SUMS OF TWO SQUARES – PAIR CORRELATION & DISTRIBUTION IN SHORT INTERVALS

YOTAM SMILANSKY

Abstract. In this work we show that based on a conjecture for the pair correlation of integers representable as sums of two squares, which was first suggested by Connors and Keating and reformulated here, the second moment of the distribution of the number of representable integers in short intervals is Poissonian, where "short" means of length comparable to the mean spacing between sums of two squares. In addition we present a method for producing such conjectures through calculations in prime powers modulo rings and describe how these conjectures, as well as the above stated result, may by generalized to other binary quadratic forms. While producing these pair correlation conjectures we arrive at a surprising result regarding Mertens' formula for primes in arithmetic progressions, and in order to test the validity of the conjectures, we present numerical computations which support our approach.

1. Introduction

Throughout this work n, k and h will denote positive integers, p denote prime numbers and for abbreviation reasons we use $a \equiv b\ (c)$ instead of $a \equiv b \bmod c$. In addition we say $m_p(n) = k$ if $p^k \mid n$ but $p^{k+1} \nmid n$.

1.1. **Background and motivation.** When studying the distribution of a sequence of integers, for example the sequence of primes or of those representable as a sum of two squares, a natural first step would be to understand the mean density of such integers. For prime numbers this was achieved by Hadamard and de la Vallee Poussin with their famous Prime Number Theorem, and for sums of squares by Landau [L] . In order to learn more about the distribution of such a set the next step would be to look at the k-point correlation, or in other words to find an expression for

$$\frac{1}{N}\sum_{n=1}^{N} f\left(n+d_1\right)\cdot\ldots\cdot f\left(n+d_k\right)\ ,\ N\to\infty$$

where f is the characteristic function of the set at hand and $d_1, ..., d_k$ are distinct integers. These correlations give increasingly more precise data about the distribution, where the 2-point correlation provides the leading quantitative estimate of the fluctuations about the mean density of the sequence.

Date: July 21, 2012.

Regarding the sequence of primes, Hardy and Littlewood gave [HL] the following k-tuple conjecture for the number $\pi_{\mathbf{d}}(N)$ of positive integers $n \leq N$ for which all of $n+d_1, ..., n+d_k$ are prime , $\mathbf{d} = (d_1, ..., d_k)$ and $d_1, ..., d_k$ distinct integers. The conjecture is:

$$\pi_{\mathbf{d}}(N) \sim \mathscr{S}_{\mathbf{d}} \frac{N}{(\log N)^k} \; as \; N \to \infty \tag{1.1}$$

provided $\mathscr{S}_{\mathbf{d}} \neq 0$, where the "singular series" $\mathscr{S}_{\mathbf{d}}$ is

$$\mathscr{S}_{\mathbf{d}} = \prod_{\text{primes}} \frac{p^{k-1}\left(p - \nu_{\mathbf{d}}(p)\right)}{(p-1)^k}$$

and $\nu_{\mathbf{d}}(p)$ stands for the number of residue classes modulo p occupied by $d_1, ..., d_k$.

For $k = 1$ this is exactly the Prime Number Theorem, and for $k \geq 2$ is has not been proved for any $\mathbf{d}$.

1.2. **From a k-tuple conjecture to distribution in short intervals.** We will follow Gallagher's work [G] on primes in order to obtain the moments of distribution of the number of integers representable as a sum of two squares in short intervals. Consider first the set of primes and the prime number theorem, which states

$$\pi(N) \sim \frac{N}{\log N} \; , \; N \to \infty.$$

This relation can be understood as the statement that the number of primes in an interval $(n, n+\alpha)$, averaged over $n \leq N$, tends to the limit λ, when N and α tend to infinity in such a way that $\alpha \sim \lambda \log N$ with λ a positive constant.

Gallagher studies the distribution of values of $\pi(n+\alpha) - \pi(n)$ for $n \leq N$ and $\alpha \sim \lambda \log N$, and shows that assuming the prime k-tuple conjecture of Hardy and Littlewood (1.1), it suffices that

$$\sum_{1 \leq d_1, .., d_k \leq H} \mathscr{S}_{\mathbf{d}} \sim H^k \tag{1.2}$$

holds for all $k \in \mathbb{N}$ in order to prove that all the moments of the distribution tend to moments of Poisson distribution, and so the distribution tends to Poisson distribution with parameter λ as $N \to \infty$. This means that the distribution of primes in such intervals is similar to the distribution of a random set of integers with mean λ, and so even though clearly primes are not distributed randomly, in the perspective of intervals such as those we deal with here they do. Gallagher has proved (1.2) in [G], and a simpler proof was presented by Kevin Ford [F]. We shall refer to this result as Gallagher's Lemma.

Consider now the set of integers which are representable as sum of squares and Landau's theorem, which states that $B(N)$, the number of such integers

up to N, is given asymptotically by

$$B(N) \sim \beta \frac{N}{\sqrt{\log N}} + O\left(\frac{N}{\log^{\frac{3}{4}} N}\right) \ , \ N \to \infty \tag{1.3}$$

where $\beta = \sqrt{\frac{1}{2} \prod_{p \equiv 3\,(4)} (1-p^{-2})^{-1}}$ is the Landau-Ramanujan constant.

Similar to the primes, this relation can be understood as the statement that the number of primes in an interval $(n, n+\alpha)$, averaged over $n \leq N$, tends to the limit λ, when N and α tend to infinity in such a way that $\alpha \sim \frac{\lambda}{\beta}\sqrt{\log N}$ with λ a positive constant.

We wish to study the distribution of values of $B(n+\alpha) - B(n)$ for $n \leq N$ and $\alpha \sim \frac{\lambda}{\beta}\sqrt{\log N}$. In order to follow Gallagher's method we need first a conjecture analogues of Hardy and Littlewood's conjecture for sums of two squares, that is an asymptotic formula for the number $B_{\mathbf{d}}(N)$ of positive integers $n \leq N$ for which all of $n+d_1, ..., n+d_k$ can be represented as a sum of two squares, $\mathbf{d} = (d_1, ..., d_k)$ and $d_1, ..., d_k$ distinct integers. The conjecture, analogous to (1.1), is that there exists a function $\mathscr{T}_{\mathbf{d}}$, the "singular series for our problem", for which the limit

$$B_{\mathbf{d}}(N) \sim \mathscr{T}_{\mathbf{d}} \frac{N}{\left(\sqrt{\log N}\right)^k} \quad as \quad N \to \infty \tag{1.4}$$

holds. If this is so, then the function $\mathscr{T}_{\mathbf{d}}$ depends only on the differences between the $d_1, ..., d_k$, in the sense that $\mathscr{T}_{\mathbf{d}} = \mathscr{T}_{\mathbf{d}+\mathbf{1}}$ where $\mathbf{1} = (1, ..., 1)$.

Assuming this conjecture, it is enough to show that the singular series $\mathscr{T}_{\mathbf{d}}$ has mean value β:

$$\sum_{1 \leq d_1, .., d_k \leq H} \mathscr{T}_{\mathbf{d}} \sim (\beta H)^k \tag{1.5}$$

for the moments to be Poisson with parameter λ.

1.3. **Main Result.** Connors and Keating conjectured in [CK] that for $k = 2$ and $h = |d_2 - d_1|$ we have

$$\mathscr{T}_{d_1,d_2} = \mathscr{T}_h = 2W_2(h) \prod_{\substack{p \equiv 3\,(4) \\ p|h}} \frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}} \tag{1.6}$$

where $m_p(h)$ is the power to which the prime p is raised in the prime decomposition of h and

$$W_2(h) \ = \ \begin{cases} \frac{1}{4} & m_2(h) = 0 \\ \frac{2^{m_2(h)+1}-3}{2^{m_2(h)+2}} & m_2(h) \geq 1 \end{cases}$$

Our main result is that

$$\sum_{1 \leq d_1 \neq d_2 \leq H} \mathscr{T}_{\mathbf{d}} \sim 2 \sum_{1 \leq h \leq H-1} (H-h)\, \mathscr{T}_h = \beta^2 H^2 + o(H^2)$$

and so assuming this pair correlation conjecture we show Gallagher's Lemma for sums of two squares and $k = 2$ holds, or in other words we show that assuming the conjecture, the second moment of the distribution of values of $B(n+\alpha) - B(n)$ for $n \leq N$ and $\alpha \sim \frac{\lambda}{\beta}\sqrt{\log N}$ is indeed Poisson.

1.4. **Mean Density and Pair correlation.** We provide a new approach to the computation of the pair correlation function stated above, which goes through the mean density and pair correlation of representable element in modulo rings of the form $\mathbb{Z}/p^k\mathbb{Z}$ for p primes and $k \to \infty$. The mean density is thus given by

$$\mathcal{M}(n) = \frac{1}{2} \prod_{\substack{p \equiv 3\,(4) \\ p \leq n}} \left(1 + p^{-1}\right)^{-1} \tag{1.7}$$

which is the product of the densities in modulo rings mentioned above. We compare this expression with the leading term of the analytic result for the density of representable integers given by Landau

$$\mathcal{L}(n) = \frac{\beta}{\sqrt{\log n}} \tag{1.8}$$

and produce the precise ratio between the two

$$\lim_{n\to\infty} \frac{\mathcal{M}(n)}{\mathcal{L}(n)} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}$$

where γ is Euler's constant, using a version of Mertens' formula in geometric progressions described in [LZ].

Next we derive (1.6) in similar methods to those used for the mean density (1.7). In Section 7 we present numeric calculations to support our conjecture.

1.5. **Generalization to other binary quadratic forms.** Our methods allow us to expand our observation also to integers representable by other binary quadratic forms $x^2 + dy^2$ with $d = 2, 3, 4, 7$ in addition to $d = 1$, which are the sums of two squares. A surprising result is that the ratio between the product formulas $\mathcal{M}_d(n)$ we present and the analytic results using variations on Landau's theorem $\mathcal{L}_d(n)$, for $n \to \infty$, is in fact constant for the five different quadratic forms inspected and is

$$\lim_{n\to\infty} \frac{\mathcal{M}_d(n)}{\mathcal{L}_d(n)} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}. \tag{1.9}$$

We next produce conjectures analogous to (1.6) and therefore to (1.4) with $k = 2$ for integers representable by the forms at hand, and finally deduce that assuming our conjectures the second moment of the distributions in the appropriate short intervals is Poisson.

Acknowledgments. This work is part of the author's M. Sc. thesis written under the supervision of Zeev Rudnick at Tel-Aviv University. Partially supported by the Israel Science Foundation (grant No. 1083/10).

2. Distribution In Small Intervals - Gallagher's Lemma

In order to obtain the second moment for the distribution of representable integers in the intervals described above, we follow Gallagher's work for primes, and we will show that

$$\sum_{1\le d_1\neq d_2\le H} \mathscr{T}_{\mathbf{d}} = \sum_{1\le d_1\neq d_2\le H} \mathscr{T}_{|d_2-d_1|} = 2\sum_{1\le h\le H-1}(H-h)\mathscr{T}_h = \beta^2H^2+o(H^2)$$

where by the Connors and Keating conjecture

$$\mathscr{T}_{d_1,d_2} = \mathscr{T}_h = 2W_2(h)\prod_{\substack{p\equiv 3\,(4)\\ p|h}}\frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}}$$

and

$$W_2(h) \;=\; \begin{cases} \frac{1}{4} & m_2(h)=0 \\ \frac{2^{m_2(h)+1}-3}{2^{m_2(h)+2}} & m_2(h)\ge 1 \end{cases}$$

We start by computing $\sum_{1\le h\le H-1}\mathscr{T}_h$.

2.1. **Dirichlet's Function.** Set

$$a(h) = 2\mathscr{T}_h = 4W_2(h)\prod_{\substack{p\equiv 3\,(4)\\ p|h}}\frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}}.$$

Notice that $a(h)$ is multiplicative: obviously $a(1)=1$ since 1 is odd and has no prime factors, and for $(m,n)=1$ we have $a(mn)=a(m)a(n)$ because our function is composed of products depending only on the prime factorizations.

Computing $a(p^k)$ gives

$$a(p^k) = \begin{cases} 1 & p\equiv 1(4) \\ 2-\frac{3}{2^k} & p=2 \\ \frac{1-\frac{1}{p^{k+1}}}{1-\frac{1}{p}} & p\equiv 3(4) \end{cases}.$$

We can thus write

$$\begin{aligned} D(s) &= \sum_{h=1}^{\infty}a(h)h^{-s} = \prod_p\left(1+\sum_{k=1}^{\infty}\frac{a(p^k)}{p^{ks}}\right) \\ &= \left(1+\sum_{k=1}^{\infty}\frac{2-\frac{3}{2^k}}{2^{ks}}\right)\prod_{p\equiv 1\,(4)}\left(1+\frac{p^{-s}}{1-p^{-s}}\right)\prod_{p\equiv 3\,(4)}\left(1+\sum_{k=1}^{\infty}\frac{1-\frac{1}{p^{k+1}}}{p^{ks}\left(1-\frac{1}{p}\right)}\right) \\ &= R(s)P(s)Q(s) \end{aligned}$$

where

$$\begin{aligned} R(s) &= 1+2\frac{2^{-s}}{1-2^{-s}}-3\frac{2^{-(s+1)}}{1-2^{-(s+1)}} \\ P(s) &= \prod_{p\equiv 1(4)}(1-p^{-s})^{-1} \\ Q(s) &= \prod_{p\equiv 3\,(4)}\left(1+\frac{1}{1-p^{-1}}\frac{p^{-s}}{1-p^{-s}}-\frac{p^{-1}}{1-p^{-1}}\frac{p^{-(s+1)}}{1-p^{-(s+1)}}\right). \end{aligned}$$

2.2. **Comparison to Riemann's ζ function.** Taking $\zeta(s)=\prod_p (1-p^{-s})^{-1}$, we will now show that $\frac{D(s)}{\zeta(s)}$ is analytic for $\mathrm{Re}(s)>0$, thus $D(s)$ is analytic in that region with a simple pole at $s=1$.

$$\frac{D(s)}{\zeta(s)}=\frac{1+2\frac{2^{-s}}{1-2^{-s}}-3\frac{2^{-(s+1)}}{1-2^{-(s+1)}}}{(1-2^{-s})^{-1}}\cdot\prod_{p\equiv 3\,(4)}\frac{1+\frac{1}{1-p^{-1}}\frac{p^{-s}}{1-p^{-s}}-\frac{p^{-1}}{1-p^{-1}}\frac{p^{-(s+1)}}{1-p^{-(s+1)}}}{(1-p^{-s})^{-1}}.$$

The first expression turns out to be

$$\frac{R(s)}{(1-2^{-s})^{-1}}=1-2^{-s}+2\frac{2^{-s}-2^{-2s}}{1-2^{-s}}-3\frac{2^{-(s+1)}-2^{-(2s+1)}}{1-2^{-(s+1)}}$$

which is clearly analytic in the desired region.

The second expression is

$$\frac{Q(s)}{\prod_{p\equiv 3\,(4)}(1-p^{-s})^{-1}} = \prod_{p\equiv 3\,(4)}\left(1-p^{-s}+\frac{p^{-s}}{1-p^{-1}}-\frac{p^{-(s+2)}-p^{-(2s+2)}}{(1-p^{-1})\left(1-p^{-(s+1)}\right)}\right).$$

Notice that

$$\begin{aligned} & 1-p^{-s}+\tfrac{p^{-s}}{1-p^{-1}}-\tfrac{p^{-(s+2)}-p^{-(2s+2)}}{(1-p^{-1})\left(1-p^{-(s+1)}\right)} \\ = \quad & 1+\tfrac{1}{p^{s+1}(1-p^{-1})}-\tfrac{1}{p^{s+2}(1-p^{-1})}+\tfrac{1}{p^{2s+2}(1-p^{-(s+1)}} \\ = \quad & 1+\tfrac{1}{p^{s+1}-p^{s}}-\tfrac{1}{p^{s+2}-p^{s+1}-p+1}+\tfrac{1}{p^{2s+2}-p^{2s+1}-p^{s+1}+p^{s}} \\ = \quad & 1+O\left(\tfrac{1}{p^{s+1}}\right) \end{aligned}$$

and so the product

$$\frac{Q(s)}{\prod_{p\equiv 3\,(4)}(1-p^{-s})^{-1}}=\prod_{p\equiv 3\,(4)}\left(1+O\left(\frac{1}{p^{s+1}}\right)\right)$$

converges in the desired region $\mathrm{Re}(s)>0$ in which it is analytic, implying that $\frac{D(s)}{\zeta(s)}$ is also analytic there.

Let $A(s)$ be an analytic function in $\mathrm{Re}(s) > 0$ defined by $D(s) = A(s)\zeta(s)$. Since $\mathrm{Res}_{s=1}\zeta(s) = 1$, in order to compute $\mathrm{Res}_{s=1}D(s)$ we can simply compute $A(1)$ and so

$$\mathrm{Res}_{s=1}D(s) = A(1) = \prod_{p\equiv 3\,(4)} \frac{1}{1-\frac{1}{p^2}} = 2\beta^2.$$

2.3. **Some Help From Harmonic Analysis.**

Theorem 1. *Let $F(s) = \sum_{n=1}^{\infty} b(n)n^{-s}$ be a Dirichlet series with positive real coefficients and absolutely convergent for $Re(s) > 1$. Suppose that $F(s)$ can be extended to a meromorphic function in the region $Re(s) \geq 1$ having no poles except for a simple pole at $s = 1$ with residue $R \geq 0$. Then*

$$\sum_{n\leq x} b(n) = Rx + o(x) \quad as\, x \to \infty.$$

This is a version of the Wiener-Ikehara Theorem, for a proof see [M].

Our series $a(h)$ meets the condition of the theorem, and so

$$\sum_{1\leq h\leq H-1} a(h) = 2\beta^2(H-1) + o(H-1) = 2\beta^2 H + o(H).$$

Since $a(h) = 2\mathscr{T}_h$ we have

$$\sum_{1\leq h\leq H-1} \mathscr{T}_h = \beta^2 H + o(H).$$

The next step is to calculate $\sum_{1\leq h\leq H-1} h\mathscr{T}_h$. Set

$$\begin{aligned} A(H-1) &= \sum_{1\leq h\leq H-1} \mathscr{T}_h = \beta^2 H + o(H) \\ f(h) &= h \end{aligned}$$

so using summation by parts

$$\begin{aligned} \sum_{1\leq h\leq H-1} h\mathscr{T}_h &= f(H-1)A(H-1) - \int_1^{H-1} A(t)f'(t)dt \\ &= \beta^2 H^2 + o(H^2) - \int_1^{H-1} \left(\beta^2\lfloor t\rfloor + o(t)\right) dt \\ &= \beta^2 H^2 + o(H^2) - \beta^2 \int_1^{H-1} (t - \{t\})dt + o(H^2) \\ &= \beta^2\left(H^2 - \frac{(H-1)^2-1}{2} + \frac{\lfloor H-1\rfloor - 1}{2} + \frac{\{H-1\}^2}{2}\right) + o(H^2) \\ &= \frac{1}{2}\beta^2 H^2 + o(H^2) \end{aligned}$$

and therefore

$$\sum_{1\leq d_1,d_2\leq H} \mathscr{T}_{\mathbf{d}} \sim 2 \sum_{1\leq h\leq H-1} (H-h)\,\mathscr{T}_h = \beta^2 H^2 + o(H^2)$$

which is effectively Gallagher's Lemma for sums of two squares and $k = 2$.

3. Sums of Squares in Modulo Rings

Following Keating-Connors we attempt to produce a 2-tuple conjecture using essentially heuristic methods and Landau's theorem. The first step would be to compute an expression for the pair correlation of representable integers:

$$\lim_{N\to\infty} \frac{1}{N} \#\left\{n \leq N \,:\, n, n+h \,\text{are both representable}\right\}.$$

To proceed, consider the consequences of the following lemma:

Lemma 2. *An integer is representable if and only if it is representable in $\mathbb{Z}/p^k\mathbb{Z}$ for every prime p and integer $k \in \mathbb{N}$.*

Equipped with this lemma we shall examine $\mathbb{Z}/p^k\mathbb{Z}$ for all primes p and $k \in \mathbb{N}$, and determine which are the representable elements in these modulo rings. This will allow us to give an expression for the the density of representable elements, and then of representable pairs.

3.1. Representable elements in modulo rings.

Definition 3. Say $a \in \mathbb{Z}/p^k\mathbb{Z}$ has a non trivial representation as a sum of two squares if there exists $x, y \in \mathbb{Z}/p^k\mathbb{Z}$ such that $a \equiv x^2 + y^2 \left(p^k\right)$ with $(x, p) = 1$.

Definition 4. Say $a \in \mathbb{Z}/p^k\mathbb{Z}$ has a completely non trivial representation as a sum of two squares if there exists $x, y \in \mathbb{Z}/p^k\mathbb{Z}$ such that $a \equiv x^2 + y^2 \left(p^k\right)$ with $(x, p) = 1$ and $(y, p) = 1$.

Definition 5. Say an element $a \in \mathbb{Z}/p^k\mathbb{Z}$ lifts to an element $b \in \mathbb{Z}/p^{k+l}\mathbb{Z}$ if $b \equiv a \left(p^k\right)$.

The following propositions give the information needed in order to prove Lemma 2, to sort the representable elements in the modulo rings and to compute their densities:

Proposition 6. *Let p be an odd prime, $k \in \mathbb{N}$ and $a \in \mathbb{Z}/p^k\mathbb{Z}$.*

(a) If a has a non trivial representation and $(a, p) = 1$, then all lifts of a in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ have non trivial representations as well.

(b) If a has a completely non trivial representation and $(a, p) > 1$, then all lifts of a in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ have completely non trivial representations as well.

Proof. For $k \geq 1$, take $a \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ such that $a \equiv x^2 + y^2 \left(p^k\right)$, $(x,p) = 1$, so a is lifted from an element with a non trivial representation in $\mathbb{Z}/p^k\mathbb{Z}$. Since $x \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ the element $x' = x - \frac{x^2+y^2-a}{2x}$ is well defined and gives

$$x'^2 + y^2 = a + \frac{(x^2+y^2-a)^2}{4x^2}.$$

We assume $x^2 + y^2 - a \equiv 0 \left(p^k\right)$ and so $(x^2+y^2-a)^2 \equiv 0 \left(p^{2k}\right)$. Since $k \geq 1$ we have $(x^2+y^2-a)^2 \equiv 0 \left(p^{k+1}\right)$, meaning $x'^2 + y^2 \equiv a \left(p^{k+1}\right)$. In case (a) we assume $(a,p) = 1$ and so p and at least one of x', y must be co-prime, as required. In case (b) we assume $(a,p) = p$ and we have $(y,p) = 1$, and so we must have $(x',p) = 1$ as well. □

Proposition 7. *Let p be an odd prime and $a \in \mathbb{Z}/p\mathbb{Z}$, $(a,p) = 1$, so a has a non trivial representation.*

Proof. We claim that for any nonzero element in $\mathbb{Z}/p\mathbb{Z}$ there are x, y so that

$$x^2 \equiv a - y^2 \ (p).$$

If $u^2 \equiv v^2 \ (p)$ then $u \equiv \pm v \ (p)$, therefore x^2 and $a - y^2$ each take $\frac{p+1}{2}$ different values. Since there are only p different elements in $\mathbb{Z}/p\mathbb{Z}$ there is a couple that solves the congruence and so a is representable. Since $a \not\equiv 0 \ (p)$ it is impossible that $(x,p) > 1$ and $(y,p) > 1$, and so we can choose a representation with $(x,p) = 1$ as required. □

Proposition 8. *Let p be a prime such that $p \equiv 1 \ (4)$, so $0 \in \mathbb{Z}/p\mathbb{Z}$ has a completely non trivial representation.*

Proof. Since $p \equiv 1 \ (4)$, -1 is a quadratic residue modulo p so there exists a nonzero element α such that $\alpha^2 \equiv -1 \ (p)$ and so $1^2 + \alpha^2 \equiv 1 + (-1) \equiv 0 \ (p)$ as required. □

Proposition 9. *Let p be prime such that $p \equiv 3 \ (4)$. Elements $0 \neq a \in \mathbb{Z}/p^k\mathbb{Z}$, $(a,p) > 1$ are representable if and only if $m_p(a)$ is even.*

Proof. If $m_p(a)$ is even, we can write $a = d \cdot p^{2l}$, $(d,p) = 1$. The element d is representable as a lift of a nonzero element in $\mathbb{Z}/p\mathbb{Z}$ by Propositions 6 and 7, while p^{2l} is a square itself and therefore obviously representable. Since the product of two representable elements is also representable, we have the required result.

Now assume $a \in \mathbb{Z}/p^k\mathbb{Z}$ is representable, $m_p(a) = 2l+1$ and $k > 2l+1$:

$$\begin{aligned} a = d \cdot p^{2l+1} \equiv x^2 + y^2 \left(p^k\right) \quad &, \ (d,p) = 1 \\ \implies \quad x^2 + y^2 = d \cdot p^{2l+1} + mp^k = (d + mp^{k-2l-1})p^{2l+1} \quad &, \ m \in \mathbb{N}. \end{aligned}$$

Since $k - 2l - 1 > 0$ and $(d,p) = 1$ we have $(d + mp^{k-2l-1}, p) = 1$, and so p has an odd multiplicity in the prime decomposition of $x^2 + y^2$, which is a contradiction. □

Using Propositions 6, 7 and 8 we establish that all elements in $\mathbb{Z}/p^k\mathbb{Z}$ for $p \equiv 1\ (4)$ are representable, while Propositions 6, 7 and 9 establish that the non representable elements in $\mathbb{Z}/p^k\mathbb{Z}$ for $p \equiv 3\ (4)$ are those with odd m_p. Let us now examine the elements in $\mathbb{Z}/2^k\mathbb{Z}$:

Proposition 10. *An element $a \in \mathbb{Z}/2^k\mathbb{Z}$ such that $a \equiv 1 + 4n \left(2^k\right)$ for some n, is representable as a sum of squares.*

Proof. For $k = 1, 2$ the only element in question is 1, and $1 \equiv 1^2 + 0^2\ (4)$, and for $k = 3$ we also have $5 \equiv 1^2 + 2^2\ (8)$. Take $k \geq 3$, $a \in \mathbb{Z}/2^{k+1}\mathbb{Z}$, $a \equiv 1\ (4)$. By our assumption there are x, y in $\mathbb{Z}/2^k\mathbb{Z}$ such that $a \equiv x^2 + y^2 \left(2^k\right)$ and we can assume $(x, 2) = 1$ since $a \equiv 1\ (4)$. If $x^2 + y^2 \equiv a \left(2^{k+1}\right)$ we are done. The only other option is that $x^2 + y^2 \equiv a + 2^k \left(2^{k+1}\right)$. In this case we have

$$\begin{aligned}(x + 2^{k-1})^2 + y^2 &\equiv x^2 + 2^k x + 2^{2k-2} + y^2 \\ &\equiv x^2 + 2^k + y^2 \\ &\equiv a + 2^k + 2^k \equiv a \left(2^{k+1}\right).\end{aligned}$$

since $2^k x \equiv 2^k \left(2^{k+1}\right)$ and $2^{2k-2} \equiv 0 \left(2^{k+1}\right)$ for $k \geq 3$. □

Proposition 11. *An element $a \in \mathbb{Z}/2^k\mathbb{Z}$ of the form $a = 2^j(1 + 4n)$, $0 \leq j \leq k - 1$ is representable, and these are all the representable elements.*

Proof. Using the multiplicativity of representable integers it is enough to show that 2^j is representable. For $j = 2l$ take $(2^l)^2 + 0^2 = 2^{2l}$, and for $j = 2l + 1$ take $(2^l)^2 + (2^l)^2 = 2^{2l+1}$. There are no other representable elements since all representable integers in $\mathbb{N}$ must take the form $2^j(1 + 4n)$, which is not changed modulo 2^k. □

The proof of Lemma 2 is now clear: Say $a = x^2 + y^2$, so obviously $a \equiv x^2 + y^2 \left(p^k\right)$. Conversely assume a is not representable, then for some $p \equiv 3\ (4)$ $m_p(a)$ is odd, so a is not representable in $\mathbb{Z}/p^k\mathbb{Z}$ for $k \geq m_p(a)$.

3.2. **Mean density of representable elements in modulo rings.** We now wish to calculate the densities of representable elements in $\mathbb{Z}/p^k\mathbb{Z}$ for all primes, $k \to \infty$. The following propositions provide a method for deriving these limits, and present ideas which can be useful also for calculating correlations of higher degrees.

Proposition 12. *The mean density of representable elements in $\mathbb{Z}/p^k\mathbb{Z}$, $p \equiv 1\ (4)$ for $k \to \infty$ is 1.*

Proof. This is immediate from the fact that all elements in $\mathbb{Z}/p^k\mathbb{Z}$ for all k are representable. □

Proposition 13. *For $p \equiv 3\ (4)$, the density of representable lifts of $0 \in \mathbb{Z}/p^{2l+1}\mathbb{Z}$ in $\mathbb{Z}/p^k\mathbb{Z}$ tends to $\frac{1}{p+1}$ as $k \to \infty$. The density of representable lifts of $0 \in \mathbb{Z}/p^{2l}\mathbb{Z}$ in $\mathbb{Z}/p^k\mathbb{Z}$ tends to $\frac{p}{p+1}$ as $k \to \infty$.*

Proof. Consider first the lifts of $0 \in \mathbb{Z}/p\mathbb{Z}$ in $\mathbb{Z}/p^2\mathbb{Z}$ given by $0, p, 2p, ..., (p-1)p$. Obviously the multiplicity of p in the nonzero lifts is odd, and therefore they are not representable in $\mathbb{Z}/p^2\mathbb{Z}$, and so are all of their lifts in $\mathbb{Z}/p^k\mathbb{Z}$ for $k \geq 2$.

Consider now $0 \in \mathbb{Z}/p^2\mathbb{Z}$ and it's lifts $0, p^2, 2p^2, ..., (p-1)p^2$ in $\mathbb{Z}/p^3\mathbb{Z}$. Here the multiplicity of p in the nonzero lifts is even, and therefore they are representable in $\mathbb{Z}/p^2\mathbb{Z}$, and so are all of their lifts in $\mathbb{Z}/p^k\mathbb{Z}$ for $k \geq 3$. So in $\mathbb{Z}/p^2\mathbb{Z}$ we have a single representable lift of $0 \in \mathbb{Z}/p\mathbb{Z}$, and in $\mathbb{Z}/p^3\mathbb{Z}$ we have $1 + (p-1)$ such lifts.

The next step is similar to the first, where for $0 \in \mathbb{Z}/p^3\mathbb{Z}$ the only representable lift is $0 \in \mathbb{Z}/p^4\mathbb{Z}$, and each of the $p-1$ nonzero lifts in $\mathbb{Z}/p^3\mathbb{Z}$ has p representable lifts in $\mathbb{Z}/p^4\mathbb{Z}$. So there are exactly $1 + p(p-1)$ representable lifts of $0 \in \mathbb{Z}/p\mathbb{Z}$ in $\mathbb{Z}/p^4\mathbb{Z}$, and similarly $1 + (p-1) + p^2(p-1)$ such lifts in $\mathbb{Z}/p^5\mathbb{Z}$, $1 + p(p-1) + p^3(p-1)$ lifts in $\mathbb{Z}/p^6\mathbb{Z}$ and so on. The total number of lifts of $0 \in \mathbb{Z}/p\mathbb{Z}$ in $\mathbb{Z}/p^k\mathbb{Z}$ is p^{k-1}, and so the density of representable lifts is given by

$$\frac{1}{p^{k-1}}\left(1 + (p-1)\sum_{n=0}^{\frac{(k-3)}{2}} p^{2n}\right) = \frac{1}{p^{k-1}} - \frac{1}{(p+1)p^{k-1}} + \frac{1}{p+1} \text{ for odd } k,$$

$$\frac{1}{p^{k-1}}\left(1 + p(p-1)\sum_{n=0}^{\frac{(k-4)}{2}} p^{2n}\right) = \frac{1}{p^{k-1}} - \frac{p}{(p+1)p^{k-1}} + \frac{1}{p+1} \text{ for even } k.$$

In both cases it is clear that the density tends to $\frac{1}{p+1}$ as $k \to \infty$.

Note that the exact same results holds for representable lifts of $0 \in \mathbb{Z}/p^{2l+1}\mathbb{Z}$ in $\mathbb{Z}/p^k\mathbb{Z}$ as $k \to \infty$. For the density of representable lifts of $0 \in \mathbb{Z}/p^{2l}\mathbb{Z}$ one follows the exact same steps with a single shift, meaning that the above expression is multiplied by p and thus the density of representable lifts of $0 \in \mathbb{Z}/p^{2l}\mathbb{Z}$ in $\mathbb{Z}/p^k\mathbb{Z}$ tends to$\frac{p}{p+1}$ as $k \to \infty$. □

Proposition 14. *The mean density of representable elements in* $\mathbb{Z}/p^k\mathbb{Z}$, $p \equiv 3\ (4)$ *for* $k \to \infty$ *is* $\left(1 + p^{-1}\right)^{-1}$.

Proof. It is enough to look at elements $a \in \mathbb{Z}/p\mathbb{Z}$. There are $p-1$ elements such that $(a, p) = 1$, and by Proposition 9 these are all representable and so are all their lifts. The density of representable lifts of $a = 0 \in \mathbb{Z}/p\mathbb{Z}$ in $\mathbb{Z}/p^k\mathbb{Z}$ tends to $\frac{1}{p+1}$ as $k \to \infty$. Combining the above we arrive at the desired expression

$$\frac{p - 1 + \frac{1}{p+1}}{p} = \frac{p}{p+1} = \left(1 + p^{-1}\right)^{-1}.$$

□

Proposition 15. *An element* $a \in \mathbb{Z}/2^k\mathbb{Z}$ *of the form* $2^j(1+4n)$, $0 \leq j \leq k-2$ *is lifted into two elements in* $\mathbb{Z}/2^{k+1}\mathbb{Z}$ *both can be written in a similar form. Only one of the two lifts of* 0 *and* 2^{k-1} *can be written in that form for all* $\mathbb{Z}/2^l\mathbb{Z}$, $l \geq k+1$.

Proof. The first lift of $2^j(1+4n)$ is itself and so trivially can be written in that form. The second is $2^j(1+4n)+2^k = 2^j(1+4n+2^{k-j}) = 2^j(1+4m)$ since $k-j \geq 2$. If $a \equiv 0 \left(2^k\right)$ it can be written as $a = 2^l \cdot c$ with c odd and $l \geq k$, so in the cases that $c \equiv 3\ (4)$ we will not be able to write a in the required form for all $\mathbb{Z}/2^l\mathbb{Z}$. If $a \equiv 2^{k-1} \left(2^k\right)$ it can be written as $a = 2^{k-1} \cdot c$ with c odd, and again we will not be able to write a in the required form for all $\mathbb{Z}/2^l\mathbb{Z}$. □

Proposition 16. *The mean density of representable elements in $\mathbb{Z}/2^k\mathbb{Z}$, for $k \to \infty$ is $\frac{1}{2}$.*

Proof. Again we look at elements in $\mathbb{Z}/2\mathbb{Z}$. By Proposition 15 the density of representable lifts of $0, 1 \in \mathbb{Z}/2\mathbb{Z}$ in $\mathbb{Z}/2^k\mathbb{Z}$ for $k \to \infty$ is $\frac{1}{2}$, and so the density of representable elements in $\mathbb{Z}/2^k\mathbb{Z}$ for $k \to \infty$ is

$$\frac{2 \cdot \frac{1}{2}}{2} = \frac{1}{2}.$$

□

We wish to calculate the mean density of representable integers, so following our approach we take the product of all the above densities for $p \leq n$:

$$\mathcal{M}(n) = \frac{1}{2} \prod_{\substack{p \equiv 3\ (4) \\ p \leq n}} \left(1 + p^{-1}\right)^{-1}. \tag{3.1}$$

On the other hand, the leading term in Landau's analytic expression for the mean density of representable integers is

$$\mathcal{L}(n) = \frac{\beta}{\sqrt{\log n}}.$$

The events that an integer is representable in modulo rings of different primes show some dependency, a dependency which gives rise to a term $y(n)$ which must be taken into consideration. This term should give

$$\mathcal{L}(n) \sim \frac{\mathcal{M}(n)}{y(n)}.$$

In the next section we show that

$$\lim_{n \to \infty} y(n) = \lim_{n \to \infty} \frac{\mathcal{M}(n)}{\mathcal{L}(n)}$$

converges to some real number y.

Unfortunately we do not have a "Landau" expression for the density of representable pairs. Using the ratio y between our product of densities to Landau's density we attempt to give a conjecture for pairs given by a product of densities in modulo rings.

4. Ratio Between the Product of Densities and Landau's Result

Our expression

$$\mathcal{M}(n) = \frac{1}{2} \cdot \prod_{\substack{p \equiv 3\,(4) \\ p \leq n}} \left(1 + p^{-1}\right)^{-1}$$

which stands for the product of the densities of representable elements in modulo rings, can be calculated using a generalization of Mertesns' famous formula for arithmetic progressions. Using these methods one can calculate the term given by y in the previous section.

Mertens' original formula states that

$$\prod_{p \leq n} \left(1 - p^{-1}\right) = \frac{e^{-\gamma}}{\log n} + O\left(\frac{1}{\log^2 n}\right)$$

where the product is over all primes less than n and γ denotes Euler's constant.

For co-prime integers a, q , Languasco and Zaccagnini show [LZ] a generalization of Mertens' formula

$$\lim_{n \to \infty} \log n^{1/\varphi(q)} \prod_{\substack{p \equiv a\,(q) \\ p \leq n}} \left(1 - p^{-1}\right) = \left[e^{-\gamma} \prod_{p} \left(1 - p^{-1}\right)^{\alpha(p;a,q)}\right]^{1/\varphi(q)} \tag{4.1}$$

where φ is Eulers totient function, and $a(p; a, q)$ is given by

$$a(p; a, q) = \begin{cases} \varphi(q) - 1 & , p \equiv a\ (q) \\ -1 & , \text{otherwise} \end{cases}$$

Theorem 17. *The ratio between Landau's leading term and the product of densities in modulo rings converges and is given by*

$$y = \lim_{n \to \infty} \frac{\mathcal{M}(n)}{\mathcal{L}(n)} = \frac{1}{2}\sqrt{\frac{\pi}{e^{\gamma}}}.$$

Proof. Plugging $a = 3$, $q = 4$ in Mertens' formula for primes in arithmetic progression we have

$$\prod_{\substack{p \equiv 3\,(4) \\ p \leq n}} \left(1 - p^{-1}\right) \sim \frac{e^{-\gamma/2}}{\sqrt{\log n}} \left[\frac{\prod_{p \equiv 3\,(4)} (1 - p^{-1})}{(1 - 2^{-1}) \prod_{p \equiv 1\,(4)} (1 - p^{-1})}\right]^{1/2}$$

and since

$$\left(1 + p^{-1}\right)^{-1} = \frac{1 - p^{-1}}{1 - p^{-2}}$$

we arrive at

$$\prod_{\substack{p\equiv 3\,(4)\\ p\leq n}}\left(1+p^{-1}\right)^{-1}\sim\frac{\sqrt{2}e^{-\gamma/2}}{\sqrt{\log n}}\prod_{p\equiv 3\,(4)}\left(1-p^{-1}\right)^{-\frac{1}{2}}\left(1+p^{-1}\right)^{-1}\prod_{p\equiv 1\,(4)}\left(1-p^{-1}\right)^{-\frac{1}{2}}.$$

We are interested in the ratio

$$\lim_{n\to\infty}\frac{\mathcal{M}(n)}{\mathcal{L}(n)}=\lim_{n\to\infty}\frac{\mathcal{M}(n)}{\beta/\sqrt{\log n}}$$

with β the Landau-Ramanujan constant given by

$$\beta=\frac{1}{\sqrt{2}}\prod_{p\equiv 3\,(4)}\left(1-p^{-2}\right)^{-1/2}$$

and so

$$\lim_{n\to\infty}\frac{\mathcal{M}(n)}{\mathcal{L}(n)}=\frac{1}{2}\cdot 2e^{-\gamma/2}\prod_{p\equiv 3\,(4)}\left(1+p^{-1}\right)^{-1/2}\prod_{p\equiv 1\,(4)}\left(1-p^{-1}\right)^{-1/2}.$$

The two products are exactly $\sqrt{L(1)}$ which is calculated in [SW], where $L(s)$ is the Dirichlet series for the non principal character modulo 4. Therefore

$$y=\lim_{n\to\infty}\frac{\mathcal{M}(n)}{\mathcal{L}(n)}=e^{-\gamma/2}\sqrt{\frac{\pi}{4}}=\frac{1}{2}\sqrt{\frac{\pi}{e^{\gamma}}}.$$

□

This is quite an elegant result, which can be easily generalized using similar tools as will be done in section 6.

5. Representable Pairs In Modulo Rings And Their Densities

We are now in a position to look at the distribution of representable pairs $n, n+h$ in $\mathbb{Z}/p^k\mathbb{Z}$ for p an odd prime. We first notice that since all elements in $\mathbb{Z}/p^k\mathbb{Z}$ for $p\equiv 1\ (4)$ are representable, for every h all couples $n, n+h$ are representable. This is not the case for primes $p\equiv 3\ (4)$.

Proposition 18. *The density of representable pairs $(a, a+h)$ in $\mathbb{Z}/p^k\mathbb{Z}$, $k\to\infty$, for primes $p\equiv 3\ (4)$ is $\dfrac{1-p^{-(m_p(h)+1)}}{1+p^{-1}}$.*

Proof. First say $m_p(h)=0$ and let us look at pairs $(a, a+h)$ in $\mathbb{Z}/p\mathbb{Z}$. There are $p-2$ pairs such that both elements are nonzero and therefore representable, and two additional pairs such that one of the elements is 0. By Propositions 6 and 7 all nonzero elements lift into representable elements and therefore all lifts of the $p-2$ nonzero pairs are representable. Therefore by Proposition 13 the density of pairs with a zero element which are lifted into representable couples is $\frac{1}{p+1}$, and so the density of representable pairs is

$$\frac{p-2+2\cdot\frac{1}{p+1}}{p}=\frac{1-\frac{1}{p}}{1+\frac{1}{p}}.$$

Next say $m_p(h) = 1$, so there are $p-1$ pairs with nonzero elements and a single pair of two zeros in $\mathbb{Z}/p\mathbb{Z}$. This does not provide enough data and so we look at these pairs in $\mathbb{Z}/p^2\mathbb{Z}$. There are $p(p-1)$ pairs $(a, a+h)$ in $\mathbb{Z}/p^2\mathbb{Z}$ which are lifts of the nonzero pairs, and p pairs which are lifted from the zero pair, each one consisting of at least one nonzero lift of zero which, as we have seen, is not representable and so these pairs are not representable. The density of representable pairs is therefore

$$\frac{p(p-1)}{p^2} = \frac{1-\frac{1}{p^2}}{1+\frac{1}{p}}.$$

For $m_p(h) = 2$, again we have $p-1$ nonzero pairs with $p(p-1)$ representable lifts into $\mathbb{Z}/p^2\mathbb{Z}$. The zero pair's lift remains a zero pair and so we look at pairs in $\mathbb{Z}/p^3\mathbb{Z}$. There are now $p^2(p-1)$ pairs in $\mathbb{Z}/p^2\mathbb{Z}$ lifted from the nonzero pairs, and in addition $p-2$ pairs which are nonzero in $\mathbb{Z}/p^3\mathbb{Z}$ but are lifts of the zero pair. These lifts are representable, and the two remaining lifts of the zero pair consist as before of a nonzero element and the zero element, and so similarly to the case of $m_p(h) = 0$ the density of representable pairs is

$$\frac{p^2(p-1) + (p-2) + 2\cdot\frac{1}{p+1}}{p^3} = \frac{1-\frac{1}{p^3}}{1+\frac{1}{p}}.$$

Following these ideas for even $m_p(h)$ yields

$$\frac{(p-1)\sum_{n=1}^{\frac{m_p(h)}{2}}\left(p^2\right)^n + p - 2 + 2\cdot\frac{1}{p+1}}{p^{m_p(h)+1}} = \frac{1-\frac{1}{p^{m_p(h)+1}}}{1+\frac{1}{p}}$$

and for odd $m_p(h)$

$$\frac{p(p-1)\sum_{n=1}^{\frac{m_p(h)-1}{2}}\left(p^2\right)^n}{p^{m_p(h)+1}} = \frac{1-\frac{1}{p^{m_p(h)+1}}}{1+\frac{1}{p}}.$$

□

Proposition 19. *The density of representable pairs $(a, a+h)$ in $\mathbb{Z}/2^k\mathbb{Z}$, $k \to \infty$, is*

$$W_2(h) = \begin{cases} \frac{1}{4} & m_2(h) = 0 \\ \frac{2^{m_2(h)+1}-3}{2^{m_2(h)+2}} & m_2(h) \geq 1 \end{cases}.$$

Proof. We now take into consideration the distribution of pairs $(a, a+h)$ with $h = 2^i$ in $\mathbb{Z}/p^k\mathbb{Z}$. For odd primes the distribution is similar to that of $(a, a+1)$ since $(1, p) = (2^i, p) = 1$ and we have seen that the distribution depends only on $m_p(h)$. This is true also for distribution in $\mathbb{Z}/2^k\mathbb{Z}$, and so it is enough to look at $\mathbb{Z}/2^{m_2(h)+1}\mathbb{Z}$. Set $l = m_2(h)$, and let us look at pairs $(a, a+h)$ in $\mathbb{Z}/2^{l+1}\mathbb{Z}$.

It is easily verified that $\frac{1}{4}$ of the pairs are of the form $\left(2^0(1+4m), 2^0(1+4m)+2^l\right)$ and similarly for all $0 \leq i \leq l-2$ we have $\frac{1}{2^{i+2}}$ of the pairs are of the form $\left(2^i(1+4m), 2^i(1+4m)+2^l\right)$. The pair $\left(2^{l-1}, 2^{l-1}+2^l\right)$ is not representable since $2^{l-1}+2^l = 3\cdot 2^{l-1}$. The last two pairs we must take into consideration are $(0, 2^l)$ and $(2^l, 0)$. As shown in proposition 15 the density of representable lifts of these pairs to $\mathbb{Z}/2^k\mathbb{Z}$ for $k \to \infty$ is $\frac{1}{2}\cdot\frac{1}{2}$.

We can now compute the density of representable pairs:

$$\sum_{n=2}^{l} \frac{1}{2^n} + 2\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2^{l+1}} = \frac{2^{l+1}-3}{2^{l+2}}.$$

For $l = 0, 1$ the sum does not contribute and so the density is $\frac{1}{4}$ and $\frac{1}{8}$ respectively, giving the desired result. □

As before the events that a pair $(m, m+h)$, $m \leq n$ is representable in all the prime power modulo rings are not independent, a dependency which gives rise to a term $Y_h(n)$ which must be taken into consideration. The density of representable pairs is thus:

$$\frac{1}{Y_h(n)}\cdot W_2(h) \prod_{\substack{p\equiv 3\,(4)\\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{1+p^{-1}}.$$

Following Connors-Keating we extract the asymptotic term depending on n from the above expression using our calculation for the mean density of representable integers:

$$\begin{aligned} &\tfrac{1}{Y_h(n)}\cdot W_2(h) \prod_{\substack{p\equiv 3\,(4)\\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{1+p^{-1}} \cdot \left(\tfrac{\mathcal{L}(n)}{\mathcal{M}(n)/y(n)}\right)^2 \\ \sim\ &\tfrac{1}{\log n}\left(\tfrac{y(n)^2}{Y_h(n)}\right)\left(\tfrac{\frac{1}{\sqrt{2}}}{\frac{1}{2}}\right)^2 W_2(h)\cdot \\ &\prod_{\substack{p\equiv 3\,(4)\\ p\leq n}} \frac{\left(1-p^{-(m_p(h)+1)}\right)\left(1-p^{-2}\right)^{-1}}{\left(1+p^{-1}\right)\left(1+p^{-1}\right)^{-2}} \\ \sim\ &\tfrac{1}{\log n}\cdot\left(\tfrac{y(n)^2}{Y_h(n)}\right)\cdot 2W_2(h) \prod_{\substack{p\equiv 3\,(4)\\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}}. \end{aligned} \tag{5.1}$$

Notice that for p such that $m_p(h) = 0$ the product is 1, and since we are interested in $n \to \infty$, we can assume $n \geq h$ and so the product is over all $p \equiv 3\ (4)$ such that $p \mid h$. The conjecture presented by Connors-Keating is thus equivalent to the conjecture that for all h

$$\frac{y(n)^2}{Y_h(n)} \to 1,\ as\, n \to \infty,$$

a conjecture for which we present some numerical computations in Section 7.

Assuming the validity of this conjecture the density of representable pairs is given by

$$\mathscr{T}_h = \frac{1}{\log n} \cdot 2W_2(h) \prod_{\substack{p\equiv 3\,(4)\\ p|h}} \frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}}.$$

6. Generalization to Other Binary Quadratic Forms

6.1. **Preliminaries.** Let us look at the following family of binary quadratic forms

$$q(d;x,y) = x^2 + dy^2.$$

Definition 20. We say that $d \in \mathbb{N}$ is a convenient (idoneal) number if there is finite set of primes S, an integer N and congruence classes $c_1, ..., c_k \bmod N$ such that for all primes $p \notin S$

$$p = x^2 + dy^2 \iff p \equiv c_1, ..., c_k \bmod N.$$

Example 21. For $d = 1$, $S = \{2\}$, $c_1 = 1$ and $N = 4$ we have Fermat's result for sums of two squares.

We focus here on convenient d's such that the form $x^2 + dy^2$ is of class number 1 which are $d = 1, 2, 3, 4, 7$. In these cases one can fully determine if an integer n is representable by the form simply by making sure that the primes which are not representable appear with an even multiplicity in the integer's prime factorization.

Again we are first interested in the mean density of representable integers, and we can calculate the densities in the modulo rings in the exact same way that we did for $d = 1$ and thus generalize (3.1) . In [SS] Shanks produces Landau's constants $\beta_1, \beta_2, \beta_3, \beta_4, \beta_7$ for which

$$\#\{n \le N |\, n\text{is of the form } x^2 + dy^2\} \sim \beta_d \frac{N}{\sqrt{\log N}}$$

and so we can again calculate the ratio between the product and the analytic expressions as was done in Section 4 for sums of squares.

First let us recall the following classical results:

Theorem 22. *An integer n is representable by the form $x^2 + dy^2$* if and only if:

- If $d = 1$, $m_p(n)$ is even for all primes $p \equiv 3\ (4)$.
- If $d = 2$, $m_p(n)$ is even for all primes $p \equiv 5, 7\ (8)$.
- If $d = 3$, $m_p(n)$ is even for all primes $p \equiv 2\ (3)$.
- If $d = 4$, $m_p(n)$ is even for all primes $p \equiv 3\ (4)$ and $m_2(n) \neq 1$.
- If $d = 7$, $m_p(n)$ is even for all primes $p \equiv 3, 5, 6\ (7)$ and $m_2(n) \neq 1$.

The conditions for representation by these forms bare obvious resemblance.

Definition 23. For convenience reasons we divide the primes into the following sets:

- Let Q_d denote primes p such that if n is of the form x^2+dy^2 then $m_p(n)$ is even. Notice that by Dirichlet's theorem this consists of approximately half of the primes.
- Let R_d denote primes p such that if n is of the form x^2+dy^2 then $m_p(n)$ has some constraint which is not that $m_p(n)$ is even, or the N for which $p=x^2+dy^2 \iff p\equiv c_1,...,c_k \bmod N$ is such that $(p,N)\neq 1$. Notice that R_d is a finite set.
- Let P_d denote primes p not in any of the above sets, or more directly primes of the form x^2+dy^2 such that $(p,N)=1$. Again this set consists of approximately half of the primes.

Example 24. $Q_1=\{p \text{ prime: } p\equiv 3\ (4)\}$, $P_1=\{p \text{ prime: } p\equiv 1\ (4)\}$, $R_1=\{2\}$.

$Q_7=\{p \text{ prime: } p\equiv 3,5,6\ (7)\}$, $P_7=\{p \text{ prime: } p\equiv 1,2,4\ (7),\ p\neq 2\}$, $R_7=\{2,7\}$.

6.2. **Ratio between the product density and Landau's density.** Following the same methods established in Section 3 for our product calculation of $\mathcal{M}(n)$ we can now give a product expression for $\mathcal{M}_d(n)$, which stands for the product formula for the mean density of integers of the form x^2+dy^2. Notice that for all the above d's the condition for being representable by the form is over half of the primes plus some local conditions, and so again we have an expression of the form

$$\mathcal{M}_d(n)=\prod_{p\in R_d} w_d(p)\prod_{\substack{p\in Q_d\\ p\leq n}}\left(1+p^{-1}\right)^{-1}$$

with $w_d(p)$ the mean density of representable element in $\mathbb{Z}/p^k\mathbb{Z}$, $k\to\infty$, for $p\in R_d$. The primes $p\in P_d$ do not participate here since similarly to the case of sum of two squares, the mean density of representable elements in $\mathbb{Z}/p^k\mathbb{Z}$, $k\to\infty$, is 1.

These products can be computed using Merten's formula for arithmetic progressions, as was done in the previous section for $d=1$:

$$\prod_{\substack{p\in Q_d\\ p\leq n}}\left(1+p^{-1}\right)^{-1} \sim \frac{e^{-\gamma/2}}{\sqrt{\log n}}\prod_{p\in Q_d}\left(1-p^{-1}\right)^{-\frac{1}{2}}\left(1+p^{-1}\right)^{-1}\prod_{p\in P_d\cup R_d}\left(1-p^{-1}\right)^{-\frac{1}{2}}.$$

Again we are interested in the analogue of (1.9), that is in the ratio between these products and the leading term of the analytic expression given by the generalization of Landau's theorem as shown in [SS]:

$$\mathcal{L}_d(n)=\frac{\beta_u}{\sqrt{\log n}}\ ,\quad \beta_d=\delta_d\cdot g_d\cdot\left(\frac{L_d(1)\cdot 2\left|d\right|}{\pi\varphi(2\left|d\right|)}\right)^{\frac{1}{2}} \tag{6.1}$$

with φ the Euler totient function and

$$\begin{aligned} g_d &= \prod_{\left(\frac{-d}{p}\right)=-1} \left(1-p^{-2}\right)^{-\frac{1}{2}} \\ L_d(s) &= \sum_{\text{odd } n} \left(\frac{-d}{n}\right) n^{-s} = \prod_{\left(\frac{-d}{p}\right)=1} \left(1-p^{-s}\right)^{-1} \prod_{\left(\frac{-d}{p}\right)=-1} \left(1+p^{-s}\right)^{-1} \\ \delta_d &= \begin{cases} 1 & , d=1,2 \\ \frac{2}{3} & , d=3 \\ \frac{3}{4} & , d=4,7 \end{cases} \end{aligned}$$

Notice that for $d=1,2,3,4,7$

$$\left(\frac{-d}{p}\right)=1 \iff p \in P_d$$

and

$$\left(\frac{-d}{p}\right)=-1 \iff p \in Q_d$$

unless $d=3$, in which case $Q_3 = \left\{p : \left(\frac{-d}{p}\right)=-1\right\} \cup \{2\}$.

Reformulating the products above we have

$$g_d = \prod_{2\neq p\in Q_d} \left(1-p^{-2}\right)^{-\frac{1}{2}} = \gamma_d \prod_{p\in Q_d} \left(1-p^{-2}\right)^{-\frac{1}{2}}$$

where $\gamma_d = \begin{cases} 1 & , d=1,2,4,7 \\ \frac{\sqrt{3}}{2} & , d=3 \end{cases}$, and

$$\begin{aligned} \sqrt{L_d(1)} &= \prod_{p\in P_d} \left(1-p^{-1}\right)^{-\frac{1}{2}} \prod_{2\neq p\in Q_d} \left(1+p^{-1}\right)^{-\frac{1}{2}} \\ &= \prod_{p\in P_d} \left(1-p^{-1}\right)^{-\frac{1}{2}} \lambda_d \prod_{p\in Q_d} \left(1+p^{-1}\right)^{-\frac{1}{2}} \end{aligned}$$

where $\lambda_d = \begin{cases} 1 & , d=1,2,4,7 \\ \sqrt{\frac{3}{2}} & , d=3 \end{cases}$.

The ratio in question is therefore given by

$$\lim_{n\to\infty} y_d(n) = \lim_{n\to\infty} \frac{\mathcal{M}_d(n)}{\mathcal{L}_d(n)} = \lim_{n\to\infty} \frac{\mathcal{M}_d(n)}{\beta_d/\sqrt{\log n}} =$$

$$\prod_{p\in R_d} w_d(p) \tfrac{1}{\delta_d} \sqrt{\tfrac{\pi}{e^\gamma}} \cdot \sqrt{\tfrac{\varphi(2|d|)}{2|d|}} \tfrac{1}{\gamma_d \lambda_d} \prod_{p\in R_d} \left(1-p^{-1}\right)^{-\frac{1}{2}}.$$

Recall $\frac{\varphi(n)}{n} = \prod_{p|n} \left(1-p^{-1}\right)$. For $d=1,2,4,7$ we have $p|2d \iff p \in R_d$ and so all the products cancel each other. For $d=3$ we have $2|2d$ and

$2 \notin R_3$, so we are left with the term $\left(1-2^{-1}\right)^{\frac{1}{2}} = \frac{1}{\sqrt{2}}$. since $\frac{1}{\sqrt{2}}\frac{2}{\sqrt{3}}\frac{\sqrt{2}}{\sqrt{3}} = \frac{2}{3}$ we can write

$$\lim_{n\to\infty} y_d(n) = \prod_{p\in R_d} w_d(p)\frac{1}{\delta_d}\sqrt{\frac{\pi}{e^\gamma}}\cdot s_d$$

where $s_d = \begin{cases} 1 & , d = 1,2,4,7 \\ \frac{2}{3} & , d = 3 \end{cases}$.

We can now examine this result for different values of d:

Theorem 25. *For $d = 1,2,3,4,7$ the ratio between the product of densities in the modulo rings and Landau's density of integers representable by the forms x^2+dy converges to $\frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}$ as $n\to\infty$, that is*

$$\lim_{n\to\infty} y_d(n) = \lim_{n\to\infty}\frac{\mathcal{M}_d(n)}{\mathcal{L}_d(n)} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}} = y.$$

Proof. We compute the ratio case by case:

$d = 1$**.** We have already seen in the previous section that $R_1 = \{2\}$, and that $w_1(2) = \frac{1}{2}$, since the representable elements in $\mathbb{Z}/2^k\mathbb{Z}$ are of the form $2^j(1+4n)$ and the density of such elements approaches $\frac{1}{2}$ as $k\to\infty$. In addition $\delta_1 = 1$ and $s_d = 1$ and so

$$\lim_{n\to\infty}\frac{\mathcal{M}_1(n)}{\mathcal{L}_1(n)} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}.$$

$d = 2$**.** Again $R_2 = \{2\}$. Here $w_2(2) = \frac{1}{2}$ because representable elements in $\mathbb{Z}/2^k\mathbb{Z}$ are of the form $2^j(1+8n)$ or $2^j(3+8n)$ and the density of such elements approaches $\frac{1}{2}$ as $k\to\infty$. Also $\delta_1 = 1$ and $s_d = 1$ and so

$$\lim_{n\to\infty}\frac{\mathcal{M}_2(n)}{\mathcal{L}_2(n)} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}.$$

$d = 3$. $R_3 = \{3\}$, and $w_3(3) = \frac{1}{2}$ since the representable elements in $\mathbb{Z}/3^k\mathbb{Z}$ are of the form $3^j(1+3n)$ and the density of such elements approaches $\frac{1}{2}$ as $k\to\infty$. Here $\delta_3 = \frac{2}{3}$ and $s_d = \frac{2}{3}$ therefore the ratio is given by

$$\lim_{n\to\infty}\frac{\mathcal{M}_3(n)}{\mathcal{L}_3(n)} = \frac{1}{2}\cdot\frac{3}{2}\sqrt{\frac{\pi}{e^\gamma}}\cdot\frac{2}{3} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}.$$

$d = 4$. Once again $R_4 = \{2\}$. This case is similar to that of $d = 1$ only here the representable elements in $\mathbb{Z}/2^k\mathbb{Z}$ are of the form $2^j(1+4n)$ with $j \neq 1$. The density of such elements is $\frac{3}{8}$ as $k\to\infty$. So $w_4(2) = \frac{3}{8}$, $\delta_4 = \frac{3}{4}$ and $s_4 = 1$

$$\lim_{n\to\infty}\frac{\mathcal{M}_4(n)}{\mathcal{L}_4(n)} = \frac{3}{8}\cdot\frac{4}{3}\sqrt{\frac{\pi}{e^\gamma}} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}.$$

$d = 7$. Here $R_7 = \{2,7\}$. Representable elements in $\mathbb{Z}/7^k\mathbb{Z}$ are of the form $7^j(1+7n)$, $7^j(2+7n)$ or $7^j(4+7n)$ and the density such elements is $\frac{1}{2}$ as $k\to\infty$. The representable elements in $\mathbb{Z}/2^k\mathbb{Z}$ are of the form $2^j(1+4n)$ or

$2^j(3+4n)$ with $j \neq 1$, and the density of such elements approaches $\frac{3}{4}$ as $k \to \infty$. We thus have $w_7(2) = \frac{3}{4}$, $w_7(7) = \frac{1}{2}$, $\delta_7 = \frac{3}{4}$ and $s_1 = 1$

$$\lim_{n\to\infty} \frac{\mathcal{M}_7(n)}{\mathcal{L}_7(n)} = \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{4}{3}\sqrt{\frac{\pi}{e^\gamma}} = \frac{1}{2}\sqrt{\frac{\pi}{e^\gamma}}.$$

□

6.3. **Pair correlation conjecture.** We can now propose a conjecture for the pair correlation function for the forms $x^2 + dy^2$ with $d = 1, 2, 3, 4, 7$, generalizing (1.6) and (1.4) . Denote by $W_{d,p}(h)$ the density of representable pairs $(a, a+h)$ in $\mathbb{Z}/p^k\mathbb{Z}$, $k \to \infty$, for $p \in R_d$, and $Y_{d,h}(n)$ the dependance term which must be taken into consideration. We extract the asymptotic term depending on n as was done in (5.1):

$$\begin{aligned}
&\frac{1}{Y_{d,h}(n)} \prod_{p\in R_d} W_{d,p}(h) \cdot \prod_{\substack{p\in Q_d \\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{1+p^{-1}} \\
\sim\ & \frac{1}{Y_{d,h}(n)} \prod_{p\in R_d} W_{d,p}(h) \prod_{\substack{p\in Q_d \\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{1+p^{-1}} \left(\frac{\mathcal{L}_d(n)}{\mathcal{M}_d(n)/y_d(n)}\right)^2 \\
\sim\ & \frac{1}{\log n} \cdot \left(\frac{y_d^2(n)}{Y_{d,h}(n)}\right) \prod_{p\in R_d} \frac{W_{d,p}(h)}{w_d^2(p)} \prod_{\substack{p\in Q_d \\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{(1+p^{-1})^{-1}} \cdot \delta_d^2 \cdot g_d^2 \cdot \frac{L_d(1)\cdot 2\,|d|}{\pi\varphi(2\,|d|)} \quad .
\end{aligned}$$

Let us first look at the products at hand. As before

$$\begin{aligned}
\prod_{\substack{p\in Q_d \\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{(1+p^{-1})^{-1}} \cdot g_d^2 &= \prod_{\substack{p\in Q_d \\ p\leq n}} \frac{1-p^{-(m_p(h)+1)}}{(1+p^{-1})^{-1}} \prod_{2\neq p\in Q_d} \left(1-p^{-2}\right)^{-1} \\
&\sim \prod_{\substack{p\in Q_d \\ p|h}} \frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}} \cdot S_d
\end{aligned}$$

where $S_d = \begin{cases} 1 & , d = 1, 2, 4, 7 \\ \frac{3}{4} & , d = 3 \end{cases}$.

Again the conjecture is that for all h

$$\frac{y_d^2(n)}{Y_{d,h}(n)} \to 1,\ as\, n \to \infty$$

and so

$$\mathscr{T}_{d,h} = c_d \prod_{p\in R_d} W_{d,p}(h) \prod_{\substack{p\in Q_d \\ p|h}} \frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}} \tag{6.2}$$

where

$$c_d = \delta_u^2 \frac{L_u(1) \cdot 2\,|u|}{\pi\varphi(2\,|u|)} \prod_{p \in R_d} \frac{1}{w_d^2(p)} S_d$$

It is left to compute c_d and $W_{d,p}(h)$ case by case. Dirichlet's class number formula (see [SW]) gives

$$L_1(1) = \frac{\pi}{4},\ L_2(1) = \frac{\pi}{2\sqrt{2}},\ L_3(1) = \frac{\pi}{2\sqrt{3}},\ L_4(1) = \frac{\pi}{4},\ L_7(1) = \frac{\pi}{2\sqrt{7}} \tag{6.3}$$

and so plugging all the different term we have

$$c_1 = 2,\ c_2 = 2\sqrt{2},\ c_3 = \frac{2}{\sqrt{3}},\ c_4 = 2,\ c_7 = \frac{2\sqrt{7}}{3}. \tag{6.4}$$

In addition, calculations similar to those shown for sums of squares in Section 5 give

$$W_{1,2}(h) = \begin{cases} \frac{1}{4} & ,\ m_2(h) = 0 \\ \frac{2^{m_2(h)+1} - 3}{2^{m_2(h)+2}} & ,\ m_2(h) \geq 1 \end{cases}$$

$$W_{2,2}(h) = \begin{cases} \frac{1}{4} & ,\ m_2(h) = 0, 1 \\ \frac{2^{m_2(h)} - 3}{2^{m_2(h)+1}} & ,\ m_2(h) \geq 2 \end{cases}$$

$$W_{3,3}(h) = \frac{1}{2} \cdot \frac{3^{m_3(h)+1} - 2}{3^{m_3(h)+1}}$$

$$W_{4,2}(h) = \begin{cases} \frac{1}{8} & ,\ m_2(h) = 0 \\ 0 & ,\ m_2(h) = 1 \\ \frac{5}{16} & ,\ m_2(h) = 2 \\ \frac{3 \cdot 2^{m_2(h)-1} - 3}{2^{m_2(h)+2}} & ,\ m_2(h) \geq 3 \end{cases}$$

$$W_{7,2}(h) = \begin{cases} \frac{1}{2} & ,\ m_2(h) = 0, 1 \\ \frac{3}{4} & ,\ m_2(h) \geq 2 \end{cases},\ W_{7,7}(h) = \frac{1}{2} \cdot \frac{7^{m_7(h)+1} - 4}{7^{m_7(h)+1}}.$$

6.4. **Distribution in short intervals - the second moment.** We wish to generalize our result from Section 2 concerning the second moments of the distribution of representable integers in short intervals.

Theorem 26. *Let $X_d(n)$ be the number of integers which can be represented by the form $x^2 + dy^2$, $d = 1, 2, 3, 4, 7$, in the interval $(n, n + \alpha_d)$, $\alpha_d \sim \frac{\lambda}{\beta_d}\sqrt{\log N}$. Denote $P_l(\alpha_d, N)$ the number of integers $n \leq N$ for which the interval $(n, n + \alpha_d)$ contains exactly l such integers. Assuming (6.2) the second moment of $P_l(\alpha_d, N)$ is Poisson.*

Proof. Following the steps described in Section 2 it is enough to show that

$$\sum_{1\le h\le H-1} \mathscr{T}_{d,h} = \beta_d^2 H + o(H).$$

In order to do that we normalize $\mathscr{T}_{d,h}$ by defining $a_d(h) = \frac{\mathscr{T}_{d,h}}{\mathscr{T}_{d,1}}$ which is now multiplicative, and show that $D_d(s) = \sum\limits_{n=1}^{\infty} a_d(h) n^{-s}$ has a simple pole at $s=1$ with residue $\frac{\beta_d}{\mathscr{T}_{d,1}}$, as was done for sums of squares. Following the exact same steps we have

$$D_d(s) = R_d(s) P_d(s) Q_d(s)$$

where

$$\begin{aligned} R_d(s) &= \prod_{p\in R_d} \left(1 + \sum_{k=1}^{\infty} \frac{a(p^k)}{p^{ks}}\right) \\ P_d(s) &= \prod_{p\in P_d} \left(1-p^{-s}\right)^{-1} \\ Q_d(s) &= \prod_{p\in Q_d} \left(1 + \frac{1}{1-p^{-1}} \frac{p^{-s}}{1-p^{-s}} - \frac{p^{-1}}{1-p^{-1}} \frac{p^{-(s+1)}}{1-p^{-(s+1)}}\right). \end{aligned}$$

It can be shown $D_d(s) = A_d(s)\zeta(s)$ with $A_d(s)$ analytic, and so to calculate the residue of $D(s)$ at $s=1$ it is left to calculate $A_d(1)$ which gives

$$A_d(1) = \lim_{s\to 1} \frac{D_d(s)}{\zeta(s)} = \prod_{p\in R_d} \frac{1 + \sum_{k=1}^{\infty} \frac{a(p^k)}{p^k}}{\left(1-p^{-1}\right)^{-1}} \prod_{p\in Q_d} \left(1-p^{-2}\right)^{-1}.$$

Recall

$$\beta_d^2 = \delta_d^2 \frac{L_d(1)\cdot 2\left|d\right|}{\pi\varphi(2\left|d\right|)} \prod_{p\in Q_d} \left(1-p^{-2}\right)^{-1}$$

and so it remains to show that indeed for $d = 1, 2, 4, 7$

$$\prod_{p\in R_d} \frac{1 + \sum_{k=1}^{\infty} \frac{a(p^k)}{p^k}}{\left(1-p^{-1}\right)^{-1}} = \frac{\delta_d^2 \frac{L_d(1)\cdot 2|d|}{\pi\varphi(2|d|)}}{\mathscr{T}_{d,1}}$$

Following the steps detailed in section 2 and plugging in all the relevant constants, all computed above, we arrive at the desired result. □

7. Numerical Computations

The approach taken in [CK] as well as ours to the pair correlation conjecture for integers representable as the sum of two squares, stated in (1.6), is essentially heuristic, and so some numerical computations are in place in order to support our conjecture. The conjecture as stated here is that

$$\frac{y(N)^2}{Y_h(N)} \to 1, \ as\, n\to\infty$$

which, as shown in (5.1), can be calculated by taking the ratio between the numeric density of pairs and the conjectured pair correlation function:

$$\frac{y(N)^2}{Y_h(N)} = \frac{\frac{1}{N}\#\{n \le N |\, n \text{ and } n+h \text{ are representable}\}}{\frac{1}{\log N}\cdot 2W_2(h)\prod_{\substack{p\equiv 3\,(4)\\ p|h}}\frac{1-p^{-(m_p(h)+1)}}{1-p^{-1}}}$$

In Figure 7.1 we present some calculations of this ratio for various h :

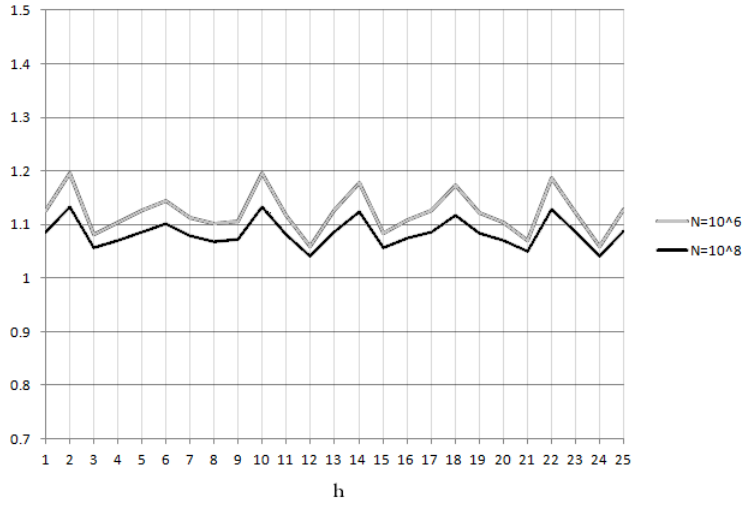

FIGURE 7.1. $\frac{y(N)^2}{Y_h(N)}$ for $1 \le h \le 25$ at $N = 10^6$,10^8

Examining different values of h for which the primes 2 and $p \equiv 3\ (4)$ appear with equal multiplicity, such as $h = 1, 5, 17, 25$ or $h = 4, 20$, one can see they take very similar values. This was checked for many more values of h which are not shown here and so strengthens our belief that the pair correlation depends only on the multiplicity of these primes in h.

One can also see that the fluctuations between different values of h diminish for larger N, where the peaks in the above graph are obtained at values of h for which $m_2(h) = 1, 2$ or $m_3(h) = 1$, since the small primes are the most dominant in our computations.

We must not be discouraged by the extremely slow decay to 1, for it is consistent with the large error term which appears in Landau's theorem in (1.3). In fact the convergence implied in Landau's theorem, or more precisely

$$\beta^2(N) = \left(\frac{\#\{n \le N |\, n \text{ is representable}\}}{\beta\frac{N}{\sqrt{\log N}}}\right)^2 \to 1\ ,\ N \to \infty$$

shows similar behavior as shown in Figure 7.2, in which the values for the ratio $\frac{y(N)^2}{Y_h(N)}$ are calculated for $h = 1$. The reason we compare the rate of convergence to that of $\beta^2(N)$ and not to $\beta(N)$ is that we look at pairs of representable integers. The values for the ratio $\frac{y(N)^2}{Y_h(N)}$ are calculated for $h = 1$.

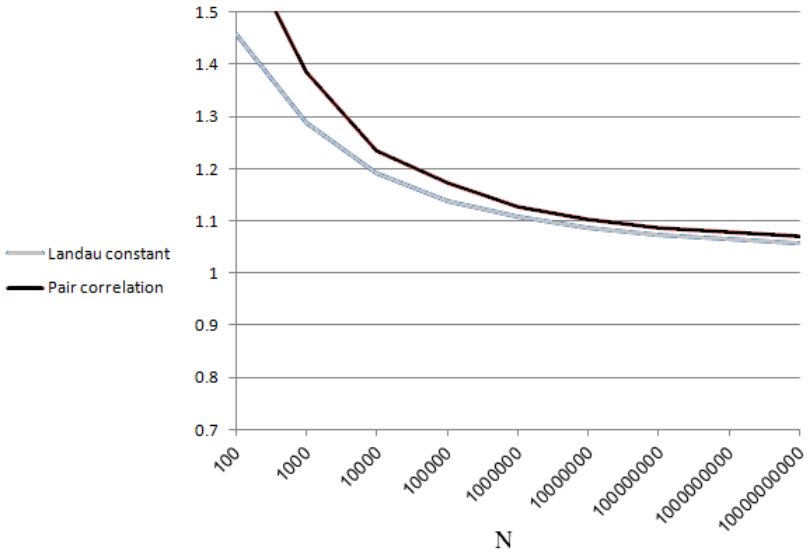

FIGURE 7.2. $\frac{y(N)^2}{Y_1(N)}$ and Landau's β^2 convergence

The generalizations presented in Section 6 for integers of the form x^2+dy^2 show similar numeric results. Figure 7.3 is the equivalent of Figure 7.1 for integers representable by $x^2 + 2y^2$.

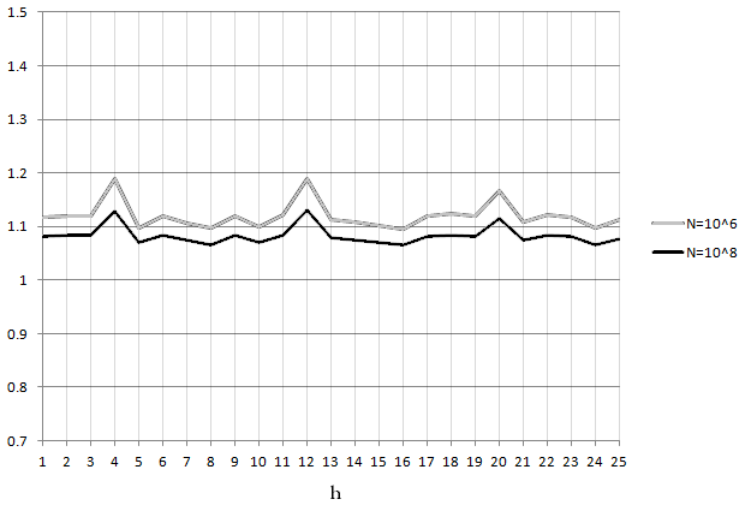

FIGURE 7.3. $\frac{y_2(N)^2}{Y_{2,h}(N)}$ for$1 \leq h \leq 25$ at $N = 10^6, 10^8$

We have obtained results of this type for the other forms in question where the main difference between the forms is the location of the peaks, which occur at values of h with small $m_p(h)$ for small primes $p \in Q_d \cup R_d$.

To conclude we have arrived with numerical results which are consistent with our expectation regarding the dependency on the prime decomposition of h, and regarding the rate of convergence. Note that the numerical data presented here improves previous computations by a factor of 10 for $1 \leq h \leq 25$ as appears in Figure 7.1 and by 1000 for $h = 1$ as appears in Figure 7.3.

8. FURTHER DIRECTIONS

The work presented here may be expanded by producing conjectures for k-correlation functions for the set of representable pairs for $k \geq 3$, as described in (1.4). For example, following the methods presented for the calculation of the mean density and the pair correlation one can derive the following result for the density of representable triplets of the form $(n, n+1, n+2)$ for $n \leq N$, given by

$$\frac{1}{\log^{\frac{3}{2}} N} \cdot \frac{1}{8\beta} \cdot \prod_{\substack{p \equiv 3\,(4) \\ n \leq N}} \frac{1 - \frac{2}{p}}{\left(1 - \frac{1}{p}\right)^2} \approx \frac{0.11698}{\log^{\frac{3}{2}} N} \tag{8.1}$$

It is possible to generalize this result for triplets $(n, n+h_1, n+h_2)$ and so on for higher degrees, though it seems difficult to obtain a general k -correlation function this way because of the inductive element of our approach. Also when comparing the expression for the density of representable triplets (8.1) to the expression for the density of representable pairs (1.6)

one can easily notice that the product for the latter depends only on primes dividing h , where in the case of the triplets the product is over all primes $p \equiv 3$ (4) and so the manipulation of such expressions is bound to be more complicated.

A second direction, assuming a k -correlation function is obtained, is to prove (1.5), which is a version of Gallagher's Lemma (1.2)for sums of two squares. Gallagher's approach in [G], and similarly the approach taken by Ford when proving the Lemma in the case of the primes, would apparently not do in the case of sums of two squares. Proving this would assert that assuming a k -correlation conjecture the distribution of representable integers in short intervals is Poissonian, and here is the place to state that we believe that this is indeed the case.

The main difference between the case of the set of primes and the case of the set of integers representable as a sum of two squares is the k-correlation conjectures. While Hardy and Littlewood's conjecture for primes (1.1) depends only on the $\nu_{\mathbf{d}}(p)$ which stands for the number of residue classes modulo p occupied by $d_1, ..., d_k$, which in the case of $k = 2$ is equivalent to whether or not p divides $d_2 - d_1$ or whether or not if $m_p(d_2 - d_1)$ is 0, in the case of the sums of squares Connors and Keating's conjecture (1.6) and the numerical work presented in Section (7) provide evidence of dependence also on the values of $m_p(d_2 - d_1)$. Our proof of Gallagher's Lemma for sums of squares and $k = 2$ uses Dirichlet analysis, though these methods become extremely difficult in higher dimensions.

We hope this work encourages the reader to further explore the set of integers representable by sums of squares an other forms, where there is a lot yet to be done.

References

[CK] Connors, R. D.; Keating, J. P. Two-point spectral correlations for the square billiard. J. Phys. A 30 (1997), no. 6, 1817–1830.

[C] Cox, D. A. Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, (1989).

[F] Ford, K. Simple proof of gallgher's singular series sum estimate, arXiv:1108.3861v1 [math.NT]

[G] Gallagher, P. X. On the distribution of primes in short intervals. Mathematika 23 (1976), no. 1, 4–9.

[HL] Hardy, G. H.; Littlewood, J. E. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. Acta Math. 44 (1923), no. 1, 1–70.

[L] Landau, E. Uber die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindeszahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate, Archiv der Math. und Physik (3), v. 13, (1908), p. 305-312.

[LZ] Languasco A.; Zaccagnini A. A note on Mertens' formula for arithmetic progressions. J. Number Theory, 127:37–46, (2007). MR2351662.

[M] Murty, M. R. Problems in analytic number theory. Graduate Texts in Mathematics, 206. Readings in Mathematics. Springer-Verlag, New York, (2001). p. 43-46.

[SS] Shanks, D.; Schmid, L. P. Variations on a theorem of Landau. I. Math. Comp. 20 (1966) 551–569.

[SW] Shanks, D.; Wrench, J. W. Jr. The calculation of certain Dirichlet series. Math. Comp. 17 (1963) 136–154.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

E-mail address: yotamsky@yahoo.com