta)^{\frac{k-2}{k-1}}a^{k-2}}$ by s. Since

$$(1-\zeta)^{\frac{k-2}{k-1}}a^{k-2} = (a^{k-1}-a^{k-1}\zeta)^{\frac{k-2}{k-1}} \geq (a^{k-1}-1)^{\frac{k-2}{k-1}} \geq 1,$$

we have

$$0 < s \leq \frac{k}{2(k-1)^2} \leq \frac{1}{k-1}.$$

Note that

$$\frac{k}{k-1}a = a + \frac{a}{k-1} = a + \left\lceil \frac{a}{k-1} \right\rceil - t$$

where t is of the form $i/(k-1)$ for some integer $0 \leq i \leq k-2$ (i is the smallest non-negative integer such that $a+i$ is divisible by $k-1$). In particular, $0 \leq t \leq (k-2)/(k-1)$. Thus we have the following equality:

$$\left(a^{k-1}-1\right)^{\frac{k}{k-1}} = a^k - a - \left\lceil \frac{a}{k-1} \right\rceil + t + s = a^k - a - \left\lceil \frac{a}{k-1} \right\rceil + 1 - r,$$

where $r = 1-(s+t)$. Clearly $0 < s+t \leq \frac{1}{k-1} + \frac{k-2}{k-1} = 1$ and therefore $0 \leq r < 1$. This proves that

$$\left\lceil \left(a^{k-1}-1\right)^{\frac{k}{k-1}} \right\rceil = a^k - a - \left\lceil \frac{a}{k-1} \right\rceil + 1.$$

Remark. We used in our solution the following simple observation, which is good to keep in mind for potential applications to other problems: if $q = m/n$ is a rational number with denominator $n > 0$ then $\lceil q \rceil - q \leq \frac{n-1}{n}$ and $q - \lfloor q \rfloor \leq \frac{n-1}{n}$.

Exercise. Prove that if $a \geq 2$, $k > 2$ are integers then

$$\left\lfloor \left(a^{k-1}+1\right)^{\frac{k}{k-1}} \right\rfloor = a^k + a + \left\lfloor \frac{a}{k-1} \right\rfloor,$$

where $\lfloor x \rfloor$ is the largest integer smaller or equal than x, called the *floor* of x.