Journal of Integer Sequences, Vol. 18 (2015),
Article 15.10.4

Counting Tuples Restricted by Pairwise Coprimality Conditions

Juan Arias de Reyna
Facultad de Matemáticas
Universidad de Sevilla
c/. Tarfia, s/n
41012-Sevilla
Spain
arias@us.es

Randell Heyman
School of Mathematics and Statistics
University of New South Wales
Sydney, N.S.W. 2052
Australia
randell@unsw.edu.au

Abstract

Given a subset A of the set $\{1,\dots,v\}^2$ we say that $(a_1,\dots,a_v)$ exhibits *pairwise coprimality over* A if $\gcd(a_i,a_j)=1$ for all $(i,j)\in A$. For a given positive x and a given set A we give an asymptotic formula for the number of $(a_1,\dots,a_v)$ with $1\le a_1,\dots,a_v\le x$ that exhibit pairwise coprimality over A. This problem has been studied before by Hu.

1 Introduction

We study tuples whose elements are positive integers of maximum value x and impose certain coprimality conditions on pairs of elements. Pairwise coprimality has a long history. It is a requirement of the Chinese remainder theorem which has been known for at least 1,700 years (see the book by Katz [9, pp. 131–132]). The Chinese remainder theorem is important in many areas of modern day mathematics. Some applications in modular multiplication, bridging computations, coding theory and cryptography can be found in the book by Ding, Pei, and Salomaa [2, pp. 33–184] and some comments regarding modular multiplication applications can be found in the book by Knuth [10, pp. 285–292]. To date pairwise coprimality calculations have also been necessary for quantifying v-tuples that are *totally pairwise non-coprime*, that is, $\gcd(a_i, a_j) > 1$ for all $1 \leq i, j \leq v$ (see articles by Hu and the second author [8, 6], and the comments by Moree [11] regarding the manuscript of Freiberg [4]).

Tóth [12] used an inductive approach to give an asymptotic formula for the number of height-constrained tuples that exhibit totally pairwise coprimality (that is, $\gcd(a_i, a_j) = 1$ for all $1 \leq i, j \leq v$). See also the article by Cai and Bach [1, Theorems 4 and 5] for another approach to asymptotic results regarding total pairwise coprimality. Recently Fernández and Fernández [3] and in subsequent discussions with the second author, have shown how to calculate the asymptotic proportion of v random positive integers that exhibit coprimality across given pairs. They give only an asymptotic value without information about the error term. Their approach is non-inductive. Hu [8] was the first to estimate the number of $(a_1, \ldots, a_v)$ with $1 \leq a_1, \ldots, a_v \leq x$ that satisfy general coprimality conditions on pairs of elements of a v-tuple. His inductive approach gives an asymptotic formula with an upper bound on the error term of $O(x^{v-1} \log^{v-1} x)$.

Our result gives an upper bound of the error term of $O(x^{v-1} \log^{d} x)$ where d is the maximum number of pairwise coprimality conditions that involve a given index. In many cases $d < v - 1$, and in these cases our main result gives a better error term than that in the article by Hu [8]. Unlike Hu [8], our approach is non-inductive. In this paper we focus exclusively on pairwise coprimality conditions, but readers interested in the generalization from pairwise to k-wise coprimality can see another article by Hu [7].

We use a graph to represent the required primality conditions as follows. Let $G = (V, E)$ be a graph with v vertices and e edges. The set of vertices, V, is given by $V = \{1, \ldots, v\}$, while the set of edges of G, denoted by E, is a subset of the set of pairs of elements of V. That is, $E \subset \{\{1, 2\}, \{1, 3\}, \ldots, \{r, s\}, \ldots, \{v - 1, v\}\}$. We admit isolated vertices (that is, vertices that are not adjacent to any other vertex). An edge is always of the form $\{r, s\}$ with $r \neq s$ and $\{r, s\} = \{s, r\}$. For each real $x > 0$ we define the set of all tuples that satisfy the primality conditions by

$$G(x) := \{(a_1, \ldots, a_v) \in \mathbb{N}^v : a_r \leq x,\ \gcd(a_r, a_s) = 1 \text{ if } \{r, s\} \in E\}.$$

We also let $g(x) = \operatorname{card}(G(x))$, and denote with d the maximum degree of the vertices of G. Finally, let $Q_G(z) = 1 + B_2 z^2 + \cdots + B_v z^v$ be the polynomial associated with the graph G defined in Section 2.

Our main result is as follows.

Theorem 1. *For real $x > 0$ we have*

$$g(x) = x^v \rho_G + O(x^{v-1} \log^d x),$$

where

$$\rho_G = \prod_{p \text{ prime}} Q_G\left(\frac{1}{p}\right).$$

The quantity ρ_G gives the asymptotic proportion of v random positive integers that exhibit the given pairwise coprimality conditions. When combined with Section 2 the formula is explicit. For example, consider the 'square' 4-tuple. That is, 4-tuples with $\gcd(a_1, a_2) = \gcd(a_2, a_3) = \gcd(a_3, a_4) = \gcd(a_4, a_1) = 1$. Then the asymptotic proportion of such 4-tuples is given by

$$\rho_G = \prod_{p \text{ prime}} \left(1 - \frac{4}{p^2} + \frac{4}{p^3} - \frac{1}{p^4}\right) = 0.217778\cdots$$

Further details can be found in Section 4.

2 Preparations

As usual, for any integer $n \geq 1$, let $\omega(n)$ and $\sigma(n)$ be the number of distinct prime factors of n and the sum of divisors of n, respectively (we also set $\omega(1) = 0$). We also use μ to denote the Möbius function, that is, $\mu(n) = (-1)^{\omega(n)}$ if n is squarefree, and $\mu(n) = 0$ otherwise. $P^+(n)$ denotes the largest prime factor of the integer $n > 1$. By convention $P^+(1) = 1$. We recall that the notation $U = O(V)$ is equivalent to the assertion that the inequality $|U| \leq c|V|$ holds for some constant $c > 0$. We use $A \subset B$ to indicate that A is a subset of B.

For each $F \subset E$, a subset of the edges of G, let $v(F)$ be the number of non-isolated vertices of F. We define two polynomials $Q_G(z)$ and $Q_G^+(z)$ by

$$Q_G(z) = \sum_{F \subset E} (-1)^{\operatorname{card}(F)} z^{v(F)}, \qquad Q_G^+(z) = \sum_{F \subset E} z^{v(F)}.$$

In this way we associate two polynomials with each graph. It is clear that the only $F \subset E$ for which $v(F) = 0$ is the empty set. Thus the constant term of $Q_G(z)$ and $Q_G^+(z)$ is always 1. If F is non-empty then there is some edge $a = \{r, s\} \in F$ so that $v(F) \geq 2$. Therefore the coefficient of z in $Q_G(z)$ and $Q_G^+(z)$ is zero. Since we do not allow repeated edges the only case in which $v(F) = 2$ is when F consists of one edge. Thus the coefficient of z^2 in $Q_G^+(z)$ is e, that is, the number of edges e in G. The corresponding z^2 coefficient in $Q_G(z)$ is $-e$.

As a matter of notation we shall sometimes use r and s to indicate vertices. The letter v always denotes the last vertex and the number of vertices in a given graph. Edges are sometimes denoted by a or b. As previously mentioned, we use d to denote the maximum degree of any vertex and e to denote the number of edges. We use terms like e_j to indicate the j-th edge.

We associate several multiplicative functions with any graph. To define these functions we consider functions $E \to \mathbb{N}$, that is, to any edge a in the graph we associate a natural number n_a. We call any of these functions, $a \mapsto n_a$, an *edge numbering* of the graph. Given an edge numbering we assign a corresponding *vertex numbering* function $r \mapsto N_r$ by the rule $N_r = \operatorname{lcm}(n_{b_1}, \dots, n_{b_u})$, where $E_r = \{b_1, \dots, b_u\} \subset E$ is the set of edges incident to r. We note that in the case where r is an isolated vertex we have $E_r = \emptyset$ and $N_r = 1$. With this notation we define

$$f_G(m) = \sum_{N_1 N_2 \cdots N_v = m} \mu(n_1) \cdots \mu(n_e), \quad f_G^+(m) = \sum_{N_1 N_2 \cdots N_v = m} |\mu(n_1) \cdots \mu(n_e)|.$$

In this and similar summations in this paper, the summation is extended to all edge numberings (that is, for all $1 \le n_1, \dots, n_e < \infty$) satisfying the condition written under the summation symbol, usually expressed in terms of the corresponding vertex numberings.

The following is interesting in its own right, but will also be used to prove Theorem 1.

Proposition 2. *Let $f : \mathbb{N} \to \mathbb{C}$ be a multiplicative function. For any graph G the function*

$$g_{f,G}(m) = \sum_{N_1 N_2 \cdots N_v = m} f(n_1) \cdots f(n_e)$$

is multiplicative.

Proof. Let $m = m_1 m_2$, where $\gcd(m_1, m_2) = 1$. Let us assume that for a given edge numbering of G we have $N_1 \cdots N_v = m$. For any edge $a = \{r, s\}$ we have $n_a | N_r$ and $n_a | N_s$. Therefore $n_a^2 | m$. It follows that we may express n_a as $n_a = n_{1,a} n_{2,a}$ with $n_{1,a} | m_1$ and $n_{2,a} | m_2$. In this case $\gcd(n_{1,a}, n_{2,a}) = 1$, and we have

$$N_r = \operatorname{lcm}(n_{b_1}, \dots, n_{b_v}) = \operatorname{lcm}(n_{1,b_1}, \dots, n_{1,b_v}) \operatorname{lcm}(n_{2,b_1}, \dots, n_{2,b_v}),$$

$$f(n_1) \cdots f(n_e) = f(n_{1,1}) \cdots f(n_{1,e}) \cdot f(n_{2,1}) \cdots f(n_{2,e}).$$

Since each edge numbering n_a splits into two edge numberings $n_{1,a}$ and $n_{2,a}$, we have

$$m_1 = N_{1,1} \cdots N_{1,v}, \quad m_2 = N_{2,1} \cdots N_{2,v}.$$

Thus

$$\begin{aligned} g_{f,G}(m_1 m_2) &= g_{f,G}(m) \\ &= \sum_{N_1 N_2 \cdots N_v = m} f(n_1) \cdots f(n_e) \\ &= \sum_{N_{1,1} \cdots N_{1,v} \cdot N_{2,1} \cdots N_{2,v} = m_1 m_2} f(n_{1,1}) \cdots f(n_{1,e}) \cdot f(n_{2,1}) \cdots f(n_{2,e}) \\ &= \sum_{N_{1,1} \cdots N_{1,v} = m_1} f(n_{1,1}) \cdots f(n_{1,e}) \sum_{N_{2,1} \cdots N_{2,v} = m_2} f(n_{2,1}) \cdots f(n_{2,e}) \\ &= g_{f,G}(m_1) g_{f,G}(m_2), \end{aligned}$$

which completes the proof. □

We now draw the link between $f^+_G(p^k)$ and $Q^+_G(z)$.

Lemma 3. *For any graph G and prime p the value $f^+_G(p^k)$ is equal to the coefficient of z^k in $Q^+_G(z)$. In the same way the value of $f_G(p^k)$ is equal to the coefficient of z^k in $Q_G(z)$.*

Proof. First we consider the case of $f_G(p^k)$. Recall that

$$Q_G(z) = \sum_{F\subset E}(-1)^{\mathrm{card}(F)}z^{v(F)}, \qquad f_G(p^k) = \sum_{N_1\cdots N_v = p^k}\mu(n_1)\cdots\mu(n_e),$$

where the last sum is on the set of edge numberings of G. In the second sum we shall only consider edge numberings of G giving a non-null term. This means that we only consider edge numberings with n_a squarefree numbers. Notice also that if $N_1\cdots N_v = p^k$, then each $n_a \mid p^k$. So the second sum extends to all edge numbering with $n_a \in \{1,p\}$ for each edge $a\in E$ and satisfying $N_1\cdots N_v = p^k$.

We need to prove the equality

$$\sum_{F\subset E,\ v(F)=k}(-1)^{\mathrm{card}(F)} = \sum_{N_1\cdots N_v=p^k}\mu(n_1)\cdots\mu(n_e). \tag{1}$$

To this end we shall define for each $F\subset E$ with $v(F)=k$ a squarefree edge numbering $\sigma(F)=(n_a)$ with $N_1\cdots N_v = p^k$, $n_a\in\{1,p\}$ and such that $(-1)^{\mathrm{card}(F)} = \mu(n_1)\cdots\mu(n_e)$. We will show that σ is a bijective mapping between the set of $F\subset E$ with $v(F)=k$ and the set of edge numberings (n_a) with $N_1\cdots N_v = p^k$. Thus equality (1) will be established and the proof finished.

Assume that $F\subset E$ with $v(F)=k$. We define $\sigma(F)$ as the edge numbering (n_a) defined by

$$n_a = p \text{ for any } a\in F, \quad n_a = 1 \text{ for } a\in E\smallsetminus F.$$

In this way it is clear that $\mu(n_1)\cdots\mu(n_e) = (-1)^{\mathrm{card}(F)}$. Also $N_r = p$ or $N_r = 1$. We have $N_r = p$ if and only if there is some $a=\{r,s\}\in F$. So that $N_1\cdots N_v = p^{v(F)}$ because by definition $v(F)$ is the cardinality of the union $\bigcup_{\{r,s\}\in F}\{r,s\}$.

The map σ is invertible. For let (n_a) be an edge numbering of squarefree numbers with $N_1\cdots N_v = p^k$ and $n_a\in\{1,p\}$. If $\sigma(F)=(n_a)$ necessarily we have $F=\{a\in E : n_a = p\}$. It is clear that defining F in this way we have $v(F)=k$ and $\sigma(F)=(n_a)$.

Therefore the coefficient of z^k in $Q_G(z)$ coincides with the value of $f_G(p^k)$.

The proof for f^+_G is the same, observing that for $\sigma(F)=(n_a)$ we have $1 = |(-1)^{\mathrm{card}(F)}| = |\mu(n_1)\cdots\mu(n_e)|$. □

3 Proof of Theorem 1

We prove the theorem in the following steps:

1. We show that

$$g(x) = \sum_{n_1,\ldots,n_e} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \left\lfloor \frac{x}{N_r} \right\rfloor.$$

2. We show that

$$g(x) = x^v \sum_{n_1=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r} + R + O\left(x^{v-1}\log^d x\right),$$

where

$$|R| \leq x^{v-1} \sum_{j=1}^{e} \sum_{n_1=1}^{\infty} \cdots \sum_{n_{j-1}=1}^{\infty} \sum_{n_j>x} \sum_{n_{j+1}=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r}.$$

3. We show that $|R| = O(x^{v-1}\log^d x)$.

We start with the following sieve result which generalizes the sieve of Eratosthenes.

Lemma 4. *Let X be a finite set, and let $A_1, A_2, \ldots, A_k \subset X$. Then*

$$\text{card}\left(X \setminus \bigcup_{j=1}^{k} A_j\right) = \sum_{J\subset\{1,2,\ldots,k\}} (-1)^{\text{card}(J)}\,\text{card}(A_J),$$

where $A_\emptyset = X$, and for $J \subset \{1, 2, \ldots, k\}$ non-empty

$$A_J = \bigcap_{j\in J} A_j.$$

To prove Theorem 1 let X be the set

$$X = \{(a_1, \ldots, a_v) \in \mathbb{N}^v : a_r \leq x, 1 \leq r \leq v\}.$$

Our set $G(x)$, associated with the graph G, is a subset of X. Now for each prime $p \leq x$ and each edge $a = \{r, s\} \in G$ define the following subset of X.

$$A_{p,a} = \{(a_1, \ldots, a_v) \in X : p|a_r, p|a_s\}.$$

Therefore the tuples in $A_{p,a}$ are not in $G(x)$. In fact it is clear that

$$G(x) = X \setminus \bigcup_{\substack{a\in E\\ p\leq x}} A_{p,a},$$

where E denotes the set of edges in our graph G. We note that we have an $A_{p,a}$ for each prime number less than or equal to x and each edge $a \in E$. Denoting P_x as the set of prime numbers less than or equal to x we can represent each $A_{p,a}$ as A_j with $j \in P_x \times E$. We now apply Lemma 4 and obtain

$$g(x) = \sum_{J \subset P_x \times E} (-1)^{\operatorname{card}(J)} \operatorname{card}(A_J). \tag{2}$$

We compute $\operatorname{card}(A_J)$ and then $\operatorname{card}(J)$. For $\operatorname{card}(A_J)$ we have

$$J = \{(p_1, e_1), \ldots, (p_m, e_m)\}, \quad A_J = \bigcap_{j=1}^{m} A_{p_j, e_j}.$$

Therefore $(a_1, \ldots, a_v) \in A_J$ is equivalent to saying that $p_j | a_{r_j}, p_j | a_{s_j}$ for all $1 \leq j \leq m$, where $e_j = \{r_j, s_j\}$. We note that if $p_{i_1}, \ldots, p_{i_\ell}$ are the primes associated in J with a given edge $a = \{r, s\}$, then the product of $p_{i_1} \cdots p_{i_\ell}$ must also divide the values a_r and a_s associated with the vertices of a. Let $T_a \subset P_x$ consist of the primes p such that $(p, a) \in J$. In addition we define

$$n_a = \prod_{p \in T_a} p,$$

observing that when $T_a = \emptyset$ we have $n_a = 1$. Then $(a_1, \ldots, a_v) \in A_J$ is equivalent to saying that for each $a = \{r, s\}$ appearing in J we have $n_a \mid a_r$ and $n_a \mid a_s$. In this way we can define J by giving a number n_a for each edge a. We note that n_a is always squarefree, and all its prime factors are less than or equal to x. We also note that $(a_1, \ldots, a_v) \in A_J$ is equivalent to saying that $n_a | a_r$ for each edge a that joins vertex r with another vertex.

Then for each vertex r, consider all the edges a joining r to other vertices, and denote the least common multiple of the corresponding n_a's by N_r. So $(a_1, \ldots, a_v) \in A_J$ is equivalent to saying that $N_r | a_r$. The number of multiples of N_r that are less than or equal to x is $\lfloor x/N_r \rfloor$, so we can express the number of elements of A_J as

$$\operatorname{card}(A_J) = \prod_{r=1}^{v} \left\lfloor \frac{x}{N_r} \right\rfloor. \tag{3}$$

We now compute $\operatorname{card}(J)$. This is the total number of prime factors across all the n_j. As mentioned before n_j is squarefree, so

$$(-1)^{\operatorname{card}(J)} = (-1)^{\sum_{j=1}^{e} \omega(n_j)} = \mu(n_1) \cdots \mu(n_e), \tag{4}$$

where the summations are over all squarefree n_j with $P^+(n_j) \leq x$. Substituting (3) and (4) into (2) yields

$$g(x) = \sum_{n_1=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} \mu(n_1) \cdots \mu(n_e) \prod_{r=1}^{v} \left\lfloor \frac{x}{N_r} \right\rfloor.$$

At first the sum extends to the $(n_1,\dots,n_e)$ that are squarefree and have all prime factors less than or equal to x. But we may extend the sum to all $(n_1,\dots,n_e)$, because if these conditions are not satisfied then the corresponding term is automatically 0. In fact we may restrict the summation to the $n_a \le x$, because otherwise for $a=\{r,s\}$ we have $n_a \mid N_r$ and $\lfloor x/N_r \rfloor = 0$. Therefore

$$g(x) = \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \left\lfloor \frac{x}{N_r} \right\rfloor .$$

We now seek to express $g(x)$ as a multiple of x^v plus a suitable error term. Observe that for all real $z_1, z_2, z_3 > 0$,

$$\lfloor z_1\rfloor\lfloor z_2\rfloor\lfloor z_3\rfloor = z_1z_2z_3 - z_1z_2\{z_3\} - z_1\{z_2\}\lfloor z_3\rfloor - \{z_1\}\lfloor z_2\rfloor\lfloor z_3\rfloor,$$

where $\{y\}$ denotes the fractional part of a number y.

Applying a similar procedure, with v factors instead of 3, we get

$$\begin{aligned} g(x) = &\sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{x}{N_r} \\ &- \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \left\{\frac{x}{N_1}\right\} \prod_{r=2}^{v} \left\lfloor \frac{x}{N_r} \right\rfloor \\ &- \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \frac{x}{N_1}\left\{\frac{x}{N_2}\right\} \prod_{r=3}^{v} \left\lfloor \frac{x}{N_r} \right\rfloor \\ &\cdots \\ &- \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \frac{x}{N_1}\cdots\frac{x}{N_{v-1}}\left\{\frac{x}{N_v}\right\} \\ &= x^v \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r} + \sum_{k=1}^{v} R_k, \end{aligned} \tag{5}$$

where for $1 \le k \le v$,

$$R_k = -\sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \frac{x}{N_1}\cdots\frac{x}{N_{k-1}}\left\{\frac{x}{N_k}\right\}\left\lfloor\frac{x}{N_{k+1}}\right\rfloor\cdots\left\lfloor\frac{x}{N_v}\right\rfloor,$$

with the obvious modifications for $j=1$ and $j=v$. We then have

$$\begin{aligned} |R_k| &\le \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} |\mu(n_1)\cdots\mu(n_e)| \frac{x}{N_1}\cdots\frac{x}{N_{k-1}}\frac{x}{N_{k+1}}\cdots\frac{x}{N_v} \\ &\le x^{v-1} \sum_{P^+(m)\le x} \frac{C_{G,k}(m)}{m}, \end{aligned}$$

where

$$C_{G,k}(m) = \sum_{m=\prod_{1\le r\le v, r\ne k} N_r} |\mu(n_1)\cdots\mu(n_e)|.$$

By similar reasoning to that of Proposition 2 the function $C_{G,k}(m)$ can be shown to be multiplicative. The numbers $C_{G,k}(p^\alpha) = C_{G,k,\alpha}$ do not depend on p, and $C_{G,k}(p^\alpha) = C_{G,k,\alpha} = 0$ for $\alpha > v$. So we have

$$\begin{aligned}\sum_{P^+(m)\le x} \frac{C_{G,k}(m)}{m} &\le \prod_{p\le x}\left(1 + \frac{C_{G,k,1}}{p} + \frac{C_{G,k,2}}{p^2} + \cdots \frac{C_{G,k,v}}{p^v}\right)\\ &= O(\log^{C_{G,k,1}} x),\end{aligned}$$

where $C_{G,k}(m)$ is the number of solutions $(n_1,\ldots,n_e)$, with n_j squarefree, to

$$\prod_{1\le r\le v, r\ne k} N_r = m.$$

Let h_k denote the degree of vertex k. It is easy to see that for a prime p we have $C_{G,k,1} = C_{G,k}(p) = h_k$. The solutions are precisely those with all $n_j = 1$, except one $n_\ell = p$, where ℓ should be one of the edges meeting at vertex k. Therefore the maximum number of solutions occurs when k is one of the vertices of maximum degree. So if we let d be this maximum degree, then the maximum value of $C_{G,k}(p)$ is d. Therefore

$$|R_k| = O(x^{v-1}\log^d x). \tag{6}$$

Substituting (6) into (5) we obtain

$$g(x) = x^v \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}\frac{1}{N_r} + O(x^{v-1}\log^d x). \tag{7}$$

We require the following lemma.

Lemma 5.

$$\lim_{x\to\infty} \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v}\frac{1}{N_r} < +\infty.$$

Proof. We have

$$\lim_{x\to\infty} \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v}\frac{1}{N_r} = \sum_{m=1}^{\infty}\frac{f_G^+(m)}{m}, \tag{8}$$

where

$$f_G^+(m) = \sum_{m=\prod_{r=1}^{v} N_r} |\mu(n_1)\cdots\mu(n_e)|.$$

We note that $f_G^+(m)$ is multiplicative by Proposition 2. It is clear that $f_G^+(1) = 1$. Also, each edge joins two vertices r and s and thus $n_j|N_r$ and $n_j|N_s$. This means that

$$n_j^2|\prod_{r=1}^{v} N_r.$$

It follows that

$$\prod_{r=1}^{v} N_r \neq p,$$

for any prime p and so $f_G^+(p) = 0$. We also note that a multiple $(n_1, \ldots, n_e)$ only counts in $f_G^+(m)$ if $|\mu(n_1)\cdots\mu(n_e)| = 1$. Therefore each n_j is squarefree. So each factor in

$$\prod_{r=1}^{v} N_r \tag{9}$$

brings at most a p. So the greatest power of p that can divide (9) is p^v. So $f_G^+(p^\alpha) = 0$ for $\alpha > v$. Recall that $f_G^+(p^\alpha)$ is equal to the coefficient of z^α in $Q_G^+(z)$. So, by Lemma 3, we note that $f_G^+(p^\alpha)$ depends on α but not on p. Putting all this together we have

$$\sum_{m=1}^{\infty} \frac{f_G^+(m)}{m} = \prod_{p \text{ prime}} \left(1 + \frac{f_G^+(p^2)}{p^2} + \ldots + \frac{f_G^+(p^v)}{p^v}\right) < +\infty. \tag{10}$$

Substituting (10) into (8) completes the proof. □

Returning to (7) it is now clear from Lemma 5 that

$$\rho_G = \lim_{x\to\infty} \sum_{1\le n_1\le x} \cdots \sum_{1\le n_e\le x} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r}$$

is absolutely convergent. In fact,

$$g(x) = x^v \rho_G + R + O(x^{v-1}\log^d x), \tag{11}$$

where

$$\rho_G = \sum_{n_1=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r},$$

and

$$|R| \le x^{v-1} \sum_{j=1}^{e} \sum_{n_1=1}^{\infty} \cdots \sum_{n_{j-1}=1}^{\infty} \sum_{n_j > x} \sum_{n_{j+1}=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r}.$$

Now

$$\rho_G = \sum_{m=1}^{\infty} \frac{1}{m} \sum_{N_1\cdots N_v = m} \mu(n_1)\cdots\mu(n_e) = \sum_{m=1}^{\infty} \frac{f_G(m)}{m}.$$

We note that $f_G(m)$ is multiplicative by Proposition 2. In a similar way to Lemma 5 we have $f_G(1) = 1, f_G(p) = 0$ and $f_G(p^\alpha) = 0$, for all $\alpha > v$. Thus, by the multiplicativity,

$$\rho_G = \sum_{m=1}^{\infty} \frac{f_G(m)}{m} = \prod_{p \text{ prime}} \left(1 + \frac{f_G(p^2)}{p^2} + \ldots + \frac{f_G(p^v)}{p^v}\right),$$

Therefore, by Lemma 3, we have

$$\rho_G = \prod_{p \text{ prime}} Q_G\left(\frac{1}{p}\right). \tag{12}$$

Substituting (12) into (11), it only remains to show that $|R| = O(x^{v-1}\log^d x)$.

We have

$$|R| \leq x^{v-1} \sum_{j=1}^{e} \sum_{n_1=1}^{\infty} \cdots \sum_{n_{j-1}=1}^{\infty} \sum_{n_j > x} \sum_{n_{j+1}=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r}.$$

All terms in the sum on j are analogous; so assuming that the first is the largest, we have

$$|R| \leq C_1 x^{v-1} \sum_{n_1 > x} \sum_{n_2=1}^{\infty} \sum_{n_{j+1}=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r},$$

where C_1 is a function of e and not x. So it suffices to show that

$$R_1 := \sum_{n_1 > x} \sum_{n_2=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r} = O(\log^d x). \tag{13}$$

We treat an edge $e_1 = \{r, s\}$ differently from the other edges. For a given $(n_1, \ldots, n_e)$ of squarefree numbers we have two special N_r,

$$N_r = \operatorname{lcm}(n_1, n_{\alpha_1}, \ldots n_{\alpha_k}), \quad N_s = \operatorname{lcm}(n_1, n_{\beta_1}, \ldots n_{\beta_k}).$$

We also remark that we may have $N_r = \operatorname{lcm}(n_1)$ or $N_s = \operatorname{lcm}(n_1)$.

For any edge e_j with $2 \leq j \leq e$ we define $d_j = \gcd(n_1, n_j)$. Since the n_j are squarefree, we have

$$n_j = d_j n'_j, \quad d_j | n_1, \quad \gcd(n_1, n'_j) = 1.$$

Then it is clear that

$$N_r = \operatorname{lcm}(n_1, d_{\alpha_1} n'_{\alpha_1}, \ldots, d_{\alpha_k} n'_{\alpha_k}) = n_1 \operatorname{lcm}(n'_{\alpha_1}, \ldots, n'_{\alpha_k}),$$

$$N_s = n_1 \operatorname{lcm}(n'_{\beta_1}, \ldots, n'_{\beta_l}).$$

For any other vertex with $t \neq r$ and $t \neq s$, we have

$$\begin{aligned} N_t &= \operatorname{lcm}(n_{t_1}, \ldots, n_{t_m}) = \operatorname{lcm}(d_{t_1} n'_{t_1}, \ldots, d_{t_m} n'_{t_m}) \\ &= \operatorname{lcm}(d_{t_1}, \ldots, d_{t_m}) \operatorname{lcm}(n'_{t_1}, \ldots, n'_{t_m}), \end{aligned}$$

where m varies with t. Substituting the equations for N_r, N_s and N_t into the definition of R_1 in (13) we obtain

$$\begin{aligned} R_1 &= \sum_{n_1 > x} \sum_{n_2=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1) \cdots \mu(n_e)| \frac{1}{N_r} \frac{1}{N_s} \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{N_t} \\ &= \sum_{n_1 > x} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} \sum_{n'_2=1}^{\infty} \cdots \sum_{n'_e=1}^{\infty} \frac{|\mu(n_2) \cdots \mu(n_e)|}{\operatorname{lcm}(n'_{\alpha_1}, \ldots, n'_{\alpha_k}) \operatorname{lcm}(n'_{\beta_1}, \ldots, n'_{\beta_l})} \\ &\qquad \times \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \ldots, d_{t_m}) \operatorname{lcm}(n'_{t_1}, \ldots, n'_{t_m})} \\ &= \sum_{n_1 > x} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \ldots, d_{t_m})} \\ &\qquad \times \sum_{n'_2=1}^{\infty} \cdots \sum_{n'_e=1}^{\infty} \frac{|\mu(d_2 n'_2) \cdots \mu(d_e n'_e)|}{\operatorname{lcm}(n'_{\alpha_1}, \ldots, n'_{\alpha_k}) \operatorname{lcm}(n'_{\beta_1}, \ldots, n'_{\beta_l})} \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(n'_{t_1}, \ldots, n'_{t_m})} \\ &\leq \sum_{n_1 > x} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} |\mu(d_2) \cdots \mu(d_e)| \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \ldots, d_{t_m})} \\ &\qquad \times \sum_{n'_2=1}^{\infty} \cdots \sum_{n'_e=1}^{\infty} \frac{|\mu(n'_2) \cdots \mu(n'_e)|}{\operatorname{lcm}(n'_{\alpha_1}, \ldots, n'_{\alpha_k}) \operatorname{lcm}(n'_{\beta_1}, \ldots, n'_{\beta_l})} \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(n'_{t_1}, \ldots, n'_{t_m})}. \end{aligned}$$

The product

$$\sum_{n'_2=1}^{\infty} \cdots \sum_{n'_e=1}^{\infty} \frac{|\mu(n'_2) \cdots \mu(n'_e)|}{\operatorname{lcm}(n'_{\alpha_1}, \ldots, n'_{\alpha_k}) \operatorname{lcm}(n'_{\beta_1}, \ldots, n'_{\beta_l})} \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(n'_{t_1}, \ldots, n'_{t_m})}$$

is finite by Lemma 5 (but this time considering the graph G without the edge $\{r, s\}$). Thus, for some constant C_1, we have

$$\begin{aligned} R_1 &\leq C_2 \sum_{n_1 > x} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} |\mu(d_2) \cdots \mu(d_e)| \prod_{\substack{1 \leq t \leq v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \ldots, d_{t_m})} \\ &= C_2 \sum_{n_1 > x} \frac{|\mu(n_1)|}{n_1^2} f_{G,e}(n_1), \end{aligned} \tag{14}$$

where the arithmetic function $f_{G,e}$ is defined as follows.

$$f_{G,e}(n) = \sum_{d_2|n} \cdots \sum_{d_e|n} |\mu(d_2)\cdots\mu(d_e)| \prod_{\substack{1\le t\le v \\ t\ne r,\ t\ne s}} \frac{1}{\operatorname{lcm}(d_{t_1},\ldots,d_{t_m})}.$$

We note that there is a factor $\operatorname{lcm}(d_{t_1},\ldots,d_{t_m})$ for each vertex other than r or s. The function $f_{G,e}$ is a multiplicative function. We have $f_{G,e}(p^k) = f_{G,e}(p)$ for any power of a prime p with $k \ge 2$, because in the definition of $f_{G,e}(p^k)$ only the divisors 1 and p of p^k give non-null terms. When $n = p$ we have

$$f_{G,e}(p) = 1 + \frac{A_1}{p} + \cdots + \frac{A_{v-2}}{p^{v-2}},$$

where A_i is the number of ways that

$$\prod_{\substack{1\le t\le v \\ t\ne r,\ t\ne s}} |\mu(d_2)\cdots\mu(d_e)| \operatorname{lcm}(d_{t_1},\ldots,d_{t_m}) = p^i,$$

where every divisor in the product $d_h \mid n = p$ can only be 1 or p. Clearly $A_i \le 2^{e-1}$ do not depend on p, and so there must be a number w, independent of p, such that

$$f_{G,e}(p^k) = f_{G,e}(p) \le \left(1 + \frac{1}{p}\right)^w.$$

Since $f_{G,e}$ is multiplicative we have, for any squarefree n,

$$f_{G,e}(n) \le \prod_{p|n} \left(1 + \frac{1}{p}\right)^w = \left(\frac{\sigma(n)}{n}\right)^w, \quad |\mu(n)| = 1. \tag{15}$$

Substituting (15) into (14) yields

$$R_1 \le C_2 \sum_{n>x}^{\infty} \frac{|\mu(n)|}{n^2} \left(\frac{\sigma(n)}{n}\right)^w \le C_2 \sum_{n>x}^{\infty} \frac{1}{n^2} \left(\frac{\sigma(n)}{n}\right)^w.$$

It is well known that $\sigma(n) = O(n \log\log n)$ (see, for example, the article by Gronwall [5]), and thus

$$R_1 = O\left(\frac{(\log\log x)^w}{x}\right). \tag{16}$$

Comparing (16) with (13) completes the proof of Theorem 1.

4 Calculations

We calculate the asymptotic proportion that 4 random positive integers exhibit 'square' pairwise coprimality conditions. That is, 4-tuples with

$$\gcd(a_1, a_2) = \gcd(a_2, a_3) = \gcd(a_3, a_4) = \gcd(a_4, a_1) = 1.$$

Here $G(V, E)$ be given by

$$V = \{1, 2, 3, 4\},\ E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 1\}\}.$$

As shown in Theorem 1 and using Section 2,

$$Q_G\left(\frac{1}{p}\right) = \sum_{F \subset E} (-1)^{\mathrm{card}(F)} \left(\frac{1}{p}\right)^{v(F)},$$

where $v(F)$ is the number of non-isolated vertices of F.

Next we examine each $F \subset E$ to compute its contribution to $Q_G(z)$. This is shown in the following table:

Table 1: Subsets of edges and the polynomial $Q_G(z)$

$F \subset E$	$\mathrm{card}(F)$	$v(F)$	term $= (-1)^{\mathrm{card}(F)} z^{v(F)}$
$\emptyset$	0	0	1
$\{\{1,2\}\}$, $\{\{2,3\}\}$, $\{\{3,4\}\}$, $\{\{4,1\}\}$	1	2	$-4z^2$
$\{\{1,2\},\{2,3\}\}$, $\{\{2,3\},\{3,4\}\}$, $\{\{3,4\},\{4,1\}\}$, $\{\{4,1\},\{1,2\}\}$	2	3	$4z^3$
$\{\{1,2\},\{3,4\}\}$, $\{\{2,3\},\{4,1\}\}$,	2	4	$2z^4$
$\{\{1,2\},\{2,3\},\{3,4\}\}$, $\{\{2,3\},\{3,4\},\{4,1\}\}$, $\{\{3,4\},\{4,1\},\{1,2\}\}$, $\{\{4,1\},\{1,2\},\{2,3\}\}$	3	4	$-4z^4$
E	4	4	z^4
			$Q_G(z) = 1 - 4z^2 + 4z^3 - z^4$

Putting this all together we have

$$\rho_G = \prod_{p \text{ prime}} \left(1 - \frac{4}{p^2} + \frac{4}{p^3} - \frac{1}{p^4}\right).$$

This gives ρ_G as an Euler product. As shown in the article by Wrench [13], Euler products such as ρ_G can be computed to high precision.

5 Acknowledgement

The authors would like to thank Igor Shparlinski and an anonymous referee for some useful comments. The second author would like to thank the first author and his colleagues for their hospitality during a pleasant visit to Seville. The first author is supported by MINECO grant MTM2012-30748.

References

[1] J. -Y. Cai and E. Bach, On testing for zero polynomials by a set of points with bounded precision, in COCOON 2001, Lect. Notes Comput Sci., Vol. 2108, Springer-Verlag 2001, pp. 473–482.

[2] C. Ding, D. Pei, and A. Salomaa, *The Chinese Remainder Theorem*, World Scientific, 1996.

[3] J. L. Fernández and P. Fernández, Equidistribution and coprimality. Preprint, 2013, available at http://arxiv.org/abs/1310.3802.

[4] T. Freiberg, The probability that 3 positive integers are pairwise noprime, (unpublished manuscript).

[5] T. H. Gronwall, Some asymptotic expressions in the theory of numbers, *Trans. Amer. Math. Soc.* **14** (1913), 113–122.

[6] R. Heyman, Pairwise non-coprimality of triples. Preprint, 2013, available at http://arxiv.org/abs/1309.5578.

[7] J. Hu, The probability that random positive integers are k-wise relatively prime, *In. J. Number Theory* **9** (2013), 1263–1271.

[8] J. Hu, Pairwise relative primality of positive integers. Preprint, 2014, available at http://arxiv.org/abs/1406.3113.

[9] V. J. Katz, *A History of Mathematics (Brief Edition)*, Pearson/Addison-Wesley, 2003.

[10] D. E. Knuth, *The Art of Computer Programming*, Volume 2: *Seminumerical Algorithms*, 3rd edition, Addison-Wesley, 1998.

[11] P. Moree, Counting carefree couples. Preprint, 2014, available at http://arxiv.org/abs/math/0510003.

[12] L. Tóth, The probability that k positive integers are pairwise relatively prime, *Fibonacci Quart.* **40** (2002), 13–18.

[13] J. W. Wrench Jr., Evaluation of Artin's constant and the twin prime conjecture, *Math Comp.* **15** (1961), 396–398.

2010 *Mathematics Subject Classification*: Primary 11N25; Secondary 11N36, 11N37, 11A25.
Keywords: pairwise coprimality, arithmetic function.

(Concerned with sequences A065473, A256390, A256391, and A256392.)

Received April 1 2015; revised versions received September 10 2015; September 16 2015. Published in *Journal of Integer Sequences*, September 16 2015.

Return to Journal of Integer Sequences home page.