Black magic: xnor's 43-byte Python answer to "Triangular Lattice Points close to the Origin"

Lynn

This document is a proof that xnor's 43-byte Python answer to "Triangular Lattice Points close to the Origin" is correct, and an explanation of how it computes what it does.

To start with, we need to define **Eisenstein integers**. These are complex numbers of the form $x+y\omega$ where $x, y \in \mathbb{Z}$ and $\omega = e^{2\pi i/3}$, the primitive third root of unity. These numbers are arranged on a triangular lattice exactly like the one in the PPCG question. (You can find a nice image on Wikipedia.)

We can compute the **norm** of an Eisenstein integer, i.e. the squared[1] Euclidean distance from the origin, in much the same way that we do so for other complex numbers:

$$\begin{aligned} N(z) = |z|^2 = z \cdot \overline{z} &= (x + y\omega)(x + y\overline{\omega}) \\ &= x^2 + xy(\omega + \overline{\omega}) + y^2(\omega\overline{\omega}) \\ &= x^2 - xy + y^2. \end{aligned}$$

The PPCG question as it is asked is then equivalent to this:

> Given N, how many Eisenstein integers are there with norm less than or equal to N^2?

Which is furthermore equivalent to this:

> How many ways are there to write N in the form $X^2 - XY + Y^2$, for integers X, Y?

[1] Yes: in number theory, *norm* refers to the square of what you might know as the *norm* from analysis or linear algebra. It's quite confusing.

To answer this question, we'll need some facts about Eisenstein integers that I won't prove in detail:[2]

- The Eisenstein integers form a **unique factorization domain**. This means that we can uniquely factor any Eisenstein integer into **irreducible elements** p_i and a **unit** u. The units are the Eisenstein integers that have a multiplicative inverse: $\{\pm 1, \pm\omega, \pm\overline{\omega}\}$. The irreducible elements are called **Eisenstein primes**: they cannot be broken down into a product of two non-units. For example, $2+\omega$ is an Eisenstein prime, but $7 = (3+\omega)(3+\overline{\omega})$ is not.
- Every ordinary prime congruent to 2 modulo 3 is an Eisenstein prime.
- Every ordinary prime congruent to 1 modulo 3 can be factored into

  $$(x + y\omega)(x + y\overline{\omega})$$

  for *some* integers x and y.

Now we can get started counting them.

> *Lemma* (xnor–Legendre). Let N be a positive integer. The number of Eisenstein integers with norm N is given by
>
> $$R(N) := 6(d_1 - d_2),$$
>
> where d_r is the number of divisors of N congruent to r mod 3.
>
> Equivalently, N can be written in the form
>
> $$X^2 - XY + Y^2,$$
>
> for integers (X, Y), in exactly $R(N)$ different ways.

(The proof below is an adaptation of a proof, given in Chapter 36 of Joseph H. Silverman's *A Friendly Introduction to Number Theory*, of Legendre's "Sum of Two Squares Theorem", which states that N can be written as a sum of two squares in exactly

$$R(N) = 4(d_1 - d_3)$$

different ways, with d_r the number of divisors of N congruent to r mod 4.)

[2]Okay, I actually don't *know* how to prove these facts, either; I'm not a very skilled ring theorist. But I read them on Wikipedia so they *must* be true.

Proof. We begin by factoring N into a product of ordinary primes:

$$N = 3^t \underbrace{p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}}_{\text{primes} \equiv 1 \bmod 3} \cdot \underbrace{q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}}_{\text{primes} \equiv 2 \bmod 3}.$$

Then we factor N into a product of Eisenstein primes. The integer 3 factors as $3 = (2+\omega)(2+\overline{\omega})$. As stated earlier, each p_i factors as $(x_i + y_i\omega)(x_i + y_i\overline{\omega})$, and the q_i are Eisenstein primes themselves.

We now set

$$N = X^2 - XY + Y^2 = (X + Y\omega)(X + Y\overline{\omega}),$$

intending to count the solutions (X, Y). Here, $X + Y\omega$ and $X + Y\overline{\omega}$ are composed of the prime factors of N, and each prime that appears in one of their factorizations *must* have its complex conjugation appearing in the other, as they are complex conjugates.[3]

If any of the f_i is odd, then there is no way at all to evenly distribute factors of q_i among $X + Y\omega$ and its conjugation, so $R(N) = 0$. For the remainder of the proof, suppose that all of the f_i are even.

Every way to write N as $X^2 - XY + Y^2$ corresponds to a possible value of $X + Y\omega$. So we will expand $X + Y\omega$ into factors, and count how many choices we can make. It factors into a unit $u \in \{\pm 1, \pm\omega, \pm\overline{\omega}\}$ and some primes π_i so that $u(\prod \pi_i)\overline{u}(\prod \overline{\pi}_i) = N$. We get something like this:

$$\begin{aligned} X + Y\omega = u(2+\omega)^t & \left((x_1 + y_1\omega)^{z_1}(x_1 + y_1\overline{\omega})^{e_1 - z_1}\right) \cdots \\ & \left((x_r + y_r\omega)^{z_r}(x_r + y_r\overline{\omega})^{e_r - z_r}\right) q_1^{f_1/2} \cdots q_s^{f_s/2}, \end{aligned}$$

where u is a unit and the exponents z_i satisfy $0 \le z_i \le e_i$.

Counting all the ways to vary u and z_i, we find

$$\#\text{ possible values of } (X + Y\omega) = R(N) = 6(e_1 + 1) \ldots (e_r + 1).$$

So far we have shown:

$$R(N) = \begin{cases} 6(e_1 + 1) \ldots (e_r + 1) & \text{if } f_j \text{ all even,} \\ 0 & \text{otherwise.} \end{cases}$$

[3] If $X + Y\omega = up_1 \ldots p_n$, then $\overline{u} \cdot \overline{p_1} \ldots \overline{p_n} = \overline{up_1 \ldots p_n} = \overline{X + Y\omega} = X + Y\overline{\omega}$, and factorizations are unique. So if p_i occurs in $X + Y\omega$ then $\overline{p_i}$ necessarily occurs in $X + Y\overline{\omega}$.

It remains to show that this equals $6(d_1 - d_2)$. Recall our factorization of N into primes:

$$N = 3^t \underbrace{p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}}_{\text{primes} \equiv 1 \bmod 3} \cdot \underbrace{q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}}_{\text{primes} \equiv 2 \bmod 3}.$$

We proceed by induction on s. If $s = 0$, then $N = 3^t p_1^{e_1} \dots p_r^{e_r}$ and every divisor $d = p_1^{e_1} \dots p_r^{e_r} \not\equiv 0 \pmod 3$ of N is congruent to 1 modulo 3. By varying the exponents we can make this many choices:

$$d_1 - d_2 = d_1 - 0 = (e_1 + 1) \cdots (e_r + 1).$$

Now let N be divisible by q for some prime $q \equiv 2 \pmod 3$, and assume that we have completed the proof for all numbers having fewer 2 modulo 3 prime divisors than N. Let q^f be the highest power of q dividing N, so $N = q^f n$ with $f \geq 1$ and $q \nmid n$.

$\boxed{\text{If } f \text{ is odd,}}$ the divisors of N that are $\not\equiv 0 \pmod 3$ are the numbers

$$q^i d, \qquad \text{with } 0 \leq i \leq f, \text{ and } d \not\equiv 0 \pmod 3 \text{ dividing } n.$$

Thus each divisor d of n gives rise to exactly $f + 1$ divisors of N, of which half are $\equiv 1 \pmod 3$ and half are $\equiv 2 \pmod 3$. Thus $d_1(N) - d_2(N) = 0$.

$\boxed{\text{If } f \text{ is even,}}$ that very same logic applies to the divisors $q^i d$ that have exponents $0 \leq i \leq f - 1$, so we are left to consider the divisors of N of the form $q^f d$. The exponent f is even, so that $q^f \equiv 1 \pmod 3$ and hence $q^f d$ contributes to d_1 if $d \equiv 1 \pmod 3$ and to d_2 if $d \equiv 2 \pmod 3$. In other words,

$$(d_1 \text{ for } N) - (d_2 \text{ for } N) = (d_1 \text{ for } n) - (d_2 \text{ for } n).$$

By the induction hypothesis, our proof is complete:

$$d_1 - d_2 = \begin{cases} (e_1 + 1) \dots (e_r + 1) & \text{if } f_j \text{ all even,} \\ 0 & \text{otherwise.} \end{cases} = R(N)/6.$$

$\square$

This lemma gives us a formula we can use to answer the PPCG question: there is obviously one Eisenstein integer of norm 0, namely $0 + 0\omega$ (the origin of the lattice), and for all $k > 0$ there are $R(k)$ Eisenstein integers of norm k. So we have to compute $1 + \sum_{k=1}^{N^2} R(k)$. It turns out that there is a very clever way to do this!

Claim (Rewriting the sum). The sum $1 + \sum_{k=1}^{n^2} R(k)$ equals

$$1 + 6 \sum_{i=0}^{\infty} \left(\left\lfloor \frac{n^2}{3i+1} \right\rfloor - \left\lfloor \frac{n^2}{3i+2} \right\rfloor \right). \tag{1}$$

The proof here follows an argument given in *Geometry and the Imagination* by David Hilbert and Stephan Cohn-Vossen, pp. 37–38. Again, that proof concerns the Gauss circle problem (on a square lattice), but we can easily adapt it to our triangular case.

Proof. We take a new perspective on the summation. Instead of iterating over all $1 \le k \le n^2$ and counting divisors of each k, we can iterate over all possible divisors d, and count how many times d occurs as a divisor in *any* of the positive integers k up to n^2.

This is an easier question: d will occur as many times as there are multiples of it that do not exceed n^2, that is, $\lfloor n^2/d \rfloor$ times. So we have

$$\sum_{k=1}^{n^2} d_1(k) = \sum_{i=0}^{\infty} \left\lfloor \frac{n^2}{3i+1} \right\rfloor \quad \text{and} \quad \sum_{k=1}^{n^2} d_2(k) = \sum_{i=0}^{\infty} \left\lfloor \frac{n^2}{3i+2} \right\rfloor$$

from which the formula follows. □

Claim. Equation (1) is computed by the Python 2.7 function

```
f=lambda n,a=1:n*n<a/3or n*n/a*6-f(n,a+a%3).
```

Proof. Note that instead of summing to ∞, we can sum until the result of the floor function will always be 0, which is when $3i + 1 > n^2$. Thus, a relatively straightforward translation of (1) is:

```
f=lambda n,i=0:1 if 3*i>n*n else
  n*n/(3*i+1)*6-n*n/(3*i+2)*6+f(n,i+1)
```

We use `or` to golf down the base case:

```
f=lambda n,i=0:3*i>n*n or
  n*n/(3*i+1)*6-n*n/(3*i+2)*6+f(n,i+1)
```

Now, we apply a clever substitution: we can replace `i=0` by `a=1` then add `a%3` to `a` every iteration to run through the values $1, 2, 4, 5, 7, 8, \ldots$ Then we could add a constantly flipping "sign" value to get the alternating sum back:

```
f=lambda n,a=1,s=1:a>n*n or n*n/a*6*s+f(n,a+a%3,-s)
```

But an even shorter way to make the terms alternate is to "fold by `-`":

```
f=lambda n,a=1:n*n<a/3or n*n/a*6-f(n,a+a%3)
```

The carefully chosen base case condition, `n*n<a/3`, will be met after an even amount of sign flips, as `a/3` (floor division) only changes every other term. This is crucial, as we want to make sure the base case will contribute 1 to the sum, not -1. (If you try replacing the base case by something like `n*n<a`, you get lots of off-by-two errors.) □