Analytical Geometric Interpretation of the Cardinality number "μ" in Gauss's Lemma

Ali Astaneh, PD (Lon). Vancouver BC, Canada

In the previous Article 1 an analytical proof was presented to formulate the exact value of the cardinality μ involved in Gauss's popular Lemma, according to parity of $1 < n \leq (p-1)$ for an odd prime p as in,

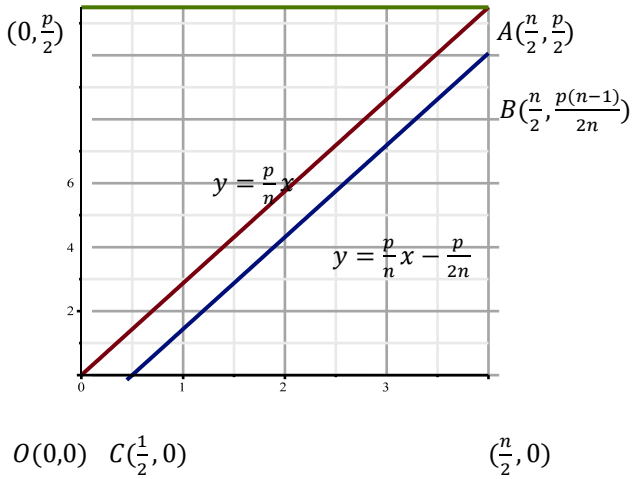
Theorem: (Astaneh) Let p be an odd prime number, $1 < n \leq (p-1)$, $P = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$, $N = -P$, and $\mu = |nP \cap N|$.

(A) If n is odd, then $$\mu = \sum_{i=1}^{\frac{n-1}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right). \qquad (1)$$

(B) If n is even, then $$\mu = \sum_{i=1}^{\frac{n}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right), \qquad (2)$$

Here, for any real number x, the notation $\lfloor x \rfloor$ means the greatest integer $\lfloor x \rfloor \leq x$.

In this article, first an analytical geometric interpretation of the exact value for μ is implied from the above part Theorem; as all possible interior lattice points (that is, points with integer coordinates) of the trapezoid OABC shown below, when n is an odd number. When n is even almost exactly the same interpretation is valid, except that, beside the interior of the trapezoid, there may be also another single lattice point on the interior of the boundary segment AB of the trapezoid as well.



$O(0,0)$ $C(\frac{1}{2}, 0)$ $(\frac{n}{2}, 0)$

Because of the extreme similarity of the argument for the two cases, we only deal with t part (A) of the Theorem where n odd number, but only bring an Example for part (B) when we may also have a lattice point on the AB boundary of the trapezoid.

Once the geometric interpretation is settled, a different independent (from above Theorem) number theoretical argument can be present to prove the validity of the said interpretation as, as a Proposition. Therefore, in a sense, proof of the Proposition on page 3 also can be considered as a second proof for above Theorem formulating the exact vale for μ.

Geometrical Interpretation of the Cardinality "μ"

We first start with Part **(A)** of the Theorem where n is odd, and rewrite formula (1) for odd prime p and odd $1 \leq n \leq p-1$ as follows,

$$\mu = \sum_{i=1}^{\frac{n-1}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right) = \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor =$$

$$\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor =$$

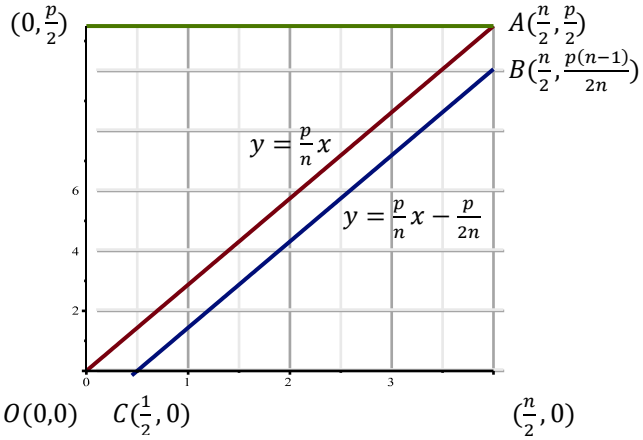
$$\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} - \frac{p}{2n} \right\rfloor.$$

Now, as it can be observed from the figure on the previous page, each term $\left\lfloor \frac{ip}{n} \right\rfloor$, $i = 1, 2, \dots, \frac{n-1}{2}$ in the first sum $\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor$ is simply the number of all lattice points below the line shown as $y = \frac{p}{n}x$, and standing directly above each of the abscissa $x = i$. Therefore the sum $\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor$ is the number of all lattice points below the line $y = \frac{p}{n}x$ and above the x-axis over the domain $\left[1, \frac{n-1}{2}\right]$. And, in the same way the second sum $\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} - \frac{p}{2n} \right\rfloor$ is the number all possible lattice points below the line $y = \frac{p}{n}x - \frac{p}{2n}$ over the domain $\left[1, \frac{n-1}{2}\right]$. Therefore the difference between the two sums, which is $\mu = \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} - \frac{p}{2n} \right\rfloor$ is exactly the number of set all possible lattice points in the interior of the trapezoid OABC. Note that, as an easy exercise one can show that neither of the two lines $y = \frac{p}{n}x$ and $y = \frac{p}{n}x - \frac{p}{2n}$ have any lattice points on them. It can also happen that some integer abscissa over the domain $\left[1, \frac{n-1}{2}\right]$ may not carry any interior point of the trapezoid on top of them, as can be verified for the case of $p = 17, n = 15$ and the abscissa. $x = 5$. Moreover (by part **(b)** of the Proposition on last page of Article 16) the total number of those lattice points satisfies $1 \leq \mu \leq (\frac{n-1}{2})(\left\lfloor \frac{p}{2n} \right\rfloor + 1)$.

As for part **(B)** of the Theorem, the argument would be very much the same, with only two minor differences. First, some lattice points in the interior of the AB segment of the boundary of the trapezoid OABC may also contribute in the exact count for cardinality μ, simply because this time $\frac{n}{2}$ is an integer. So, in a general case **(B)** the cardinality μ would be in a one to one correspondence with all lattice points in the trapezoid over the domain $\left[1, \frac{n}{2}\right]$ instead. The only other difference (again by **(b)** of the Proposition on last page of Article 16), the upper bound for the cardinality changes to $1 \leq \mu \leq (\frac{n}{2})(\left\lfloor \frac{p}{2n} \right\rfloor + 1)$.

Having completed the interpretation of the exact count μ for the two parts of the Theorem, we now provide an independent proof (from the Theorem), for the geometric interpretation delivered above, using simpler number theory argument. Let us then formally present this as a Proposition.

Proposition: Let p be an odd prime number, $1 \leq n \leq (p-1)$ and odd number, $P = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$, $N = -P$, and $\mu = |nP \cap N|$. Then the cardinality μ is exactly the same as the number lattice points in the interior of the trapezoid OABC shown below,



Proof: Let us first assume that $(u,v)$is a lattice point in the interior of the trapezoid OABC. Then $\frac{p}{n}u-\frac{p}{2n}<v<\frac{p}{n}u$, so $-\frac{p}{2n}<v-\frac{p}{n}u<0$, and $-\frac{p}{2}<nv-up<0$, This latter inequality means the number nv has a negative least remainder $mod(p)$, with $v\in P=\left\{1,2,\dots,\frac{p-1}{2}\right\}$. Hence a member of $nP\cap N$ corresponds to (u,v). Conversely, assume that for some $v\in P=\left\{1,2,\dots,\frac{p-1}{2}\right\}$ the multiplication nv has a negative least remainder $mod(p)$. Then there exists a unique n integer $u\geq 1$ such that $-\frac{p}{2}<nv-up<0$. This double inequality (manipulated in reverse to the above) implies $\frac{p}{n}u-\frac{p}{2n}<v<\frac{p}{n}u$. On the other hand the right part $\frac{p}{n}u-\frac{p}{2n}<v$ of the latter double inequality implies $u<\frac{n}{p}\left(v+\frac{p}{2n}\right)<\frac{n}{p}\left(\frac{p}{2}+\frac{p}{2n}\right)=\frac{n+1}{2}$. Since n is an odd integer this means $u<\frac{n}{2}$, and together with $v<\frac{p}{2}$ it follows that (u,v) is an interior lattice point of the trapezoid OABC . Since the horizontal distance between the lines $y=\frac{p}{n}x$ and $y=\frac{p}{n}x-\frac{p}{2n}$ is only $\frac{1}{2}$, there can be at most one lattice point in the interior of the trapezoid with second coordinate v, and therefore the correspondence between the set $nP\cap N$ and all the interior lattice pontsp inside the Trapezoid of one to one, and the proof is complete.

Note that the above proof was designed for Part (A) of the Corollary, however the argument for part part (B) would be word by word the same , except that we should add possible lattice points on the interior points of the segment AB of the boundary of the trapezoid to the interior lattice points of the trapezoid to get a one to one correspondence with the set $nP\cap N$, and here is an example,

Example: For $p=13$ and $n=12$, the lattice point $\left(\frac{n}{2},\frac{p-1}{2}\right)=(6,6)=(u.v)$ is a lattice point in the interior of the line segment boundary AB of the trapezoid, which happens to correspond to the negative least residue

$$-\frac{13}{2}=-\frac{p}{2}<nv-up=12\times 6-6\times 13=-6<0$$

Indeed, the congruency $5^2\equiv 12\ (mod 13)$ shows that $n=12$ is a quadratic residue $(mod 13)$, and this fact can already be decided by finding that the sum in part (B) of the Theorem is an odd, as seen below

$$\mu=\sum_{i=1}^{6}\left(\left\lfloor\frac{13i}{12}\right\rfloor-\left\lfloor\frac{13i}{12}-\frac{13}{24}\right\rfloor\right)=1+1+1+1+1+1=6$$

Note that, in this example it means we have a single lattice point in the interior of the trapezoid directly above $x = 2, 3, 4, 5$; and the lattice point (6,6) on the interior of the boundary line of the trapezoid which is on top of $x = 6$.