Project Euler Problem 153 - Gaussian Integers

Stephen Fay

2019 July 19

Contents

1 Problem

As we all know the equation $x^2 = -1$ has no solutions for real x.
If we however introduce the imaginary number i this equation has two solutions: $x = i$ and $x = -i$.
If we go a step further the equation $(x-3)^2 = -4$ has two complex solutions: $x = 3+2i$ and $x = 3-2i$.
$x = 3+2i$ and $x = 3-2i$ are called each others' complex conjugate.
Numbers of the form a+bi are called complex numbers.
In general $a+bi$ and abi are each other's complex conjugate.

A Gaussian Integer is a complex number $a+bi$ such that both a and b are integers.
The regular integers are also Gaussian integers (with $b = 0$).
To distinguish them from Gaussian integers with $b \neq 0$ we call such integers "rational integers."
A Gaussian integer is called a divisor of a rational integer k if the result is also a Gaussian integer.

Let $s(k)$ denote the sum of all the positive real parts of the Gaussian divisors of k

Find

$$\gamma = \sum_{k=1}^{10^8} s(k) \tag{1}$$

Helper:

$$\sum_{k=1}^{10^5} s(k) = 17924657155 \tag{2}$$

2 Some Math behind the Algorithm: Explanation and Proofs

Note: I mainly use the symbol $\mathbb{N}$ instead of $\mathbb{Z}$ because this problem doesn't concern it's self with negative parts.

2.1 $\mathbb{N}$

The first thing to do is to solve the problem considering only the integer factors. We want to find an efficient way of calculating the following sum where $n = 10^8$

$$\sum_{k=1}^{n} S_{\mathbb{Z}}(k) \qquad \text{where} \quad S_{\mathbb{Z}}(k) = S(k) \quad \text{restricted to the integers}$$

Rather than factoring each $k \in [1, n]$ and summing the factors we instead consider, for each number $q < n$, what is q a factor of? Which is simple to answer, we just do the q times table; we then add the number of positive numbers in the q times table that are smaller or equal to n; we do this for every $q < n$ to find κ

$$\kappa := \sum_{k=1}^{n} S_{\mathbb{Z}}(k) = \sum_{q=1}^{n} q \cdot \lfloor n/q \rfloor \tag{3}$$

This reformulation of the sum lends it's self to much speedier computation, in python it can be written in a single line of code:

```python
sum([q*(n//q) for q in range(1,n+1)])
```

2.2 $\mathbb{C}$

All we have to do is now is to find the sum of the positive real parts of the non-integer complex factors of all the numbers smaller than n. We will use the same trick as with the integer factors: instead of trying to factor each natural number smaller than $n = 10^8$ we will look at each Gaussian integer smaller than n and determine how many natural numbers (also smaller than n) it is a factor of. All it takes to reduce this problem to something my computer can tackle in under 2 minuets is to a) draw some straight lines and b) exploit the symmetries of the complex plane. We will start with b), the symmetries:

Observation 1. $(a + ib)|k$ with $a, b, k \in \mathbb{N} \quad \Rightarrow (a \pm ib)|k \quad$ and $\quad (b \pm ia)|k$

Proof.

$$(a + ib)|k \Rightarrow \frac{k}{a + ib} = c + id \quad \text{for some} \quad c, d \in \mathbb{Z}$$

$$\Rightarrow \frac{k}{a + ib} = \frac{k(a - ib)}{a^2 + b^2} \Rightarrow \frac{a}{a^2 + b^2} \in \mathbb{Z} \text{ and } \frac{b}{a^2 + b^2} \in \mathbb{Z}$$

Hence

$$\frac{k}{a - ib} = \frac{k \cdot a}{a^2 + b^2} + i\frac{k \cdot b}{a^2 + b^2} \in \mathbb{Z}[i] \quad \text{and} \quad \frac{k}{b \pm ia} = \frac{k \cdot b}{a^2 + b^2} \mp \frac{k \cdot a}{a^2 + b^2} \in \mathbb{Z}[i]$$

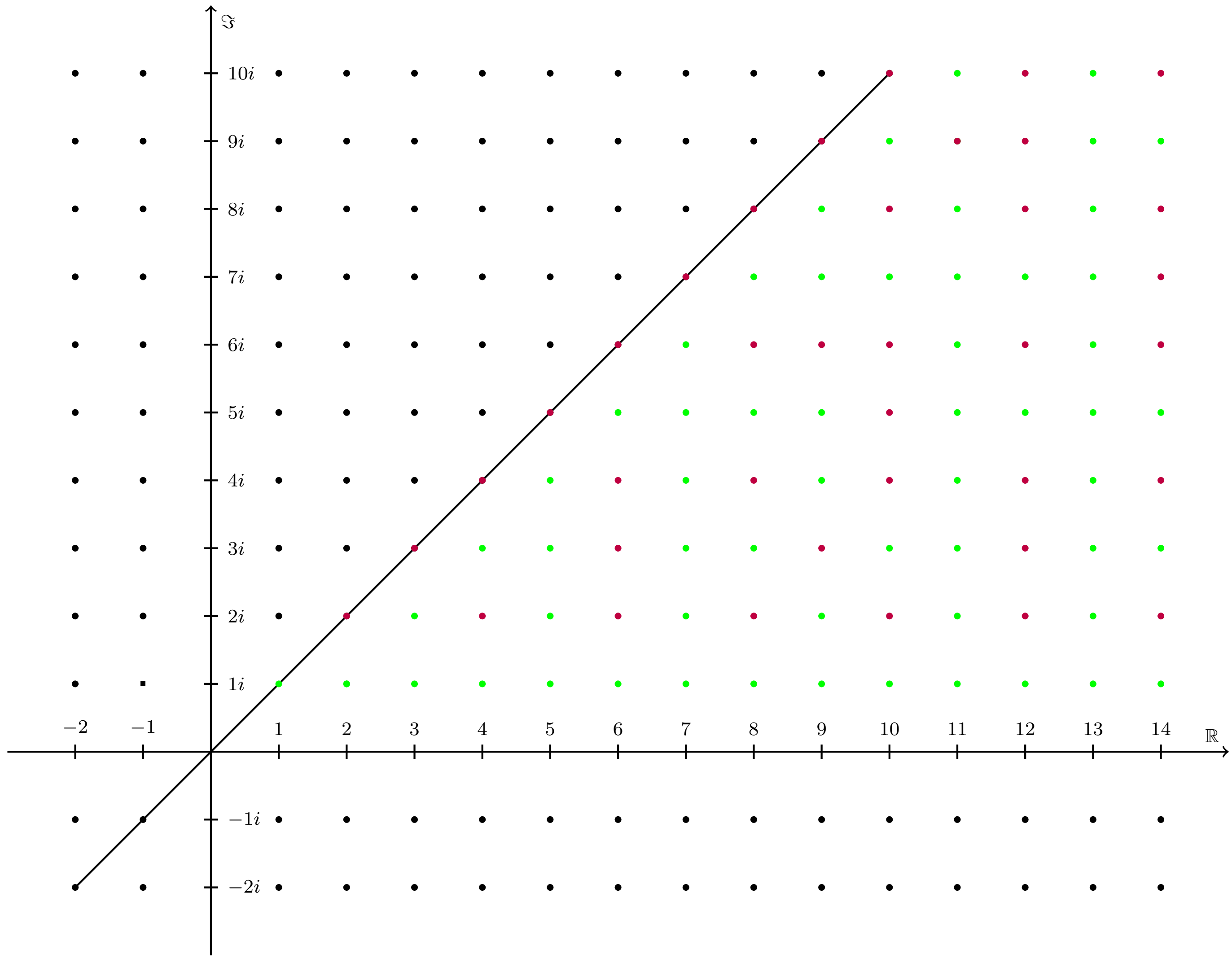
☺

This can be made intuitive if you consider that multiplication in the complex plane as multiplying absolute values and summing angles; if there is one Gaussian integer that lies on the circle centered at the origin of radius $r = \sqrt{a^2 + b^2}$, then there are at the very least 3 others. And if $a \neq b$ then there are at least 7 others, 4 of these 8 divisors have positive real components and are therefore candidates for consideration. This has the effect of cutting in 4 the number of Gaussian integers we need to inspect

Further, we notice that each Gaussian factor (and it's conjugate pair) $(a \pm ib)|k$ with $a, b, k \in \mathbb{N}$ and $k \leq n$ is part of a pair since

$$\frac{k}{a \pm ib} = \frac{k(a \mp ib)}{a^2 + b^2} \in \mathbb{Z}[i] \Rightarrow \frac{ka}{a^2 + b^2} \in \mathbb{Z} \text{ and } \frac{kb}{a^2 + b^2} \in \mathbb{Z}$$

Is also a factor of k



Observation 2. If $\gcd(a,b)=1$ and $(a+ib)|k \Rightarrow k = m\cdot(a^2+b^2)$ with $a,b\in\mathbb{Z}$ for any $k\in\mathbb{N}$ where $m\in\mathbb{N}$
In English: for every Gaussian integer whereby the real and imaginary components share no prime factors, the smallest natural number that they divide is a^2+b^2 and all the other numbers that they divide are multiples of this.

Proof. We can see from our proof of observation 1 that $(a+ib)|(a^2+b^2) \quad \forall(a+ib)\in\mathbb{Z}[i]$ and thus $(a+ib)|m\cdot(a^2+b^2) \quad \forall m\in\mathbb{N}$
We now show that there are no other natural numbers divisible by $(a+ib)$:

$$(a^2+b^2)|ka \text{ and } (a^2+b^2)|kb \Rightarrow (a^2+b^2)|\gcd(ka,kb) \quad , \quad \gcd(ka,kb)=k\gcd(a,b)=k \ \Rightarrow (a^2+b^2)|k$$

☺

Corollary 1.

$$\text{If } \gcd(a,b)=q \Rightarrow \{k \text{ s.t. } (a+ib)|k\} = \{k : k = \frac{m(a^2+b^2)}{q} \text{ for } m\in\mathbb{N}\}$$

Proof. Since $\gcd(\frac{a}{q},\frac{b}{q})=1 \Rightarrow \{h \text{ s.t. } (\frac{a}{q}+i\frac{b}{q})|h\} = \{h : h = m\cdot\frac{a^2+b^2}{q^2}\}$, we divide h by $(a+ib)$

$$\frac{h}{a+ib} = \frac{m\cdot(a^2+b^2)}{q^2(a+ib)}\cdot\frac{a-ib}{a-ib} = \frac{am\cdot(a^2+b^2)-ibm\cdot(a^2+b^2)}{q^2(a^2+b^2)} = m\cdot\frac{a+ib}{q^2} = m\cdot\frac{a/q+ib/q}{q}$$

Thus we must multiply by h by q to obtain integer solutions for all $m\in\mathbb{N}$, so our set of solutions is

$$\{k \text{ s.t. } k = hq = m\cdot\frac{a^2+b^2}{q}\}$$

☺

Intuition: considering multiplication between complex numbers to be a binary operation whereby you multiply the lengths and sum the arguments of pointy arrows in the complex plane and consider $u = (a + ib) = ze^{i\theta}$ such that $\gcd(a, b) = 1$. Now draw a straight line that passes through 0 and u. If you follow the line from the origin outwards, the first Gaussian integer you encounter will be u, and all the other Gaussian integers you encounter will be integer multiples of u. Because of the way our complex binary operator behaves, dividing any real number by u will give you a complex number that lies on the line that is the reflection of this line on the real line, in other words the argument is negated: $\frac{r}{ze^{i\theta}} = \frac{r}{z}e^{-i\theta}$.
So any integer k s.t. $u|k$ is the product of u and v where $\arg(v) = -\theta$, so $v = \alpha(a - ib)$

Corollary 2. If $gcd(a, b) = 1$ and $a^2 + b^2 > n$ then $a + ib$ is not a Gaussian factor of *any* natural number smaller than n.

We are now ready to design an efficient algorithm.

3 The Algorithm

3.1 The core calculation loop

Consider $u = ze^{i\theta} = a + ib \in \mathbb{Z}[i]$ with $a, b > 0$ and $\gcd(a, b) = 1$. Let λ be the number of natural numbers $k < n$ are there such that $u|k$? Applying observation 2, $k \in \{m \cdot z^2 : m \in \mathbb{N}\}$. So $\lambda = \lfloor n/z^2 \rfloor$. That's it! So the net contribution of u to the sum is $\lambda \cdot a$. But we can take this further : employing the symmetry of observation 1, we know that for λ is the same lambda for $u^* = a - ib$ and also $b \pm ia$. So with only a, b we can add to our final sum

$$\gamma \mathrel{+}= 2(a + b) \cdot \left\lfloor \frac{n}{a^2 + b^2} \right\rfloor$$

But we can take this further still! From $u = a + ib$ alone we can find quickly all the contributions given by multiples of u and it's reflected counter-parts – What λ is associated with $q \cdot u$?: $\lambda = \lfloor n/(q \cdot z^2) \rfloor$. Put concisely: the total of the contributions of all the Gaussian integers whereby the ratio of the real and complex components is either a/b or b/a with $\gcd(a, b) = 1$ to $\gamma = \sum_{k=1}^{n} s(k)$ is

$$\sum_{q=1}^{\lfloor n/z^2 \rfloor} 2 \cdot (a + b) \cdot \left\lfloor \frac{n}{q \cdot z^2} \right\rfloor = 2(a + b) \cdot \sum_{q=1}^{\lfloor n/z^2 \rfloor} \left\lfloor \frac{n}{q \cdot z^2} \right\rfloor$$

If $a \neq b$. If $a = b$ it is:

$$2a \cdot \sum_{q=1}^{\lfloor n/z^2 \rfloor} \left\lfloor \frac{n}{q \cdot z^2} \right\rfloor$$

In python this translates to

```
zsq = a**2+b**2
if a==b: the_sum += 2 * a * sum([zsq * (n//(q * zsq)) for q in range(1,n//zsq +1)])
else: the_sum += 2 * (a + b) * sum([zsq * (n//(q * zsq)) for q in range(1,n//zsq +1)])
```

3.2 Main loop

All we need now is a couple of for loops to find us every relatively prime a, b such that $a^2 + b^2 < n$ and apply the above formula to them. The symmetries reduces our domain to an eighth of a circle of the complex plane, for the sake of the illustration we will pick the 'bottom' half of the 1^{st} quadrant.

```
for b in range(1,int(0.5*(np.sqrt(2*n-1)-1)+1)):
    for a in relatively_primes(b,n): eta += factors_sum_line(a,b,n)
```

`relatively_primes(b,n)` returns all the natural numbers $a < n$ s.t. $\gcd(a, b) = 1$
`factors_sum_line(a,b,n)` returns what is added to `the_sum` in the code box above this one.

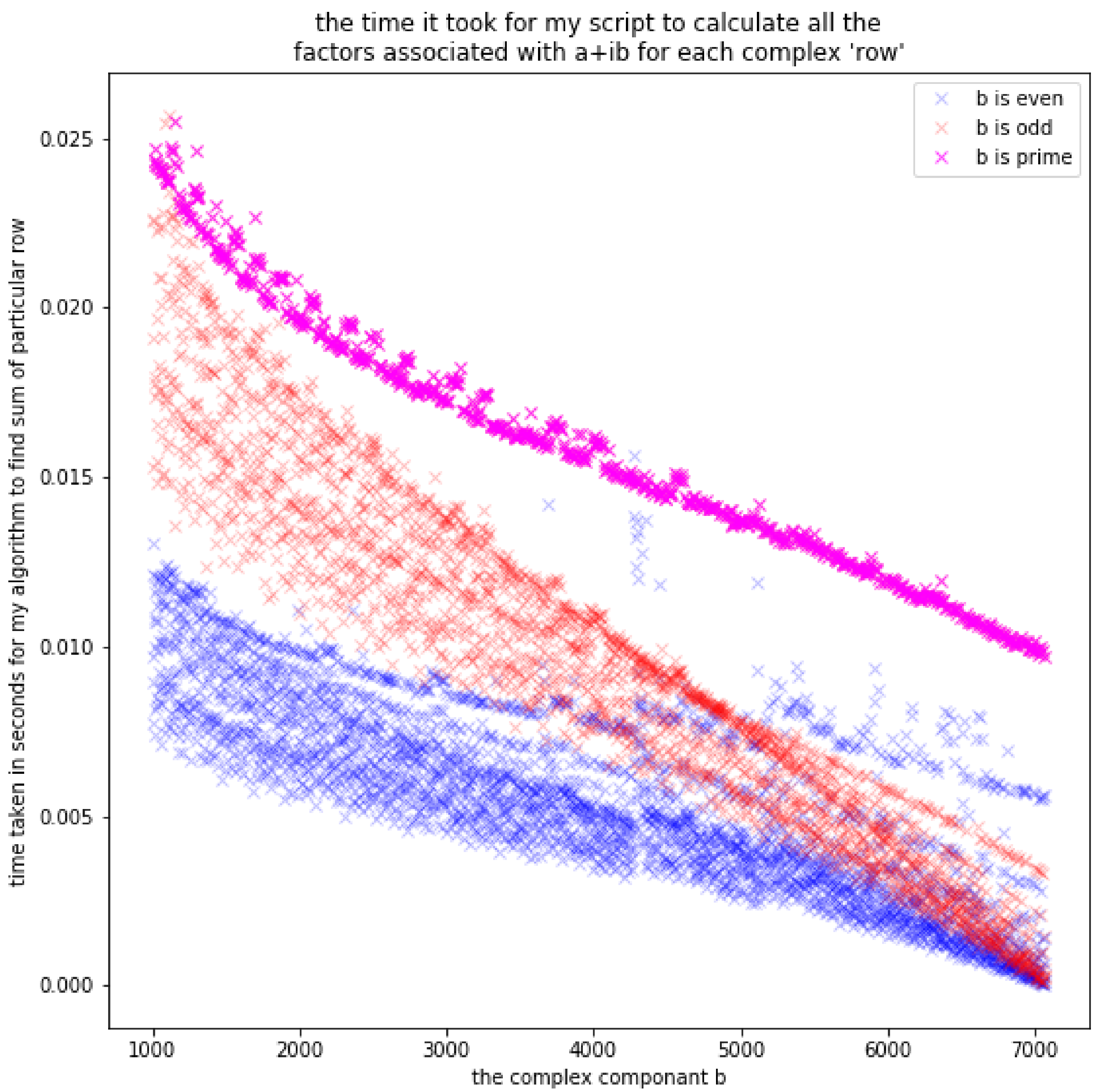
4 Links

Project Euler Problem 153

Code

My post about this problem

Check out the relative run-times of each 'row' of complex numbers:



run time