On the elemental symmetric functions of $1^{p^k}, 2^{p^k}, 3^{p^k}..., (p-1)^{p^k}$

Pascual Restrepo Mesa

[1]*Universidad de los Andes, Bogotá, Colombia, email:* p.restrepo23@uniandes.edu.co

1. Introduction

It is a well-known and classic result that if p is a prime, then we have:

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}$$

This tells us what is the remainder of the elemental symmetric functions of the numbers $1, 2\cdots, p-1 \pmod{p}$, we even get that their product is $\equiv -1 \pmod{p}$ which is Wilson's theorem.

More over, Wolstenholme also proved that the numerator of the fraction:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3}\cdots + \frac{1}{p-1}$$

when written in lowest terms is a multiple of p^2 for every prime number $p \geq 5$.

But this type of problems kept appearing even in olympiads, for example in the XX Iberoamerican Olympiad held in Cartagena, Colombia, one of the problems asked to prove that the numerator of the fraction

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

when written in lowest terms was divisible by p^3 for every $p \geq 5$.

The purpose of this article is not only to prove these results, but also providing a solution for a more general case, showing some ideas that might be useful for this kind of problems.

Of course all the discussed problems have a "very elementary" solution, however the techniques used for them do not work in a more general case and we are forced to use stronger artillery.

It is time to do some maths before the reader gets bored of all this talking.

2. The Result

Before continuing, lets first introduce the theorem we are going to prove.

Theorem 1

Let p be a prime number bigger than 5 and k a positive integer.

Let

$$\begin{aligned} P(x) &= (x-1^{p^k})(x-2^{p^k})(x-3^{p^k})\cdots(x-(p-1)^{p^k}) \\ &= x^{p-1} - x^{p-2}A_{(1,k)} + x^{p-3}A_{(2,k)} \cdots - xA_{(p-2,k)} + A_{(p-1,k)} \end{aligned}$$

Then the following statements are true:

1) $A_{(i,k)}$ is divisible by p^{k+1} for $1 \leq i \leq p-3$

2) $A_{(p-2,k)}$ is divisible by p^{k+2}

3) $A_{(p-1,k)} + 1$ is divisible by p^{k+1}

Before proving the result we must take into account the following lemma:

Lemma 1: "Lifting the exponent":

Let p be an odd prime, If $a \equiv b \pmod{p^t}$ then $a^p \equiv b^p \pmod{p^{t+1}}$

Proof:

Lets write $a = b + mp^t$, therefore:

$$a^p = b^p + \sum_{k=1}^{p} \binom{p}{k} b^{p-k} m^k p^{tk}$$

and looking at this relation $\pmod{p^{t+1}}$, and since $p|\binom{p}{k}$ for $k = 1, 2 \cdots, p-1$, it follows that in fact $a^p \equiv b^p \pmod{p^{t+1}}$ and this completes the proof of the lemma.

Now we can continue, but for those that thought we were only going to use classical number theory arguments, they were wrong!!!, instead we try a more algebraic approach by considering the polynomial

$$\begin{aligned} Q(x,y) &= (x-y)(x-y^2)\cdots(x-y^{p-1}) \\ &= x^{p-1} + x^{p-2}f_1(y) + x^{p-3}f_2(y)\cdots + xf_{p-2}(y) + f_{p-1}(y) \end{aligned}$$

We will have to work a little with this polynomial and the reason why we picked it will be clear later. The first thing we are going to prove is that $\phi_{p-1}(x)$ divides $f_i(x)$ for $i = 1, 2 \cdots, p-2$ in $\mathbb{Z}[x]$, where $\phi_{p-1}(x)$ is the $(p-1)$th cyclotomic polynomial.

This follows easily by plugging $y = \zeta$ where ζ is a $(p-1)$th primitive root of unity. For this values we get $Q(x, \zeta) = x^{p-1} - 1$ so $f_i(\zeta) = 0$ for $i = 1, 2 \cdots, p-2$ because the latter is a polynomial identity in x. Since the roots of $\phi_{p-1}(x)$ are precisely the $(p-1)$th primitive roots of unity, and since $\phi_{p-1}(x) \in \mathbb{Z}[x]$ we get the desired divisibility.

Now, it is known that a primitive root mod p^2 is also a primitive root mod p^t for every positive integer t, so we need to prove another technical fact using it. Let g be a primitive root mod p^t for all t (just pick one mod p^2 and it works), then we have that:

$$p^{k+1} | \phi_{p-1}(g^{p^k})$$

This is not hard at all, since $p^{k+1} | (g^{p^k})^{p-1} - 1$, p^{k+1} must divide some cyclotomic polynomials that are divisors of $x^{p-1} - 1$ evaluated in g^{p^k}. Suppose $p | \phi_d(g^{p^k})$, then $p | g^{p^k d} - 1$ and since the

order of g mod p is $(p-1)$ and $d|p-1$, we must have $d = p-1$ proving that all factors of p must divide $\phi_{p-1}(g^{p^k})$ hence we get the desired divisibility.

Now, using the last divisibility is easy to finish the proof of the first part of the theorem. The numbers $g^{1p^k}, g^{2p^k} \cdots, g^{(p-1)p^k}$ are in some order the remainders $1^{p^k}, 2^{p^k}, 3^{p^k} \cdots, (p-1)^{p^k}$ mod p^{k+1} because of the lifting lemma. Now consider:

$$\begin{aligned} Q(x, g^{p^k}) &= (x - g^{p^k})(x - g^{2p^k}) \cdots (x - g^{(p-1)p^k}) \\ &= x^{p-1} + x^{p-2} f_1(g^{p^k}) \cdots + x f_{p-2}(g^{p^k}) + f_{p-1}(g^{p^k}) \end{aligned}$$

By the previous remarks we now that $f_i(g^{p^k}) = 0 \pmod{p^{k+1}}$, for $i = 1, 2, 3 \cdots, p-2$, but $f_i(g^{p^k}) \equiv A_{(i,k)} \pmod{p^{k+1}}$, also from the previous remarks, thus the first part of the theorem follows.

In order to prove the second part we must deal with a complicated divisibility relation first, we prove it here as a lemma.

Lemma 2

Let p be an odd prime and k a positive integer, then, for every integer a not divisible by p we have

$$p^{2k+3} | p^{2k+2} - p^{k+1}(a^{p^k} + (p-a)^{p^k})$$

Proof

The divisibility is equivalent to $p^{k+2} | p^{k+1} - (a^{p^k} + (p-a)^{p^k})$ and we will prove it by induction on k using the lifting lemma. The case $k = 0, k = 1$, are directly verified and are easily reduced to Fermat's theorem

The inductive step is not easy at all, however here it goes:

$$\begin{aligned}
p^{k+1} &= a^{p^k} + (p-a)^{p^k} && (\text{mod } p^{k+2}) \\
p^{k+1} - a^{p^k} &= (p-a)^{p^k} && (\text{mod } p^{k+2}) \\
(p^{k+1} - a^{p^k})^p &= (p-a)^{p^{k+1}} && (\text{mod } p^{k+3}) \\
p^{k+2}a^{(p-1)p^k} - a^{p^{k+1}} &= (p-a)^{p^{k+1}} && (\text{mod } p^{k+3}) \\
p^{k+2} &= a^{p^{k+1}} + (p-a)^{p^{k+1}} && (\text{mod } p^{k+3})
\end{aligned}$$

Where the third step is due to the binomial formula and the second one in virtue of the lifting lemma. And that finishes the proof of the lemma.

In order to prove the second part of the theorem we will prove that the difference $P(p^{k+1}) - A_{(p-1,k)}$ is divisible by p^{2k+3}. However multiplying and using the lemma 2 we get:

$$(p^{k+1} - a^{p^k})(p^{k+1} - (p-a)^{p^k}) \equiv a^{p^k}(p-a)^{p^k} \pmod{p^{2k+3}}$$

multiplying this congruence for $a = 1, 2 \cdots, (p-1)/2$ we obtain the stated divisibility, since $A_{(p-1,k)} = \prod_{i=1}^{p-1} i^{p^k}$.

But we can also expand the difference as

$$P(p^{k+1}) - A_{(p-1,k)} = p^{(k+1)(p-1)} - p^{(k+1)(p-2)}A_{(1,k)} + p^{(k+1)(p-3)}A_{(2,k)} \cdots - p^{k+1}A_{(p-2,k)}$$

and since p^{2k+3} divide all terms but the last one in that sum, (by the first part of the theorem and a simple p-adic valuation) we get that p^{2k+3} must divide the last term. But this in turn implies that $p^{k+2}|A_{(p-2,k)}$ as wished.

Note that Wolstenholme Theorem and the Iberoamerican olympiad Problem follows from this part of the theorem with $k = 0, k = 1$ respectively.

To finish with the third part of the theorem we only have to take Wilson's congruence and apply the lifting k times. Doing this we get

$$1^{p^k}2^{p^k} \cdots (p-1)^{p^k} = (-1)^{p^k} \pmod{p^{k+1}}$$

Which is exactly the third part of the theorem and this concludes our proof.

3. Concluding Remarks

By a well known fact due to Euler, we know that we can write all symmetric polynomials in terms of the elemental ones, moreover, if it is an integer symmetric polynomial, we can write it as an integer polynomials in the arithmetic means of the elemental symmetric ones. Since we show how rising everything to the pth power increased the exponent of p in the p-adic valuation of the functions considered above, we could ask under which conditions it also happens for other integer symmetric polynomials? However this is not clear by now, but we can still try to compute the symmetric polynomial we are given in terms of the elemental symmetric functions and treat it as a particular case and see what happens then.