The Greatest Common Divisor
of \( k \) Positive Integers

Rafael Jakimczuk

División Matemática, Universidad Nacional de Luján
Buenos Aires, Argentina

Copyright © 2018 Rafael Jakimczuk. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

We study using the inclusion-exclusion principle and very elementary methods the distribution of \( k \) positive integers not exceeding \( x \) with the same greatest common divisor.

Mathematics Subject Classification: 11A99, 11B99

Keywords: \( k \)-tuples of positive integers, sets of \( k \) positive integers, greatest common divisor

1 Introduction and Preliminary Notes

Let \( k \geq 2 \) an arbitrary but fixed positive integer. Let us consider a \( k \)-tuple of positive integers \((a_1, \ldots, a_k)\) where \( 1 \leq a_i \leq x \) \( (i = 1, \ldots, k) \). The number of these \( k \)-tuples such that \( \gcd(a_1, \ldots, a_k) = g \geq 1 \) will be denoted \( N_{g,k}(x) \) and the number of these \( k \)-tuples such that \( \gcd(a_1, \ldots, a_k) > 1 \) will be denoted \( N_{0,k}(x) \). On the other hand, let us consider a set of \( k \) distinct positive integers \( \{a_1, \ldots, a_k\} \) where \( 1 \leq a_i \leq x \) \( (i = 1, \ldots, k) \). The number of these sets such that \( \gcd(a_1, \ldots, a_k) = g \geq 1 \) will be denoted \( D_{g,k}(x) \) and the number of these sets such that \( \gcd(a_1, \ldots, a_k) > 1 \) will be denoted \( D_{0,k}(x) \).

Let us consider a positive integer \( n \) such that its prime factorization is \( n = q_1^{r_1} \cdots q_s^{r_s} \). The number of \( k \)-tuples of positive integers \((a_1, \ldots, a_k)\) not exceeding \( x \) such that \( \gcd(a_1, \ldots, a_k) = 1 \) and \( \gcd(a_i, n) = 1 \) \( (i = 1, \ldots, k) \) will be denoted \( P_{k,n}(x) \). The number of \( k \)-tuples of positive integers \((a_1, \ldots, a_k)\) not exceeding \( x \) such that \( \gcd(a_1, \ldots, a_k) = 1 \) and \( \gcd(a_i, n) > 1 \) \( (i = 1, \ldots, k) \) will be denoted \( P_{0,k,n}(x) \).
not exceeding $x$ such that the $a_i$ are pairwise relatively prime and such that $\gcd(a_i, n) = 1$ for $i = 1, \ldots, k$ will be denoted $P_k^{(n)}(x)$. Note that if $n = 1$ then $P_k^{(1)}(x)$ is the number of $k$-tuples of positive integers $(a_1, \ldots, a_k)$ not exceeding $x$ such that the $a_i$ are pairwise relatively prime.

We shall need the following well-known theorem.

**Theorem 1.1** (Inclusion-exclusion principle) Let $S$ be a set of $N$ distinct elements, and let $S_1, \ldots, S_r$ be arbitrary subsets of $S$ containing $N_1, \ldots, N_r$ elements, respectively. For $1 \leq i < j < \cdots < l \leq r$, let $S_{ij\ldots l}$ be the intersection of $S_i, S_j, \ldots, S_l$ and let $N_{ij\ldots l}$ be the number of elements of $S_{ij\ldots l}$. Then the number $K$ of elements of $S$ not in any of $S_1, \ldots, S_r$ is

$$K = N - \sum_{1 \leq i \leq r} N_i + \sum_{1 \leq i < j \leq r} N_{ij} - \sum_{1 \leq i < j < k \leq r} N_{ijk} + \cdots + (-1)^r N_{12\ldots r}$$

**Proof.** See, for example, [3] (page 84) or [2] (page 233).

## 2 Main Results

Nymann [4] proved the following theorem (with a better error term) using a Möbius inversion formula. In this note, we prove the theorem using the inclusion-exclusion principle, the proof is very elementary and short. In this proof $p_n$ denotes the $n$-th prime, $\zeta(s)$ denotes the Riemann zeta function and $\lfloor . \rfloor$ denotes the integer-part function.

**Theorem 2.1** Let $k \geq 2$ an arbitrary but fixed integer. The following asymptotic formula holds.

$$N_{1,k}(x) = \frac{1}{\zeta(k)} x^k + o(x^k)$$  \hspace{1cm} (1)

**Proof.** Let $A_{p_h,k}(x)$ be the number of $k$-tuples of $k$ positive integers not exceeding $x$ such that the least prime factor in their greatest common divisor is $p_h$. The inclusion-exclusion principle gives

$$A_{p_h,k}(x) = \left\lfloor \frac{x}{p_h} \right\rfloor^k - \sum_{1 \leq j \leq h-1} \left\lfloor \frac{x}{p_h p_j} \right\rfloor^k + \sum_{1 \leq i < j \leq h-1} \left\lfloor \frac{x}{p_h p_i p_j} \right\rfloor^k - \cdots$$

$$= x^k \frac{1}{p_h^k} \prod_{i=1}^{h-1} \left( 1 - \frac{1}{p_i^k} \right) + o(x^k)$$  \hspace{1cm} (2)

Note that

$$A_{p_h,k}(x) \leq \left\lfloor \frac{x}{p_h} \right\rfloor^k \leq \frac{x^k}{p_h^k}$$  \hspace{1cm} (3)
The greatest common divisor of \( k \) positive integers

The following equation can be proved without difficulty using mathematical induction

\[
\sum_{h=1}^{n} \frac{1}{p_h^k} \prod_{i=1}^{h-1} \left( 1 - \frac{1}{p_i^k} \right) = 1 - \prod_{i=1}^{n} \left( 1 - \frac{1}{p_i^k} \right)
\]

Therefore we have

\[
\sum_{h=1}^{\infty} \frac{1}{p_h^k} \prod_{i=1}^{h-1} \left( 1 - \frac{1}{p_i^k} \right) = 1 - \frac{1}{\zeta(k)}
\] (4)

Let \( \epsilon > 0 \). We shall choose \( n \) such that the following inequality holds

\[
\sum_{h=n+1}^{\infty} \frac{1}{p_h^k} \leq \epsilon
\] (5)

We have (see (2) and (4))

\[
N_{0,k}(x) = \sum_{2 \leq p_h \leq x} A_{p_h,k}(x) = x^k \sum_{1 \leq h \leq n} \frac{1}{p_h^k} \prod_{i=1}^{h-1} \left( 1 - \frac{1}{p_i^k} \right) + o(x^k) + F(x)
\]

\[= \left( 1 - \frac{1}{\zeta(k)} \right) x^k - x^k \sum_{h=n+1}^{\infty} \frac{1}{p_h^k} \prod_{i=1}^{h-1} \left( 1 - \frac{1}{p_i^k} \right) + o(x^k) + F(x) \] (6)

where (see (3))

\[0 \leq F(x) \leq x^k \sum_{h=n+1}^{\infty} \frac{1}{p_h^k} \leq \epsilon x^k \] (7)

Equations (6), (7) and (5) give

\[
\left| \frac{N_{0,k}(x)}{x^k} - \left( 1 - \frac{1}{\zeta(k)} \right) \right| \leq \epsilon + \epsilon = 3\epsilon \quad (x \geq x_\epsilon) \] (8)

Consequently, since \( \epsilon > 0 \) can be arbitrarily small, equation (8) gives

\[
N_{0,k}(x) = \left( 1 - \frac{1}{\zeta(k)} \right) x^k + o(x^k)
\] (9)

Now

\[
N_{1,k}(x) + N_{0,k}(x) = \lfloor x \rfloor^k = x^k + o(x^k)
\] (10)

Equations (9) and (10) give (1). The theorem is proved.

**Remark 2.2** Since \( \zeta(k) \to 1 \), if \( k \) is large the number of \( k \)-tuples not exceeding \( x \) such that the gcd of the \( a_i \) is greater than 1 is negligible compared with the number \( k \)-tuples not exceeding \( x \) such that gcd of the \( a_i \) is 1.
Corollary 2.3 The following asymptotic formula holds.

\[ N_{g,k}(x) = \frac{1}{g^k \zeta(k)} x^k + o(x^k) \]

Proof. We have \( N_{g,k}(x) = N_{1,k} \left( \frac{x}{g} \right) \). The corollary is proved.

Theorem 2.4 The following asymptotic formula holds.

\[ D_{1,k}(x) = \frac{1}{k! \zeta(k)} x^k + o(x^k) \]

Proof. The proof is the same as the proof of Theorem 2.1. In this case, in equation (2) (inclusion-exclusion principle), we substitute

\[ \left\lfloor \frac{x}{p_h} \right\rfloor \]

by

\[ \frac{1}{k!} \left( \left\lfloor \frac{x}{p_h} \right\rfloor \left( \left\lfloor \frac{x}{p_h} \right\rfloor - 1 \right) \ldots \left( \left\lfloor \frac{x}{p_h} \right\rfloor - (k - 1) \right) \right) \]

etc. Note also that

\[ D_{0,k}(x) + D_{1,k}(x) = \binom{\left\lfloor \frac{x}{k} \right\rfloor}{k} = \frac{1}{k!} x^k + o(x^k) \]

The theorem is proved.

Corollary 2.5 The following asymptotic formula holds.

\[ D_{g,k}(x) = \frac{1}{k! g^k \zeta(k)} x^k + o(x^k) \]

Theorem 2.6 The following asymptotic formula holds.

\[ P_{k,n}(x) = \frac{1}{\zeta(k)} \prod_{i=1}^{s} \left( \frac{1 - \frac{1}{q_i}}{1 - \frac{1}{q_i}} \right)^k x^k + o(x^k) \quad (11) \]

Proof. Let \( N(x) \) be the number of numbers not exceeding \( x \) and relatively prime to \( n \). The inclusion-exclusion principle gives

\[ N(x) = \left\lfloor x \right\rfloor - \sum_{1 \leq i \leq s} \left\lfloor \frac{x}{q_i} \right\rfloor + \sum_{1 \leq i < j \leq s} \left\lfloor \frac{x}{q_i q_j} \right\rfloor - \cdots = x \prod_{i=1}^{s} \left( 1 - \frac{1}{q_i} \right) + o(x) \quad (12) \]
Let us consider a positive integer $C$ relatively prime to $n$ such that its prime factorization is $c_1^{r_1} \cdots c_t^{r_t}$. For sake of simplicity we put $y = \frac{x}{c_1^{r_1} \cdots c_t^{r_t}}$. Then the number of numbers not exceeding $x$ relatively prime to $n$ and multiple of $C$ is (inclusion exclusion principle)

$$[y] - \sum_{1 \leq i \leq s} \left\lfloor \frac{y}{q_i} \right\rfloor + \sum_{1 \leq i < j \leq s} \left\lfloor \frac{y}{q_i q_j} \right\rfloor - \cdots = \frac{x}{c_1 \cdots c_t} \prod_{i=1}^{s} \left( 1 - \frac{1}{q_i} \right) + o(x) \quad (13)$$

In this proof $p_n$ denotes the $n$-th prime. Let $p_h$ be the $h$-th prime, where $p_h \neq q_i$ ($i = 1, \ldots, s$). For sake of simplicity we put $S = \prod_{i=1}^{s} \left( 1 - \frac{1}{q_i} \right)$. Let $A_{p_h}(x)$ be the number of $k$-tuples $(a_1, \ldots, a_k)$ not exceeding $x$ such that $\gcd(a_1, n) = 1$ ($i = 1, \ldots, k$) and such that the least prime factor in their greatest common divisor is $p_h$. The inclusion-exclusion principle and equation (13) give

$$A_{p_h}(x) = \left( \frac{x}{p_h} S + o(x) \right)^k - \sum_{1 \leq j \leq h-1, p_j \neq q_i (i=1, \ldots, s)} \left( \frac{x}{p_h p_j} S + o(x) \right)^k + \cdots$$

$$= x^k \prod_{i=1}^{s} \left( 1 - \frac{1}{q_i} \right)^k \frac{1}{p_h^k} \prod_{1 \leq j \leq h-1, p_j \neq q_i (i=1, \ldots, s)} \left( 1 - \frac{1}{p_j^k} \right) + o(x^k) \quad (14)$$

Let $N_0(x)$ be the number of $k$-tuples $(a_1, \ldots, a_k)$ not exceeding $x$ such that $\gcd(a_i, n) = 1$ ($i = 1, \ldots, k$) and such that $\gcd(a_1, \ldots, a_k) > 1$. Equation (14) and an identical proof as in Theorem 2.1 give

$$N_0(x) = \left( \sum_{p_h \neq q_i (i=1, \ldots, s)} \frac{1}{p_h^k} \prod_{1 \leq j \leq h-1, p_j \neq q_i (i=1, \ldots, s)} \left( 1 - \frac{1}{p_j^k} \right) \right) \prod_{i=1}^s \left( 1 - \frac{1}{q_i} \right)^k x^k$$

$$+ \quad o(x^k) \quad (15)$$

Now, we have the equality

$$\sum_{p_h \neq q_i (i=1, \ldots, s)} \frac{1}{p_h^k} \prod_{1 \leq j \leq h-1, p_j \neq q_i (i=1, \ldots, s)} \left( 1 - \frac{1}{p_j^k} \right) = 1 - \prod_{p_j \neq q_i (i=1, \ldots, s)} \left( 1 - \frac{1}{p_j^k} \right) \quad (16)$$

since both series have the same terms. The term $r^k_1 \cdots r^k_t$, where the different primes $r_i (i = 1, \ldots, t)$ satisfy the inequality $r_1 > \cdots > r_t$ is obtained in the series of the left hand when $p_h = r_1$.

Note that (see equation(12))

$$N_0(x) + P_{k,n}(x) = x^k \prod_{i=1}^{s} \left( 1 - \frac{1}{q_i} \right)^k x^k + o(x^k) \quad (17)$$

Equations (15), (16) and (17) give

$$P_{k,n}(x) = \left( \prod_{p_j \neq q_i (i=1, \ldots, s)} \left( 1 - \frac{1}{p_j^k} \right) \right) \prod_{i=1}^s \left( 1 - \frac{1}{q_i} \right)^k x^k + o(x^k)$$
\[
\frac{1}{\zeta(k)} \prod_{i=1}^{s} \left(1 - \frac{1}{q_i} \right)^k x^k + o(x^k)
\]

That is, equation (11). The theorem is proved.

**Remark 2.7** Note that if \( n \) is fixed then we have

\[
\lim_{k \to \infty} \frac{1}{\zeta(k)} \prod_{i=1}^{s} \left(1 - \frac{1}{q_i} \right)^k \prod_{i=1}^{s} \left(1 - \frac{1}{q_i^k} \right) = 0
\] (18)

Tóth [5] proved, using mathematical induction, the following theorem (with a better error term)

**Theorem 2.8** The following asymptotic formulae hold.

\[
P_k^{(n)}(x) = A_k \prod_{i=1}^{s} \left(1 - \frac{k}{q_i + k - 1} \right) x^k + o(x^k)
\]

\[
P_k^{(1)}(x) = A_k x^k + o(x^k)
\]

where

\[
A_k = \prod_{p} \left(1 - \frac{1}{p} \right)^{k-1} \left(1 + \frac{k-1}{p} \right)
\]

Now, we give a simple proof of the following theorem.

**Theorem 2.9** The following limit holds.

\[
\lim_{k \to \infty} A_k = 0
\] (19)

The following inequality holds.

\[
A_k \leq \frac{k + 2}{2^k}
\] (20)

Proof. The number of even numbers not exceeding \( x \) is \( \left\lfloor \frac{x}{2} \right\rfloor = \frac{x}{2} + o(x) \) and the number of odd numbers not exceeding \( x \) is \( \left| x - \left\lfloor \frac{x}{2} \right\rfloor \right| = \frac{x}{2} + o(x) \). Therefore the number of \( k \)-tuples \( (a_1, \ldots, a_k) \) not exceeding \( x \) with all \( a_i \) odd is \( N_1(x) = \frac{x^k}{2^k} + o(x^k) \) and the number of \( k \)-tuples with only one even \( a_i \) is \( N_2(x) = \frac{k+1}{2^k} x^k + o(x^k) \). From this inequality we obtain inequality (20). Limit (19) is an immediate consequence of inequality (20). The theorem is proved.
Remark 2.10  Since $\zeta(k) \to 1$ and $A_k \to 0$ we see that if $k$ is large then the number of $k$-tuples $(a_1, \ldots, a_k)$ not exceeding $x$ such that the $a_i$ are pairwise relatively prime is negligible compared with the number of $k$-tuples $(a_1, \ldots, a_k)$ not exceeding $x$ such that $\gcd(a_1, \ldots, a_k) = 1$.

In the opposite side, let us consider the number of $k$-tuples $(a_1, \ldots, a_k)$ not exceeding $x$ such that if $i \neq j$ ($i = 1, \ldots, k$) ($j = 1, \ldots, k$) then $\gcd(a_i, a_j) > 1$. Let $B_k(x)$ be the number of these $k$-tuples not exceeding $x$. We have the following simple theorem.

**Theorem 2.11**  The following inequality hold

If $k$ is even

$$\frac{B_k(x)}{x^k} \leq 2 \left( 1 - \frac{1}{\zeta(2)} \right)^{k/2} \quad (x \geq x_k)$$

If $k$ is odd

$$\frac{B_k(x)}{x^k} \leq 2 \left( 1 - \frac{1}{\zeta(2)} \right)^{(k-1)/2} \quad (x \geq x_k)$$

Therefore if $B_k(x) = B_k x^k + o(x^k)$, for a positive constant $B_k$, then $B_k \to 0$.

Proof. If $k = 2$ is well-known that $B_2(x) = \left( 1 - \frac{1}{\zeta(2)} \right) x^2 + o(x^2)$. Therefore if $k$ is even we have $B_k(x) \leq (B_2(x))^{k/2} = \left( 1 - \frac{1}{\zeta(2)} \right)^{k/2} x^k + o_k(x^k)$, since there are $k/2$ consecutive pairs $a_i, a_{i+1}$ ($i = 1,3,\ldots,k-1$) in the $k$-tuple $(a_1, \ldots, a_k)$.

If $k$ is odd in the same way we obtain

$$B_k(x) \leq (B_2(x))^{(k-1)/2} x = \left( 1 - \frac{1}{\zeta(2)} \right)^{(k-1)/2} x^k + o_k(x^k).$$

The theorem is proved.

To finish, we give another proof of Theorem 2.1 using mathematical induction. Before, we need the following lemma.

**Lemma 2.12**  Let $k \geq 2$ an arbitrary but fixed positive integer. The following asymptotic formula holds.

$$\sum_{n>x} \frac{1}{n^k} = O \left( x^{1-k} \right) \quad (x \geq 1) \quad (21)$$

Let $k$ an arbitrary but fixed positive integer. The following asymptotic formula holds.

$$\sum \prod_{n \leq x \atop p \mid n} \left( 1 - \frac{1}{p^k} \right) = \frac{1}{\zeta(k+1)} x + o(x) \quad (22)$$
Proof. Equation (21) is proved in [1, Chapter 3, page 55]. Equation (22) can be proved as [1, Chapter 3, Theorem 3.7, page 62] since we have

\[
\sum_{n \leq x} n^k \prod_{p\mid n} \left( 1 - \frac{1}{p^k} \right) = \sum_{n \leq x} \left( \sum_{d\mid n} \mu(d) \left( \frac{n}{d} \right)^k \right)
\]

\[= \ldots = \frac{1}{(k+1)\zeta(k+1)} x^{k+1} + o(x^{k+1})\]

From here, using partial summation, we obtain (22). The lemma is proved.

We also need the following definition. Let \( N_{n,k+1}^{k+1}(x) \) be the number of \((k+1)-\)tuples \((a_1, \ldots, a_{k+1})\) such that \(\gcd(a_1, \ldots, a_{k+1}) = 1\) and \(a_1 = n\).

**Theorem 2.13** If \(n = 1\) we have

\[N_{1,k+1}^{k+1}(x) = x^k + o(x^k)\]
(23)

If \(n \geq 2\) we have

\[N_n^{k+1} = x^k \prod_{p\mid n} \left( 1 - \frac{1}{p^k} \right) + o(x^k) \quad (n \leq x)\]
(24)

Finally, we have

\[N_{1,k}(x) = \frac{1}{\zeta(k)} x^k + o(x^k)\]
(25)

Proof. The theorem is true for \(k = 2\). Suppose the theorem is true for \(k\), then we shall prove that the theorem is also true for \(k+1\). Therefore, we have

\[N_{1,k}(x) = \frac{1}{\zeta(k)} x^k + f(x)x^k\]
(26)

where \(|f(x)| \leq M_1\) and \(\lim_{x \to \infty} f(x) = 0\). Equation (26) gives

\[N_n^{k+1} = N_{1,k} \left( \frac{x}{g} \right) = \frac{1}{g^k\zeta(k)} x^k + f \left( \frac{x}{g} \right) \frac{1}{g^k} x^k\]
(27)

Note that (see (21))

\[\sum_{g > x, (g,x) = 1} \frac{1}{g^k} \leq \sum_{g > x} \frac{1}{g^k} \leq M_2 x^{1-k}\]
(28)

On the other hand, let us consider the function

\[F_n(x) = \sum_{g \leq x, (g,n) = 1} f \left( \frac{x}{g} \right) \frac{1}{g^k}\]
(29)
The greatest common divisor of \( k \) positive integers

We have

\[
|F_n(x)| \leq \sum_{g \leq x, (g,n)=1} |f \left( \frac{x}{g} \right) | \frac{1}{g^k} \leq \sum_{g \leq x} \left| \frac{1}{g^k} \right| = \sum_{y \leq \sqrt{x}} \left| \frac{1}{f \left( \frac{x}{g} \right) g^k} \right| \\
+ \sum_{\sqrt{x} < g \leq x} \left| \frac{1}{g^k} \right| \leq \epsilon \zeta(k) + M_1 \epsilon \leq \epsilon' \quad (x \geq x_{\epsilon'})
\]

where \( \epsilon > 0 \) and consequently \( \epsilon' > 0 \) can be arbitrarily small. Hence \( \lim_{x \to \infty} F_n(x) = 0 \). Using equations (26), (27), (28) and (29) we find that

\[
N^{k+1}_n(x) = \sum_{1 \leq g \leq x, (g,n)=1} N_{g,k}(x) = x^k \prod_{p|n} \left( 1 - \frac{1}{p^k} \right) + o_n(x^k) \quad (n \leq x) \quad (30)
\]

That is, equation (24). Using equations (30), (23) and (22) we obtain

\[
N_{1,k+1}(x) = \sum_{1 \leq n \leq x} N^{k+1}_n(x) = \frac{1}{\zeta(k+1)} x^{k+1} + o(x^{k+1})
\]

The theorem is proved.

Acknowledgements. The author is very grateful to Universidad Nacional de Luján.

References


Received: March 11, 2018; March 28, 2018