Deterministic percolation*

Ilan Vardi†

Abstract

This paper examines percolation questions in a deterministic setting. In particular, I consider $\mathcal{R}$, the set of elements of $\mathbf{Z}^2$ with greatest common divisor equal to 1, where two sites are connected if they are at distance 1. The main result of the paper proves that the infinite component has an asymptotic density. An "almost everywhere" sieve of J. Friedlander is used to obtain the result.

1 Introduction

One can often gain insight about a deterministic problem by comparing it to a probabilistic model. For example, Hardy and Littlewood [30] made precise conjectures about the existence of twin primes based on the assumption that the prime numbers area generic set, i.e., have "pseudo random" properties. Similarly, in [47] the theory of percolation was used to make some precise conjectures about the existence of unbounded walks of bounded step size along Gaussian primes, a question posed by Basil Gordon, see [24] for a survey.

Percolation theory deals with the same question of unbounded walks of bounded step size on a lattice, but in a probabilistic context, see [14] [23] [26]. For example, consider the plane integer lattice $\{(m,n) : m,n \in \mathbf{Z}\}$, and a fixed $0 \le p \le 1$. Say that a lattice point (or *site*) is *open* with probability p and *closed* with probability $1-p$. If these events occur independently for each lattice point, what is the probability that there is an unbounded walk using step size k or less? The main result of percolation theory discovered by Broadbent and Hammersley in 1957 [10] is that this exhibits *phase transition*, in other words, there is a $0 < p_c < 1$ for which the probability of an unbounded walk is zero if $p < p_c$ and one if $p > p_c$ (this is called the *critical point*). For this reason, percolation theory has been of great interest in physics, as it is one of the simplest models to exhibit phase transition.

In this paper, I will examine how questions of percolation theory can be posed in a deterministic setting. Thus *deterministic percolation* is the study of unbounded walks on a single subset of a graph, e.g., defined by number theoretic conditions. This might be of interest in physics and probability theory as it studies percolation in a deterministic setting and in number theory where it can be interpreted as studying the disorder inherent in the natural numbers.

Instead of just providing a conjectural framework for percolation properties of these sets as was done in [47], I would like to show what unconditional results can be obtained so I will focus on

$$\mathcal{R} = \{(m,n) \in \mathbf{Z}^2 : \ \gcd(m,n) = 1\},$$

*Running title: "Deterministic percolation."

†ilan@ihes.fr, IHES, 35 route de Chartres, 91440 Bures–sur–Yvette, France

where two sites are connected when they are at Euclidean distance 1. This example is more tractable than Gaussian primes yet retains some similar features. Studying the connectivity properties of $\mathcal{R}$ was posed as a problem in [15, p. 109].

The analysis of $\mathcal{R}$ will use sieve methods. This seems quite natural, as sieve methods can be interpreted as an application of probabilistic methods to number theory, for example, the large sieve [6] shows that arithmetic progressions behave like independent random variables. Moreover, as Doron Zeilberger has shown [50], sieve methods like the ones used in this paper can be thought of as special cass of the Lace Expansion which has been used successfully to study percolation problems [11] [29].

The sieve method used here is due to Friedlander [20] and it proves very general "almost everywhere" results. Thus, if $U = U(y)$ is a function increasing to infinity, then the Rosser sieve [36] shows that for *every* sufficiently large y, the interval $[y, y+U]$ always contains a number whose smallest prime factor is $\geq U^{1/2-\varepsilon}$ (Corollary 5.1 below). However, Friedlander's sieve shows that for *almost every* y, the interval $[y, y+U]$ contains a number all of whose prime factors are $\geq e^{U^{1/5-\varepsilon}}$ (Proposition 5.1 below).

One can look at other examples of deterministic percolation. For example, the generalization of $\mathcal{R}$ to

$$\mathcal{R}_n = \{(a_1, \ldots, a_n) \in \mathbf{Z}^n : \ \gcd(a_1, \ldots, a_n) = 1\},$$

where two points are connected when they are at Euclidean distance 1. When $n \geq 3$, this is substantially simpler since all elements $(a_1, \ldots, a_n)$ for which $(a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n) \in \mathcal{R}_{n-1}$ lie on the infinite component. Thus the case $\mathcal{R}_2$ is harder since the reduction to $\mathcal{R}_1$ essentially corresponds to primes. Hopefully, the techniques developed here will shed some light on the original question about Gaussian primes which can also be thought of as an analogue of $\mathcal{R}_1$. Sieve techniques for Gaussian primes have been developed by Coleman [12], Fouvry and Iwaniec [19], and Friedlander and Iwaniec [22].

Finally, an interesting problem might be to study deterministic percolation for Fuchsian groups, e.g., by using the recent work of Lalley [38].

Acknowledgement. I would like to thank Cécile Dartyge for checking the method of Section 7 and Gérald Tenenbaum for helpful comments and a crucial observation (Lemma 7.4).

2 Problems of deterministic percolation

Consider a graph $\mathcal{G}$ and a subset $\mathcal{V}$ of vertices. A vertex, or *site* will be *open* if it belongs to $\mathcal{V}$ and *closed,* otherwise. Percolation studies the properties shared by "almost all" subsets of $\mathcal{G}$ which have a given density p. One should therefore compare the properties of $\mathcal{V}$ with those of a "generic" set of the same density (such questions are investigated for random graphs in [39]). In order to do this one must first answer

Problem 1. Does $\mathcal{V}$ have a probability?

Since one is trying to give analogues of percolation, one needs an analogue of a probability for a deterministic set. In this paper I will use *asymptotic density* $\delta(\mathcal{V})$ as defined in the next section. As will be seen, calculating the asymptotic density of a finite event can be nontrivial, even in the simplest cases.

Problem 2. Does $\mathcal{V}$ have an infinite connected component?

One might expect there to be an unbounded component if $\delta(\mathcal{V}) > p_c(\mathcal{G})$, where $p_c(\mathcal{G})$ is the critical percolation probability of $\mathcal{G}$, and not otherwise.

Problem 3. How many unbounded components does $\mathcal{V}$ have?

For site and bond percolation in $\mathbf{Z}^n$, it has been shown that, with probability one, there is a unique unbounded component for $p > p_c$ [1] [26]. For other models [38], with probability one, there can be zero, one, or infinitely many infinite components, depending on p.

Problem 4. Do the unbounded components of $\mathcal{V}$ have densities?

Percolation theory also predicts that unbounded components have, with probability one, a density, denoted by $\theta(p)$.

Problem 5. In general, let $f(p)$ be a function defined, with probability one, in the random model. Can the corresponding quantity be defined for $\mathcal{V}$? If so, how is it related to $f(\delta(\mathcal{V}))$?

Percolation theory considers other functions related to the cluster distribution. For example, $\chi(p)$, the average size of a connected component ($\chi^f(p)$, the average size of finite components when $p > p_c$), and $\kappa(p)$, the cluster size per vertex. In the Ising model, θ, χ (or χ^f), and κ represent magnetization, susceptibility, and free energy, respectively.

3 Percolation on $\mathcal{R}$

The subject of this section is deterministic percolation for $\mathcal{R}$. Note that $\mathcal{R}$ can be thought of as the points of $\mathbf{Z}^2$ which are *visible* from the origin. One can thus restate the percolation properties of $\mathcal{R}$ as "Lecture Hall Percolation" (compare with [9]): Consider a classroom with a regular array of tables so students sit only where they can see the teacher. The teacher starts passing out exam booklets to the closest student and each student passes on the booklets to his closest neighbors. What percentage of the class will receive an exam?

To get a feeling for the problem, consider Figures 1 through 4 which depict sites of $\mathbf{Z}^2$, where a disk or radius $1/2$ surrounds each open site, so connected sets of disks correspond to connected components.

Figure 1. Relatively prime pairs near the origin.

Figure 2. Random sites open with probability $6/\pi^2$.

Figure 3. Relatively prime pairs near $(10^{10}, 10^{10})$.

Figure 4. Relatively prime pairs near $(10^{100}, 10^{100})$.

In Figures 1, 3, and 4, sites are considered open if they belong to $\mathcal{R}$. Figure 1 gives all sites (m,n) with $-50 \le m,n \le 50$. Figure 2 represent a 100×100 square where sites are randomly open with probability $6/\pi^2$. In Figure 3, the sites were $(a,b)+(m,n)$ where $(a,b) = (8660313549, 3102586521)$ and $0 \le m,n, \le 100$. A similar computation was done in Figure 4, where a, b were randomly chosen 100 digit numbers

$$8184798876661786858004843858100520155766428318796807790541881689416654357533055575739845797590171065,$$

$$5258627195794198788220463515375759096523698556698348004291249422348890633805215110415985087652598121.$$

The reader is invited to explain the obvious differences between the random and deterministic models, e.g., show that independence is false for $\mathcal{R}$.

An interesting feature of the experimental data for $\mathcal{R}$ is that local properties do not seem to change when increasing the scale. Thus, a 100×100 snapshot appears roughly the same whether at distance from the origin 10^{10} or 10^{100}. One can explain this phenomenon as follows: Long unbroken lines corresponds to numbers with no small prime factors. Very roughly, a number with no prime factors $< k$ will produce a line with breaks at average spacing k, which is the expected spacing between numbers with no prime factors $< e^k$. For example, numbers with no prime factors $< \log^{1+\varepsilon} X$ will most likely produce unbroken lines of length $\ge \log^{1+\varepsilon} X$, but the Prime Number Theorem suggests that, on average, consecutive primes are distance $\log X$ apart, so these intervals will most likely contain a prime number. Since lines corresponding to primes lie on the infinite component, these lines will most likely belong to the infinite component. Moreover, the number of numbers with no prime factors $> \log^{1+\varepsilon} X$ is about $X/\log\log X$, so iterating this process seems to indicate that there is a scale invariance $X \mapsto e^X$. The lines segments produced by this process seem to form a regular grid and, consistent with the philosophy of de Gennes [14] [23], one observes that the infinite component is a large interconnected mesh with holes. These observations are used in the proof of Theorem 3.4 below and will be the key to the proof that the infinite component has an asymptotic density. Having gained some feeling for the empirical evidence, one now tries to address the problems of deterministic percolation.

Problem 1. Asymptotic density.

In the case of $\mathcal{R}$, the answer to Problem 1 is known: The asymptotic density of $\mathcal{R}$ is $1/\zeta(2)$, which is the well known result that the "probability" that two random integers are relatively prime is $6/\pi^2$. In order to prove this, one needs to define density

Definition. The *asymptotic density* of an *event* $P(z)$ occurring in $\mathcal{R}$ is

$$\delta(P) = \lim_{R\to\infty} \delta(P,R), \quad \text{where}\, \delta(P,R) = \frac{|\{z \in \mathcal{R} \cap B(R) :\ P(z) \text{ holds}\}|}{|B(R)|},$$

whenever this limit exists. Here $B(R) = B_\square(R) = \{z \in \mathbf{Z}^2 :\ \|z\| < R\}$, and $\|(m,n)\| = \max(|m|,|n|)$ gives a *square summation*. One can also use *circular summation,* i.e., the usual Euclidean norm $|z|$ and $B_\circ(R)$ is a disk of radius R. The subtle differences between such choices is well known, e.g., in the theory of multiple trigonometric series [2] [7] and will be discussed below.

The density of $\mathcal{R}$ is easily computed by the classical estimate [44]

$$\sum_{\substack{|m|,|n|\le R\\ \gcd(m,n)=1}} 1 = 8\sum_{d\le R}\varphi(d) = \frac{24}{\pi^2}R^2 + E(R), \quad E(R) = O(R\log R).$$

The error term cannot be improved much further as Montgomery has shown that $E(R) = \Omega_\pm(R\sqrt{\log\log R})$. However, as noted above, the situation is much different if one uses circular summation: One is then estimating

$$S(R) = \sum_{\substack{m^2+n^2\le R^2\\ \gcd(m,n)=1}} 1 = \pi R^2 + \Delta(R)\,,$$

and it is easily shown that $\Delta(R) = O(R)$ using a nontrivial bound on the error term in the Gauss circle problem (the prime number theorem also implies that the error is $o(R)$). The error term $\Delta(R)$ has been studied by Moroz [41] and by Huxley and Nowak [35]. The latter showed, using results of Baker [3] that, assuming the Riemann Hypothesis, $\Delta(R) = O(R^{3/4+\epsilon})$. It seems that the actual error is $O(R^{1/2}+\varepsilon)$ and in analogy with the Gauss circle problem [33] [5], one can ask whether $\Delta(R)/R^{1/2}$ has a limiting (logarithmic) distribution (this would require very strong assumptions as in [42])

Continuing with the analysis of $\mathcal{R}$, it is also true that any finite configuration in $\mathcal{R}$ has a density. In other words, let Ω a finite subset of $\mathbf{Z}^2$ which contains the origin and define $\delta(\Omega)$ to be the asymptotic density of Ω in the sense that $\Omega(z)$ is true if and only if $z+\Omega\subset\mathcal{R}$.

Theorem 3.1. *Let Ω be a finite subset of $\mathbf{Z}^2$, then $\delta(\Omega)$ exists.*

This result is more subtle than expected and a direct approach to compute $\delta(\Omega)$ fails (I would like to thank G. Tenenbaum for explaining this point to me). For example, let $\Omega = \{(0,0),(1,1),(2,2)\}$, then one is counting

$$S(\Omega) = \sum_{\substack{\|(m,n)\|\le R\\ \gcd(m+j,n+j)=1,\ j=0,1,2}} 1\,.$$

The direct approach uses the identity

$$\sum_{d|n}\mu(d) = \begin{cases} 1, & \text{if } n=1,\\ 0 & \text{if } n>1,\end{cases} \tag{1}$$

where $\mu(d)$ is the Möbius function and this gives rise to terms of the form

$$\sum_{d_1,d_2,d_3\le R}\mu(d_1)\mu(d_2)\mu(d_3)\left(\frac{R}{d_1d_2d_3}+O(1)\right)^2\,.$$

The term corresponding to $O(1)^3$ will be of order R^3 and no known estimates will be able to reduce this to $o(R^2)$. However, one can still hope that such a bound exists and this leads to

Conjecture 1. *If Ω is a finite set containing the origin, then*

$$\delta(\Omega) = \prod_{p \text{ prime}}\left(\frac{p^n - |\Omega \bmod p|}{p^n}\right)\,.$$

This is an analogue of the Hardy–Littlewood conjectures for prime k–tuplets [30]. The conjecture states that the global density should be a product of the local densities for each prime. A similar result was proved by Hafner, Sarnak, and McCurley [27] in which the density of relatively prime values of polynomials is computed.

Problems 2 and 3. Existence and uniqueness of the infinite component

Existence is trivial since the line $\{(m,1): m = 1,2,3,\ldots\}$ lies in $\mathcal{R}$. Comparing $\mathcal{R}$ to the random model, one sees that an unbounded component should exist since $6/\pi^2 > .5927$, the conjectured approximation to $p_c(\mathbf{Z}^2)$ [51] (the best rigorous bounds are are $.556 < p_c(2) < .679492$ of [4] and [49], respectively).

Problem 3. This has an elementary answer consistent with the probabilistic model:

Proposition 3.1. *$\mathcal{R}$ has a unique infinite component.*

Proof: Call C_1 the infinite component containing the line $\{(m,1): 1 \le m < \infty\}$. Then for each prime p, the vertical line $\{(p,n): 1 \le n \le p-1\}$ is in C_1. Thus, a large connected component in the region $\{(m,n): m > n\}$ will eventually have to cross one of these line, and therefore belong to C_1. By symmetry, the same holds true for the other 7 lines $\{\pm 1, \pm k\}$, $\{\pm k, \pm 1\}$. Finally, these lines are all joined together, either at $(\pm 1, \pm 1)$ or by passing through $(\pm 1, 0)$ and $(0, \pm 1)$, where, by definition, $\gcd(1,0) = 1$. □

Problem 4. The asymptotic density of the infinite component.

This is the main question of this paper and I prove

Theorem 3.2. *The infinite component of $\mathcal{R}$ has an asymptotic density.*

Let $\theta = \theta(\mathcal{R})$ be the asymptotic density of the infinite component, i.e., $\theta = \delta(C_\infty)$, where $C_\infty(z)$ is true if and only if z lies on the infinite component, which, by abuse of notation, will also be denoted by C_∞. The value of θ can examined experimentally and preliminary computations seem to indicate that $\theta/p(\mathcal{R}_2) \approx .96 \pm .01$, i.e., about 96% of open sites lie on the unbounded component. In fact, I will prove

Theorem 3.3. *The asymptotic density of the infinite component of $\mathcal{R}$ is not zero.*

Both these theorems are quite subtle and follow from

Theorem 3.4. *Let $f(R)$ be any function increasing to infinity then, except for a set of zero asymptotic density, every $(m,n) \in B(R)$ is surrounded by a rectangle of perimeter $< f(R)$ all of whose edges are contained in C_∞.*

As noted above, this result is consistent with de Gennes' philosophy that the infinite component consists of a mesh with small holes [14] [23]. Theorem 3.4 suggests that a stronger result is true, namely if one defines $\operatorname{rect}(m,n)$ to be the perimeter of the smallest rectangle containing (m,n) all of whose edges are in C_∞, then $\operatorname{rect}(m,n)$ should have a limiting distribution.

An examination of the proof of Theorem 3.2 (Section 8) reveals that it works with $f(R)$ in Theorem 3.4 replaced by $(\log R)^{1/2-\varepsilon}$, so Theorem 3.2 follows from the weaker result of Lemma 7.3 below. It should be noted that one can similarly show that the infinite component of $\mathcal{R}_n$ has an asymptotic density for $n \ge 3$, and it is trivially nonzero since it is $\ge 6/\pi^2$ in these cases.

One can easily give an upper bound $\theta < 6/\pi^2$. Thus, consider $\gamma(z)$ to be true if $z \equiv (4,15) \pmod{30}$, then z is isolated if $\gamma(z)$ and $z \in \mathcal{R}$ are both true. Since

$$\sum_{\substack{\|(m,n)\| \le R \\ \gamma(z),\ (m,n)=1}} = \sum_{\substack{\gcd(d,30)=1 \\ d \le R}} \mu(d) \sum_{\substack{m \equiv 4/d \pmod{30} \\ n \equiv 15/d \pmod{30} \\ \|(m,n)\| \le R/d}} 1 + O(R)$$

one gets

$$\delta(\gamma) = \frac{1}{30^2} \prod_{p>5} \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2} \prod_{p\le 5} \frac{1}{p^2-1}\,.$$

so

$$\theta \le \frac{6}{\pi^2} - 4\delta(\gamma) = \left(1 - \frac{1}{144}\right) \frac{6}{\pi^2} = .9930\bar{5}\,\frac{6}{\pi^2}\,.$$

More generally, define an *animal* α to be a connected set containing the origin and $\alpha(z)$ is true if $z+\omega \in \mathcal{R}$ for every $\omega \in \alpha$, but $z+\omega \notin \mathcal{R}$ if $\omega \in \partial\alpha$ (a site is in $\partial\alpha$ if it is connected to α but not in α). It should be noted that this definition of animal is *not* translation invariant, see [8] for general results on animals. The inclusion–exclusion principle implies that

$$\delta(\alpha) = \sum_{s\subset\partial\alpha} (-1)^n \delta(\alpha \cup s)\,,$$

where each $\delta(\alpha\cup s)$ on the right represent an ordinary density of a configuration. It follows that the density of animals exists and moreover, Lemma 8.4 below shows that

$$\theta = \frac{6}{\pi^2} - \sum_{\alpha} \delta(\alpha)\,.$$

One can therefore try to estimate θ by computing $\delta(\alpha)$ in small cases. As noted above, this is does not seem possible using current methods. However, if one accepts Conjecture 1, then one has

$$\alpha_1 = \zeta_1(2) - 4\zeta_2(2) + 8\zeta_3(2) - \zeta_4^\times(2) - \zeta_5(2) = .0110235396\ldots,,$$

$$\alpha_2 = 4\zeta_2(2) - 32\zeta_3(2) + \frac{62}{5}\zeta_4^\times(2) + 36\zeta_5(2) - \frac{16}{3}\zeta_6(2) = .0013019993\ldots,$$

where α_1 and α_2 are the densities of elements in $\mathcal{R}$ belonging to animals of size 1 and 2 respectively, and

$$\zeta_m(s) = \prod_{p \text{ prime}} \left(1 - \frac{m}{p^s}\right), \quad \zeta_m^\times(s) = \prod_{\substack{p \text{ prime}\\ p^s \ne m}} \left(1 - \frac{m}{p^s}\right).$$

Conjecture 1 therefore implies

$$\theta < 24\zeta_3(2) - \frac{57}{5}\,\zeta_4^\times(2) - 35\zeta_5(2) + \frac{16}{3}\,\zeta_6(2) \approx .9797253010901\,\frac{6}{\pi^2}\,.$$

Note that the functions $\zeta_m(s)$ do not have an analytic continuation if $m>1$ since a result of Estermann [16] states that for a polynomial $f(x)$, the Euler product $\zeta(s,f(x)) = \prod_p f(p^{-s})$ has an analytic continuation to the complex plane only if $f(x)$ is a product of cyclotomic polynomials. However, one can easily these numerically using the formula

$$\zeta(s,f(x)) = \prod_{p\le m} f(1/p^s) \prod_{\ell=1}^{\infty} \left[\zeta(\ell s) \prod_{p\le m}\left(1 - \frac{1}{p^{\ell s}}\right)\right]^{\frac{1}{\ell}\sum_{d|\ell} a_d \mu(\ell/d)},$$

where $\log f(x) = \sum_{k=1}^{\infty} a_k x^k$, see [18] [46].

Problem 5. Functions of percolation

The evaluation of θ indicates that other functions might also have deterministic analogues. One therefore defines

$$\kappa(\mathcal{R}) = \lim_{R\to\infty} \frac{\text{Number of connected components in } B(R)}{|B(R)|},$$

$$\chi^f(\mathcal{R}) = \lim_{R\to\infty} \frac{1}{|B(R)|} \sum_{\substack{\|z\|\leq R \\ z\notin C_\infty}} |C(z)|,$$

if these limits exist, where $C(z)$ represents the connected component containing z. Since the sum for $\kappa(\mathcal{R})$ has better convergence properties than $\theta(\mathcal{R})$, the methods used to prove Theorem 3.2 also show that this exists. However, the existence of $\chi^f(\mathcal{R})$ is left as an open problem.

A problem related to percolation is computing the asymptotics of the largest $\mathcal{R}$–free square. This question is a generalization the Cramer conjecture [13] which states that the largest prime gap $\leq R$ should tend to $(\log R)^2$ (though this is now believed to inaccurately model the primes [25]). One can compare results for the random and deterministic models.

Proposition 3.2. *Let $F_p(R)$ be the area of the largest closed square inside $B(R)$, where sites are open with probability p, then, with probability 1,*

$$\lim_{R\to\infty} \frac{F_p(R)}{\log R} = \frac{-2}{\log(1-p)}.$$

Proposition 3.3. *Let $F(R)$ be the area of the largest $\mathcal{R}$–free square in $B(R)$, then*

$$\frac{\log R}{(\log\log R)^2} \gg \frac{F(R)}{\log R} \gg \frac{1}{\log\log R}.$$

4 Finite configurations have a density

This section is devoted to the proof of Theorem 3.1. I will prove this by showing that the asymptotic density of a configuration is the limit of its density modulo a product of initial sets of primes. The idea is that $\mathbf{Z}^2$ is approximated by $\mathbf{Z}^2 \bmod \prod_{p\leq X} p$ and, using an idea from ordinary percolation [26], one can think of some events as being monotonic.

Definition. Two integers m, n are *relatively prime modulo h* if $\gcd(m,n,h) = 1$. Furthermore, let

$$\delta_h(\Omega, R) = \frac{|\{(m,n) \in B(R) :\ \Omega_h(m,n)\}|}{B(R)},$$

where $\Omega_h(m,n)$ means that $\Omega(m,n)$ holds as well as $(m,n,h) = 1$.

Lemma 4.1. *$\delta_h(\Omega) = \lim_{R\to\infty} \delta_h(\Omega, R)$ exists (and will be called the density of Ω modulo h).*

Proof: This follows from the fact that this relative primality is periodic modulo h and so $B(h)$ tiles the plane. $\square$

The next step is to consider a product of an initial set of primes $P(X) = \prod_{p \le X} p$ and let $h = P(X)$. Thus the pairs relatively prime modulo $P(X)$ will be an approximation to $\mathcal{R}$. The main result thus follows from

Lemma 4.2. *If $Y > X$ and $X \to \infty$, then $\delta_{P(Y)}(\Omega, P(Y)) = \delta_{P(X)}(\Omega, P(X)) + O(|\Omega|/X)$.*

Lemma 4.3 *If both $X \to \infty$ and $R/P(X) \to \infty$, then*

$$\delta(\Omega, R) = \delta_{P(X)}(\Omega, P(X)) + O(|\Omega|/X + RP(X)/|B(R)|).$$

If these results are true, then one can can take an increasing sequence of X_j's such that $\sum 1/X_j < \infty$, so that Lemma 4.2 shows that $\delta_{P(X_j)}(\Omega, P(X_j))$ approaches a limit. Lemma 4.3 then implies that this limit equals the limit of $\delta(\Omega, R)$ as $R \to \infty$. This proves Theorem 3.1.

Proof of Lemma 4.2: Let $Y > X$, then $P(X)|P(Y)$ and $B(P(X))$ exactly tiles $B(P(Y))$. Now consider $z \in B(P(Y))$ for which $\Omega_{P(Y)}(z)$ is true. Then $\Omega_{P(X)}(z \bmod P(X))$ is true except if the distance of $z \bmod B(P(X))$ from the boundary of $B(P(X))$ is less than $|\Omega|$.

Conversely, if $\Omega_{P(Y)}(z)$ is false, then $\Omega_{P(X)}(z \bmod B(P(X)))$ could be true if $d|z+\alpha$ where d is divisible only by primes $> X$. It follows that

$$\sum_{\substack{z \in B(P(Y)) \\ \Omega_{P(Y)}(z)}} 1 = \frac{|B(P(Y))|}{|B(P(X))|} \left[\sum_{\substack{z \in B(P(X)) \\ \Omega_{P(X)}(z)}} 1 + O\left(|\Omega| \sqrt{|B(P(X))|}\right) \right] + O\left(|B(P(Y))|\, |\Omega| \sum_{d > X} \frac{1}{d^2} \right).$$

Dividing this by $|B(P(Y))|$ gives the result. □

Proof of Lemma 4.3. Let $R > P(X)$, where $R/P(X)$ is large. Let $z \in B(R)$, then if $\Omega(z)$ is true, then $\Omega_{P(X)}(z \bmod P(X))$ is true unless $z \bmod P(X)$ is close to the boundary of $B(P(X))$.

Conversely, if $\Omega(z)$ is false, then $\Omega_{P(X)}(z \bmod B(P(X)))$ could be true if $d|z+\alpha$ where d is divisible only by primes $> X$. One gets a similar estimate as in the above, except that the tiling of $B(R)$ by $B(P(X))$ is no longer exact and there is an extra factor of size $O(R\,|B(P(X)))|$. Thus

$$\sum_{\substack{z \in B(R) \\ \Omega(z)}} 1 = \frac{|B(R)|}{|B(P(X))|} \left[\sum_{\substack{z \in B(P(X)) \\ \Omega_{P(X)}(z)}} 1 + O\left(|\Omega| \sqrt{|B(P(X))|}\right) \right] + O\left(|B(R)|\, |\Omega| \sum_{d > X} \frac{1}{d^2} \right) + O(R\, P(X)).$$

The result follows upon dividing by $|B(R)|$. □

5 Sieve methods

The sieve methods used here are due to Friedlander [20] who used them to show that for any fixed $E > 5$, almost every interval $[y, y + \log^E y]$ contains a number with at most 4 prime factors. The term "almost every" means that the measure of $y \le X$ for which this fails to hold is $o(X)$. Such results were first obtained by A. Selberg [43] who showed that, assuming the Riemann Hypothesis, for any function $f(n) \to \infty$, almost every interval $[y, y + f(y) \log^2 y]$ contains a prime. Heath–Brown [32] later showed that the further assumption of Montgomery's pair correlation conjectured implied the similar result with $\log y$ replacing $\log^2 y$, and this is in some sense optimal. Unconditional results were proved by various authors and the result used here is due to N. Watt [48] and shows that almost every interval of length $y^{1/14+\varepsilon}$ contains a prime, An unconditional result of Heath–Brown and Iwaniec [34] states that every interval of length $y^{11/20}$ contains a prime (this has subsequently been improved, see [48]).

In [21], Friedlander improved his methods and showed that almost every interval $[y, y+f(y)\log y]$ contains a number with at most 21 prime factors. This is a much more accurate result, as the optimal interval length is $f(y)\log y/(\log\log y)^{21}$.

There are other techniques to prove such results and Harman [31] has shown that almost every interval $[y, y+\log^7 y]$ contained a number with *exactly* two prime factors. Unlike Friedlander's papers, this does not seem to yield techniques that are directly applicable to the problems of this paper.

I will closely follow Friedlander's paper which starts with a modified form of Rosser's sieve [36] (see also [28, Chapter 8]). As usual [28] consider an interval $\mathcal{A}$ and let $S(\mathcal{A}, Z)$ be the set of element of $\mathcal{A}$ which are not divisible by any prime $p < Z$. In this case $\mathcal{A}$ will be the interval $[y, y+U]$.

Theorem 5.1. (Friedlander) *Let $2 \le Z \le D$. There exists a function $f(u)$ which is positive for $u > 2$, and a sequence λ_d of real numbers, this sequence depending on D and Z, and satisfying $|\lambda_d| \le 1$, such that*

$$S(\mathcal{A}, Z) > \frac{U}{\log Z}\left\{f\left(\frac{\log D}{\log Z}\right) + O(\log^{-1/3} D)\right\} - |R_y(D)|\,, \tag{2}$$

where

$$R_y(D) = \sum_{d<D} \lambda_d r_y(d)\,, \qquad r_y(d) = \psi\left(\frac{y}{d}\right) - \psi\left(\frac{y+U}{d}\right), \qquad \psi(t) = t - \lfloor t \rfloor - \frac{1}{2}\,.$$

The following is the best "everywhere" result available using the Rosser sieve.

Corollary 5.1. *For any $\varepsilon > 0$, there exists a constants E such that for all sufficiently large k and X, every interval $[y, y+U]$ contains at least $EU/\log U$ numbers all of whose prime divisors are greater than $U^{1/2-\varepsilon}$,*

This result follows by letting $U = D^{1+\delta} = Z^{2+3\delta}$ in Theorem 5.1, where $\delta > 0$ and the trivial bound $|R_y(D)| \le 2D$ is used. Theorem 5.1 formulates the error term $R_y(D)$ in analytic form which allows one to average the error as y varies over an interval $[X/2, X]$.

Theorem 5.2. (Friedlander) *Let $4 \le D^2 \le V/2 \le X/(2\log D)$, where $V = y/U$, then*

$$\frac{1}{X}\int_{X/2}^{X} |R_y(D)|dy \ll U^{1/2}(\log D)^{3/2} + (\log D)^2\,. \tag{3}$$

Remark. One can can improve this result slightly by using Friedlander's second paper [21]. This would result in replacing the $U^{1/2}(\log D)^{3/2}$ term in (3) with $U\,(\log Z)^{-1/2}$, under the conditions $D^2\,(\log D)^7 \le V \le X$ and $Z^{11} \le D$. The exponent in Proposition 5.1 below would be improved from 1/5 to 1/3 (the true exponent seems to be 1).

The proof of Theorem 5.2 follows exactly as in the paper of Friedlander [20] except that the $\log D$ term is everywhere substituted for $\log X$, written as $\mathcal{L}$ in [20]. An examination of Friedlander's proof reveals that this substitution is valid at each step of his argument. Friedlander used this result to prove

Theorem 5.3 (Friedlander) *For any $A > 5$, there is a constant c such that almost every interval $[y, y + (\log y)^A]$ contains at least $c\,(\log y)^{A-1}$ numbers x such that $P_-(x) > x^{1/4-\varepsilon}$, where $P_-(x)$ is the smallest prime factor of x (so x has at most 4 prime factors).*

This result will be generalized to arbitrary interval lengths of small size.

Proposition 5.1. *Let $g(R)$ be an unbounded increasing function such that $g(R) < (\log R)^5$. Given any fixed $\varepsilon > 0$, then for all $y < R$, except for a set of measure $O(R\,[g(R)]^{-\varepsilon/2})$, the interval $[y, y+g(R)]$, contains an x with $P_-(x) > \exp([g(R)]^{1/5-\varepsilon})$.*

Proof: One takes a large T and has to show that almost all $y \le T$ have an $x \in [y, y + g(R)]$ with $P_-(x) > \exp([g(R)]^{1/5-\varepsilon})$. Using the above notation, one writes $U = g(R)$ and in order to get the result of Proposition 5.1, one must choose $Z = e^{U^{1/5-\varepsilon}}$. Also, in order to have $f((\log D)/(\log Z)) > 0$, one takes $D = Z^{2+\varepsilon}$.

Since $U \to \infty$, assume that $y > T/U$ and divide the interval $[T/U, T]$ into disjoint subintervals of the form $(X, 2X]$. Taking $V = X/U$ and applying Theorem 5.1 gives a lower bound

$$S(\mathcal{A}, Z) > U^{4/5+\varepsilon}\left\{f(2+\varepsilon') + O((\log D)^{-1/3})\right\} - |R_y(D)|\,,$$

so the main term has order $U^{4/5+\varepsilon}$. Now consider $G \subset (X, 2X]$ given as the set of y's for which $|R_y(D)| > U^{4/5-\varepsilon}$. It follows that

$$\int_X^{2X} |R_y(D)|dy > |G|\,U^{4/5-\varepsilon}\,.$$

Since $U < (\log X)^5$, one has $Z < e^{(\log X)^{1-\varepsilon}}$ and so

$$D^2 \le e^{3(\log X)^{1-\varepsilon}} \le \frac{X}{2(\log X)^5} \le \frac{X}{2U} = \frac{V}{2}\,,$$

for all sufficiently large X. Also, since $D = \exp((2+\varepsilon)U^{1/5-\varepsilon})$, one has $U = C_1(\log X)^{5+\varepsilon'}D$ for some constants C_1, ε', so

$$\frac{V}{2} = \frac{X}{2U} \le C_1\frac{X}{(\log D)^5} \le \frac{X}{2\log D}$$

for all sufficiently large X. The conditions of Theorem 5.2 are therefore satisfied, and applying it gives

$$\int_X^{2X} |R_y(D)|dy \ll X(U^{1/2}(\log D)^{3/2} + (\log D)^2) \ll X\,U^{4/5-3/2\varepsilon}$$

It follows that

$$|G| \ll X\,U^{-\varepsilon/2} = o(R)\,,$$

i.e., the proportion of exceptional y's goes to zero. Thus almost all $y \in (X/2, X]$ have $|R_y(D)| < U^{4/5-\varepsilon}$ and this is dominated by the main term $U^{4/5+\varepsilon}$ of (3), so $S(\mathcal{A}, Z)$ is nonzero for almost all such y. Taking the union of the intervals gives the result. □

6 $\mathcal{R}$–free squares

Before embarking on the rather daunting task of proving Theorem 3.4, I will do a "warmup" consisting of proving Propositions 3.2 and 3.3.

Proof of Proposition 3.2: (a) $\limsup F_p(R)/\log R \le -2/\log(1-p)$: Let $c > -2/\log(1-p)$, and at each site (m,n) in $B(R)$, consider a square of area $c\log\|(m,n)\|$ and with lower left hand corner at (m,n). The probability that all sites in the square are closed is $(1-p)^{c\log\|(m,n)\|} < \|(m,n)\|^{-2-\varepsilon}$, where $\varepsilon > 0$. Summing over all sites in $\mathbf{Z}^2$ gives

$$\sum_{\substack{(m,n)\in\mathbf{Z}^2\\ \|(m,n)\|>2}} \frac{1}{\|(m,n)\|^{2+\varepsilon}},$$

which converges. The Borel-Cantelli Lemma [17] shows that the probability of infinitely many such squares being closed is zero.

(b) $\liminf F_p(R)/\log R \ge -2/\log(1-p)$: Let $c < -2/\log(1-p)$ and for each site (m,n) with $\|(m,n)\| > 2$, consider a square of area $c\log\|(m,n)\|$ with bottom left hand corner at $\lfloor (m,n)\,(\log\|(m,n)\|)^2 \rfloor$. As in part (a), it follows that each square has a probability $\gg \|(m,n)\|^{-2-\varepsilon}$ of being closed. Moreover, all these events are independent so the result follows from the Borel Cantelli Lemma and the divergence of

$$\sum_{\substack{(m,n)\in\mathbf{Z}^2\\ \|(m,n)\|>2}} \frac{(\log\|(m,n)\|)^2}{\|(m,n)\|^{2+\varepsilon}}\,. \ \square$$

Proof of Proposition 3.3: (a) Lower bound: Consider an integer k, and the first k^2 primes $q_1,\ldots,q_{k^2}$. By the Chinese Remainder Theorem, the following congruences have solutions $m,n \le \prod_{i=1}^{k^2} q_i$,

$$m \equiv -i \left(\bmod \prod_{j=1}^{k} q_{ik+j}\right), \qquad n \equiv -j \left(\bmod \prod_{j=1}^{k} q_{jk+i}\right),$$

so $\gcd(m+i, n+j) > 0$, for $1 \le i,j \le k$. The prime number theorem gives $k^{2(1+\varepsilon')k^2} > \|(m,n)\| > k^{2(1-\varepsilon)k}$, which yields the estimate $k^2 > (1-\varepsilon'')\,\frac{1}{2}\,\log R/\log\log R$ (one can improve the $1/2$ term to $\pi^2/12$).

(b) Upper bound: Assume that there is an $\mathcal{R}$–free square $\{(m+i, n+j) :\ 1 \le i,j \le k\}$. By Corollary 5.1, there are $x_1,\ldots,x_\ell \in [m+1, m+k]$ for which $P_-(x_i) > k^{1/2-\varepsilon}$, and such that $\ell \gg k/\log k$. Write $x_i = \prod_{j=1}^{r_i} q_{ij}^{e_{ij}}$. One notes that if q is a prime, then the number of integers in a set $\mathcal{S}$ which are relatively prime to q is $\ge \min\{|\mathcal{S}|(1-1/q), |\mathcal{S}|-1\}$. The asymptotic relation

$$\sum_{\substack{k^{1/2-\varepsilon}<q\le k\\ q \text{ prime}}} \frac{1}{q} \sim -\log(1/2-\varepsilon) < 1\,.$$

thus implies that the number of integers in $[m+1, m+k]$ relatively prime to x_i, is $\gg (1+\log(1/2-\varepsilon))\,k - |\{j \le r_i :\ q_{ij} \ge k\}|$, and so each $r_i > (1+\log(1/2-2\varepsilon))\,k$. One further notes that $\gcd(x_i, x_j) \le k$ for $i \ne j$, so that x_i and x_j can share at most 2 distinct prime factors. This implies that the number of distinct q_{ij}'s is $\gg k^2/\log k$. The prime number theorem gives

$$\prod_{i=1}^{\ell} x_i \gg \prod_{\substack{y<q\le D\,k^2\\ q \text{ prime}}} q = e^{D\,k^2 - k^{1/2-\varepsilon} + o(1)},$$

for some constant D, and so $\log x_i \gg k\log k$ for all i. This therefore gives $\log R \gg k\log k$ and the result follows since $\log k$ is of order $\log\log R$. $\square$

7 The structure of the infinite component

In this section, I prove Theorem 3.4. One begins identifying some subsets of the infinite component.

Lemma 7.1. *The following sets are in C_∞*

(1) $\{(m,1):\ m>0\}$. (2) $\{(p,n):\ p>n\}$, p prime. (3) $\{(m,q):\ q<m<(q/2)^{20/11},\ q\not| m\}$, q prime.

Proof: The first two results were proved above. The third follows from the unconditional result of Heath–Brown and Iwaniec [34] which states that every interval of length $y^{11/20}$ contains a prime (this has subsequently been improved, see [48]). Thus, if $q \not| m$, then since $q > 2\,m^{11/20}$, one of the intervals $[m+m^{11/20}]$ or $[m-m^{11/20},m]$ has none of its elements divisible by q and the corresponding line segment lies completely in $\mathcal{R}$. By the result of Heath–Brown and Iwaniec, this line segment will cross a line $\{(p,n)\}$, where p is prime, and by (2), this is in C_∞, so (m,q) is also in C_∞. □

One proceeds by proving an initial version of Theorem 3.4.

Lemma 7.2. *All but $O(R^2/\log R)$ pairs of $B(R)$ are surrounded by a rectangle of perimeter $O((\log R)^7)$ all of whose edges are contained in C_∞.*

Proof: Consider the set

$$S_0=\{(m,n)\in B(R):\ \exists n',\ P_-(n')>R^{1/5},\ (\log R)^7+n>n'>n,\ \text{minimal},$$
$$(d,n')=1 \text{ if } |d-m|<R^{1/13},\ \exists p\in[m-R^{1/13},m+R^{1/13}]\}\,.$$

By Watt's result that almost every interval of length $y^{1/14+\varepsilon}$ contains a prime,

$$E_{0,1}=\{(m,n)\in B(R):\ [m-R^{1/13},m+R^{1/13}] \text{ has no primes}\}$$

has density zero. In fact, his result shows that $|E_{0,1}|\ll R^2/(\log R)^2$, since substituting $E=3$ in Theorem 1 of [48] already gives this estimate for intervals of length $R^{1/14}(\log R)^{22}$.

Next, if

$$E_{0,2}=\{(m,n)\in B(R):\ P_-(n')\le R^{1/5},\ \text{for all } (\log R)^7+n>n'>n\}\,,$$

then $|E_{1,2}|\ll R^2/\log R$. This bound follows by an argument similar to the proof of Proposition 5.1: Partition $[R^{1/2},R]$ into intervals of the form $[X,2X]$ and in each of these intervals, let $U=(\log X)^7$, $D=V^{1/2}/2$, and for a fixed $1/10>\varepsilon>0$, let $Z=D^{1/2-\varepsilon}$. The main term in equation (2) of Theorem 5.1 is then $\gg(\log X)^6$ while Theorem 5.2 gives

$$\frac{1}{X}\int_X^{2X}|R_y(D)|dy\ll(\log X)^5\,.$$

Therefore G defined as the set of $y\in(X,2X]$ for which $|R_y(D)|\gg(\log X)^6$ satisfies $|G|\ll X/\log X$.

Finally, one considers

$$E_{0,3}=\{(m,n)\in B(R):\ P_-(n')>R^{1/5},\ (\log R)^7+n>n'>n \text{ minimal } \exists d\ |d-m|<R^{1/13},\ (d,n')>1\}.$$

But if $P_-(n')>R^{1/5}$, then

$$|E_{0,3}|\ll R(\log R)^7\sum_{\substack{P_-(n')>R^{1/5}\\ |d-m|<R^{1/13}\,,\ (d,n')>1}}1\ll R^{1+1/13}(\log R)^7R\sum_{p|n'}\frac{R}{p}\ll R^{2+1/13-1/5}\,(\log R)^7\ll\frac{R^2}{\log R}\,.$$

Since $B(R) - S_0 \subset E_{0,1} \cup E_{0,2} \cup E_{0,3}$, it follows that $|B(R) - S_0| \ll R^2/\log R$, and so S_0 represents almost all points of $B(R)$.

An examination of the definition of S_0 shows that for every $(m,n) \in S_0$ there is an unbroken horizontal line segment $L_{0,1}(m,n) \subset C_\infty$ of length $R^{1/13}$, centered at (m,n) and which passes above (m,n) within distance $O((\log R)^7)$, and which crosses a vertical line $\{(p,n)\}$, where p is prime. By Lemma 7.1 (2), this vertical line is in C_∞, so it follows that $L_{0,1}(m,n)$ is also in C_∞.

Replacing the condition $n' > n$ with $n' < n$ yields the similar result with a line segment $L_{0,2}(m,n)$, passing below (m,n). To construct the corresponding vertical line segments $L_{0,3}(m,n)$, $L_{0,4}(m,n)$, one must include the condition that $m,n \gg R^{11/20}$ in order to apply part 3 of Lemma 7.1. The result then follows. □

The next iteration already contains most of the ideas of the general procedure and is included in order to give a self–contained proof of Theorem 3.3.

Lemma 7.3. *All but $O(R^2/(\log\log R)^3)$ pairs of $B(R)$ are surrounded by a rectangle of perimeter $O((\log\log R)^{36})$ all of whose edges are contained in C_∞.*

Proof: Consider the set

$$S_1 = \{(m,n) \in B(R) : \exists m' \;\; P_-(m') > (\log R)^{42},\; (\log\log R)^{36} + m > m' > m \text{ minimal},$$
$$(m',d) = 1,\; |d-n| < (\log R)^{40}\}\,.$$

Now let

$$E_{1,1} = \{(m,n) \in B(R) :\; P_-(m') < (\log R)^{42},\; \text{for all } (\log\log R)^{36} + m > m' > m\}\,.$$

By Proposition 5.1, for almost all y, $[y, y+(\log\log R)^{36}]$ contains an integer x with $P_-(x) > \exp((\log\log R)^{36(1/5-\varepsilon)})$, and this is $> (\log R)^{42}$ for all sufficiently large R. The error term of Proposition 5.1 gives

$$|E_{1,1}| \ll \frac{R^2}{(\log\log R)^{36\varepsilon/2}} = \frac{R^2}{(\log\log R)^3}\,,$$

by letting $\varepsilon = 1/6$. Next, one considers

$$E_{1,2} = \{(m,n) \in B(R) : P_-(m') > (\log R)^{42},\; (\log\log R)^{36} + m > m' > m \text{ minimal}\,,$$
$$\exists d \;\; |d-n| < (\log R)^{40},\; (m',d) > 1\}.$$

As before, one gets

$$|E_{1,2}| \ll R(\log\log R)^{36} \sum_{\substack{P_-(m') > (\log R)^{42} \\ |d-n| < (\log R)^{40},\; (m',d)>1}} 1$$
$$\ll R\,(\log\log R)^{36} (\log R)^{40} \sum_{p|m'} \frac{R}{p} \ll \frac{R^2\,(\log\log R)^{37}}{(\log R)^2}$$
$$\ll \frac{R^2}{\log R}\,,$$

for all sufficiently large R. This last estimate used the fact that if $P_-(m') > (\log R)^{42}$ and $m' < R$, then m' can have at most $O(\log R/\log\log R)$ prime factors.

It follows that S_1 consists of almost all elements of $B(R)$. The definition of S_1 then shows that for almost all $(m,n) \in B(R)$, there is a line segment $L_{1,1}(m,n) \subset \mathcal{R}$ of length at least $(\log R)^{40}$, centered at (m,n) and which passes by (m,n) at distance $O((\log\log R)^{36})$.

One now observes that $S_0 \cap S_1$ also comprises almost all elements of $B(R)$. The definition of S_0 implies that for almost all (m,n), the line segment $L_{1,1}(m,n)$ intersects a rectangle of perimeter $O((\log R)^7)$ whose edges lie in C_∞ (note that these extend in C_∞ to length $R^{1/13}$), so $L_{1,1}(m,n)$ will also be contained in C_∞. Clearly, one can similarly show that for almost all (m,n), there are line segments $L_{1,j} \subset \mathcal{R}$, $j = 2,3,4$, of length $(\log R)^{40}$ and which pass within $(\log\log R)^{36}$ of (m,n) on all four sides, and by the same argument $L_{1,j} \subset C_\infty$, $j = 2,3,4$. □

An examination of the proof of Lemma 7.3 reveals that the obstacle in continuing this process is the term $\sum_{p|m'} 1/p$, which must be $o(1)$. The trivial estimate

$$\sum_{p|m} \frac{1}{p} \ll \frac{\omega(m)}{P_-(m)} \tag{4}$$

was used and this will only allow one more iteration, if one first removes all m for which $\omega(n) > 2\log\log R$ (as is well known, this set has zero density [44]). In fact, in this context, it is easy to improve substantially on (4), as was noted to me by G. Tenenbaum.

Lemma 7.4. *Let $f(R)$ be any function increasing to infinity, then except for a set of m of size $O(R/\sqrt{f(R)\log f(R)})$, one has the bound*

$$\sum_{\substack{p|m \\ p \geq f(R)}} \frac{1}{p} \ll \frac{1}{\sqrt{f(R)\log f(R)}}\,.$$

Proof: One uses the simple estimate

$$\sum_{m \leq R} \sum_{\substack{p|m \\ p \geq f(R)}} \frac{1}{p} = \sum_{p \geq f(R)} \frac{R}{p^2} = \frac{R}{f(R)\log f(R)}\,.$$

This result reflects the fact that $\sum_{p|m} 1/p$ has a limiting density, as follows easily from the Erdős–Wintner Theorem [44]. □

This result allows one to iterate the above argument. Recall that $\mathrm{rect}\,(m,n)$ is the perimeter of the smallest rectangle surrounding (m,n) which has all its edges in C_∞.

Lemma 7.5. *Let $\log_1 z = \log z$ and $\log_{k+1} z = \log(\log_k z)$, and let $\exp_k z$ be the inverse of $\log_k z$, then for $R > \exp_{k+2}(10^{15})$,*

$$|(m,n) \in B(R) : \ \mathrm{rect}\,(m,n) \leq (\log_{k+1} R)^{36}\}| = |B(R)| \left[1 - O\left(\frac{1}{(\log_{k+1} R)^3}\right)\right]\,, \tag{5}$$

where the $O(\ )$ term is independent of k.

Proof: One proves this by induction on k. The initial step $k = 1$ is exactly Lemma 7.3. Now assume that (5) holds for k, then I will show that it holds for $k+1$.

Thus assume that one has constructed for almost all (m,n), line segments $L_{k,j}(m,n)$, $j=1,2,3,4$, as above, but of length $(\log_k R)^{40}$, which pass within $(\log_{k+1} R)^{36}$, are centered at (m,n) and lie completely in C_∞. In particular, one assumes that the set

$$S_k = \{(m,n) \in B(R) : \exists n' \;\; P_-(n') > (\log_k R)^{100},\; (\log_{k+1} R)^{36} + n > n' > n \text{ minimal},$$
$$(d,n')=1,\; |d-m| < (\log_k R)^{40},\; (m,n') \in C_\infty\}\,,$$

is such that $|B(R)-S_k| \ll R^2/(\log_{k+1} R)^3$. One then considers

$$S_{k+1} = \{(m,n) \in B(R) : \exists m' \;\; P_-(m') > (\log_{k+1} R)^{100},\; (\log_{k+2} R)^{36} + m > m' > m \text{ minimal},$$
$$(m',d)=1,\; |d-n| < (\log_{k+1} R)^{40}\}\,.$$

Now let

$$E_{k+1,1} = \{(m,n) \in B(R) : \; P_-(m') < (\log_{k+1} R)^{100}, \text{ for all } (\log_{k+2} R)^{36} + m > m' > m\}\,.$$

By Proposition 5.1, for any $\varepsilon > 0$, except for $O(R/(\log_{k+2} R)^{36\varepsilon/2})$ values of y, the interval $[y, y+(\log_{k+2} R)^{36}]$ contains an integer x with $P_-(x) > \exp((\log_{k+2} R)^{36(1/5-\varepsilon)})$. Letting $\varepsilon = 1/6$, this says that except for $O(R/(\log_{k+2} R)^3)$ values of y, the interval $[y, y+(\log_{k+2} R)^{36}]$ contains an integer x with $P_-(x) > \exp((\log_{k+2} R)^{1+2/15})$. This last quantity is eventually $> (\log_{k+1} R)^{100}$, in particular, when $\log_{k+2} R > 100^{15/2}$, i.e., when $R > \exp_{k+2}(10^{15})$. Thus, one concludes that

$$|E_{k+1,1}| \ll \frac{R^2}{(\log_{k+2} R)^3}, \qquad \text{for } \; R > \exp_{k+2}(10^{15})\,.$$

Next, one considers

$$E_{k+1,2} = \{(m,n) \in B(R) : P_-(m') > (\log_{k+1} R)^{100},\; (\log_{k+2} R)^{36} + m > m' > m \text{ minimal}\,,$$
$$\exists d\,,\; |d-n| < (\log_{k+1} R)^{40},\; (m',d) > 1\}.$$

As before, one gets

$$\begin{aligned} |E_{k+1,2}| &\ll R(\log_{k+2} R)^{36} \sum_{\substack{P_-(m') > (\log_{k+1} R)^{100} \\ |d-n| < (\log_{k+1} R)^{40}\,,\; (m',d)>1}} 1 \\ &\ll R\,(\log_{k+2} R)^{36} (\log_{k+1} R)^{40} \sum_{\substack{m \le R \\ P_-(m) > (\log_{k+1} R)^{100}}} \sum_{p|m} \frac{1}{p}\,. \end{aligned}$$

Now let

$$E_{k+1,3} = \{(m,n) \in B(R) : \sum_{\substack{p|m' \\ p > (\log_{k+1} R)^{100}}} \frac{1}{p} \ge \frac{1}{(\log_{k+1} R)^{50} \sqrt{\log_{k+2} R}}$$
$$\text{for all } (\log_{k+2} R)^{36} + m > m' > m\}\,.$$

Applying Lemma 7.4 gives

$$|E_{k+1,3}| \ll \frac{R^2\,(\log_{k+2} R)^{36}}{(\log_{k+1} R)^{50}\,\sqrt{\log_{k+2} R}}\,,$$

so

$$|E_{k+1,2} - E_{k+1,3}| \ll \frac{R^2 (\log_{k+2} R)^{36} (\log_{k+1} R)^{40}}{(\log_{k+1} R)^{50} \sqrt{\log_{k+1} R}} \ll \frac{R^2}{\log_{k+1} R},$$

whenever $(\log_{k+1} R)^9 > (\log_{k+2} R)^{36}$, for example, when $R > \exp_{k+2}(16)$. It follows that S_{k+1} consists of almost all elements of $B(R)$, where the exceptional set is $\ll R^2/(\log_{k+2} R)^3$.

The definition of S_{k+1} also shows that for almost all $(m,n) \in B(R)$, there is a line segment $L_{k+1,1}(m,n) \subset \mathcal{R}$ of length at least $(\log_{k+1} R)^{40}$, centered at (m,n) and which passes by (m,n) at distance $O((\log_{k+2} R)^{36})$.

One now observes that $S_k \cap S_{k+1}$ also comprises almost all elements of $B(R)$ except for an exceptional set of size

$$\ll \frac{R^2}{(\log_{k+1} R)^3} + \frac{R^2}{(\log_{k+2} R)^3} = (1 + A_k)\, \frac{R^2}{(\log_{k+1} R)^3},$$

for sufficiently large R, where

$$\prod_{j=1}^{k} (1 + A_j) \ll \prod_{j=1}^{k} \left[1 + O\left(\frac{1}{(\log_j R)^3} \right) \right] = O(1).$$

The definition of S_{k+1} implies that for almost all (m,n), the line segment $L_{k+1,1}(m,n)$ of length $(\log_{k+1} R)^{40}$ will intersect the perimeter of the rectangle of perimeter $(\log_{k+1} R)^{36}$ constructed in the previous iteration (note that its sides extend to line segments in C_∞ of length $(\log_k R)^{40}$). Since the sides of this rectangle lie in C_∞, it follows that $L_{k+1,1}(m,n)$ will also be contained in C_∞. Thus, the line segments defined in S_{k+1} also lie in C_∞.

Clearly, one can similarly show that for almost all (m,n), there are lines segments $L_{k+1,j} \subset \mathcal{R}$, $j = 2,3,4$, of length $(\log_{k+1} R)^{40}$ and which pass within $(\log_{k+2} R)^{36}$ of (m,n) on all four sides, and $L_{k+1,j} \subset C_\infty$, $j = 2,3,4$. □

Proof of Theorem 3.4: Assume that there is a function $f(R)$ increasing to infinity, and a fixed $\lambda > 0$ such that for at least λR_i^2 pairs (m,n) one has $\operatorname{rect}(m,n) > f(R_i)$, where R_i is a sequence increasing to infinity.

One defines $\log_* z$ to be the minimum number of iterations of log required to be ≤ 2, i.e., $\log_{\log_* z} z \le 2$. Let $k = \log_* R - \log_* f(R) - 2$, then $\log_k R \ll \log f(R)$ for all sufficiently large R.

One can now apply Lemma 7.5 since the bound

$$\exp_{k+2}(10^{15}) = \exp_{\log_* R - \log_f(R) + 4}(10^{15}) \ll \log R = o(R)$$

holds. Furthermore, one has

$$\frac{1}{(\log_{k+1} R)^3} \ll \frac{1}{\log_4 f(R)} \to 0,$$

since $\log_k R \gg \log_3 f(R)$ and $f(R) \to \infty$. Substituting this in (5) shows that for almost all $(m,n) \in B(R)$ one has $\operatorname{rect}(m,n) \le f(R)$, which contradicts the above assumption. The result follows. □

Proof of Theorem 3.3: Assuming Theorem 3.2, then this follows directly from Theorem 3.4. For if the result were not true, then there would be a function $f(R)$ increasing to infinity such that $\theta(R) < 1/f(R)$ for all sufficiently large R. However, Theorem 3.4 implies that for sufficiently large R, almost all points of $B(R)$ are surrounded by a rectangle of perimeter $\sqrt{f(R)}$ all of whose edges lie in C_∞. This implies that $\theta(R) \gg 1/\sqrt{f(R)}$ which is a contradiction. □

8 The infinite component has a density

As in Section 4, the idea is to compare the density of the infinite component in a big square

$$\theta(R) = \frac{|B(R) \cap C_\infty|}{|B(R)|}$$

with this density modulo a product of primes. Thus, let

$$\theta_h = \lim_{R\to\infty} \frac{|\{(m,n) \in B(R) : \ (m,n) \in \text{ infinite component modulo } h\}|}{|B(R)|} .$$

The following gives a local characterization of the infinite component modulo h.

Lemma 8.1. *z is in the infinite component modulo h if and only if $z \bmod h$ is connected modulo h to all sides of $B(h)$.*

Proof: In fact, this holds for the fundamental domain $B^*(h) = \{0 \le m, n < h\}$ of $\mathbf{Z}^2 \bmod h$ (so $B(h)$ consists of 4 copies of $B^*(h)$). To see this, note that $B^*(h)$ has reflection symmetries generated by $(m,n) \mapsto (n,m)$ and $(m,n) \mapsto (m,-n) \bmod h$ which preserve relatively prime pairs mod h. Thus $B^*(h)$ consists of 8 triangles each of which is a reflection of its adjacent neighbor, see Figure 5. It is clear that z is on the infinite component if and only if it is h–connected to all three sides of the triangle on which it lies and this is clearly equivalent to being h–connected to all four sides of $B^*(h)$. □

Figure 5. Reflection symmetries modulo h

Lemma 8.2. *If $X < Y$ then $\theta_{P(X)} \ge \theta_{P(Y)}$.*

Proof: If $z \in B(P(Y))$ is in the infinite component modulo $P(Y)$ then $z \bmod P(Y)$ is $P(Y)$ connected to three boundaries of $B(P(Y))$. Since reducing modulo $P(X)$ does not remove any connections, it follows that $z \bmod P(X)$ is $P(X)$ connected to the boundary of $B(P(X))$. □

One concludes that $\theta_{P(X)}$ is decreasing and therefore the limit $\theta_* = \lim_{X\to\infty} \theta_{P(X)}$ exists.

Lemma 8.3. *If both $X \to \infty$ and $R/P(X) \to \infty$, then $\theta(R) \le \theta_{P(X)} + o(1)$.*

Proof: This follows exactly as in the above also following the proof of Lemma 4.3. Note that the boundary error in tiling $B(R)$ with $B(P(X))$ is $O(P(X)/R) = o(1)$ by assumption □

One therefore has $\theta(R) \le \theta_* + o(1)$ and the main result follows from

Lemma 8.4. $\lim_{R\to\infty} \theta(R) = \theta_*$.

Proof: If $\theta_* = 0$, then Lemma 8.3 shows that $\theta = 0$ as well and there is nothing to prove. On the other hand, if $\theta_* > 0$ consider a large R and by Lemma 8.2, find a large X such that $\theta_{P(X)}$ is very close to θ_*, with $P(X) < R$ and $R/P(X)$ large. Since the prime number theorem says that $P(X) = e^{X+o(1)}$, one can choose X such that $R^{1/2}/4 < P(X) < R^{1/2}$. It follows that X is of order $\log R$, i.e., there are two constants A, B, such that $A \log R < X < B \log R$.

Now going from $\mathcal{R}$ modulo $P(X)$ to $\mathcal{R}$ in $B(R)$ removes at most $|B(R)| \sum_{d>X} 1/d^2 \ll |B(R)|/X$ elements. So, by the above estimate, one is removing $O(R^2/\log R)$ sites. By Lemma 7.3, given $0 < \varepsilon < 1/2$, one can surround almost all sites with a C_∞ rectangle of perimeter $< (\log R)^{1/2-\varepsilon}$. Thus apart from a set of zero density, each individual removal can disconnect at most $(\log R)^{1-2\varepsilon}$ sites from the connected component (note that none of the elements on the rectangles specified by Lemma 7.3 are removed, since these belong to C_∞ of $\mathcal{R}$). It follows that at most $O(R^2(\log R)^{1-2\varepsilon}/\log R)$ sites are disconnected, a vanishingly small percentage of the infinite connected component modulo $P(X)$. This implies that $\theta(R)$ is asymptotically close to $\theta_{P(X)}$. $\square$

References

[1] Aizenman, M., Kesten, H., Newman, C.M.: Uniqueness of the infinite cluster and continuity of connectivity functions for short and long range percolation, Comm. Math. Phys. **111**, 505–531 (1987).

[2] Ash, J.M., Wang, G. A survey of uniqueness questions in multiple trigonometric series. In: Harper, L.H. (editor) Harmonic Analysis and nonlinear differential equations. pp. 35–71. American Math. Soc. Contemp. Math. **208** (1997).

[3] Baker, R.C.: The square–free divisor problem, Quart. J. Math. Oxford **45**, 269–277 (1994).

[4] van den Berg, J., Ermakov, A.: A new lower bound for the critical probability of site percolation on the square lattice, Random Structures and Algorithms **8**, (1996), 199–212.

[5] Bleher, P.M., Cheng, Z., Dyson, F.J., Lebowitz, J.L.: Distribution of the error term for the number of lattice points inside a shifted circle, Comm. Math. Phys. **54**, 433–469 (1993).

[6] Bombieri, E.: Le grand crible dans la théorie analytique des nombres, 2nd edition, Astérisque **18**, 1987.

[7] Bourgain, J.: Spherical summation and uniqueness of multiple trigonometric series, Int. Math. Research Notices **3**, 93–107 (1996).

[8] Bousquet-Mélou, M.: Percolation models and animals, European J. Combin. **17**, 343–369 (1996).

[9] Bousquet-Mélou, M., Eriksson, K.: Lecture hall partitions, Ramanujan J. **1**, 101–111 (1997).

[10] Broadbent, S.R., Hammersley, J.M.: Percolation processes, Proc. Cambridge Phil. Soc. **53**, 629–641 (1957).

[11] Brydges, D.C., Spencer, T.: Self–avoiding walk in 5 or more dimensions, Comm. Math. Phys. **97**, 125–148 (1985).

[12] Coleman, M.D.: The Rosser–Iwaniec sieve in number fields, with an application, Acta Arithmetica **66**, 53–83 (1993).

[13] Cramér, H.: On the order of magnitude of the difference between consecutive prime numbers, Acta Arithmetica **2**, 23–46 (1937).

[14] Efros, A.L.: Physics and Geometry of Disorder, Percolation Theory. Moscow: Mir 1986.

[15] Erdős, P., Gruber, P.M., Hammer, J.: Lattice Points, Longman, Wiley, New York 1989.

[16] Estermann, T.: On certain functions represented by Dirichlet series, Proc. London Math. Soc. **27**, 435–448 (1928).

[17] Feller, W.: An Introduction to Probability Theory and its Applications, Vol. I, Wiley, New York 1964.

[18] Flajolet, P., Vardi, I.: Zeta expansions of classical constants, preprint (1996).

[19] Fouvry, E., Iwaniec, H.: Gaussian primes, Acta Arithmetica **79**, 249–287 (1997).

[20] Friedlander, J.B.: Sifting short intervals, Math. Proc. Camb. Phil. Soc. **91**, 9–15 (1982).

[21] Friedlander, J.B.: Sifting short intervals II, Math. Proc. Camb. Phil. Soc. **92**, 381–384 (1982).

[22] Friedlander, J.B., Iwaniec, H.: Using a parity–sensitive sieve to count prime values of a polynomial, Proc. Nat. Acad. Sci. U.S.A. **94**, 1054–1058 (1997).

[23] de Gennes, P.G.: La percolation: un concept unificateur, La Recherche **7**, 919–927 (1976).

[24] Gethner, E., Wagon, S., Wick, B.: A stroll through the Gaussian primes, American Math. Monthly **105**, 327–337 (1998).

[25] Granville, A.: Unexpected irregularities in the distribution of prime numbers. Proceedings of the International Congress of Mathematicians, (Zurich, 1994), 388–399, Basel: Birkhäuser 1995.

[26] Grimmett, G.: Percolation, New York: Springer–Verlag 1989.

[27] Hafner, J.L., Sarnak, P., McCurley, K. Relatively prime values of polynomials. In: Knopp, M., Sheingorn, M. (eds) A tribute to Emil Grosswald: Number theory and related analysis, pp. 437–443, Contemp. Math. **143**, Amer. Math. Soc., Providence, RI, 1993.

[28] Halberstam, H.,Richert, H.–E.: Sieve Methods, Academic Press, New York, 1974.

[29] Hara, T., Slade, G.: Mean–field critical behavior for percolation in high dimensions, Comm. Math. Phys. **128**, 339–391 (1990).

[30] 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**, 1–70, also in G.H. Hardy, *Coll. Papers*, vol. 1, 561–630 (1922).

[31] Harman, G.: Almost primes in short intervals, Math. Ann. **258**, 107–112 (1981).

[32] Heath–Brown, D.R.: Gaps between primes and the pair correlation of zeros of the zeta–function, Acta Arithmetica **41**, 85–99 (1982).

[33] Heath–Brown, D.R.: The distribution and moments of the error term in the Dirichlet divisor problems, Acta Arithmetica **60**, 389–415 (1992).

[34] Heath–Brown, D.R., Iwaniec, H.: On the difference between consecutive primes, Invent. Math. **55**, 49–69 (1979).

[35] Huxley, M.N., Nowak, W.G.: Primitive lattice points in convex planar domains, Acta Arithmetica **76**, 271–283 (1996).

[36] Iwaniec, H.: Rosser's sieve, Acta Arithmetica **36**, 171–202 (1980).

[37] Iwaniec, I., Mozzochi, C.J.: On the divisor and circle problems, J. Number Theory **29**, 60–93 (1988).

[38] Lalley, S.: Percolation on Fuchsian groups, Ann. Inst. H. Poincaré Probab. Statist. **34**, 151–177 (1998).

[39] Lubotzky, A., Phillips, R., Sarnak, P.: Ramanujan graphs, Combinatorica **8**, 261–277 (1988).

[40] Montgomery, H.L.: Fluctuations in the mean of Euler's phi function, Proc. Indian Acad. Sci. Math. Sci. **97**, 239–245 (1987).

[41] Moroz, B.Z.: On the number of primitive lattice points in plane domains, Monatschrift Math. **99**, 37–43 (1985).

[42] Sarnak, P., Rubinstein, M.: Chebyshev's bias, Experimental Math. **3**, 173–197 (1994).

[43] Selberg, A.: On the normal density of primes in short intervals, and the difference between consecutive primes, Arch. Math. Naturvid. **47**, 87–105 (1943).

[44] Tenenbaum, G.: Introduction to analytic and probabilistic number theory, Cambridge University Press, Cambridge, 1995.

[45] Turán, P.: On a theorem of Hardy and Ramanujan, J. London Math. Soc. **9**, 274–276 (1934).

[46] Vardi, I.: Computational Recreations in Mathematica, Addison–Wesley, Reading, MA, 1991.

[47] Vardi, I.: Prime Percolation, Experimental Mathematics **7**, 275–289 (1998).

[48] Watt, N.: Short intervals almost all containing primes, Acta Arithmetica **72**, 131–167 (1995).

[49] Wierman, J.C.: Substitution method critical probability bounds for the square lattice site percolation model, Combin. Probab. Comput. **4**, 181–188, (1995).

[50] Zeilberger, D.: The Abstract Lace Expansion, Adv. Appl. Math. **19**, 355–359 (1997).

[51] Ziff, R.M., Sapoval, B.: The efficient determination of the percolation threshold by a frontier–generating walk in a gradient, J. Phys A: Math. Gen. **19**, L1169–L1172 (1986).