The lattice points of an n–dimensional tetrahedron †

by

Andrew Granville

at the Institute for Advanced Study in Princeton.

Summary

We show that the number of ordered m-tuples of points on the integer lattice, inside or on the n–dimensional tetrahedron bounded by the hyperplanes $X_1 = 0, X_2 = 0, \ldots X_n = 0$ and $w_1X_1 + w_2X_n + \ldots + w_nX_n = X$, with the property that, for each j, no more than k such points have non–zero jth ordinate, is asymptotically

$$\left\{ \prod_{j=1}^{n} \left(\frac{X}{w_j} \right) \right\}^k \times \sum \binom{n}{\mathbf{c}} \frac{1}{\prod_{i=1}^{m} d_i!}$$

as $X \to \infty$, where $\binom{n}{\mathbf{c}}: = n!/\prod c_I!$, this product and the sum above are taken over all sets $\{c_I : I \subseteq \{1, \ldots m\}, |I| = k\}$ of non–negative integers which sum to n, and $d_i: = \sum_{I:\ i \in I} c_I$ for each i.

As a consequence we deduce estimates for functions that have been used to provide lower bounds for the smallest exception to the first case of Fermat's Last Theorem.

---

† AMS Subject Classification (1980): 11P21

The lattice points of an n–dimensional tetrahedron

by

Andrew Granville *

at the Institute for Advanced Study in Princeton.

We count sets of lattice points, that satisfy certain orthogonality conditions, in n–dimensional tetrahedra. Our estimates are related to studies of Fermat's Last Theorem.

1. Introduction.

In this paper we consider the set of integer lattice points inside or on the boundary of the n–dimensional tetrahedron bounded by the hyperplanes

(1.1) $$X_1 = 0, \quad X_2 = 0, \ \ldots \ , \quad X_n = 0$$

and

(1.2) $$w_1 X_1 + w_2 X_n + \ldots + w_n X_n = X$$

where $w_1, w_2, \ldots, w_n$ are given positive real numbers. In other words, the n–tuples of non–negative integers $(a_1, a_2, \ldots, a_n)$ for which

(1.3) $$a_1 w_1 + a_2 w_2 + \ldots + a_n w_n \leq X.$$

Our interest in this question comes from number theory for, if each $w_j = \log p_j$ for some prime p_j (with the p_j's distinct), then this is equivalent to considering the set of positive integers $\leq e^X$, whose prime factors belong to $P = \{p_1, p_2, \ldots, p_n\}$. In particular, if P is the set of primes up to some prime y, then the question of estimating the size of this set has received considerable attention (see [No] or [HT], for instance).

* The author is supported, in part, by the National Science Foundation (grant number DMS–8610730)

The following simple arguments allow us to obtain bounds on the number of integer lattice points within our tetrahedron:

Draw a box, of size 1 in each dimension, in the positive direction from each lattice point in our tetrahedron. The resulting shape S has volume equal to the number of lattice points. Now the tetrahedron, which we began with, is clearly contained inside S and so provides a lower bound for the volume of S; that is

$$\text{vol } S \ \geq \ X^n \ / \ n!p(w) \tag{1.4}$$

where $p(w) := w_1 w_2 \dots w_n$. On the other hand, S is contained in the tetrahedron defined by the bounding hyperplanes in (1.1) together with

$$w_1(X_1 - 1) + w_2(X_2 - 1) + \ldots + w_n(X_n - 1) \leq X, \tag{1.2$'$}$$

and so we get the upper bound

$$\text{vol } S \ \leq \ (X + s(w))^n \ / \ n!p(w) \tag{1.5}$$

where $s(w) := w_1 + w_2 + \ldots + w_n$. Thus, in the range

$$X \ \gg ns(w), \tag{1.6}$$

the number of lattice points is

$$\frac{X^n}{n!p(w)} \ \left\{1 + O\left(\frac{ns(w)}{X}\right)\right\}. \tag{1.7}$$

(This argument is usually credited to [En], though it is implicit in earlier works.)

Upper and lower bounds that improve those above were given in the beautiful paper [Le] of D.H. Lehmer. It is, however, impossible to obtain much stronger estimates, in general: Take each $w_i = 1$, then the number of lattice points is

$$\begin{aligned}\binom{[X]+n}{n} &= \frac{1}{n!}\left([X]^n + \binom{n+1}{2}[X]^{n-1} + O(X^{n-2})\right)\\ &= \frac{1}{n!}\left(X^n + \left(\binom{n+1}{2} - n\{X\}\right) X^{n-1} + O(X^{n-2})\right)\end{aligned}$$

where $\{X\} := X - [X]$ denotes the fractional part of X. Thus the coefficient of X^{n-1} 'oscillates' as $X \to \infty$. By a similar argument it may be shown that this coefficient 'oscillates' as $X \to \infty$, whenever the ratios w_i/w_j are all rational; and otherwise this coefficient is fixed (see [HL]). Spencer [Sp] showed that for 'almost all' choices of the w_i, one can obtain an asymptotic series that counts the points in our tetrahedron with error $O(\log^{n+\varepsilon} X)$; however one can also exhibit sets of w_i, linearly independent over the rationals, such that the coefficient of X^{n-2} 'oscillates' as $X \to \infty$. We do not investigate such questions here; we just note that there are significant difficulties when trying to improve (1.7).

Estimates for the size of the set of lattice points, when w_j is the logarithm of the jth smallest prime, have many applications in number theory — for instance, to finding large gaps between primes, to Waring's problem, to primality testing and factoring algorithms, to finding 'popular' values for Euler's totient function, as well as to bounds for the least prime kth power residues and non–residues (mod n) (when k divides $\varphi(n)$). This last application leads to a method of obtaining lower bounds for the exponent in any exception to the first case of Fermat's Last Theorem. The method goes as follows:

In 1909, Wieferich showed that if the first case of Fermat's Last Theorem is false for prime exponent p (that is that there exist integers x, y and z, coprime to p, such that $x^p + y^p = z^p$) then 2 is a pth power residue (mod p^2); and this has been extended recently [GM] to q is a pth power residue for each prime $q \le 89$. There are only p residue classes (mod p^2) whose entries are pth power residues, so we get a contradiction if we can show that the primes ≤ 89 generate more than p residue classes (mod p^2). Thus, by counting those integers $\le p^2$ with only such 'small' prime factors, Lehmer and Lehmer [LL] gave lower bounds on p for which the first case of Fermat's Last Theorem is false. In 1948, Gunderson [Gu] instead counted pairs of coprime integers $\le p$ with only 'small' prime factors, and improved the Lehmers' result. Recently Coppersmith [Co] counted pairs (m, n) of coprime integers, with only 'small' prime factors, satisfying $m^2 + n^2 \le p^2$, and got the best result yet — the first case of Fermat's Last Theorem is true for all exponents $\le 7.568 \times 10^{17}$.

Gunderson and Coppersmith both developed interesting methods to obtain strong lower bounds for the functions that they defined, but did not obtain asymptotic estimates.

In [Gr] we obtained sharp estimates for the number of pairs of coprime integers $\leq x$, free of prime factors $> y$, when x is 'small' ($x < e^{y^{1/(2+\varepsilon)}}$), and here we shall do so when x is 'large' ($x > e^{y^2}$) — the range in–between is much harder, and probably there is no 'smooth' estimate there. We use combinatorial methods to provide upper and lower bounds for a much more general function:

2. The results.

Theorem. *Suppose that k is an integer ≥ 2 and $w_1, w_2, \dots w_n$ and $x_1 \leq x_2 \leq \dots \leq x_m$ are positive real numbers such that (1.6) is satisfied for $X = x_1$. The number of ordered sets $(A_1, A_2, \dots, A_m)$ of n–vectors of non–negative integers (that is $A_i = (a_{i1}, \dots, a_{in})$) such that*

$$a_{i1}w_1 + a_{i2}w_2 + \dots + a_{in}w_n \leq x_i \tag{2.1}$$

for each i, and such that a_{ij} is non–zero for no more than k values of i for each j, is given by

$$\left\{1 + O\left(\frac{ns(w)}{X}\right)\right\} \times \frac{1}{p(w)^k} \times \sum \binom{n}{\mathbf{c}} \frac{1}{\prod_{i=1}^m d_i!} \tag{2.2}$$

where $\binom{n}{\mathbf{c}}:= n!/\prod c_I!$, this product and the sum in (2.2) are taken over all sets $\{c_I : I \subseteq \{1, \dots m\},\ |I| = k\}$ of non–negative integers which sum to n, and $d_i := \sum_{I:\ i\in I} c_I$ for each i.

The number theory applications come from

Corollary 1. *Suppose that k is an integer ≥ 2, $P := \{p_1, p_2, \dots, p_n\}$ is a set of n primes, and x a real number satisfying $\log x \gg n\log(\Pi_P)$, where Π_P is the product of the elements in P. The number of ordered sets $(r_1, r_2, \dots, r_m)$ of positive integers $\leq x$, all of whose prime factors come from the set P, such that no $k+1$ have a common divisor, is given by*

$$\left\{1 + O\left(\frac{n\log \Pi_P}{\log x}\right)\right\} \times \left(\prod_{p\in P} \frac{\log x}{\log p}\right)^k \times \sum \binom{n}{\mathbf{c}} \frac{1}{\prod_{i=1}^m d_i!}, \tag{2.3}$$

where the sum, c_I and d_i are as in the Theorem.

Corollary 1 follows from the Theorem by taking each $w_i = \log p_i$ and each $x_i = \log x$.

We have been unable to find a more elegant expression for the sum in (2.3); though the current one is suitable for examining certain special cases:

(i) <u>$k = m$</u>: Here we are just counting the number of ordered m–tuples of lattice points, and the main term in (2.3) is $\left(\frac{1}{n!}\prod_{p\in P}\frac{\log x}{\log p}\right)^m$ as expected.

(ii) <u>$k = m - 1$</u>: Now we are counting the number of ordered m–tuples of such integers which do not all have a common factor. Letting $e_i = c_I$ where $I = \{1, \dots m\} \setminus \{i\}$ for each i, the sum in (2.3) becomes

$$\frac{1}{n!^{m-1}} \sum_{e_1+\ldots+e_m=n} \prod_i \binom{n}{e_i}.$$

This last sum is precisely the coefficient of X^n in $((1+X)^n)^m = (1+X)^{mn}$ which equals $\binom{mn}{n}$. Thus the main term in (2.3) is

$$\binom{nm}{n}\left(\frac{1}{n!}\prod_{p\in P}\frac{\log x}{\log p}\right)^{m-1}.$$

(iii) <u>$k = 1$</u>: Now we are counting the number of ordered m–tuples of such integers that are pairwise coprime. The main term in (2.3) is easily seen to be

$$\left\{\sum_{j_1+j_2+\ldots+j_m=n}\binom{n}{j_1, j_2, \ldots, j_m}^2\right\}\left(\frac{1}{n!}\prod_{p\in P}\frac{\log x}{\log p}\right).$$

The expression for $k = 2$ is rather complicated; it would be interesting to find a simplification.

Define $\Psi(x, y)$ to be the number of integers $\leq x$, whose prime factors are all $\leq y$. If we take $k = m = 1$ in (iii) above, and use the Prime Number Theorem to note that $\pi(y) \sim y/\log y$ and $\sum_{p\leq y}\log p \sim y$, then we have

$$\Psi(x,y) = \frac{1}{\pi(y)!}\prod_{p\leq y}\left(\frac{\log x}{\log p}\right)\left\{1 + O\left(\frac{y^2}{\log x \log y}\right)\right\} \tag{2.4}$$

for all $y \ll \log^{1/2} x$. Next taking $k = 1,\ m = 2$ in (iii) gives

Corollary 2. *The number of pairs of coprime integers, each $\leq x$, whose prime factors are all $\leq y$, is*

$$\binom{2\pi(y)}{\pi(y)}\Psi(x,y)\left\{1+O\left(\frac{y^2}{\log x\log y}\right)\right\}, \tag{2.5}$$

for all $y \ll \log^{1/2} x$.

Remark: Gunderson [Gu] gave the lower bound

$$\frac{2}{n!\prod_{p\leq y}\log p}\sum_{j=1}^{n-1}\binom{n-2}{j-1}\binom{n}{j}\log^j x\log^{n-j} x'$$

for the number of pairs (a,b) of coprime integers, free of prime factors $> y$, with $a \leq x$ and $b \leq x'$, where $n=\pi(y)$. By our Theorem we have the better estimate

$$\frac{1}{n!\prod_{p\leq y}\log p}\sum_{j=0}^{n}\binom{n}{j}^2\log^j x\log^{n-j} x'\left\{1+O\left(\frac{y^2}{\log x\log y}\right)\right\}$$

uniformly in the range $y \ll \log^{1/2} x$ and $x \leq x'$.

Finally, for Coppersmith's function we will obtain

Corollary 3. *The number of pairs of coprime integers (m,n) with $m^2+n^2 \leq x$, whose prime factors are all $\leq y$, where $y \ll \log^{1/2} x$, is given by (2.5).*

3. The proofs.

The Proof of the Theorem: We shall assume that $X > s(w)$. Suppose that $(A_1,\dots,A_m)$ is an ordered set that we are counting in the theorem. For each subset I of $\{1,2,\dots,m\}$ let B_I be the set of integers $j, 1\leq j\leq n$ such that $a_{ij}\neq 0$ if and only if $i\in I$. Then $\{B_I : I\subseteq\{1,2,\dots,m\}\}$ gives a partition of $\{1,2,\dots,n\}$ and we know, by the hypothesis, that B_I is empty if I has more than k elements.

An upper bound may thus be obtained by summing, over the partitions of $\{1,2,\dots,n\}$ into sets C_I with $|I|=k$, the number of ordered sets $(A_1,\dots,A_m)$ of n–vectors of non–negative integers (where $A_i=(a_{i1},a_{i2},\dots,a_{in})$) such that (2.1) holds and a_{ij} can be > 0

only if $j \in C_I$ for some I which contains i. (One can see that this is an upper bound by supposing that each B_J with $|J| < k$ is included in some unique C_I with $J \subseteq I$.) So let $D_i = \cup_{I:i\in I} C_I$. Then, by (1.5), the number of possibilities for each A_i is

$$\begin{aligned}
&\leq \frac{1}{d_i!} \prod_{j\in D_i} \left(\frac{x_i + \sum_{k\in D_i} w_k}{w_j} \right) \\
&\leq \frac{1}{d_i!} \left(\prod_{j\in D_i} \left(\frac{x_i}{w_j} \right) \right) \left(1 + \frac{s(w)}{x_i} \right)^{d_i},
\end{aligned}$$

where d_i denotes the cardinality of D_i for each i. Thus the number of possibilities for $(A_1, A_2, \ldots, A_m)$ is

$$\begin{aligned}
&\leq \prod_{i=1}^{m} \left\{ \frac{1}{d_i!} \left(\prod_{j\in D_i} \left(\frac{x_i}{w_j} \right) \right) \left(1 + \frac{s(w)}{X} \right)^{d_i} \right\} \\
&\leq \frac{1}{p(w)^k} \left(\prod_{i=1}^{m} \frac{x_i^{d_i}}{d_i!} \right) \left(1 + \frac{s(w)}{X} \right)^{kn}.
\end{aligned}$$

Therefore, summing over all possible partitions $\{C_I : |I| = k\}$, we get the upper bound in (2.2), in the range (1.6).

A lower bound may be obtained by summing over the same partitions as above, but this time also ensuring that each $a_{ij} \geq 1$ whenever $j \in D_i$. (We are thus counting precisely all possibilities where exactly k values of a_{ij} are non–zero for each fixed j.) Now the number of n–vectors of positive integers $(a_1, a_2, \ldots, a_n)$ satisfying (1.3) is equal to the number of n–vectors of non–negative integers $(b_1, b_2, \ldots, b_n)$ satisfying

$$b_1 w_1 + b_2 w_2 + \ldots + b_n w_n \leq X - s(w),$$

which may be seen by taking each $b_i = a_i - 1$. Thus, by (1.4), the number of possibilities for each A_i is

$$\begin{aligned}
&\geq \frac{1}{d_i!} \prod_{j\in D_i} \left(\frac{x_i - \sum_{k\in D_i} w_k}{w_j} \right) \\
&\geq \frac{1}{d_i!} \left(\prod_{j\in D_i} \left(\frac{x_i}{w_j} \right) \right) \left(1 - \frac{s(w)}{x_i} \right)^{d_i},
\end{aligned}$$

The rest of the argument follows exactly as for the upper bound, but with the inequalities reversed.

The Proof of Corollary 3: An upper bound on the number of pairs here is given by the number of pairs counted in Corollary 2. On the other hand a lower bound is given by the number of pairs counted in Corollary 2 when x is replaced by $x/\sqrt{2}$. The result then follows as

$$\Psi(x/\sqrt{2}, y) = \Psi(x, y)\left\{1 + O\left(\frac{y^2}{\log x \log y}\right)\right\}$$

by (2.4).

Acknowledgements: I'd like to thank both referees for doing a very careful job.

References

[Co] D. Coppersmith, *Fermat's Last Theorem (case I) and the Wieferich Criterion*, Math. Comp., **54** (1990), 895–902.

[En] V. Ennola, *On numbers with small prime divisors*, Ann. Acad. Sci. Fenn. Ser. A1, **440** (1969), 16 pp.

[Gr] A. Granville, *On pairs of coprime integers with no large prime factors*, to appear in Expo. Math.

[GM] A. Granville and M.B. Monagan, *The First Case of Fermat's Last Theorem is true for all prime exponents up to 714,591,416,091,389*, Trans. Amer. Math. Soc., **306** (1988), 329-359.

[Gu] N.G. Gunderson, *Derivation of Criteria for the first Case of Fermat's Last Theorem and the Combination of these Criteria to produce a new lower bound for the exponent*, Ph.D. Thesis, Cornell University, (1948).

[HL] G.H. Hardy and J.E. Littlewood, *The lattice points of a right–angled triangle*, Proc. London Math. Soc. **20** (1921), 15–36.

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

[Le] D.H. Lehmer, *The lattice points of an n–dimensional tetrahedron*, Duke J. Math. **7** (1940), 341–353.

[LL] D.H. Lehmer and E. Lehmer, *On the first case of Fermat's Last Theorem*, Bull. Amer. Math. Soc. **47** (1941), 139–142.

[No] K.K. Norton, *Numbers with small prime factors and the least kth power non residue*, Mem. Amer. Math. Soc. **106** (1971).

[Sp] D.C. Spencer, *The lattice points of tetrahedra*, J. of Math. and Phys. **21** (1942), 189–197.

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540, USA.