Running time predictions for factoring algorithms

Ernie Croot[1]
School of Mathematics
Georgia Tech
Atlanta, GA 30332-0160
ecroot@math.gatech.edu

Andrew Granville[2]
Départment de mathématiques et de statistique
Université de Montréal
Montréal QC H3C 3J7, Canada
andrew@dms.umontreal.ca

Robin Pemantle[3]
Department of Mathematics
University of Pennsylvania
209 S. 33rd Street
Philadelphia, Pennsylvania 19104, USA
pemantle@math.upenn.edu

Prasad Tetali
School of Mathematics and College of Computing
Georgia Tech
Atlanta, GA 30332-0160
tetali@math.gatech.edu

[1]Supported in part by an NSF grant.
[2]Partiellement soutenu par une bourse de la Conseil de recherches en sciences naturelles et en génie du Canada.
[3]Supported in part by NSF Grant DMS-01-03635.

Abstract

In 1994, Carl Pomerance proposed the following problem:
Select integers $a_1, a_2, \dots, a_J$ at random from the interval $[1, x]$, stopping when some (non-empty) subsequence, $\{a_i : i \in I\}$ where $I \subseteq \{1, 2, \dots, J\}$, has a square product (that is $\prod_{i \in I} a_i \in \mathbb{Z}^2$). *What can we say about the possible stopping times, J?*

A 1985 algorithm of Schroeppel can be used to show that this process stops after selecting $(1+\epsilon)J_0(x)$ integers a_j with probability $1-o(1)$ (where the function $J_0(x)$ is given explicitly in (1) below). Schroeppel's algorithm actually finds the square product, and this has subsequently been adopted, with relatively minor modifications, by all factorers. In 1994 Pomerance showed that, with probability $1-o(1)$, the process will run through at least $J_0(x)^{1-o(1)}$ integers a_j, and asked for a more precise estimate of the stopping time. We conjecture that there is a "sharp threshold" for this stopping time, that is, with probability $1-o(1)$ one will first obtain a square product when (precisely) $\{e^{-\gamma}+o(1)\}J_0(x)$ integers have been selected. Herein we will give a heuristic to justify our belief in this sharp transition.

In our paper [4] we prove that, with probability $1-o(1)$, the first square product appears in time

$$[(\pi/4)(e^{-\gamma}-o(1))J_0(x),\ (e^{-\gamma}+o(1))J_0(x)],$$

where $\gamma = 0.577...$ is the Euler-Mascheroni constant, improving both Schroeppel and Pomerance's results. In this article we will prove a weak version of this theorem (though still improving on the results of both Schroeppel and Pomerance). We also confirm the well established belief that, typically, none of the integers in the square product have large prime factors.

Our methods provide an appropriate combinatorial framework for studying the large prime variations associated with the quadratic sieve and other factoring algorithms. This allows us to analyze what factorers have discovered in practice.

1 Introduction

Most factoring algorithms (including Dixon's random squares algorithm [5], the quadratic sieve [14], the multiple polynomial quadratic sieve [19], and the number field sieve [2] – see [18] for a nice expository article on factoring algorithms) work by generating a pseudorandom sequence of integers $a_1, a_2, ...$, with each

$$a_i \equiv b_i^2 \pmod{n},$$

for some known integer b_i (where n is the number to be factored), until some subsequence of the a_i's has product equal to a square, say

$$Y^2 = a_{i_1} \cdots a_{i_k},$$

and set

$$X^2 = (b_{i_1} \cdots b_{i_k})^2.$$

Then

$$n \mid Y^2 - X^2 = (Y - X)(Y + X),$$

and there is a good chance that $\gcd(n, Y - X)$ is a non-trivial factor of n. If so, we have factored n.

In his lecture at the 1994 International Congress of Mathematicians, Pomerance [16, 17] observed that in the (heuristic) analysis of such factoring algorithms one assumes that the pseudo-random sequence $a_1, a_2, ...$ is close enough to random that we can make predictions based on this assumption. Hence it makes sense to formulate this question in its own right.

Pomerance's Problem. Select positive integers $a_1, a_2, \ldots \le x$ independently at random (that is, $a_j = m$ with probability $1/x$ for each integer m, $1 \le m \le x$), stopping when some subsequence of the a_i's has product equal to a square (a *square product*). What is the expected stopping time of this process ?

There are several feasible positive practical consequences of resolving this question:

— It may be that the expected stopping time is far less than what is obtained by the algorithms currently used. Hence such an answer might point the way to speeding up factoring algorithms.

— Even if this part of the process can not be easily sped up, a good understanding of this stopping time might help us better determine the optimal choice of parameters for most factoring algorithms.

Let $\pi(y)$ denote the number of primes up to y. Call n a *y-smooth integer* if all of its prime factors are $\le y$, and let $\Psi(x, y)$ denote the number of y-smooth integers up to x. Let $y_0 = y_0(x)$ be a value of y which maximizes $\Psi(x, y)/y$, and

$$J_0(x) := \frac{\pi(y_0)}{\Psi(x, y_0)} \cdot x. \tag{1}$$

In Pomerance's problem, let T be the smallest integer t for which $a_1, ..., a_t$ has a square dependence (note that T is itself a random variable). As we will see in section 4.1, Schroeppel's 1985 algorithm can be formalized to prove that for any $\epsilon > 0$ we have

$$\text{Prob}(T \ < \ (1+\epsilon)J_0(x)) \ = \ 1 - o_\epsilon(1)$$

as $x \to \infty$. In 1994 Pomerance showed that

$$\text{Prob}(T \ > \ J_0(x)^{1-\epsilon}) \ = \ 1 - o_\epsilon(1).$$

as $x \to \infty$. Therefore there is a transition from "unlikely to have a square product" to "almost certain to have a square product" at $T = J_0(x)^{1+o(1)}$. Pomerance asked in [3] whether there is a sharper transition, and we conjecture that T has a *sharp threshold*:

Conjecture 1.1 *For every $\epsilon > 0$ we have*

$$\text{Prob}(T \in [(e^{-\gamma} - \epsilon)J_0(x), \ (e^{-\gamma} + \epsilon)J_0(x)]) \ = \ 1 - o_\epsilon(1), \tag{2}$$

as $x \to \infty$, where $\gamma = 0.577...$ is the Euler-Mascheroni constant.

The bulk of this article will be devoted to explaining how we arrived at this conjecture. In [4] we prove the upper bound in this conjecture using deep probabilistic methods in an associated random graph. Here we discuss a quite different approach which justifies the upper bound in this conjecture, but we have not been able to make all steps of the proof rigorous.

The constant $e^{-\gamma}$ in this conjecture is well-known to number theorists. It appears as the ratio of the proportion of integers free of prime divisors smaller than y, to the proportion of integers up to y that are prime, but this is not how it appears in our discusssion. Indeed herein it emerges from some complicated combinatorial identities, which have little to do with number theory, and we have failed to find a more direct route to this prediction.

Herein we will prove something a little weaker than the above conjecture (though stronger than the previously known results) using methods from combinatorics, analytic and probabilistic number theory:

Theorem 1.2 *We have*

$$\text{Prob}(T \ \in \ [(\pi/4)(e^{-\gamma} - o(1))J_0(x), \ (3/4)J_0(x)]) \ = \ 1 - o(1),$$

as $x \to \infty$.

To obtain the lower bound in our theorem, we obtain a good upper bound on the expected number of sub-products of the large prime factors of the a_i's that equal a square, which allows us to bound the probability that such a sub-product exists, for $T < (\pi/4)(e^{-\gamma} - o(1))J_0(x)$. This is the "first moment method". Moreover the proof gives us some idea of what the set I looks like: In the unlikely event that $T < (\pi/4)(e^{-\gamma} - o(1))J_0(x)$, with probability $1 - o(1)$, the set I consists of a single number a_T, which is

therefore a square. If T lies in the interval given in Theorem 1.2 (which happens with probability $1 - o(1)$), then the square product I is composed of $y_0^{1+o(1)} = J_0(x)^{1/2+o(1)}$ numbers a_i (which will be made more precise in [4]).

Schroeppel upper bound, $T \leq (1 + o(1))J_0(x)$ follows by showing that one expects to have more than $\pi(y_0)$ y_0-smooth integers amongst $a_1, a_2, \ldots, a_T$, which guarantees a square product. To see this, create a matrix over $\mathbb{F}_2$ whose columns are indexed by the primes up to y_0, and whose (i, p)th entry is given by the exponent on p in the factorization of a_i, for each y_0-smooth a_i. Then a square product is equivalent to a linear dependence over $\mathbb{F}_2$ amongst the corresponding rows of our matrix: we are guaranteed such a linear dependence once the matrix has more than $\pi(y_0)$ rows. Of course it might be that we obtain a linear dependence when there are far fewer rows; however, in section 3.1, we give a crude model for this process which suggests that we should not expect there to be a linear dependence until we have very close to $\pi(y_0)$ rows

Schroeppel's approach is not only good for theoretical analysis, in practice one searches among the a_i for y_0-smooth integers and hunts amongst these for a square product, using linear algebra in $\mathbb{F}_2$ on the primes' exponents. Computing specialists have also found that it is easy and profitable to keep track of a_i of the form $s_i q_i$, where s_i is y_0-smooth and q_i is a prime exceeding y_0; if both a_i and a_j have exactly the same large prime factor $q_i = q_j$ then their product is a y_0-smooth integer times a square, and so can be used in our matrix as an extra smooth number. This is called the *large prime variation*, and the upper bound in Theorem 1.2 is obtained in section 4 by computing the limit of this method. (The best possible constant is actually a tiny bit smaller than 3/4.)

One can also consider the *double large prime variation* in which one allows two largish prime factors so that, for example, the product of three a_is of the form pqs_1, prs_2, qrs_3 can be used as an extra smooth number. Experience has shown that each of these variations has allowed a small speed up of various factoring algorithms (though at the cost of some non-trivial extra programming), and a long open question has been to formulate all of the possibilities for multi-large prime variations and to analyze how they affect the running time. Sorting out this combinatorial mess is the most difficult part of our paper. To our surprise we found that it can be described in terms of the theory of Huisimi cacti graphs (see section 6). In attempting to count the number of such smooth numbers (including those created as products of smooths times a few large primes) we run into a subtle convergence issue. We believe that we have a power series which yields the number of smooth numbers, created independently from $a_1, \ldots, a_J$, simply as a function of J/J_0; if it is correct then we obtain the upper bound in our conjecture.

In the graphs constructed here (which lead to the Husimi graphs), the vertices correspond to the a_j's, and the edges to common prime factors which are $> y_0$. In the random hypergraphs considered in [4] the vertices correspond to the prime factors which are $> y_0$ and the hyperedges, which are presented as subsets of the set of vertices, correspond to the prime factors of each a_j, which divide a_j to an odd power.

In [4] we were able to understand the speed up in running time using the k-large prime variation for each $k \geq 1$. We discuss the details of the main results of this work, along with some numerics, in section 8. We also compare, there, these theoretical findings, with the speed-ups obtained using large prime variations by the researchers

who actually factor numbers. Their findings and our predictions differ significantly and we discuss what might contribute to this.

When our process terminates (at time T) we have some subset I of $a_1, ..., a_T$, including a_T, whose product equals a square.[4] If Schroeppel's argument comes close to reflecting the right answer then one would guess that that a_i's in the square product are typically "smooth". In section 3.2 we prove that they will all be J_0^2-smooth with probability $1 - o(1)$, which we improve to

$$y_0^2 \exp((2+\epsilon)\sqrt{\log y_0 \log\log y_0}) \ - \ \text{smooth.}$$

in [4], Theorem 2. We guess that this may be improvable to $y_0^{1+\epsilon}$-smooth for any fixed $\epsilon > 0$.

Pomerance's main goal in enunciating the random squares problem was to provide a model that would prove useful in analyzing the running time of factoring algorithms, such as the quadratic sieve. In section 7 we will analyze the running time of Pomerance's random squares problem showing that the running time will be inevitably dominated by finding the actual square product once we have enough integers. Hence to optimize the running time of the quadratic sieve we look for a square dependence among the y-smooth integers with y significantly smaller than y_0, so that Pomerance's problem is not quite so germane to factoring questions as it had at first appeared.

This article uses methods from several different areas not usually associated with factoring questions: the first and second moment methods from probabilistic combinatorics, Husimi graphs from statistical physics, Lagrange inversion from algebraic combinatorics, as well as comparative estimates on smooth numbers using precise information on saddle points.

2 Smooth numbers

In this technical section we state some sharp results comparing the number of smooth numbers up to two different points (which are proved in [4]). The key idea, which we took from [10], is that such ratios are easily determined because one can compare very precisely associated saddle points – this seems to be the first time this idea has been used in the context of analyzing factoring algorithms.

2.1 Classical smooth number estimates

From [10] we have that the estimate

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\} \quad \text{as} \quad x \to \infty \quad \text{where} \quad x = y^u, \tag{3}$$

holds in the range

$$\exp\left((\log\log x)^2\right) \ \le \ y \ \le \ x, \tag{4}$$

[4]Note that I is unique, else if we have two such subsets I and J then $(I \cup J) \setminus (I \cap J)$ is also a set whose product equals a square, but does not contain a_T, and so the process would have stopped earlier than at time T.

where $\rho(u) = 1$ for $0 \le u \le 1$, and where

$$\rho(u) = \frac{1}{u}\int_{u-1}^{u} \rho(t)\,dt \quad \text{for all } u > 1.$$

This function $\rho(u)$ satisfies

$$\rho(u) \;=\; \left(\frac{e+o(1)}{u\log u}\right)^u \;=\; \exp(-(u+o(u))\log u); \tag{5}$$

and so

$$\Psi(x,y) \;=\; x\exp(-(u+o(u))\log u). \tag{6}$$

Now let

$$L := L(x) = \exp\left(\sqrt{\frac{1}{2}\log x \log\log x}\right).$$

Then, using (6) we deduce that for $\beta > 0$,

$$\Psi(x, L(x)^{\beta+o(1)}) \;=\; xL(x)^{-1/\beta+o(1)}. \tag{7}$$

From this one can easily deduce that

$$y_0(x) = L(x)^{1+o(1)}, \text{ and } J_0(x) = y_0^{2-\{1+o(1)\}/\log\log y_0} = L(x)^{2+o(1)}, \tag{8}$$

where y_0 and J_0 are as in the introduction (see (1)). From these last two equations we deduce that if $y = y_0^{\beta+o(1)}$, where $\beta > 0$, then

$$\frac{\Psi(x,y)/y}{\Psi(x,y_0)/y_0} \;=\; y_0^{2-\beta-\beta^{-1}+o(1)}.$$

For any $\alpha > 0$, one has

$$\Psi(x,y) \le \sum_{\substack{n\le x\\ P(n)\le y}} (x/n)^\alpha \le x^\alpha \prod_{p\le y}\Big(1-\frac{1}{p^\alpha}\Big)^{-1}, \tag{9}$$

which is minimized by selecting $\alpha = \alpha(x,y)$ to be the solution to

$$\log x = \sum_{p\le y}\frac{\log p}{p^\alpha - 1}. \tag{10}$$

We show in [4] that for $y \;=\; L(x)^{\beta+o(1)} \;=\; y_0^{\beta+o(1)}$ we have

$$y^{1-\alpha} \;\sim\; \beta^{-2}\log y \;\sim\; \beta^{-1}\log y_0. \tag{11}$$

Moreover, by [10, Theorem 3], we have

$$\Psi\left(\frac{x}{d},y\right) = \frac{1}{d^{\alpha(x,y)}}\Psi(x,y)\left\{1+O\left(\frac{1}{u}+\frac{\log y}{y}\right)\right\}, \text{ when } 1 \;\le\; d \;\le\; y \;\le\; \frac{x}{d}. \tag{12}$$

By iterating this result we can deduce (see [4]) the following:

Proposition 2.1 *Throughout the range (4), for any $1 \le d \le x$, we have*

$$\Psi\left(\frac{x}{d}, y\right) \le \frac{1}{d^{\alpha(x,y)}}\Psi(x,y)\{1+o(1)\},$$

where α is the solution to (10).

Now Lemma 2.4 of [4] gives the following more accurate value for y_0:

$$\log y_0 = \log L(x)\left(1 + \frac{\log_3 x - \log 2}{2\log_2 x} + O\left(\left(\frac{\log_3 x}{\log_2 x}\right)^2\right)\right). \tag{13}$$

It is usual in factoring algorithms to optimize by taking $\psi(x,y)$ to be roughly x/y:

Lemma 2.2 *If $\psi(x,y) = x/y^{1+o(1/\log\log y)}$ then*

$$\log y = \log y_0\left(1 - \frac{1+o(1)}{\log_2 x}\right).$$

Proof. By (3) and (5) we have

$$u(\log u + \log\log u - 1 + o(1)) = \log y\left(1 + o\left(\frac{1}{\log\log y}\right)\right),$$

and from here it is a simple exercise to show that

$$u = \frac{\log y}{\log\log y}\left(1 + \frac{1+o(1)}{\log\log y}\right).$$

Substituting $u = (\log x)/(\log y)$ and solving we obtain

$$\log y = \log L(x)\left(1 + \frac{\log_3 x - \log 2 - 2 + o(1)}{2\log_2 x}\right),$$

from which our result follows using (13). □

3 Some simple observations

3.1 A heuristic analysis

Let $M = \pi(y)$ and

$$p_1 \;=\; 2 \;<\; p_2 \;=\; 3 \;<\; \ldots \;<\; p_M$$

be the primes up to y. Any y-smooth integer

$$p_1^{e_1} p_2^{e_2} \ldots p_M^{e_M}$$

gives rise to the element $(e_1, e_2, \ldots e_M)$ of the vector space $\mathbb{F}_2^M$. The probability that any given element of $\mathbb{F}_2^M$ arises from Pomerance's problem (corresponding to a y-smooth

value of a_i) varies depending on the entries in that element. Pomerance's problem can be rephrased as: Let $y = x$. Select elements $v_1, v_2, \dots$ of $\mathbb{F}_2^M$, each with some specific probability (as above), and stop at v_T as soon as $v_1, v_2, \dots, v_T$ are linearly dependent. The difficulty in this version is in quantifying the probabilities that each different $v \in \mathbb{F}_2^M$ occurs, and then manipulating those probabilities in a proof since they are so basis dependent.

As a first model we will work with an approximation to this question that avoids these difficulties: Now our problem will be to determine the distribution of T when each element of $\mathbb{F}_2^M$ is selected with probability $1/2^M$. We hope that this model will help us gain some insight into Pomerance's question.

If $v_1, v_2, .., v_{\ell-1}$ are linearly independent they generate a subspace S_ℓ of dimension $\ell - 1$, which contains $2^{\ell-1}$ elements (if $1 \le \ell \le M+1$). Then the probability that $v_1, v_2, .., v_\ell$ are linearly dependent is the same as the probability that v_ℓ belongs to S_ℓ, which is $2^{\ell-1}/2^M$. Thus the expectation of T is

$$\begin{aligned}\sum_{\ell=1}^{M+1} \ell \, \frac{2^{\ell-1}}{2^M} \prod_{i=1}^{\ell-1} \left(1 - \frac{2^{i-1}}{2^M}\right) \;&\to\; \prod_{i\ge 1}\left(1-\frac{1}{2^i}\right)\left(\sum_{j=0}^{M} \frac{(M+1-j)}{2^j} \prod_{i=1}^{j}\left(1-\frac{1}{2^i}\right)^{-1}\right) \\ &= M - .60669515\ldots \quad \text{as } M \to \infty.\end{aligned}$$

(By convention, empty products have value 1.) Therefore $|T - M|$ has expected value $O(1)$. Furthermore,

$$\text{Prob}(|T - M| > n) \;=\; \sum_{\ell \ge n+1} \text{Prob}(T = M - \ell) \;<\; \sum_{\ell \ge n+1} 2^{-\ell-1} \;=\; 2^{-n-1},$$

for each $n \ge 1$, so that if $\phi(t) \to \infty$ as $t \to \infty$ then

$$\text{Prob}(T \in [M - \phi(M),\ M]) \;=\; 1 \;-\; o(1).$$

Hence this simplified problem has a very sharp transition function, suggesting that this might be so in Pomerance's problem.

3.2 No large primes, I

Suppose that we have selected integers $a_1, a_2, ..., a_T$ at random from $[1, x]$, stopping at T since there is a non-empty subset of these integers whose product is a square. Let q be the largest prime that divides this square. Then either q^2 divides one of $a_1, a_2, ..., a_T$, or q divides at least two of them. The probability that p^2 divides at least one of $a_1, a_2, ..., a_T$, for a given prime p, is $\le T/p^2$; and the probability that p divides at least two of $a_1, a_2, ..., a_T$ is $\le \binom{T}{2}/p^2$. Thus

$$\text{Prob}(q > T^2) \;\ll\; T^2 \sum_{p > T^2} \frac{1}{p^2} \;\ll\; \frac{1}{\log T},$$

by the Prime Number Theorem.

By Pomerance's result we know that $T \to \infty$ with probability $1 + o(1)$; and so the largest prime that divides the square product is $\le T^2$ with probability $1 - o(1)$. We will improve this result later by more involved arguments.

4 Proof of the upper bound on T in Theorem 1.2

Our goal in this section is to prove that

$$\text{Prob}(T \ < \ (3/4)J_0(x)) \ = \ 1 - o(1),$$

as $x \to \infty$.

We use the following notation throughout. Given a sequence

$$a_1, \ \dots, \ a_J \ \leq \ x$$

of randomly chosen positive integers, let

$$p_1 \ = \ 2 \ < \ p_2 \ = \ 3 \ < \ \dots \ < \ p_{\pi(x)}$$

denote the primes up to x, and construct the J-by-$\pi(x)$ matrix A, which we take mod 2, where

$$a_i \ = \ \prod_{1 \leq j \leq \pi(x)} p_j^{A_{i,j}}.$$

Then, a given subsequence of the a_i has square product if the corresponding row vectors of A sum to the 0 vector modulo 2; and, this happens if and only if $\text{rank}(A) < J$. Here, and henceforth, the rank is always the $\mathbb{F}_2$-rank.

4.1 Schroeppel's argument

Schroeppel's idea was to focus only on those rows corresponding to y_0-smooth integers so that they have no 1's beyond the $\pi(y_0)$th column. If we let $S(y_0)$ denote the set of all such rows, then Schroeppel's approach amounts to showing that

$$|S(y_0)| \ > \ \pi(y_0)$$

holds with probability $1 - o(1)$ for $J = (1+\epsilon)J_0$, where J_0 and y_0 are as defined in (1). If this inequality holds, then the $|S(y_0)|$ rows are linearly dependent mod 2, and therefore some subset of them sums to the 0 vector mod 2.

Although Pomerance [15] gave a complete proof that Schroeppel's idea works, it does not seem to be flexible enough to be easily modified when we alter Schroeppel's argument, so we will give our own proof, seemingly more complicated but actually requiring less depth: Define the independent random variables $Y_1, Y_2, \dots$ so that $Y_j = 1$ if a_j is y-smooth, and $Y_j = 0$ otherwise, where y will be chosen later. Let

$$N = Y_1 + \cdots + Y_J,$$

which is the number of y-smooth integers amongst $a_1, ..., a_J$. The probability that any such integer is y-smooth, that is that $Y_j = 1$, is $\Psi(x, y)/x$; and so,

$$\mathbb{E}(N) \ = \ \frac{J\psi(x, y)}{x}.$$

Since the Y_i are independent, we also have

$$V(N) \;=\; \sum_i (\mathbb{E}(Y_i^2) - \mathbb{E}(Y_i)^2) \;=\; \sum_i (\mathbb{E}(Y_i) - \mathbb{E}(Y_i)^2) \;\le\; \frac{J\psi(x,y)}{x}.$$

Thus, selecting $J = (1+\epsilon)x\pi(y)/\Psi(x,y)$, we have, with probability $1 + o_\epsilon(1)$, that

$$N \;=\; (1+\epsilon+o(1))\pi(y) \;>\; \pi(y).$$

Therefore, there must be some non-empty subset of the a_i's whose product is a square. Taking $y = y_0$ we deduce that

$$\text{Prob}(T \;<\; (1+\epsilon)J_0(x)) \;=\; 1 - o_\epsilon(1).$$

Remark. One might alter Schroeppel's construction to focus on those rows having only entries that are $0 \pmod 2$ beyond the $\pi(y_0)$th column. These rows all correspond to integers that are a y_0-smooth integer times a square. The number of additional such rows equals

$$\sum_{\substack{d>1\\ p(d)>y_0}} \Psi\left(\frac{x}{d^2}, y_0\right) \le \sum_{y_0<d\le y_0^2} \Psi\left(\frac{x}{d^2}, y_0\right) + \sum_{d>y_0^2} \frac{x}{d^2} \ll \frac{\Psi(x,y_0)}{y_0^{1+o(1)}}$$

by Proposition 2.1, the prime number theorem, (11) and (7), respectively, which one readily sees are too few to significantly affect the above analysis. Here and henceforth, $p(n)$ denotes the smallest prime factor of n, and later on we will use $P(n)$ to denote the largest prime factor of n.

4.2 The single large prime variation

If, for some prime $p > y$, we have $ps_1, ps_2, \ldots, ps_r$ amongst the a_i, where each s_j is y-smooth, then this provides us with precisely $r-1$ multiplicatively independent pseudo-smooths, $(ps_1)(ps_2), (ps_1)(ps_3), \ldots, (ps_1)(ps_r)$. We will count these using the combinatorial identity

$$r - 1 = \sum_{\substack{I\subset\{1,\ldots,r\}\\ |I|\ge 2}} (-1)^{|I|},$$

which fits well with our argument. Hence the expected number of smooths and pseudo-smooths amongst $a_1, \ldots, a_J$ equals

$$\frac{J\Psi(x,y)}{x} + \sum_{\substack{I\subset\{1,\ldots,J\}\\ |I|\ge 2}} (-1)^{|I|} \text{ Prob}(a_i = ps_i \;\forall i \in I,\; P(s_i) \le y < p,\; p \text{ prime})$$

$$= \frac{J\Psi(x,y)}{x} + \sum_{k\ge 2} \binom{J}{k} (-1)^k \sum_{p>y} \left(\frac{\Psi(x/p,y)}{x}\right)^k. \tag{14}$$

Using (12) we have, by the prime number theorem, that

$$\sum_{p>y}\left(\frac{\Psi(x/p,y)}{\Psi(x,y)}\right)^k \sim \sum_{p>y}\frac{1}{p^{\alpha k}} \sim \frac{y^{1-\alpha k}}{(\alpha k-1)\log y} \sim \frac{1}{(k-1)\pi(y)^{k-1}}$$

using (11) for $y \asymp y_0$. Hence the above becomes, letting $J = \eta x\pi(y)/\Psi(x,y)$,

$$\sim \left(\eta + \sum_{k\geq 2}\frac{(-\eta)^k}{k!(k-1)}\right)\pi(y). \tag{15}$$

(One needs to be a little careful here since the accumulated error terms might get large as $k \to \infty$. To avoid this problem we can replace the identity (14) by the usual inclusion-exclusion inequalities; that is the partial sum up to k even is an upper bound, and the partial sum up to k odd is a lower bound. Since these converge as $k \to \infty$, independently of x, we recover (15).) One can compute that the constant in (15) equals 1 for $\eta = .74997591747934498263\ldots$; or one might observe that this expression is $> 1.00003\pi(y)$ when $\eta = 3/4$.

4.3 From expectation to probability

Proposition 4.1 *The number of smooth and pseudosmooth integers amongst $a_1, a_2, \ldots, a_J$ with $J = \eta J_0$ is given by (15), with probability $1 - o(1)$, as $x \to \infty$.*

Hence, with probability $1 - o(1)$, we have that the number of linear dependencies arising from the single large prime variation is (15) for $J = \eta J_0(x)$ with $y = y_0$ as $x \to \infty$. This is $> (1+\epsilon)\pi(y_0)$ for $J = (3/4)J_0(x)$ with probability $1 - o(1)$, as $x \to \infty$, implying the upper bound on T in Theorem 1.2.

Proof of Proposition 4.1. Suppose that $a_1, ..., a_J \leq x$ have been chosen randomly. For each integer $r \geq 2$ and subset S of $\{1, ..., J\}$ we define a random variable $X_r(S)$ as follows: Let $X_r(S) = 1$ if each $a_s, s \in S$ equals p times a y-smooth for the same prime $p > y$, and let $X_r(S) = 0$ otherwise. Therefore if

$$Y_r \;=\; \sum_{\substack{S\subset\{1,\ldots,J\}\\ |S|=r}} X_r(S),$$

then we have seen that

$$\mathbb{E}(Y_r) \;\sim \frac{\eta^r}{r!(r-1)}\pi(y).$$

Hence each

$$\mathbb{E}(X_r(S)) \;\sim\; \binom{J}{r}^{-1}\frac{\eta^r}{r!(r-1)}\pi(y),$$

for every $S \subset \{1, ..., J\}$, since each of the $X_r(S)$ have the same probability distribution.

Now, if S_1 and S_2 are disjoint, then $X_r(S_1)$ and $X_r(S_2)$ are independent, so that

$$\mathbb{E}(X_r(S_1)X_r(S_2)) \;=\; \mathbb{E}(X_r(S_1))\mathbb{E}(X_r(S_2)).$$

If S_1 and S_2 are not disjoint and both $X_r(S_1)$ and $X_r(S_2)$ equal 1, then $X_R(S) = 1$ where $S = S_1 \cup S_2$ and $R = |S|$. We just saw that

$$\mathbb{E}(X_R(S)) \ \sim \ \binom{J}{R}^{-1} \frac{\eta^R}{R!(R-1)}\pi(y).$$

Hence if $|S_1 \cap S_2| = j$ then

$$\mathbb{E}(X_r(S_1)X_r(S_2)) \ \sim \ \binom{J}{2r-j}^{-1} \frac{\eta^{2r-j}}{(2r-j)!(2r-j-1)}\pi(y).$$

Therefore

$$\begin{aligned}
\mathbb{E}(Y_r^2) - \mathbb{E}(Y_r)^2 &= \sum_{\substack{S_1,S_2\subset\{1,\dots,J\}\\ |S_1|=|S_2|=r}} \mathbb{E}(X_r(S_1)X_r(S_2)) - \mathbb{E}(X_r(S_1))\mathbb{E}(X_r(S_2)) \\
&\lesssim \ \pi(y)\sum_{j=1}^{r}\binom{J}{2r-j}^{-1}\frac{\eta^{2r-j}}{(2r-j)!(2r-j-1)} \sum_{\substack{S_1,S_2\subset\{1,\dots,J\}\\ |S_1|=|S_2|=r\\ |S_1\cap S_2|=j}} 1 \\
&= \ \pi(y)\sum_{j=1}^{r}\frac{\eta^{2r-j}}{(2r-j-1)j!(r-j)!^2} \le (1+\eta^{2r-1})\pi(y).
\end{aligned}$$

Hence by Tchebychev's inequality we deduce that

$$\text{Prob}(|Y_r - \mathbb{E}(Y_r)| > \epsilon\mathbb{E}(Y_r)) \ \ll_r \ \frac{\mathbb{E}(Y_r^2) - \mathbb{E}(Y_r)^2}{\epsilon^2\mathbb{E}(Y_r)^2} \ \ll_r \ \frac{1}{\epsilon^2\pi(y)},$$

so that $Y_r \ \sim \ \mathbb{E}(Y_r)$ with probability $1 - o(1)$. □

5 The lower bound on T; a sketch

We prove that

$$\text{Prob}(T \ > \ (\pi/4)(e^{-\gamma} - o(1))J_0(x)) \ = \ 1 - o(1),$$

in [4], by showing that the expected number of square products amongst $a_1, \dots, a_J$ is $o(1)$, for $J(x) = (\pi/4)(e^{-\gamma} - o(1))J_0(x)$.

By considering the common divisors of all pairs of integers from $a_1, \dots, a_J$ we begin by showing that the probability that a square product has size k, with $2 \le k \le \log x/2\log\log x$, is $O(J^2\log x/x)$ provided $J < x^{o(1)}$.

Next we shall write $a_i = b_i d_i$ where $P(b_i) \le y$ and where either $d_i = 1$ or $p(d_i) > y$ (here, $p(n)$ denotes the smallest prime divisor of n), for $1 \le i \le k$. If $a_1, \dots, a_k$ are chosen at random from $[1, x]$ then

$$\begin{aligned}
\text{Prob}(a_1 \dots a_k \in \mathbb{Z}^2) &\le \ \text{Prob}(d_1 \dots d_k \in \mathbb{Z}^2) \\
&= \sum_{\substack{d_1,\dots,d_k\ge 1\\ d_1\dots d_k\in\mathbb{Z}^2\\ d_i=1 \text{ or } p(d_i)>y}} \prod_{i=1}^{k}\frac{\Psi(x/d_i, y)}{x}
\end{aligned}$$

$$\leq \left(\{1+o(1)\}\frac{\Psi(x,y)}{x}\right)^k \sum_{n=1 \text{ or } p(n)>y} \frac{\tau_k(n^2)}{n^{2\alpha}}, \qquad (16)$$

by Proposition 2.1. Out of $J = \eta J_0$ integers, the number of k-tuples is $\binom{J}{k} \leq (eJ/k)^k$; and so the expected number of k-tuples whose product is a square is

$$\leq \left((e+o(1))\frac{\eta y}{k\log y_0}\frac{\Psi(x,y)/y}{\Psi(x,y_0)/y_0}\right)^k \prod_{p>y}\left(1+\frac{\tau_k(p^2)}{p^{2\alpha}}+\frac{\tau_k(p^4)}{p^{4\alpha}}+\dots\right). \qquad (17)$$

For $\log x/2\log\log x < k \leq y_0^{1/4}$ we take $y = y_0^{1/3}$ and show that the quantity in (17) is $< 1/x^2$.

For $y_0^{1/4} \leq k = y_0^{\beta} \leq J = \eta J_0 \leq J_0$ we choose y so that $[k/C] = \pi(y)$, with C sufficiently large. One can show that the quantity in (17) is $< ((1+\epsilon)4\eta e^{\gamma}/\pi)^k$ and is significantly smaller unless $\beta = 1+o(1)$. This quantity is $< 1/x^2$ since $\eta < 4\pi e^{-\gamma} - \epsilon$ and the result follows.

This proof yields further useful information: If either $J < (\pi/4)(e^{-\gamma} - o(1))J_0(x)$, or if $k < y_0^{1-o(1)}$ or $k > y_0^{1+o(1)}$, then the expected number of square products with $k > 1$ is $O(J_0(x)^2 \log x/x)$, whereas the expected number of squares in our sequence is $\sim J/\sqrt{x}$. This justifies the remarks immediately after the statement of Theorem 1.2.

Moreover with only minor modifications we showed the following in [4]: Let $y_1 = y_0 \exp((1+\epsilon)\sqrt{\log y_0 \log\log y_0})$ and write each $a_i = b_i d_i$ where $P(b_i) \leq y = y_1 < p(d_i)$. If $d_{i_1} \dots d_{i_l}$ is a subproduct which equals a square n^2, but such that no subproduct of this is a square, then, with probability $1 - o(1)$, we have $l = o(\log y_0)$ and n is a squarefree integer composed of precisely $l-1$ prime factors, each $\leq y^2$, where $n \leq y^{2l}$.

6 A method to examine all smooth products

In proving his upper bound on T, Schroeppel worked with the y_0-smooth integers amongst $a_1, \dots, a_T$ (which correspond to rows of A with no 1's in any column that represents a prime $> y_0$), and in our improvement in section 4.2 we worked with integers that have no more than one prime factor $> y_0$ (which correspond to rows of A with at most one 1 in the set of columns representing primes $> y_0$). We now work with all of the rows of A, at the cost of significant complications.

Let A_{y_0} be the matrix obtained by deleting the first $\pi(y_0)$ columns of A. Note that the row vectors corresponding to y_0-smooth numbers will be 0 in this new matrix. If

$$\text{rank}(A_{y_0}) < J - \pi(y_0), \qquad (18)$$

then

$$\text{rank}(A) \leq \text{rank}(A_{y_0}) + \pi(y_0) < J,$$

which therefore means that the rows of A are dependent over $\mathbb{F}_2$, and thus the sequence $a_1, ..., a_J$ contains a square dependence.

So let us suppose we are given a matrix A corresponding to a sequence of a_j's. We begin by removing (extraneous) rows from A_{y_0}, one at a time: that is, we remove a row containing a 1 in its lth column if there are no other 1s in the lth column of the matrix (since this row cannot participate in a linear dependence). This way we end up with a matrix B in which no column contains exactly one 1, and for which

$$r(A_{y_0}) - \text{rank}(A_{y_0}) = r(B) - \text{rank}(B)$$

(since we reduce the rank by 1 each time we remove a row). Next we partition the rows of B into minimal subsets, in which the primes involved in each subset are disjoint from the primes involved in the other subsets (in other words, if two rows have a 1 in the same column then they must belong to the same subset). The ith subset forms a submatrix, S_i, of rank ℓ_i, containing r_i rows, and then

$$r(B) - \text{rank}(B) \ = \ \sum_i (r_i - \ell_i).$$

We will define a power series $f(\eta)$ for which we believe that

$$\mathbb{E}\left(\sum_i (r_i - \ell_i)\right) \sim f(\eta)\pi(y_0) \tag{19}$$

when $J = (\eta + o(1))J_0$, and we can show that

$$\lim_{\eta \to \eta_0^-} f(\eta) \ = \ 1, \tag{20}$$

where $\eta_0 \ := \ e^{-\gamma}$. Using the idea of section 4.3, we will deduce in section 6.9 that if (19) holds then

$$\sum_i (r_i - \ell_i) \sim f(\eta)\pi(y_0) \tag{21}$$

holds with probability $1 - o(1)$, and hence (18) holds with probability $1 - o(1)$ for $J = (\eta_0 + o(1))J_0$. That is we can replace the upper bound $3/4$ in Theorem 1.2 by $e^{-\gamma}$.

The simple model of section 3.1 suggests that A will not contain a square dependence until we have $\sim \pi(y_0)$ smooth or pseudo-smooth numbers; hence we believe that one can replace the lower bound $(\pi/4)e^{-\gamma}$ in Theorem 1.2 by $e^{-\gamma}$. This is our heuristic in support of Conjecture 1.1 .

6.1 The submatrices

Let M_R denote the matrix composed of the set R of rows (allowing multiplicity), removing columns of 0's. We now describe the matrices M_{S_i} for the submatrices S_i of B from the previous subsection.

For an $r(M)$-by-$\ell(M)$ matrix M we denote the (i,j)th entry $e_{i,j} \in \mathbb{F}_2$ for $1 \le i \le r,\ 1 \le j \le \ell$. We let

$$N(M) \ = \ \sum_{i,j} e_{i,j}$$

denote the number of 1's in M, and

$$\Delta(M) := N(M) - r(M) - \ell(M) + 1.$$

We denote the number of 1's in column j by

$$m_j \ = \ \sum_i e_{i,j},$$

and require each $m_j \geq 2$.[5] We also require that M is *transitive*. That is, for any $j,\ 2 \leq j \leq \ell$ there exists a sequence of row indices $i_1, \ldots, i_g$, and column indices $j_1, \ldots, j_{g-1}$, such that

$$e_{i_1,1} \ = \ e_{i_g,j} \ = \ 1; \text{ and, } e_{i_h,j_h} \ = \ e_{i_{h+1},j_h} = 1 \text{ for } 1 \ \leq \ h \ \leq \ g-1.$$

In other words we do not study M if, after a permutation, it can be split into a block diagonal matrix with more than one block, since this would correspond to independent squares.

It is convenient to keep in mind two reformulations:

Integer version: Given primes $p_1 < p_2 < \ldots < p_\ell$, we assign, to each row, a squarefree integer

$$n_i \ = \ \prod_{1 \leq j \leq \ell} p_j^{e_{i,j}}, \text{ for } 1 \leq i \leq r.$$

Graph version: Take a graph $G(M)$ with r vertices, where v_i is adjacent to v_I with an edge of colour p_j if p_j divides both n_i and n_I (or, equivalently, $e_{i,j} = e_{I,j} = 1$). Notice that M being *transitive* is equivalent to the graph $G(M)$ being *connected*, which is much easier to visualize.

Now we define a class of matrices $\mathcal{M}_k$, where $M \in \mathcal{M}_k$ if M is as above, is transitive and $\Delta(M) = k$. Note that the "matrix" with one row and no columns is in $\mathcal{M}_0$ (in the "integer version" this corresponds to the set with just the one element, 1, and in the graph version to the graph with a single vertex and no edges).

6.2 Isomorphism classes of submatrices

Let us re-order the rows of M so that, in the graph theory version, each new vertex connects to the graph that we already have, which is always possible as the overall graph is connected. Let

$$\ell_I = \#\{j : \ \exists i \leq I \text{ with } e_{i,j} = 1\},$$

the number of columns with a 1 in or before the Ith row, and

$$N_I := \sum_{i \leq I,\ j \leq \ell} e_{i,j},$$

[5] Else the prime corresponding to that column cannot participate in a square product.

the number of 1's up to, and including in, the Ith row. Define

$$\Delta_I \;=\; N_I - I - \ell_I + 1,$$

so that $\Delta_r = \Delta(M)$.

Now $N_1 = \ell_1$ and therefore $\Delta_1 = 0$. Let us consider the transition when we add in the $(I+1)$th row. The condition that each new row connects to what we already have means that the number of new colours (that is, columns with a non-zero entry) is less than the number of 1's in the new row, that is

$$\ell_{I+1} - \ell_I \;\leq\; N_{I+1} - N_I - 1;$$

and so

$$\begin{aligned}\Delta_{I+1} \;=\; N_{I+1} - I - \ell_{I+1} \quad &= \quad N_I - I - \ell_I + (N_{I+1} - N_I) - (\ell_{I+1} - \ell_I) \\ &\geq \quad N_I - I - \ell_I + 1 \\ &= \quad \Delta_I.\end{aligned}$$

Therefore

$$\Delta(M) = \Delta_r \geq \Delta_{r-1} \geq \ldots \geq \Delta_2 \geq \Delta_1 = 0. \tag{22}$$

6.3 Restricting to the key class of submatrices

Two matrices are said to be "isomorphic" if one can be obtained from the other by permuting rows and columns. In this subsection we estimate how many submatrices of A_{y_0} are isomorphic to a given matrix M, in order to exclude from our considerations all those M that occur infrequently.

Proposition 6.1 *Fix $M \in \mathcal{M}_k$. The expected number of submatrices S of A_{y_0} for which M_S is isomorphic to M is*

$$\sim \frac{\eta^r \pi(y_0)^{1-k}}{|\mathrm{Aut}_{\mathrm{Rows}}(M)|} \prod_{1 \leq j \leq \ell} \frac{1}{\nu_j}, \tag{23}$$

where $\nu_j \;:=\; \sum_{i=j}^{\ell}(m_i - 1)$.

Note that we are not counting here the number of times a component S_i is isomorphic to M, but rather how many submatrices of A_{y_0} are isomorphic to M.

Since $\eta \leq 1$, the quantity in (23) is bounded if $k \geq 1$, but is a constant times $\pi(y_0)$ if $k = 0$. This is why we will restrict our attention to $M \in \mathcal{M}_0$, and our goal becomes to prove that

$$\mathbb{E}\left(\sum_{i:\; S_i \in \mathcal{M}} (r_i - \ell_i)\right) \;>\; \pi(y_0) \tag{24}$$

in place of (19), where henceforth we write $\mathcal{M} = \mathcal{M}_0$.

Proof. The expected number of times we get a set of integers of the form $\prod_{1\le j\le \ell} p_j^{e_{i,j}}$ times a y_0-smooth times a square, for $i = 1, ..., r$, within our sequence of integers $a_1, ..., a_J$ is

$$\sim \binom{J}{r} |\mathrm{Orbit}_{\mathrm{Rows}}(M)| \prod_{1\le i\le r} \frac{\Psi^*(x/\prod_{1\le j\le \ell} p_j^{e_{i,j}}, y_0)}{x}, \tag{25}$$

where by $\mathrm{Orbit}_{\mathrm{Rows}}(M)$ we mean the set of distinct matrices produced by permuting the rows of M, and $\Psi^*(X, y) := \#\{n = mr^2 : \ P(m) \le y < p(r)\}$ which is insignificantly larger than $\Psi(X, y)$ (as we saw at the end of section 4.1). Since r is fixed and J tends to infinity, we have

$$\binom{J}{r} \ \sim \ \frac{J^r}{r!};$$

and we know that[6]

$$r! \ = \ |\mathrm{Orbit}_{\mathrm{Rows}}(M)| \cdot |\mathrm{Aut}_{\mathrm{Rows}}(M)|$$

where $\mathrm{Aut}_{\mathrm{Rows}}(M)$ denotes the number of ways to obtain exactly the same matrix by permuting the rows (this corresponds to permuting identical integers that occur). Therefore (25) is

$$\begin{aligned} &\sim \frac{J^r}{|\mathrm{Aut}_{\mathrm{Rows}}(M)|} \prod_{1\le i\le r} \frac{\Psi(x/\prod_{1\le j\le \ell} p_j^{e_{i,j}}, y_0)}{x} \\ &\sim \frac{1}{|\mathrm{Aut}_{\mathrm{Rows}}(M)|} \left(\frac{J\Psi(x, y_0)}{x}\right)^r \prod_{1\le j\le \ell} \frac{1}{p_j^{m_j\alpha}}, \end{aligned} \tag{26}$$

where $m_j = \sum_i e_{i,j} \ge 2$, by (12). Summing the last quantity in (26) over all $y_0 < p_1 < p_2 < \ldots < p_\ell$, we obtain, by the prime number theorem,

$$\begin{aligned} &\sim \frac{(\eta\pi(y_0))^r}{|\mathrm{Aut}_{\mathrm{Rows}}(M)|} \int_{y_0<v_1<v_2<\ldots<v_\ell} \prod_{1\le j\le \ell} \frac{dv_j}{v_j^{m_j\alpha}\log v_j} \\ &\sim \frac{\eta^r \pi(y_0)^{r+\ell-\sum_j m_j}}{|\mathrm{Aut}_{\mathrm{Rows}}(M)|} \int_{1<t_1<t_2<\ldots<t_\ell} \prod_{1\le j\le \ell} \frac{dt_j}{t_j^{m_j}} \end{aligned}$$

using the approximation $\log v_j \sim \log y_0$ (because this range of values of v_j gives the main contribution to the integral), and the fact that $v_j^\alpha \ \sim \ v_j/\log y_0$ for v_j in this range. The result follows by making the substitution $t_j = v_j/y_0$.

6.4 Properties of $M \in \mathcal{M} := \mathcal{M}_\prime$

Lemma 6.2 *Suppose that $M \in \mathcal{M} := \mathcal{M}_\prime$. For each row of M, other than the first, there exists a unique column which has a 1 in that row as well as an earlier row. The last row of M contains exactly one 1.*

[6]This is a consequence of the "Orbit-Stabilizer Theorem" from elementary group theory. It follows from the fact that the cosets of $\mathrm{Aut}_{\mathrm{Rows}}(M)$ in the permutation group on the r rows of M, correspond to the distinct matrices (orbit elements) obtained by performing row interchanges on M.

Proof. For each $M \in \mathcal{M}$, we have $\Delta_j = 0$ for each $j \geq 0$ by (22) so that

$$\ell_{j+1} - \ell_j \;=\; N_{j+1} - N_j - 1.$$

That is, each new vertex connects with a unique colour to the set of previous vertices, which is the first part of our result.[7] The second part comes from noting that the last row cannot have a 1 in a column that has not contained a 1 in an earlier row of M. □

Lemma 6.3 *If $M \in \mathcal{M}$ then all cycles in its graph, $G(M)$, are monochromatic.*

Proof. If not, then consider a minimal cycle in the graph, where not all the edges are of the same color. We first show that, in fact, each edge in the cycle has a different color. To see this, we start with a cycle where not all edges are of the same color, but where at least two edges have the same color. Say we arrange the vertices $v_1, ..., v_k$ of this cycle so that the edge (v_1, v_2) has the same color as (v_j, v_{j+1}), for some $2 \leq j \leq k-1$, or the same color as (v_k, v_1), and there are no two edges of the same colour in-between. If we are in the former case, then we reduce to the smaller cycle $v_2, v_3, ..., v_j$, where not all edges have the same color; and, if we are in the latter case, we reduce to the smaller cycle $v_2, v_3, ..., v_k$, where again not all the edges have the same color. Thus, if not all of the edges of the cycle have the same color, but the cycle does contain more than one edge of the same color, then it cannot be a minimal cycle.

Now let I be the number of vertices in our minimal cycle of different colored edges, and reorder the rows of M so that this cycle appears as the first I rows.[8] Then

$$N_I \;\geq\; 2I + (\ell_I - I) \;=\; \ell_I + I.$$

The term $2I$ accounts for the fact that each prime corresponding to a different colored edge in the cycle must divide at least two members of the cycle, and the $\ell_I - I$ accounts for the remaining primes that divide members of the cycle (that don't correspond to the different colored edges). This then gives $\Delta_I \geq 1$; and thus by (22) we have $\Delta(M) \geq 1$, a contradiction. We conclude that every cycle in our graph is monochromatic. □

Lemma 6.4 *Every $M \in \mathcal{M}$ has rank $\ell(M)$.*

Proof by induction on ℓ. For $\ell = 0, 1$ this is trivial. Otherwise, as there are no cycles the graph must end in a "leaf"; that is a vertex of degree one. Suppose this corresponds to row r and color ℓ. We now construct a new matrix M' which is matrix M less column ℓ, and any rows that only contained a 1 in the ℓth column. The new graph now consists of $m_\ell - 1$ disjoint subgraphs, each of which corresponds to an element of $\mathcal{M}$. Thus the rank of M is given by 1 (corresponding to the rth row, which acts as a pivot element in Gaussian elimination on the ℓth column) plus the sum of the ranks of new connected subgraphs. By the induction hypothesis, they each have rank equal to the number of their primes, thus in total we have $1 + (\ell - 1) = \ell$, as claimed. □

[7] Hence we confirm that $\ell = N - (r-1)$, since the number of primes involved is the total number of 1's less the unique "old prime" in each row after the first.

[8] This we are allowed to do, because the connectivity of successive rows can be maintained, and because we will still have $\Delta(M) = 0$ after this permutation of rows.

6.5 An identity, and inclusion-exclusion inequalities, for $\mathcal{M}$.

Proposition 6.5 *If $M_R \in \mathcal{M}$ then*

$$\sum_{\substack{S\subset R\\ M_S\in\mathcal{M}}} (-1)^{N(S)} = r(M) - \mathrm{rank}(M). \tag{27}$$

Furthermore, if $N \geq 2$ is an even integer then

$$\sum_{\substack{S\subset R, N(S)\leq N\\ M_S\in\mathcal{M}}} (-1)^{N(S)} \;\geq\; r(M) - \mathrm{rank}(M), \tag{28}$$

and if $N \geq 3$ is odd then

$$\sum_{\substack{S\subset R, N(S)\leq N\\ M_S\in\mathcal{M}}} (-1)^{N(S)} \;\leq\; r(M) - \mathrm{rank}(M). \tag{29}$$

Proof by induction on $|R|$. It is easy to show when R has just one row and that has no 1's, and when $|R| = 2$, so we will assume that it holds for all R satisfying $|R| \leq r-1$, and prove the result for $|R| = r$.

Let $\mathcal{N}$ be the set of integers that correspond to the rows of R

By Lemma 3 we know that the integer in $\mathcal{N}$ which corresponds to the last row of M must be a prime, which we will call p_ℓ. Note that p_ℓ must divide at least one other integer in $\mathcal{N}$, since $M_R \in \mathcal{M}$.

Case 1: p_ℓ divides at least three elements from our set.

We partition R into three subsets: R_0, the rows without a 1 in the ℓth column; R_1, the rows with a 1 in the ℓth column, but no other 1s (that is, rows which correspond to the prime p_ℓ); and R_2, the rows with a 1 in the ℓth column, as well as other 1s. Note that $|R_1| \geq 1$ and $|R_1| + |R_2| \geq 3$ by hypothesis.

Write each $S \subset R$ with $M_S \in \mathcal{M}$ as $S_0 \cup S_1 \cup S_2$ where $S_i \subset R_i$. If we fix S_0 and S_2 with $|S_2| \geq 2$ then $S_0 \cup S_2 \in \mathcal{M}$ if and only if $S_0 \cup S_1 \cup S_2 \in \mathcal{M}$ for any $S_1 \subset R_1$. Therefore the contribution of all of these S to the sum in (27) is

$$(-1)^{N(S_0)+N(S_2)} \sum_{S_1\subset R_1} (-1)^{|S_1|} = (-1)^{N(S_0)+N(S_2)}(1-1)^{|R_1|} = 0 \tag{30}$$

Now consider those sets S with $|S_2| = 1$. In this case we must have $|S_1| \geq 1$ and equally we have $S_0 \cup \{p_\ell\} \cup S_2 \in \mathcal{M}$ if and only if $S_0 \cup S_1 \cup S_2 \in \mathcal{M}$ for any $S_1 \subset R_1$ with $|S_1| \geq 1$. Therefore the contribution of all of these S to the sum in (27) is

$$\begin{aligned}(-1)^{N(S_0)+N(S_2)} \sum_{\substack{S_1\subset R_1\\ |S_1|\geq 1}} (-1)^{|S_1|} &= (-1)^{N(S_0)+N(S_2)}((1-1)^{|R_1|} - 1)\\ &= (-1)^{N(S_0\cup\{p_\ell\}\cup S_2)}. \end{aligned}\tag{31}$$

Regardless of whether $|S_2| = 1$ or $|S_2| \geq 2$, we get that if we truncate the sums (30) or (31) to all those $S_1 \subset R_1$ with

$$N(S_1) \ = \ |S_1| \ \leq \ N - N(S_0) - N(S_2),$$

then the total sum is ≤ 0 if N is odd, and is ≥ 0 if N is even; furthermore, note that we get that these truncations are 0 in two cases: If $N - N(S_0) - N(S_2) \leq 0$ (which means that the above sums are empty, and therefore 0 by convention), or if $N - N(S_0) - N(S_2) \geq N(R_1)$ (which means that we have the complete sum over all $S_1 \subset R_1$).

It remains to handle those S where $|S_2| = 0$. We begin by defining certain sets H_j and T_j: If the elements of R_2 correspond to the integers $h_1, \ldots, h_k$ then let H_j be the connected component of the subgraph containing h_j, of the graph obtained by removing all rows divisible by p_ℓ except h_j. Let $T_j = H_j \cup \{p_\ell\}$. Note that if $S_2 = \{h_j\}$ then $S_0 \cup \{p_\ell\} \cup S_2 \subset T_j$ (in the paragraph immediately above).

Note that if S has $|S_2| = 0$, then $S = S_0 \subset T_j$ for some j (since the graph of S is connected), or $S = S_1$ with $|S| \geq 2$. The contribution of those $S = S_1$ with $|S| \geq 2$ to the sum in (27) is

$$\sum_{\substack{S_1 \subset R_1 \\ |S_1| \geq 2}} (-1)^{|S_1|} = (1-1)^{|R_1|} - (1 - |R_1|) = |R_1| - 1.$$

Furthermore, if we truncate this sum to all those S_1 satisfying

$$N(S_1) \ = \ |S_1| \ \leq \ N,$$

then the sum is $\geq |R_1| - 1$ if $N \geq 2$ is even, and the sum is $\leq |R_1| - 1$ if $N \geq 3$ is odd.

Finally note that if $S \subset T_j$ with $M_S \in \mathcal{M}$ then either $|S_2| = 0$ or $S = S_0 \cup \{p_\ell, h_j\}$ and therefore, combining all of this information,

$$\sum_{\substack{S \subset R \\ M_S \in \mathcal{M}}} (-1)^{N(S)} = |R_1| - 1 + \sum_{j=1}^{k} \sum_{\substack{S \subset T_j \\ M_S \in \mathcal{M}}} (-1)^{N(S)} = |R_1| - 1 + \sum_{j=1}^{k} (r(T_j) - \ell(T_j))$$

by the induction hypothesis (as each $|T_j| < |M|$). Also by the induction hypothesis, along with what we worked out above for N even and odd, in all possibilities for $|S_2|$ (i.e. $|S_2| = 0$, 1 or exceeds 1), we have that for $N \geq 3$ odd,

$$\sum_{\substack{S \subset R, \ N(S) \leq N \\ M_S \in \mathcal{M}}} (-1)^{N(S)} \ \leq \ |R_1| - 1 + \sum_{j=1}^{k} (r(T_j) - \ell(T_j));$$

and for $N \geq 2$ even,

$$\sum_{\substack{S \subset R, \ N(S) \leq N \\ M_S \in \mathcal{M}}} (-1)^{N(S)} \ \geq \ |R_1| - 1 + \sum_{j=1}^{k} (r(T_j) - \ell(T_j)).$$

The T_j less the rows $\{p_\ell\}$ is a partition of the rows of M less the rows $\{p_\ell\}$, and so

$$\sum_j (r(T_j) - 1) \;=\; r(M) - |R_1|.$$

The primes in T_j other than p_ℓ is a partition of the primes in M other than p_ℓ, and so

$$\sum_j (\ell(T_j) - 1) \;=\; \ell(M) - 1.$$

Combining this information gives (27), (28), and (29).

Case 2 : p_ℓ divides exactly two elements from our set.

Suppose these two elements are $n_r = p_\ell$ and $n_{r-1} = p_\ell q$ for some integer q. If $q = 1$ this is our whole graph and (27), (28) and (29) all hold, so we may assume $q > 1$. If $n_j \neq q$ for all j, then we create $M_1 \in \mathcal{M}$ with $r-1$ rows, the first $r-2$ the same, and with $n_{r-1} = q$. We have

$$N(M_1) = N(M) - 2,\; r(M_1) = r(M) - 1,\; \text{and } \ell(M_1) = \ell(M) - 1.$$

We claim that there is a 1-1 correspondence between the subsets $S \subset \mathcal{R}(M)$ with $M_S \in \mathcal{M}$ and the subsets $T \subset \mathcal{R}(M_1)$ with $(M_1)_T \in \mathcal{M}$. The key observation to make is that $p_\ell \in S$ (ie row r) if and only if $p_\ell q \in S$ (ie row $r-1$), since $M_S \in \mathcal{M}$. Thus if rows $r-1$ and r are in S then S corresponds to T (ie $T = S_1$), which we obtain by replacing rows $r-1$ and r of S by row $r-1$ of T which corresponds to q. Otherwise we let $S = T$. Either way $(-1)^{N(S)} = (-1)^{N(T)}$ and so

$$\sum_{\substack{S \subset R \\ M_S \in \mathcal{M}}} (-1)^{N(S)} \;=\; \sum_{\substack{T \subset \mathcal{R}(M_1) \\ (M_1)_T \in \mathcal{M}}} (-1)^{N(T)} = r(M_1) - \ell(M_1) = r(M) - \ell(M),$$

by the induction hypothesis. Further, we have that for N even,

$$\sum_{\substack{S \subset R, N(S) \leq N \\ M_S \in \mathcal{M}}} (-1)^{N(S)} \;=\; \sum_{\substack{T \subset \mathcal{R}(M_1), N(T) \leq N-2 \\ (M_1)_T \in \mathcal{M}}} (-1)^{N(T)} \;\geq\; r(M) - \ell(M).$$

The analogous inequality holds in the case where N is odd. Thus, we have that (27), (28) and (29) all hold.

Finally, suppose that $n_j = q$ for some j, say $n_{r-2} = q$. Then q must be prime else there would be a non-monochromatic cycle in $M \in \mathcal{M}$. But since prime q is in our set it can only divide two of the integers of the set (by our previous deductions) and these are n_{r-2} and n_{r-1}. However this is then the whole graph and we observe that (27), (28), and (29) all hold. $\square$

6.6 Counting Configurations

We partitioned B into connected components $S_1, \ldots, S_h$. Now we form the matrices B_k, the union of the $S_j \in \mathcal{M}_k$, for each $k \geq 0$, so that

$$r(B) - \text{rank}(B) \;=\; \sum_{k \geq 0} r(B_k) - \text{rank}(B_k), \tag{32}$$

and

$$r(B_k) - \text{rank}(B_k) \;=\; \sum_{j:\ S_j \in \mathcal{M}_k} r(S_j) - \text{rank}(S_j).$$

More importantly

$$\sum_{j:\ M_j \in \mathcal{M}_0} r(M_j) - \text{rank}(M_j) = \sum_{j:\ M_j \in \mathcal{M}_0} \sum_{\substack{S \subset \mathcal{R}(M_j) \\ M_S \in \mathcal{M}}} (-1)^{N(S)} = \sum_{\substack{S \subset \mathcal{R}(B_0) \\ M_S \in \mathcal{M}}} (-1)^{N(S)}, \tag{33}$$

by Proposition 6.5. If $k \geq 1$ then there are a bounded number of S_j isomorphic to any given matrix $M \in \mathcal{M}_k$, by Proposition 6.1, and so we believe that these contribute little to our sum (32). In particular we conjecture that

$$\sum_{k \geq 1} \sum_{j:\ M_j \in \mathcal{M}_k} \left\{ r(M_j) - \text{rank}(M_j) - \sum_{\substack{S \subset \mathcal{R}(M_j) \\ M_S \in \mathcal{M}}} (-1)^{N(S)} \right\} = o(\pi(y_0))$$

with probability $1 - o(1)$. Hence the last few equations combine to give what will now be our

Assumption:

$$r(B) - \text{rank}(B) \;=\; \sum_{\substack{S \subset \mathcal{R}(B) \\ M_S \in \mathcal{M}}} (-1)^{N(S)} + o(\pi(y_0)). \tag{34}$$

By combining (23), (34), and the identity

$$\sum_{\sigma \in S_\ell} \prod_{j=1}^{\ell} \frac{1}{\sum_{i=j}^{\ell} c_{\sigma(i)}} \;=\; \prod_{j=1}^{\ell} \frac{1}{c_i},$$

(here S_ℓ is the symmetric group on $1, ..., \ell$, and taking $c_i = m_i - 1$) we obtain, by summing over all orderings of the primes,

$$\mathbb{E}(r(B) - \text{rank}(B)) \sim f(\eta)\pi(y_0) \tag{35}$$

where

$$f(\eta) := \sum_{M \in \mathcal{M}^*} \frac{(-1)^{N(M)}}{|\text{Aut}_{\text{Cols}}(M)| \cdot |\text{Aut}_{\text{Rows}}(M)|} \cdot \frac{\eta^{r(M)}}{\prod_{j=1}^{\ell}(m_j - 1)} \quad , \tag{36}$$

assuming that when we sum and re-order our initial series, we do not change the value of the sum. Here $\text{Aut}_{\text{Cols}}(M)$ denotes the number of ways to obtain exactly the same matrix M when permuting the columns, and $\mathcal{M}^* = \mathcal{M}/\sim$ where two matrices are considered to be "equivalent" if they are isomorphic.

6.7 Husimi graphs

All of the graphs $G(M), M \in \mathcal{M}$ are simple graphs, and have only monochromatic cycles: notice that these cycles are subsets of the complete graph formed by the edges of a particular colour (corresponding to the integers divisible by a particular prime). Hence any two-connected subgraph of $G(M)$ is actually a complete graph: This is precisely the definition of a *Husimi* graph (see [11]), and so the isomorphism classes of Husimi graphs are in one-to-one correspondence with the matrices in $\mathcal{M}^*$.

Husimi graphs have a rich history, inspiring the combinatorial theory of species, and are central to the thermodynamical study of imperfect gases (see [11] for references and discussion).

Lemma 6.6 *If G is a Husimi graph then*

$$\mathrm{Aut}(G) \cong \mathrm{Aut}_{\mathrm{Rows}}(M) \times \mathrm{Aut}_{\mathrm{Cols}}(M). \tag{37}$$

Proof. If $\sigma \in \mathrm{Aut}(G)$ then it must define a permutation of the colors of G; that is an element $\tau \in \mathrm{Aut}_{\mathrm{Cols}}(M)$. Then $\tau^{-1}\sigma \in \mathrm{Aut}(G)$ is an automorphism of G that leaves the colors alone; and therefore must permute the elements of each given color. However if two vertices of the same color in G are each adjacent to an edge of another color then permuting them would permute those colors which is impossible. Therefore $\tau^{-1}\sigma$ only permutes the vertices of a given color which are not adjacent to edges of any other color; and these correspond to automorphisms of the rows of M containing just one 1. However this is all of $\mathrm{Aut}_{\mathrm{Rows}}(M)$ since if two rows of M are identical then they must contain a single element, else G would contain a non-monochromatic cycle. □

Let $\mathrm{Hu}(j_2, j_3, \ldots)$ denote the set of Husimi graphs with j_i blocks of size i for each i, on

$$r \;=\; 1 + \sum_{i\geq 2} (i-1) j_i \tag{38}$$

vertices, with $\ell = \sum_i j_i$ and $N(M) = \sum_i i j_i$. (This corresponds to a matrix M in which exactly j_i columns contain precisely i 1's.) In this definition we count all distinct labellings, so that

$$\mathrm{Hu}(j_2, j_3, \ldots) = \sum_G \frac{r!}{|\mathrm{Aut}(G)|} \ ,$$

where the sum is over all isomorphism classes of Husimi graphs G with exactly j_i blocks of size i for each i. The Mayer-Husimi formula (which is (42) in [11]) gives

$$\mathrm{Hu}(j_2, j_3, \ldots) = \frac{(r-1)!}{\prod_{i\geq 2}((i-1)!^{j_i} j_i!)} \cdot r^{\ell-1}, \tag{39}$$

and so, by (36), (37) and the last two displayed equations we obtain

$$f(\eta) = \sum_{\substack{j_2, j_3, \ldots \geq 0 \\ j_2 + j_3 + \cdots < \infty}} (-1)^{r+\ell-1} \frac{r^{\ell-2}}{\prod_{i\geq 2}((i-1)!^{j_i} (i-1)^{j_i} j_i!)} \cdot \eta^r. \tag{40}$$

6.8 Convergence of $f(\eta)$.

In this section we prove, under an appropriate (analytic) assumption, the following

"Theorem" *The function $f(\eta)$ has radius of convergence $e^{-\gamma}$, is increasing in $[0, e^{-\gamma})$, and $\lim_{\eta\to(e^{-\gamma})^-} f(\eta) = 1$.*

So far we have paid scant attention to necessary convergence issues. First note the identity

$$\exp\left(\sum_{i=1}^{\infty} c_i\right) \;=\; \sum_{\substack{k_1,k_2,\ldots\geq 0\\ k_1+k_2+\cdots<\infty}} \prod_{i\geq 1} \frac{c_i^{k_i}}{k_i!}, \tag{41}$$

which converges absolutely for any sequence of numbers $c_1, c_2, ...$ for which $|c_1|+|c_2|+\cdots$ converges, so that the terms in the series on the right-hand-side can be summed in any order we please.

The summands of $f(\eta)$, for given values of r and ℓ, equal $(-1)^{r+\ell-1}r^{\ell-2}\eta^r$ times

$$\sum_{\substack{j_2,j_3,\ldots\geq 0\\ \sum_{i\geq 2} j_i=\ell,\ \sum_{i\geq 2}(i-1)j_i=r-1}} \frac{1}{\prod_{i\geq 2}((i-1)!^{j_i}(i-1)^{j_i}j_i!)}, \tag{42}$$

which is exactly the coefficient of t^{r-1} in

$$\frac{1}{\ell!}\left(t+\frac{t^2}{2\cdot 2!}+\frac{t^3}{3\cdot 3!}+\ldots\right)^{\ell},$$

and so is less than $\tau^\ell/\ell!$ where $\tau = \sum_{j\geq 1} 1/(j\cdot j!) \approx 1.317902152$. Note that if $r\geq 2$ then $1\leq \ell\leq r-1$. Therefore the sum of the absolute values of all of the coefficients of η^r in $f(\eta)$ is less than

$$\sum_{2\leq\ell\leq r-1} r^{\ell-2}\frac{\tau^\ell}{\ell!} \ll r^{r-2}\frac{\tau^r}{r!} \ll \frac{(e\tau)^r}{r^{5/2}}$$

The first inequality holds since $\tau > 1$, the second by Stirling's formula. Thus $f(\eta)$ is absolutely convergent for $|\eta| \leq \rho_0 := 1/(e\tau) \approx 0.2791401779$. We can therefore manipulate the power series for f, as we wish, inside the ball $|\eta|\leq\rho_0$, and we want to extend this range.

Let

$$A(T) \;:=\; -\sum_{j\geq 1}\frac{(-1)^j T^j}{j\cdot j!} = \int_0^T \frac{1-e^{-t}}{t}dt.$$

The identity (41) implies that the coefficient of t^{r-1} in $\exp(rA(\eta t))$ is

$$\sum_{\substack{j_2,j_3,\cdots\\ j_2+2j_3+3j_4+\cdots=r-1}} \frac{(-1)^{r+\ell-1}r^\ell\eta^{r-1}}{\prod_{i\geq 2}((i-1)!^{j_i}(i-1)^{j_i}j_i!)},$$

so that

$$f'(\eta) \;=\; \sum_{r\geq 1}\frac{\text{coeff of } t^{r-1} \text{ in } \exp(rA(\eta t))}{r}. \tag{43}$$

We will now obtain a functional equation for f' using Lagrange's Inversion formula:

Lagrange's Inversion formula: *If $g(w)$ is analytic at $w = 0$, with $g(0) = a$ and $g'(0) \neq 0$, then*

$$h(z) \;=\; \sum_{r=1}^{\infty} \left(\frac{d}{dw}\right)^{r-1} \left(\frac{w}{g(w)-a}\right)^{r}\Big|_{w=0} \frac{(z-a)^r}{r!}$$

is the inverse of $g(w)$ in some neighbourhood around a (that is we have $h(g(w)) = 1$).

If $g(w) = w/\varphi(w)$, where $\varphi(w)$ is analytic and non-zero in some neighbourhood of 0, then

$$h(z) \;=\; \sum_{r=1}^{\infty} \frac{c_{r-1} z^r}{r}$$

is the inverse of $g(w)$ in some neighbourhood around 0, where c_j is the coefficient of w^j in $\varphi(w)^{j+1}$. Applying this with $\varphi(w) \;=\; e^{A(\eta w)}$ we find that $g(w) = we^{-A(\eta w)}$ has an inverse $h(z)$ in a neighbourhood, Γ, around 0 where

$$h(1) \;=\; \sum_{r\geq 1} \frac{\text{coeff. of } z^{r-1} \text{ in } \exp(rA(\eta z))}{r} \;=\; f'(\eta).$$

We will assume that the neighbourhood Γ includes 1. Therefore, since

$$1 \;=\; g(h(1)) \;=\; h(1)e^{-A(\eta h(1))} \;=\; f'(\eta)e^{-A(\eta f'(\eta))},$$

we deduce that

$$f'(\eta) = e^{A(\eta f'(\eta))}. \tag{44}$$

(Note that this can only hold for η in some neighborhood of 0 in which the power series for $f'(\eta)$ converges.) Taking the logarithm of (44) and differentiating we get, using the formula $A'(T) \;=\; \frac{1-e^{-T}}{T}$,

$$\frac{f''(\eta)}{f'(\eta)} = (\eta f'(\eta))' \; \frac{1-e^{-\eta f'(\eta)}}{\eta f'(\eta)}$$

so that $f'(\eta) = (\eta f'(\eta))' - \eta f''(\eta) = (\eta f'(\eta))' \; e^{-\eta f'(\eta)}$. Integrating and using the facts that $f(0) = 0$ and $f'(0) = 1$, we have

$$f(\eta) = 1 - e^{-\eta f'(\eta)}. \tag{45}$$

We therefore deduce that

$$\eta f'(\eta) = -\log(1-f(\eta)) = \sum_{k\geq 1} \frac{f(\eta)^k}{k}. \tag{46}$$

Lemma 6.7 *The coefficients of $f(\eta)$ are all non-negative. Therefore $|f(z)| \leq f(|z|)$ so that $f(z)$ is absolutely convergent for $|z| < R$ if $f(\eta)$ converges for $0 \leq \eta < R$. Also all of the coefficients of $f'(\eta)$ are non-negative and $f'(0) = 1$ so that $f'(\eta) > 1$ for $0 \leq \eta < R$.*

Proof. Write $f(\eta) = \sum_{r\geq 0} a_r \eta^r$. We prove that $a_r > 0$ for each $r \geq 1$, by induction. We already know that $a_1 = 1$ so suppose $r \geq 2$. We will compare the coefficient of η^r on both sides of (46). On the left side this is obviously ra_r. For the right side, note that the coefficient of η^r in $f(\eta)^k$ is a polynomial, with positive integer coefficients (by the multinomial theorem), in variables $a_1, \ldots, a_{r+1-k}$ for each $k \geq 1$. This is 0 for $k > r$, and is positive for $2 \leq k \leq r$ by the induction hypothesis. Finally, for $r = 1$, the coefficient is a_r. Therefore we have that $ra_r > a_r$ which implies that $a_r > 0$ as desired. □

Our plan is to determine R, the radius of convergence of $f(\eta)$, by determining the largest possible R_1 for which $f'(\eta)$ is convergent for $0 \leq \eta < R_1$. Then $R = R_1$.

Since f' is monotone increasing (as all the coefficients of f' are positive), we can define an inverse on the reals $\geq f'(0) = 1$. That is, for any given $y \geq 1$, let η_y be the (unique) value of $\eta \geq 0$ for which $f'(\eta) = y$. Therefore $R_1 = \lim_{y\to\infty} \eta_y$:

We claim that the value of $f'(\eta)$ is that unique real number y for which $B_\eta(y) := A(\eta y) - \log y = 0$: By (44) we do have that $B_\eta(f'(\eta)) = 0$, and this value is unique if it exists since $B_\eta(y)$ is monotone decreasing, as

$$B'_\eta(y) = \eta A'(\eta y) - 1/y = -e^{-\eta y}/y < 0.$$

This last equality follows since $A'(T) = \frac{1-e^{-T}}{T}$. Now $A'(T) > 0$ for $T > 0$, and so $A(t) > 0$ for all $t > 0$ as $A(0) = 0$. Therefore $B_\eta(1) = A(\eta) > 0$, and so, remembering that $B_\eta(y)$ is monotone decreasing, we have that a solution y exists to $B_\eta(y) := A(\eta y) - \log y = 0$ if and only if $B_\eta(\infty) < 0$. Therefore R_1 is precisely that value of $\eta = \eta_1$ for which $B_{\eta_1}(\infty) = 0$. Now

$$B_\eta(y) \;=\; B_\eta(1) + \int_1^y B'_\eta(t)dt \;=\; A(\eta) - \int_1^y \frac{e^{-\eta t}}{t} dt.$$

so that

$$B_\eta(\infty) \;=\; A(\eta) - \int_1^\infty \frac{e^{-\eta y}}{y} dy.$$

Therefore

$$\int_1^\infty \frac{e^{-\eta_1 y}}{y} dy = A(\eta_1) = A(0) + \int_0^{\eta_1} A'(v)dv \;=\; \int_0^{\eta_1} \frac{(1-e^{-v})}{v} dv,$$

so that

$$\int_1^{\eta_1} \frac{dv}{v} \;=\; \int_1^\infty \frac{e^{-v}}{v} dv - \int_0^1 \frac{(1-e^{-v})}{v} dv = -\gamma$$

(as is easily deduced from the third line of (6.3.22) in [1]). Exponentiating we find that $R_1 = \eta_1 \;=\; e^{-\gamma} \;=\; .561459...$

Finally by (45) we see that $f(\eta) < 1$ when $f'(\eta)$ converges, that is when $0 \leq \eta < \eta_0$, and $f(\eta) \to 1$ as $\eta \to \eta_0^-$.

6.9 From expectation to probability

One can easily generalize Proposition 2 to prove the following result, which implies that if $\mathbb{E}(r(B)-\text{rank}(B)) > (1+2\epsilon)\pi(y_0)$ then $r(B)-\text{rank}(B) > (1+\epsilon)\pi(y_0)$ with probability $1-o_\epsilon(1)$.

Proposition 6.8 *If $M \in \mathcal{M}$ then*

$$\#\{S \subseteq A_{y_0} : \ M_S \simeq M\} \sim \mathbb{E}(\#\{S \subseteq A_{y_0} : \ M_S \simeq M\})$$

with probability $1-o(1)$, as $x \to \infty$.

Hence, with probability $1-o(1)$ we have, assuming (34) is true, that

$$\sum_{j:\ M_j \in \mathcal{M}} r(M_j) - \text{rank}(M_j) \sim \mathbb{E}\left(\sum_{j:\ M_j \in \mathcal{M}} r(M_j) - \text{rank}(M_j) \right)$$

as $x \to \infty$, which is why we believe that one can take $J = (e^{-\gamma} + o(1))J_0(x)$ with probability $1-o(1)$.

7 Algorithms

7.1 The running time for Pomerance's problem

We will show that, with current methods, the running time in the hunt for the first square product is dominated by the speed of finding a linear dependence in our matrix of exponents:

Let us suppose that we select a sequence of integers $a_1, a_2, \dots, a_J$ in $[1,n]$ that appear to be random, as in Pomerance's problem, with $J \asymp J_0$. We will suppose that the time taken to determine each a_j, and then to decide whether a_j is y_0-smooth and, if so, to factor it, is $\ll y_0^{(1-\epsilon)/\log\log y_0}$ steps (note that the factoring can easily be done in $\exp(O(\sqrt{\log y_0 \log\log y_0}))$ steps by the elliptic curve method, according to [3], section 7.4.1). Therefore, with probability $1-o(1)$, the time taken to obtain the factored integers in the square dependence is $\ll y_0^{2-\epsilon/\log\log y_0}$ by (8).

In order to determine square product we need a linear dependence mod 2 in the matrix of exponents. Using the Wiedemann or Lanczos methods (see section 6.1.3 of [3]) this takes time $O(\pi(y_0)^2\mu)$, where μ is the average number of prime factors of an a_i which has been kept, so this is by far the lengthiest part of the running time.

7.2 Improving the running time for Pomerance's problem

If instead of wanting to simply find the first square dependence, we require an algorithm that proceeds as quickly as possible to find any square dependence then we should select our parameters so as to make the matrix smaller. Indeed if we simply create the matrix of y-smooths then we will optimize by taking

$$\frac{\pi(y)}{\Psi(x,y)/x} \asymp \pi(y)^2\mu,$$

that is the expected number of a_j's selected should be roughly the running time to determine the square product. Here μ, is as in the previous section, and so we expect that μ is roughly

$$\frac{1}{\psi(x,y)} \sum_{n\le x, P(n)\le y} \sum_{p\le y:\ p|n} 1 = \sum_{p\le y} \frac{\psi(x/p,y)}{\psi(x,y)} \sim \sum_{p\le y} \frac{1}{p^\alpha} \sim \frac{y^{1-\alpha}}{(1-\alpha)\log y} \sim \frac{\log y}{\log\log y}$$

by (12), the prime number theorem and (11). Hence we optimize by selecting $y = y_1$ so that $\rho(u_1) \asymp (\log\log y_1)/y_1$, which implies that

$$y_1 = y_0^{1-(1+o(1))/\log\log x},$$

by Lemma 2.2, which is considerably smaller than y_0. On the other hand, if J_1 is the expected running time, $\pi(y_1)/(\Psi(x,y_1)/x)$ then

$$J_1/J_0 \sim \frac{y_1/\rho(u_1)}{y_0/\rho(u_0)} = \exp\left(\{1+o(1)\}\frac{u_0\log u_0}{(\log\log x)^2}\right) = y_0^{(1+o(1))/(\log\log x)^2}$$

by the prime number theorem, (3), and (22) in the proof of Lemma 2.3 in [4].

7.3 Smooth squares

In factoring algorithms, the a_i are squares mod n (as explained at the beginning of section 1), which is not taken into account in Pomerance's problem. For instance, in Dixon's random squares algorithm one selects $b_1, b_2, \dots, b_J \in [1,n]$ at random and lets a_i be the least residue of $b_i^2 \pmod n$. We keep only those a_i that are y-smooth, and so to complete the analysis we need some idea of the probability that a y-smooth integer is also a square mod n. Dixon [5] gives an (unconditionally proven) lower bound for this probability which is too small by a non-trivial factor. We shall estimate this probability much more accurately though under the assumption of the Generalized Riemann Hypothesis.

Theorem 7.1 *Assume the Generalized Riemann Hypothesis and let n be an integer with smallest prime factor $> y$, which is $> 2^{3\omega(n)}L^\epsilon$ (where $\omega(n)$ denotes the number of distinct prime factors of n). For any $n \ge x \ge n^{1/4+\delta}$, the proportion of the positive integers $a \le x$ where a is a square mod n and coprime to n, which are y-smooth, is $\sim \Psi(x,y)/x$.*

We use the following result which is easily deduced from the remark following Theorem 2 of [9]:

Lemma 7.2 *Assume the Generalized Riemann Hypothesis. For any non-principal character $\chi \pmod n$, and $1 \le x \le n$ we have, uniformly,*

$$\left| \sum_{\substack{a\le x \\ \text{a } y-\text{smooth}}} \chi(a) - \sum_{a\le x} \chi(a) \right| \ll \frac{\Psi(x,y)(\log n)^3}{\sqrt{y}}.$$

Proof of Theorem 7.1. Let $M(x)$ be the number of $a \le x$ which are coprime with n, let $N(x)$ be the number of these a which are a square mod n, and let $N(x,y)$ be the number of these a which are also y-smooth. Then

$$\left(N(x,y) - \frac{\Psi(x,y)}{2^{\omega(n)}}\right) - \left(N(x) - \frac{M(x)}{2^{\omega(n)}}\right) =$$

$$= \left(\sum_{\substack{a\le x,(a,n)=1\\ \text{a } y-\text{smooth}}} - \sum_{\substack{a\le x\\ (a,n)=1}}\right)\left(\prod_{p|n}\frac{1}{2}\left\{1+\left(\frac{a}{p}\right)\right\} - \frac{1}{2^{\omega(n)}}\right)$$

$$= \frac{1}{2^{\omega(n)}}\sum_{\substack{d|n\\ d\neq 1}}\mu^2(d)\left(\sum_{\substack{a\le x,(a,n)=1\\ \text{a } y-\text{smooth}}}\left(\frac{a}{d}\right) - \sum_{\substack{a\le x\\ (a,n)=1}}\left(\frac{a}{d}\right)\right) \ll \frac{\Psi(x,y)(\log n)^3}{\sqrt{y}}$$

by Lemma 7.2. Now Burgess's theorem tells us that $N(x) - M(x)/2^{\omega(n)} \ll x^{1-\epsilon}$ if $x \ge n^{1/4+\delta}$, the prime number theorem that $\omega(n) \le \log n/\log y = o(\log x)$, and (7) that $\Psi(x,y) \ge x^{1-\epsilon/2}$ as $y > L^\epsilon$. Hence $N(x,y) \sim \Psi(n,y)/2^{\omega(n)}$. The number of integers $a \le x$ which are coprime to n and a square mod n is $\sim (\phi(n)/n)(x/2^{\omega(n)})$, and $\phi(n) = n(1+O(1/y))^{\omega(n)} \sim n$, so the result follows. □

7.4 Making the numbers smaller

In Pomerance's quadratic sieve the factoring stage of the algorithm is sped up by having the a_i be the reduced values of a polynomial, so that every pth a_i is divisible by p, if any a_j is. This regularity means that we can proceed quite rapidly, algorithmically in factoring the a_i's. In addition, by an astute choice of polynomials, the values of a_i are guaranteed to be not much bigger than $\sqrt{n}$, which gives a big saving, and one can do a little better (though still bigger than $\sqrt{n}$) with Peter Montgomery's "multiple polynomial variation". For all this see section 6 of [3].

8 Large prime variations

8.1 A discussion of Theorem 4.2 in [4] and its consequences.

Define

$$\exp_k(z) := \sum_{j=0}^{k-1}\frac{z^j}{j!} \quad \text{so that } \lim_{k\to\infty}\exp_k(z) = \exp(z), \text{ and}$$

$$A_M(z) := \int_{1/M}^1 \frac{1-e^{-zt}}{t}\,dt \quad \text{so that } \lim_{M\to\infty} A_M(z) = A(z) = \int_0^1 \frac{1-e^{-zt}}{t}\,dt\,.$$

Recursively, define functions $\gamma_{m,M,k}$ by $\gamma_{0,M,k}(u) := u$ and

$$\gamma_{m+1,M,k}(u) := u\,\exp_k\left[A_M(\gamma_{m,M,k}(u))\right]$$

for $m = 0, 1, 2, \dots$ Note that $\gamma_{m,M,k}(u)$ is increasing in all four arguments. From this it follows that $\gamma_{m,M,k}(u)$ increases to $\gamma_{M,k}(u)$ as $m \to \infty$, a fixed point of the map $z \mapsto u \exp_k(A_m(z))$, so that

$$\gamma_{M,k}(u) := u \exp_k \left[A_M(\gamma_{M,k}(u)) \right]. \tag{47}$$

We now establish that $\gamma_{M,k}(u) < \infty$ except perhaps when $M = k = \infty$: We have $0 \le A_M(z) \le \log M$ for all z, so that $u < \gamma_{M,k}(u) \le Mu$ for all u; in particular $\gamma_{M,k}(u) < \infty$ if $M < \infty$. We have $A(z) = \log z + O(1)$ so that if $\gamma_{\infty,k}(u)$ is sufficiently large, we deduce from (47) that $\gamma_{\infty,k}(u) \sim u(\log u)^{k-1}/(k-1)!$; in particular $\gamma_{\infty,k}(u) < \infty$. As $M, k \to \infty$, the fixed point $\gamma_{M,k}(u)$ increases to the fixed point $\gamma(u)$ of the map $z \mapsto ue^{A(z)}$ (by comparing this with (44) we see that $\gamma(u) = uf'(u)$). In [4] we show that this map has a fixed point if and only if $u \le e^{-\gamma}$. Otherwise $\gamma(u) = \infty$ for $u > e^{-\gamma}$ so that $\int_0^\eta \frac{\gamma(u)}{u}\, du = \infty > 1$ for any $\eta > e^{-\gamma}$.

One might ask how the variables m, M, k, u relate to our problem? We are looking at the possible pseudosquares (that is integers which are a y_0-smooth times a square) composed of products of a_j with $j \le uJ_0$. We restrict our attention to a_j that are My_0-smooth, and which have at most k prime factors $\ge y_0$. In the construction of our hypergraph we examine the a_j selecting only those with certain (convenient) properties, which corresponds to $m = 0$. Then we pass through the a_j again, selecting only those with convenient properties given the a_j already selected at the $m = 0$ stage: this corresponds to $m = 1$. We iterate this procedure which is how the variable m arises. The advantage in this rather complicated construction is that the count of the number of pseudosquares created, namely

$$\sim \pi(y_0) \cdot \int_0^\eta \frac{\gamma_{m,M,k}(u)}{u}\, du\ ,$$

increases as we increase any of the variables so that it is relatively easy to deal with convergence issues (this is Theorem 2 in [4]). This technique is more amenable to analysis than the construction that we give in section 6, because here we use the inclusion-exclusion type formula (36) to determine $f(\eta)$, which has both positive and negative terms, and it has proved to be beyond us to establish unconditionally that this sum converges.

Note that as $m \to \infty$ we have that the number of pseudosquares created is

$$\sim \pi(y_0) \cdot \int_0^\eta \frac{\gamma_{M,k}(u)}{u}\, du\ ; \tag{48}$$

hence if the value of this integral is > 1 then we are guaranteed that there is a square product. If we let M and k go to ∞ then the number of pseudosquares created is

$$\sim \pi(y_0) \cdot \int_0^\eta \frac{\gamma(u)}{u}\, du\ .$$

The upper bound in Conjecture 1.1 follows. In terms of what we have proposed in section 6, we have now shown that the number of pseudosquares created is indeed $\sim f(\eta)\pi(y_0)$.

We remarked above that this integral is an increasing function of η and equals 1 for $\eta = e^{-\gamma}$. Hence if $\eta > e^{-\gamma}$ then we are guaranteed that there is a square product. One might expect that if $\eta = e^{-\gamma} + \epsilon$ then we are guaranteed $C(\epsilon)\pi(y_0)$ square products for some $C(\epsilon) > 0$. However we get rather more than that: if $\eta > e^{-\gamma}$ then $\int_0^\eta \frac{\gamma(u)}{u}\,du = \infty$ (that is $f(\eta)$ diverges) and hence the number of square products is bigger than any fixed multiple of $\pi(y_0)$ (we are unable to be more precise than this).

8.2 Speed-ups

From what we have discussed above we know that we will find a square product amongst the y_0-smooth a_j's once $J = \{1 + o(1)\}J_0$ with probability $1 - o(1)$. When we allow the a_j's that are either y_0-smooth, or y_0-smooth times a single larger prime then we get a stopping time of $\{c_1 + o(1)\}J_0$ with probability $1 - o(1)$ where c_1 is close to $3/4$. When we allow any of the a_j's in our square product then we get a stopping time of $\{e^{-\gamma} + o(1)\}J_0$ with probability $1 - o(1)$ where $e^{-\gamma} = .561459\ldots$. It is also of interest to get some idea of the stopping time for the k-large primes variations, for values of k other than $0, 1$ and ∞. In practice we cannot store arbitrarily large primes in the large prime variation, but rather keep only those a_j where all of the prime factors are $\leq My_0$ for a suitable value of M – it would be good to understand the stopping time with the feasible prime factors restricted in this way. We have prepared a table of such values using the result from [4] as explained in section 8.1: First we determined a Taylor series for $\gamma_{M,k}(u)$ by solving for it in the equation (47). Next we found the appropriate multiple of $\pi(y_0)$, a Taylor series in the variable η, by substituting our Taylor series for $\gamma_{M,k}(u)$ into (48). Finally, by setting this multiple equal to 1, we determined the value of η for which the stopping time is $\{\eta + o(1)\}J_0$ with probability $1 - o(1)$, when we only use the a_j allowed by this choice of k and M, to make square products.

k	$M = \infty$	$M = 100$	$M = 10$
0	1	1	1
1	.7499	.7517	.7677
2	.6415	.6448	.6745
3	.5962	.6011	.6422
4	.5764	.5823	.6324
5	.567	.575	.630

The expected stopping time, as a multiple of J_0.

8.3 A practical perspective

One approaches Pomerance's question, in practice, as part of an implementation of a factoring algorithm. The design of the computer, the language and the implementation of the algorithm, all affect the running time of each particular step. Optimally balancing the relative costs of the various steps of an algorithm (like the quadratic sieve) may be substantially different as these environmental factors change. This all makes it difficult to analyze the overall algorithm and to give one definitive answer.

The key parameter in Pomerance's problem and its use in factoring algorithms is the smoothness parameter $y = y_1$: We completely factor that part of a_j which is y-smooth. Given the origin of the a_j's it may be possible to do this very efficiently using a sieve method. One may obtain a significant speed-up by employing an "early abort" strategy for the a_j that have a particularly small y_1-smooth part, where y_1 is substantially smaller than y. The size of y also determines the size of the matrix in which we need to find a linear dependence – note though that the possible size of the matrix may be limited by the size of memory, and by the computer's ability to handle arrays above a certain size.

Suppose that a_j equals its y-smooth part times b_j, so that b_j is what is left after the initial sieving. We only intend to retain a_j if $b_j = 1$, or if b_j has no more than k prime factors, all of which are $\leq My$. Hence the variables M and k are also key parameters. If M is large then we retain more a_j's, and thus the chance of obtaining more pseudosquares. However this also slows down the sieving, as one must test for divisibility by more primes. Once we have obtained the b_j by dividing out of the a_j all of their prime factors $\leq y$ we must retain all of those $b_j \leq (My)^k$. If we allow k to be large then this means that only a very small proportion of the b_j that are retained at this stage will turn out to be My-smooth (as desired), so we will have wasted a lot of machine cycles on useless a_j. A recent successful idea to overcome this problem is to keep only those a_j where at most one of the prime factors is $> M'y$ for some M' that is not much bigger than 1 — this means that little time is wasted on a_j with two "large" prime factors. The resulting choice of parameters varies from program to program, depending on how reports are handled etc. etc., and on the prejudices and prior experiences of the programmers. Again, it is hard to make this an exact science.

Arjen Lenstra told us, in a private communication, that in his experience of practical implementations of the quadratic sieve, once n and y are large enough, the single large prime variation speeds things up by a factor between 2 and 2.5, and the double large prime variation by another factor between 2 and 2.5 (see, e.g. [13]), for a total speed-up of a factor between 4 and 6. An experiment with the triple large prime variation [12] seemed to speed things up by another factor of around 1.7.

Factorers had believed (see, e.g. [13] and [3]) that, in the quadratic sieve, there would be little profit in trying the triple large prime variation, postulating that the speed-up due to the extra pseudosquares obtained had little chance of compensating for the slowdown due to the large number of superfluous a_js considered, that is those for which $b_j \leq (My)^3$ but turned out to not be My-smooth. On the other hand, in practical implementations of the number field sieve, one obtains a_j with more than two large prime factors relatively cheaply and, after a slow start, the number of pseudosquares obtained suddenly increases very rapidly (see [6]). This is what led the authors of [12] to their recent surprising and successful experiment with the triple large prime variation for the quadratic sieve. (See Willemien Ekkelkamp's contribution to these proceedings [7] for further discussion of multiple prime variation speed-ups to the number field sieve.)

This practical data is quite different from what we have obtained, theoretically, at the end of the previous section. There are two reasons for this – the data in the last section was for Pomerance's problem in which the smoothness parameter is y_0, whereas in these questions the smoothness parameter is y_1, which is substantially smaller. Secondly, in our analysis of Pomerance's problem, the variations in M and k simply affect the

number of a_j being considered, whereas here these affect not only the number of a_j being considered, but also several other important quantities. For instance, the amount of sieving that needs to be done, and also the amount of data that needs to be "swapped" (typically one saves the a_j with several large prime factors to the disk, or somewhere else suitable for a lot of data). It would certainly be interesting to run experiments on Pomerance's problem directly to see whether our predicted speed comparisons are close to correct for numbers within computational range.

9 Acknowledgements

We thank Francois Bergeron for pointing out the connection with Husimi graphs, for providing mathematical insight and for citing references such as [11]. Thanks to Carl Pomerance for useful remarks, which helped us develop our analysis of the random squares algorithm in section 7, and to Arjen Lenstra for discussing with us a more practical perspective which helped us to formulate many of the remarks given in section 8.3.

References

[1] M. Abramowitz and I. Stegun, Handbook of mathematical functions, Dover Publications, New York 1965.

[2] J. Buhler, H. W. Lenstra Jr., and C. Pomerance, *Factoring integers with the number field sieve*, Lecture Notes in Math, 1554, Springer, Berlin, 1993.

[3] R. Crandall and C. Pomerance, *Prime numbers; A computational perspective*, Springer, New York (2005).

[4] E. Croot, A. Granville, R. Pemantle, and P. Tetali, *Sharp transitions in making squares*, (to appear).

[5] J. D. Dixon, *Asymptotically fast factorization of integers*, Math. Comp. **36** (1981), 255-260.

[6] Bruce Dodson and Arjen K. Lenstra, *NFS with four large primes: an explosive experiment*. Advances in cryptology—CRYPTO '95 (Santa Barbara, CA, 1995), Lecture Notes in Comput. Sci. **963**, Springer, Berlin, (1995), 372–385.

[7] Willemien Ekkelkamp, *Predicting the Sieving Effort for the Number Field Sieve*, these proceedings.

[8] E. Friedgut, *Sharp Thresholds of Graph Properties, and the k-SAT Problem*, J. Amer. Math. Soc. **12** (1999), 1017-1054.

[9] A. Granville and K. Soundararajan, *Large Character Sums*, J. Amer. Math. Soc. **14** (2001), 365-397.

[10] A. Hildebrand and G. Tenenbaum, *On integers free of large prime factors*, Trans. Amer. Math. Soc **296** (1986), 265–290.

[11] Pierre Leroux, *Enumerative Problems Inspired by Mayer's Theory of Cluster Integrals*, Electronic Journal of Combinatorics, paper R32, May 14, 2004.

[12] Paul Leyland, Arjen Lenstra, Bruce Dodson, Alec Muffett and Sam Wagstaff *MPQS with three large primes*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., **2369**, Springer, Berlin, (2002), 446–460.

[13] A.K. Lenstra and M.S. Manasse, *Factoring with two large primes*, Math. Comp. **63** (1994), 785–798.

[14] C. Pomerance, *The quadratic sieve factoring algorithm.* Advances in cryptology, Paris (1984), 169-182.

[15] C. Pomerance, *The number field sieve* in Mathematics of Computation 1943–1993: a half century of computational mathematics (W. Gautschi, ed.), Proc. Symp. Appl. Math. **48**, Amer. Math. Soc., Providence (1994), 465 - 480.

[16] C. Pomerance, *The role of smooth numbers in number theoretic algorithms*, Proc. International Cong. of Mathematicians (Zurich, 1994), Birhäuser **1** (1995), 411 - 422.

[17] C. Pomerance, *Multiplicative independence for random integers*, Analytic number theory: Proceedings of a conference in honor of Heini Halberstam (eds., B.C. Berndt et. al.), Birhäuser **2** (1996), 703 - 711.

[18] C. Pomerance, *Smooth numbers and the quadratic sieve*, Proc. of an MSRI workshop, J. Buhler and P. Stevenhagen, eds. (to appear).

[19] R. Silverman, *The multiple polynomial quadratic sieve*, Math. Comp. bf 48 (1987), 329-339.

[20] G. Tenenbaum, Introduction to the analytic and probabilistic theory of numbers, Cambridge Univ. Press 1995.