Proof: We determine the average signal energy for the Gaussian integers modulo the Gaussian prime $\pi = a + ib$, where $p = \pi \cdot \pi^*$ with $p \equiv 1 \bmod 4$. The star denotes complex conjugation. We therefore determine the sum $S = \sum_{k=0}^{p-1} N(k \bmod \pi)$, where the norm $N(\gamma)$ of a Gaussian integer $\gamma$ is defined by $N(\gamma) = \gamma \cdot \gamma^*$. The average energy then equals $S/p$.
To compute $A + iB \bmod \pi$ one can proceed as follows. Let $x + iy$ be $A + iB \bmod \pi$, then $(A + iB)(a - ib) \bmod \pi\pi^*$ — i.e. modulo $p$ — equals $f + ig$ where

$$\begin{aligned} aA + bB &= F \cdot p + f \\ aB - bA &= G \cdot p + g \ . \end{aligned}$$

Hence

$$A + iB \bmod \pi = x + iy = \frac{f + ig}{a - ib} \ . \tag{1}$$

Equation (1) can already be found in [1]. Hence setting $k \bmod \pi = x_k + iy_k$ with $x_k + iy_k = (f_k + ig_k)/(a - ib)$ and

$$\begin{aligned} a \cdot k &= F_k \cdot p + f_k \\ -b \cdot k &= G_k \cdot p + g_k \ , \end{aligned}$$

we get

$$S = \sum_{k=0}^{p-1} (x_k^2 + y_k^2) = \sum_{k=0}^{p-1} N(x_k + iy_k) = \sum_{k=0}^{p-1} \frac{N(f_k + ig_k)}{N(a + ib)} = \frac{1}{p} \sum_{k=0}^{p-1} (f_k^2 + g_k^2) \ .$$

Now if $k$ runs from 0 to $p - 1$ then $ak \bmod p$ which equals $f_k$ runs through all residues modulo $p$. The same is true for $g_k$. Clearly to get the residues $k \bmod \pi$ of smallest norm, we select $f_k$ and $g_k$ from the interval $-(p-1)/2 ... (p-1)/2$. Thus

$$\sum_{k=0}^{p-1} f_k^2 = \sum_{k=0}^{p-1} g_k^2 = 2 \sum_{k=1}^{(p-1)/2} k^2 \ , \quad \Rightarrow \quad S = \frac{4}{p} \sum_{k=0}^{(p-1)/2} k^2 \ .$$

The latter sum however is well known. We thus get

$$S = \frac{4}{p} \cdot \frac{\frac{(p-1)}{2}(\frac{(p-1)}{2} + 1)(p - 1 + 1)}{6} = \frac{p^2 - 1}{6} \Rightarrow S/p = \frac{p^2 - 1}{6p} \ , \tag{2}$$

as was to be proved.

## References


[1] C.F.Gauss, "Theorie der biquadratischen Reste, Zweite Abhandlung", Commentationes soc. reg. Gotting.recentiores. Vol.VII. Gottengae 1832, *also contained in* C.F.Gauss, *Untersuchungen über Höhere Arithmetik*, (german translation of the latin *Disquisitiones Arithmeticae* by H.Maser1889), Chelsea Publishing Company, second reprint 1981, New York.

[2] K.Huber, "Codes over Gaussian Integers," *IEEE Trans. Inform. Theory*, pp.207-216, Jan. 1994.