

CUBICAL DECOMPOSITIONS BELOW n^n : ERDŐS PROBLEM #769

PINGYOU LTD

ABSTRACT. We prove that $c(n) < (4\sqrt{n} + 2)^n$ for every odd $n \geq 3$ and $c(n) < n^n$ for every $n \geq 5$ with $n + 1$ composite, where $c(n)$ is the least integer such that the unit n -cube decomposes into K cubes whenever $K \geq c(n)$. Therefore $c(n)/n^n \rightarrow 0$ along odd n , which answers the question of Erdős whether $c(n) \gg n^n$, and the question is confined to prime $n + 1$, where $c(n) \leq (e + o(1))n^{n+1}$. The proofs use no computation. Grid refinements make the attainable counts, less one, a numerical semigroup, and a prime dividing every increment $m^n - 1$ with $m \leq M$ would place more than n reduced fractions among the n th roots of unity of a prime field or exhaust its multiplicative group.

We show that $\gcd(2^n - 1, \dots, M^n - 1)$ is the product of the primes $q > M$ with $q - 1 \mid n$ once $\{u/v : 1 \leq u, v \leq M\}$ has more than n elements, first at $M_n = (\pi/\sqrt{6})\sqrt{n} + O(\log n)$, and each such prime p adds at most $(p-1)(p^n-1)$ to the conductor. The least M with $\gcd(2^n - 1, \dots, M^n - 1) = 1$, written $h(n)$, satisfies $P(n) \leq h(n) \leq \max\{P(n), M_n\}$, where $P(n)$ is the largest prime with $P(n) - 1 \mid n$, and $h(n) = P(n)$ whenever $P(n) \geq M_n$, which answers the third question of Problem 770 above $2\sqrt{n}$. Guillotine tilings give $c(4) \leq 719$, below the conjectured 734. Taken together, the primes p with $p - 1 \mid n$ govern the upper bounds for $c(n)$, and where none exceeds $\sqrt{n}$ it falls below $n^{n/2+o(n)}$.

1. INTRODUCTION

For an integer $n \geq 2$, a cubical decomposition of the unit cube $[0, 1]^n$ is a finite family of closed cubes $v_i + s_i[0, 1]^n$ with $v_i \in \mathbb{R}^n$ and $0 < s_i \leq 1$, with pairwise disjoint interiors and with union $[0, 1]^n$. The cubes are homothetic copies of the unit cube, so their sides are parallel to its sides, and they may touch along their boundaries. Write $\mathcal{D}(n)$ for the set of integers K for which a cubical decomposition with exactly K cubes exists, and let $c(n)$ be the least integer C such that every integer $K \geq C$ belongs to $\mathcal{D}(n)$. The problem of determining $\mathcal{D}(n)$ was posed by Fine and Niven [6] and by Hadwiger, and Erdős [5, p. 199] asked for good bounds on $c(n)$, and in particular whether

$$c(n) \gg n^n, \tag{1.1}$$

that is, whether $c(n) \geq \eta n^n$ for some $\eta > 0$ and all large n . The question is recorded as Problem 769 at <https://www.erdosproblems.com/769>. Meier [9] proved that $c(n)$ is finite and conjectured that $c(3) = 48$, and $c(2) = 6$ is classical, since a square can be divided into K squares exactly when $K \notin \{2, 3, 5\}$. Every decomposition has at least 2^n cubes when it has more than one, since an axis-parallel cube of side less than one contains at most one vertex of the unit cube, and Hadwiger's lower bound $c(n) \geq 2^n + 2^{n-1}$ was sharpened by Connor and Marmorino [3] to $c(n) \geq 2^{n+1} - 1$ for $n \geq 3$. Burgess and Erdős [5] proved that the integers $m^n - 1$ with $2 \leq m \leq n + 1$ have no common prime divisor, and deduced $c(n) \ll n^{n+1}$ from the theorem of Brauer on numerical semigroups. Erdős wrote that he was certain that $c(n) > n^n$ whenever $n + 1$ is prime. Hudelson [8] proved $c(n) < 6^n$ whenever $\gcd(2^n - 1, 3^n - 1) = 1$ and $c(n) \ll (2n)^{n-1}$ in general, and his tables of tilings in dimensions four and five give $c(4) \leq 809$ and $c(5) \leq 1891$. Prather (arXiv:1910.06206, 2019) obtained $c(4) \leq 734$, $c(6) \leq 246964$ and $c(7) \leq 67375$ from explicit tilings and conjectured that $c(4) = 734$. In the notation of Prather, which records the integer below the cutoff, these bounds read 808, 1890, 733, 246963 and 67374. Connor and Marmorino [3] proved $c(n) \leq e^2 n^n$ when $n + 1$ is composite and $c(n) \leq 1.8 n^{n+1}$ when $n + 1$ is prime. Every one of these bounds is consistent with (1.1).

Problem 770 on the same page of [5] concerns the arithmetic function behind these bounds. For $n \geq 2$ define

$$h(n) = \min\{b \geq 2 : \gcd(2^n - 1, 3^n - 1, \dots, b^n - 1) = 1\}, \quad (1.2)$$

where the greatest common divisor is that of the whole list, and define $P(n)$ to be the largest prime p with $p - 1 \mid n$. The set of such primes contains 2 and is finite, since $p \leq n + 1$. Fermat's theorem shows that every $m^n - 1$ with $2 \leq m < P(n)$ is divisible by $P(n)$, so $h(n) \geq P(n)$, and the lemma of Burgess and Erdős says that $h(n) \leq n + 1$. Erdős observed that $h(n) = n + 1$ exactly when $n + 1$ is prime and that $h(n)$ is unbounded along the odd integers, and he asked whether the integers n with $h(n) = p$ have a density for every prime p , whether $\liminf h(n) = \infty$, and whether $h(n) = P(n)$ whenever $P(n) > n^\varepsilon$.

For an integer $M \geq 1$ let $N(M)$ be the number of pairs (u, v) of coprime integers with $1 \leq u, v \leq M$, which is the number of reduced fractions u/v with numerator and denominator at most M , and let M_n be the least integer $M \geq 2$ with $N(M) > n$.

Theorem A (Odd dimensions). Let $n \geq 3$ be odd, and let $M \geq 2$ be an integer with $N(M) > n$. Then $\gcd(2^n - 1, 3^n - 1, \dots, M^n - 1) = 1$ and

$$c(n) \leq 1 + (2^n - 2)(M^n - 2) < (2M)^n. \quad (1.3)$$

The choice $M = \lceil 2\sqrt{n} \rceil$ is admissible, so $c(n) < (4\sqrt{n} + 2)^n$, and $M_n = (\pi/\sqrt{6})\sqrt{n} + O(\log n)$, so $c(n) < ((2\pi/\sqrt{6} + o(1))\sqrt{n})^n$. Furthermore

$$\lim_{\substack{n \rightarrow \infty \\ n \text{ odd}}} \frac{c(n)}{n^n} = 0, \quad c(n) < n^n \quad \text{for every odd } n \geq 5. \quad (1.4)$$

Theorem B (The exact common divisor). Let $n \geq 2$ and let $M \geq 2$ be an integer with $N(M) > n$. Then

$$\gcd(2^n - 1, 3^n - 1, \dots, M^n - 1) = \prod_{\substack{q > M \\ \text{prime} \\ q-1 \mid n}} q, \quad (1.5)$$

a squarefree integer (the empty product is 1). Consequently

$$P(n) \leq h(n) \leq \max\{P(n), M_n\} \leq \max\{P(n), \lceil 2\sqrt{n} \rceil\}, \quad (1.6)$$

with $h(n) = P(n)$ whenever $P(n) \geq M_n$, and in every dimension

$$c(n) \leq 1 + (2^n - 2)(h(n)^n - 2) < (2h(n))^n. \quad (1.7)$$

Corollary C. Let $n \geq 2$.

- (i) $h(n) \leq n + 1$ and $c(n) < (2n + 2)^n$. If $\gcd(2^n - 1, 3^n - 1) = 1$, then $h(n) = 3$ and $c(n) < 6^n$.
- (ii) $h(n) = n + 1$ if and only if $n + 1$ is prime.
- (iii) If $P(n) \geq M_n$, in particular if $P(n) \geq 2\sqrt{n}$, then $h(n) = P(n)$.
- (iv) If $n \geq 5$ and $n + 1$ is composite, then $h(n) \leq n/2 + 1$ and $c(n) < (n + 2)^n < e^2 n^n$.
- (v) $c(n) < n^n$ whenever $2h(n) \leq n$, in particular for every $n \geq 8$ with $P(n) \leq n/2$.

Theorem D (The chain bound). Let $n \geq 2$, and let D be the product of the primes $q > M_n$ with $q - 1 \mid n$, which is the greatest common divisor of $2^n - 1, \dots, M_n^n - 1$. Then

$$c(n) \leq 2 - D + \frac{(2^n - 1 - D)(M_n^n - 1 - D)}{D} + \sum_{p \mid D} (p - 1)(p^n - 1). \quad (1.8)$$

Consequently $c(n) < n^n$ for every $n \geq 5$ such that $n + 1$ is composite, and

$$c(n) < n(n + 1)^n + (2M_n)^n + \frac{e^2 n^{n+2}}{2^{n+2}} = (e + o(1)) n^{n+1} \quad (1.9)$$

whenever $n + 1$ is prime.

Theorem E (Dimension four). Every integer $K \geq 719$ is the number of cubes of a cubical decomposition of $[0, 1]^4$, that is, $c(4) \leq 719$.

Part (i) contains the lemma $h(n) \leq n + 1$ of Burgess and Erdős and the 6^n theorem of Hudelson, part (ii) is the observation of Erdős, part (iii) answers the third question of Problem 770 for every threshold n^ε with $\varepsilon > 1/2$ and all sufficiently large n , part (iv) contains the bound of Connor and Marmorino for composite $n + 1$, and part (v) places $c(n)$ below n^n in every dimension with $2h(n) \leq n$. [Theorem D](#) turns the obstruction into a bound. The increments $m^n - 1$ with $m \leq M_n$ generate a semigroup whose elements are the multiples of D beyond a cutoff below $(2M_n)^n/D$, and each prime $p \mid D$, adjoined through the increment $p^n - 1$, costs at most $(p - 1)(p^n - 1)$, by the chain bound of Brauer proved in [Section 3](#). The question (1.1) is thereby confined to the dimensions in which $n + 1$ is prime, where the bound (1.9) has the order n^{n+1} of the bounds of Burgess and Erdős and of Connor and Marmorino, with the constant e in place of 1.8. [Theorem E](#) improves $c(4) \leq 734$ to $c(4) \leq 719$, so 733 is the number of cubes of a decomposition of $[0, 1]^4$ and the conjectured value $c(4) = 734$ is false. Its fourteen guillotine tilings have grids of side at most twelve, the size that Prather singled out as a candidate for an improvement, and [Appendix A](#) records their counts and the residue representatives modulo 15 that they generate. Beyond these, [Theorem B](#) says exactly what the method can and cannot do. It gives the collective greatest common divisor itself, which is one as soon as the grids reach the size M_n , except in the dimensions where a prime p with $p - 1 \mid n$ exceeds that size, and there [Proposition 5.3](#) shows that no composition of tilings of grids of side less than p leaves the class 1 modulo p .

The proofs are elementary. Refining one cube of a decomposition into an $m \times \cdots \times m$ grid adds $m^n - 1$ cubes, so $\mathcal{D}(n) - 1$ contains the additive semigroup generated by the increments $m^n - 1$, and a conductor bound for numerical semigroups, which [Section 3](#) proves by minimum representatives of the residue classes modulo $2^n - 1$, shows that a collective greatest common divisor of one among the increments with $m \leq b$ gives every count beyond $1 + (2^n - 2)(b^n - 2)$. A prime q dividing every increment with $m \leq M$ exceeds M , and the residues of $1, \dots, M$ then lie in the group H of n th roots of unity in $\mathbb{F}_q^*$, which has at most n elements. If $q > M^2$, the $N(M)$ reduced fractions with numerator and denominator at most M are distinct elements of H , which is impossible when $N(M) > n$. If $q \leq M^2$, the division $q = Mk + r$ and a pigeonhole argument on the multiples of any element of $\mathbb{F}_q^*$ force $H = \mathbb{F}_q^*$ and $q - 1 \mid n$, and a binomial expansion of $(q - r)^n$ modulo q^2 excludes q^2 . This identifies the common divisor as the product in (1.5), which is [Theorem B](#), and for odd n no such q exists, which proves [Theorem A](#). The count $N(M) > M^2/4$ is elementary, and the classical asymptotic for Euler's function gives the constant $\pi/\sqrt{6}$. The bound $N(M) \geq 2M + 3$ settles every odd $n \geq 9$, the identity $809 \cdot 127 - 47 \cdot 2186 = 1$ settles $n = 7$, and an explicit family of decompositions settles $n = 5$.

[Section 2](#) records the semigroup structure of $\mathcal{D}(n)$ and the grid refinements, [Section 3](#) proves the conductor bound, [Section 4](#) proves the exact common divisor, [Section 5](#) proves [Theorems A, B and D](#) and [Corollary C](#) together with the five-dimensional construction and the congruence obstruction, and [Appendix A](#) tabulates $h(n)$, compares the exact conductors of the refinement semigroups with the bound (1.7), and proves [Theorem E](#) from explicit guillotine tilings, with bounds in dimensions five to eight.

The negative answer to (1.1) was posted on the problem's page by Zeng on 24 July 2026 (<https://www.erdosproblems.com/forum/thread/769/proof-claims>, AI-assisted): for odd n , $c(n) \leq 1 + (M - 1)(2^n - 2)(M^n - 1)$ with $M = \lfloor 2\sqrt{n} \rfloor + 1$, and in every dimension $h(n) \leq \max\{P(n), M\}$. That argument places the reduced fractions in H as in [Section 4](#) and treats $q \leq M^2$ by the least quadratic non-residue for odd n and by Dirichlet's approximation theorem for even n . Korsky (5 August 2026, same thread, AI-assisted) announced the bound $c(n) \leq (C_\varepsilon n^{1/(4\sqrt{e})+\varepsilon})^n$ for odd n and every $\varepsilon > 0$ by character-sum estimates, which goes below the scale $\sqrt{n}$ of this paper, together with a lower bound of order $n2^n$ for even n . The `formal-conjectures` repository of Google DeepMind

(<https://github.com/google-deepmind/formal-conjectures>, entry for Problem 769) records the problem as resolved in the negative. The present paper gives complete elementary proofs with the smaller cutoff $1 + (2^n - 2)(M^n - 2)$, the exact squarefree common divisor in every dimension, the threshold M_n , the chain bound of [Theorem D](#), and the bound $c(4) \leq 719$.

2. COUNTS OF CUBES AND GRID REFINEMENTS

Let $n \geq 2$. A cubical decomposition with one cube is the unit cube itself, so $1 \in \mathcal{D}(n)$. Define

$$\Gamma_n = \{K - 1 : K \in \mathcal{D}(n)\} \subseteq \mathbb{Z}_{\geq 0}.$$

Lemma 2.1 (Composition). *If $K_1, K_2 \in \mathcal{D}(n)$, then $K_1 + K_2 - 1 \in \mathcal{D}(n)$. Consequently Γ_n contains 0 and is closed under addition, and $c(n) - 1$ is the least integer C such that every integer $S \geq C$ belongs to Γ_n .*

Proof. Let $C_1, \dots, C_{K_1}$ be the cubes of a decomposition, with $C_1 = v + s[0, 1]^n$, and let $v_j + s_j[0, 1]^n$, $1 \leq j \leq K_2$, be the cubes of a second decomposition. The cubes $v + sv_j + ss_j[0, 1]^n$ lie in C_1 , have pairwise disjoint interiors and have union C_1 , since the map $x \mapsto v + sx$ carries $[0, 1]^n$ onto C_1 . Replacing C_1 by them gives a decomposition with $K_1 + K_2 - 1$ cubes. The remaining assertions restate the definitions. $\square$

Lemma 2.2 (Grid refinement). *Let $m \geq 1$ and $b \geq 2$ be integers. Then $m^n \in \mathcal{D}(n)$, and every integer*

$$K = 1 + \sum_{j=2}^b t_j(j^n - 1), \quad t_j \in \mathbb{Z}_{\geq 0}, \quad (2.1)$$

belongs to $\mathcal{D}(n)$. For such K the cubes can be chosen with rational vertices.

Proof. For a cube $C = v + s[0, 1]^n$ and an integer $m \geq 1$, the m^n cubes

$$v + \frac{s}{m}j + \left[0, \frac{s}{m}\right]^n, \quad j \in \{0, \dots, m-1\}^n, \quad (2.2)$$

have pairwise disjoint interiors and union C . Applied to the unit cube this gives $m^n \in \mathcal{D}(n)$, and [Lemma 2.1](#) gives (2.1). Starting from the unit cube and refining the cube at the origin t_j times with the parameter j , for each j in turn, produces vertices in $\mathbb{Q}^n$ by (2.2). $\square$

The cubes of such a chain of refinements can be written down without further choices. For a word $m_1, \dots, m_L$ of integers $m_j \geq 2$ define $\ell_0 = 1$ and $\ell_j = (m_1 \cdots m_j)^{-1}$ for $1 \leq j \leq L$. At step j the cube $[0, \ell_{j-1}]^n$ is refined into m_j^n cubes of side ℓ_j , and the one at the origin is refined at the next step. The final family is

$$\{\ell_j(v + [0, 1]^n) : 1 \leq j \leq L, v \in \{0, \dots, m_j - 1\}^n, v \neq 0\} \cup \{[0, \ell_L]^n\}, \quad (2.3)$$

with $1 + \sum_{j=1}^L (m_j^n - 1)$ cubes, and the volumes add up to $\sum_{j=1}^L (\ell_{j-1}^n - \ell_j^n) + \ell_L^n = 1$.

Dehn [4] proved that the squares of a decomposition of a square have rational sides, and the cross-sections by the hyperplanes $x_n = t$ carry this to every dimension by induction, so every decomposition is, after scaling, a tiling of a cube of integer side by cubes of integer side. Guillotine tilings are the computable part of these, and the computations of [Appendix A](#) rest on them. For positive integers $l_1, \dots, l_n$ write $B(l) = \prod_{i=1}^n [0, l_i]$. A guillotine tiling of $B(l)$ is either the box itself, when $l_1 = \dots = l_n$, or the union of guillotine tilings of the two boxes into which a hyperplane $x_i = p$ with $1 \leq p < l_i$ cuts $B(l)$, where the second box is translated to the origin. Write $G(l)$ for the set of numbers of cubes of the guillotine tilings of $B(l)$.

Lemma 2.3 (Guillotine tilings). *Let $l = (l_1, \dots, l_n)$ be positive integers. Then $1 \in G(l)$ if and only if all l_i are equal, $G(l)$ contains $G(l') + G(l'')$ whenever $B(l')$ and $B(l'')$ are the two parts of a cut of $B(l)$, and $G(l)$ depends only on the multiset $\{l_1, \dots, l_n\}$. For every $m \geq 1$, $G(m, \dots, m) \subseteq \mathcal{D}(n)$.*

Proof. The first two assertions are the definition, since the cubes of the two parts have disjoint interiors and union $B(l)$. Permuting the coordinates carries guillotine tilings of $B(l)$ to guillotine tilings of the permuted box. The map $x \mapsto x/m$ carries a tiling of $B(m, \dots, m)$ by cubes of integer side to a cubical decomposition of $[0, 1]^n$ with the same number of cubes. $\square$

3. RESIDUE REPRESENTATIVES AND THE CONDUCTOR

Let $\mathcal{A}$ be a finite nonempty set of positive integers. Define the additive semigroup

$$\Gamma(\mathcal{A}) = \left\{ \sum_{u \in \mathcal{A}} t_u u : t_u \in \mathbb{Z}_{\geq 0} \right\},$$

which contains 0, and when every sufficiently large integer belongs to $\Gamma(\mathcal{A})$ define the conductor $\text{cond } \mathcal{A}$ to be the least integer $C \geq 0$ such that every integer $S \geq C$ belongs to $\Gamma(\mathcal{A})$.

Proposition 3.1 (Residue representatives). *Assume that the elements of $\mathcal{A}$ have greatest common divisor 1, and let $a = \min \mathcal{A}$ and $X = \max \mathcal{A}$. For $0 \leq r < a$ let w_r be the least element of $\Gamma(\mathcal{A})$ congruent to r modulo a , and let $W = \max_r w_r$. These representatives exist, they satisfy $w_r \leq (a-1)X$, and the conductor exists and equals*

$$\text{cond } \mathcal{A} = W - a + 1 \leq (a-1)(X-1).$$

Proof. The residues modulo a of the elements of $\Gamma(\mathcal{A})$ form a subset of $\mathbb{Z}/a\mathbb{Z}$ that contains 0 and is closed under addition. Such a subset is a subgroup, because the inverse of a residue x of additive order d is $(d-1)x$, a sum of copies of x . The residues of the elements of $\mathcal{A}$ generate $\mathbb{Z}/a\mathbb{Z}$, since their greatest common divisor together with a is 1. Every residue therefore occurs in $\Gamma(\mathcal{A})$, and w_r exists.

Let $w_r = u_1 + \dots + u_t$ with $u_i \in \mathcal{A}$, where $t = 0$ for $r = 0$. If two of the partial sums $0, u_1, u_1+u_2, \dots, w_r$ were congruent modulo a , deleting the summands between them would produce a smaller element of $\Gamma(\mathcal{A})$ in the residue r , because the deleted summands are positive. So the $t+1$ partial sums have distinct residues, $t \leq a-1$, and $w_r \leq (a-1)X$.

An integer $S \geq 0$ congruent to r belongs to $\Gamma(\mathcal{A})$ if $S \geq w_r$, since $S = w_r + ja$ with $j \in \mathbb{Z}_{\geq 0}$, and does not belong to it if $S < w_r$, by the minimality of w_r . Therefore every $S > W - a$ belongs to $\Gamma(\mathcal{A})$: if $S \notin \Gamma(\mathcal{A})$, then $S < w_r$ for its residue r , so $S \leq w_r - a \leq W - a$. If $W \geq a$, the integer $W - a$ is congruent to the residue r with $w_r = W$ and is smaller than w_r , so it is not in $\Gamma(\mathcal{A})$, and $\text{cond } \mathcal{A} = W - a + 1$. If $W < a$, then $W = a - 1$, because $w_r \geq r$ for every r , and every nonnegative integer belongs to $\Gamma(\mathcal{A})$, so $\text{cond } \mathcal{A} = 0 = W - a + 1$. The final inequality is $W - a + 1 \leq (a-1)X - a + 1 = (a-1)(X-1)$. $\square$

The formula $\text{cond } \mathcal{A} = W - a + 1$ is due to Brauer and Shockley [2], the bound $(a-1)(X-1)$ is the bound of Schur reported by Brauer [1], whose own theorem is sharper and is the one Erdős used for $c(n) \ll n^{n+1}$, and $(a-1)(X-1)$ is the exact conductor when $\mathcal{A} = \{a, X\}$, by the theorem of Sylvester recorded in [10].

Corollary 3.2 (A collective greatest common divisor gives every large count). *Let $n \geq 2$ and $b \geq 2$ be integers with $\gcd(m^n - 1 : 2 \leq m \leq b) = 1$. Then*

$$c(n) \leq 1 + (2^n - 2)(b^n - 2), \tag{3.1}$$

and every integer K at least the right-hand side is the number of cubes of a decomposition of the form (2.3) with all $m_j \leq b$. In particular $c(n) \leq 1 + (2^n - 2)(h(n)^n - 2) < (2h(n))^n$.

Proof. Apply Proposition 3.1 to $\mathcal{A} = \{m^n - 1 : 2 \leq m \leq b\}$, for which $a = 2^n - 1$ and $X = b^n - 1$. For $K \geq 1 + (2^n - 2)(b^n - 2)$ the integer $K - 1$ is at least $(a-1)(X-1) \geq \text{cond } \mathcal{A}$, so $K - 1 \in \Gamma(\mathcal{A})$, and Lemma 2.2 realises K by a chain of refinements. The case $b = h(n)$ is the definition of $h(n)$, which is finite by the lemma of Burgess and Erdős and by Theorem B, and $1 + (2^n - 2)(h(n)^n - 2) < 2^n h(n)^n$. $\square$

Proposition 3.3 (Adjoining a generator). *Let $\mathcal{A}$ be a finite nonempty set of positive integers with greatest common divisor d , let a be a positive integer prime to d , and let C be the conductor of $\mathcal{A}/d = \{u/d : u \in \mathcal{A}\}$. Then every integer $S \geq (d-1)(a-1) + dC$ belongs to $\Gamma(\mathcal{A} \cup \{a\})$, so the conductor of $\mathcal{A} \cup \{a\}$ is at most $(d-1)(a-1) + dC$.*

Proof. The set $\mathcal{A}/d$ has greatest common divisor 1, so C exists by Proposition 3.1. Let $S \geq (d-1)(a-1) + dC$. Since a is invertible modulo d , there is an integer $0 \leq t \leq d-1$ with $ta \equiv S \pmod{d}$. Then $S - ta$ is a multiple of d with $S - ta \geq S - (d-1)a \geq dC - d + 1 > d(C-1)$, so $S - ta \geq dC$ and $(S - ta)/d \geq C$ belongs to $\Gamma(\mathcal{A}/d)$. Therefore $S - ta$ belongs to $\Gamma(\mathcal{A})$, and $S = (S - ta) + ta$ belongs to $\Gamma(\mathcal{A} \cup \{a\})$. $\square$

For $\mathcal{A} = \{a\}$ and $d = a$ the proposition is the theorem of Sylvester again. Applied along a chain $a_1, \dots, a_k$ with $d_i = \gcd(a_1, \dots, a_i)$ and $d_k = 1$, it gives the bound $\text{cond}\{a_1, \dots, a_k\} \leq \sum_{i=2}^k a_i(d_{i-1}/d_i - 1) - a_1 + 1$ of Brauer [1], and Theorem D is this bound for a chain whose ratios d_{i-1}/d_i are read off from Theorem B.

4. REDUCED FRACTIONS IN A PRIME FIELD AND THE EXACT COMMON DIVISOR

Lemma 4.1 (Reduced fractions). *For every integer $M \geq 1$,*

$$N(M) = 2 \sum_{v=1}^M \varphi(v) - 1 > \frac{M^2}{4}, \quad (4.1)$$

where φ is Euler's function, and $N(M) = \frac{6}{\pi^2} M^2 + O(M \log M)$. The lower bounds $N(M) \geq 2M - 1$ for $M \geq 1$, $N(M) \geq 2M + 1$ for $M \geq 3$ and $N(M) \geq 2M + 3$ for $M \geq 4$ hold. Consequently $M_n \leq \lceil 2\sqrt{n} \rceil$ and $M_n \leq n$ for every $n \geq 2$, $M_n \leq \lfloor n/2 \rfloor$ for every $n \geq 8$, and

$$M_n = \frac{\pi}{\sqrt{6}} \sqrt{n} + O(\log n).$$

If $q > M^2$ is prime, the $N(M)$ reduced fractions u/v with $1 \leq u, v \leq M$ are distinct elements of $\mathbb{F}_q^*$.

Proof. The coprime pairs (u, v) with $u < v \leq M$ number $\sum_{v=2}^M \varphi(v)$, the pairs with $u > v$ number the same, and $(1, 1)$ is the only coprime pair with $u = v$. This proves the identity in (4.1), and the asymptotic follows from $\sum_{v \leq M} \varphi(v) = 3M^2/\pi^2 + O(M \log M)$ [7, Theorem 330]. For the lower bound in (4.1), every pair that is not coprime has a common divisor $d \geq 2$, and the pairs with $d \mid u$ and $d \mid v$ number $\lfloor M/d \rfloor^2$. Therefore

$$M^2 - N(M) \leq \sum_{d=2}^M \left\lfloor \frac{M}{d} \right\rfloor^2 \leq M^2 \sum_{d=2}^{\infty} \frac{1}{d^2} < M^2 \left(\frac{1}{4} + \sum_{d=3}^{\infty} \int_{d-1}^d \frac{dx}{x^2} \right) = \frac{3M^2}{4},$$

which gives $N(M) > M^2/4$. The pairs $(1, v)$ and $(u, 1)$ with $1 \leq u, v \leq M$ are coprime and number $2M - 1$, which gives $N(M) \geq 2M - 1$. For $M \geq 3$ the pairs $(2, 3)$ and $(3, 2)$ are two further coprime pairs, and for $M \geq 4$ the pairs $(3, 4)$ and $(4, 3)$ are two more.

The integer $M = \lceil 2\sqrt{n} \rceil \geq 2$ has $N(M) > M^2/4 \geq n$, so $M_n \leq \lceil 2\sqrt{n} \rceil$. For $n \geq 2$, $N(n) \geq 2n - 1 > n$, so $M_n \leq n$. For $n \geq 8$ the integer $M = \lfloor n/2 \rfloor \geq 4$ has $N(M) \geq 2M + 3 \geq n + 2 > n$, so $M_n \leq \lfloor n/2 \rfloor$.

For the asymptotic of M_n , let $n \geq 3$. Then $N(2) = 3 \leq n$ gives $M_n \geq 3$, and the minimality of M_n gives $N(M_n - 1) \leq n < N(M_n)$. The asymptotic for N gives a constant A with $|N(M) - 6M^2/\pi^2| \leq AM \log M$ for $M \geq 2$, so

$$\frac{6(M_n - 1)^2}{\pi^2} - AM_n \log M_n \leq n < \frac{6M_n^2}{\pi^2} + AM_n \log M_n,$$

and $6M_n^2/\pi^2 = n + O(M_n \log M_n)$. Since $N(M) \leq M^2$, the inequality $N(M_n) > n$ gives $M_n > \sqrt{n}$, and $M_n \leq \lceil 2\sqrt{n} \rceil$ gives $M_n \log M_n = O(\sqrt{n} \log n)$. The two bounds give $M_n^2 = \frac{\pi^2}{6} n (1 + \delta_n)$ with $\delta_n = O(n^{-1/2} \log n)$ and $1 + \delta_n > 0$, and $\sqrt{1 + \delta_n} = 1 + O(\delta_n)$ gives $M_n = \frac{\pi}{\sqrt{6}} \sqrt{n} + O(\log n)$.

Let $q > M^2$ be prime and assume that $uv' \equiv u'v \pmod{q}$ for two reduced fractions u/v and u'/v' with entries at most M . The integer $uv' - u'v$ has absolute value less than $M^2 < q$, so it is zero, and two equal reduced fractions have the same numerator and denominator. Since $q > M$, every denominator is invertible in $\mathbb{F}_q$, so the fractions are elements of $\mathbb{F}_q^*$ and distinct ones remain distinct. $\square$

Lemma 4.2 (The division by M). *Let $M \geq 2$ be an integer and q a prime with $M < q \leq M^2$. Then $q = Mk + r$ with integers $1 \leq k \leq M - 1$ and $1 \leq r \leq M - 1$.*

Proof. Let $k = \lfloor q/M \rfloor$ and $r = q - Mk$. Then $k \geq 1$ because $q > M$, and $k \leq M - 1$ because $q < M^2$, as M^2 is not prime. The remainder satisfies $0 \leq r \leq M - 1$, and $r \neq 0$ because the prime q exceeds $M \geq 2$ and is therefore not a multiple of M . $\square$

Lemma 4.3 (An interval generates the group). *Let $M \geq 2$ be an integer, let q be a prime with $M < q \leq M^2$, and let H be a subgroup of $\mathbb{F}_q^*$ containing the residues of $1, \dots, M$. Then $H = \mathbb{F}_q^*$.*

Proof. By Lemma 4.2, $q = Mk + r$ with $1 \leq k, r \leq M - 1$, so $-1 = Mk/r \in H$. Let $x \in \mathbb{F}_q^*$. The $M + 1$ residues $0, x, 2x, \dots, Mx$ are distinct, because $M < q$. Order their representatives in $\{0, \dots, q - 1\}$ increasingly. The M gaps between consecutive representatives are positive integers with sum at most $q - 1$, so one gap u satisfies $1 \leq u \leq (q - 1)/M < M$. The two endpoints of this gap represent ix and jx for distinct $i, j \in \{0, \dots, M\}$, and $u = (j - i)x$ in $\mathbb{F}_q$ with $1 \leq |j - i| \leq M$. Both u and $j - i$ lie in H , the latter because H contains $1, \dots, M$ and -1 . Therefore $x = u/(j - i) \in H$. $\square$

Theorem 4.4 (The exact common divisor). *Let $n \geq 2$, and let $M \geq 2$ be an integer with $N(M) > n$. Then*

$$\gcd(2^n - 1, 3^n - 1, \dots, M^n - 1) = \prod_{\substack{q > M \text{ prime} \\ q-1 \mid n}} q,$$

where the empty product is 1. In particular the greatest common divisor is squarefree.

Proof. Let D be the greatest common divisor of the list, and let q be a prime divisor of D . Then $q > M$, since $m^n - 1 \equiv -1 \pmod{q}$ for $m = q \leq M$. In the field $\mathbb{F}_q$ define

$$H = \{x \in \mathbb{F}_q^* : x^n = 1\},$$

a multiplicative subgroup that contains the residues of $1, \dots, M$ and has at most n elements, since the nonzero polynomial $X^n - 1$ has at most n roots in a field. If $q > M^2$, the $N(M)$ reduced fractions of Lemma 4.1 are distinct elements of $\mathbb{F}_q^*$, and each of them lies in H as a quotient of two elements of H , so $|H| \geq N(M) > n$, a contradiction. This gives $q \leq M^2$, and $H = \mathbb{F}_q^*$ by Lemma 4.3. Let $n = (q - 1)t + s$ with integers $t \geq 0$ and $0 \leq s < q - 1$. Every $x \in \mathbb{F}_q^*$ satisfies $x^{q-1} = 1$ by Fermat's theorem and $x^n = 1$ because $H = \mathbb{F}_q^*$, so $x^s = 1$. If $s > 0$, the nonzero polynomial $X^s - 1$ would have $q - 1 > s$ roots in $\mathbb{F}_q$, so $s = 0$ and $q - 1 \mid n$. Conversely, if $q > M$ is a prime with $q - 1 \mid n$, every $m \in \{2, \dots, M\}$ is prime to q , and Fermat's theorem gives $m^n \equiv 1 \pmod{q}$, so q divides D . The prime divisors of D are exactly the primes $q > M$ with $q - 1 \mid n$.

Let q be one of these primes. Then $q \leq M^2$ by the first paragraph, and q is odd because $q > M \geq 2$, so $q - 1$ is even and n is even. The inequalities $n < N(M) \leq M^2 < q(q - 1)$ hold, the last because $q \geq M + 1$. If q divided n , then $q(q - 1)$ would divide n , because q and $q - 1$ are coprime, which is impossible for $0 < n < q(q - 1)$, so $q \nmid n$. By Lemma 4.2, $q = Mk + r$ with $1 \leq k, r \leq M - 1$. Assume that q^2 divides D . Then $M^n \equiv k^n \equiv r^n \equiv 1 \pmod{q^2}$, where an

entry equal to 1 is trivial and the other entries belong to the list, so $(Mk)^n \equiv r^n \pmod{q^2}$. Since $Mk = q - r$ and n is even, the binomial theorem gives

$$(Mk)^n = (q - r)^n \equiv r^n - nqr^{n-1} \pmod{q^2}.$$

Then q^2 divides nqr^{n-1} , so q divides nr^{n-1} , which is impossible because $q \nmid n$ and $0 < r < q$. This contradiction shows that $q^2 \nmid D$. Every prime divisor of D has exponent one, and D is the displayed product. $\square$

5. BOUNDS IN EVERY DIMENSION

Proof of Theorem A. A prime q with $q - 1 \mid n$ has $q - 1$ odd, so $q = 2 \leq M$, and the product in Theorem 4.4 is empty. The greatest common divisor is 1, and (3.1) with $b = M$ gives $c(n) \leq 1 + (2^n - 2)(M^n - 2) < 2^n M^n$, which is (1.3). For $M = \lceil 2\sqrt{n} \rceil$, Lemma 4.1 gives $N(M) > M^2/4 \geq n$, so this M is admissible, and $c(n) < (2M)^n < (4\sqrt{n} + 2)^n$ because $M < 2\sqrt{n} + 1$. The choice $M = M_n$ and the asymptotic $M_n = (\pi/\sqrt{6})\sqrt{n} + O(\log n)$ of Lemma 4.1 give $c(n) < (2M_n)^n = ((2\pi/\sqrt{6} + o(1))\sqrt{n})^n$.

For the limit, $c(n) < (4\sqrt{n} + 2)^n$ gives

$$0 \leq \frac{c(n)}{n^n} < \left(\frac{4}{\sqrt{n}} + \frac{2}{n} \right)^n,$$

and the base is at most $1/2$ for $n \geq 81$, so the right-hand side tends to 0.

For the inequality $c(n) < n^n$, let $n \geq 9$ be odd and let $M = (n - 1)/2 \geq 4$. Then $N(M) \geq 2M + 3 = n + 2 > n$ by Lemma 4.1, so M is admissible and $c(n) < (2M)^n = (n - 1)^n < n^n$. For $n = 7$, the identity $809 \cdot 127 - 47 \cdot 2186 = 1$ gives $\gcd(2^7 - 1, 3^7 - 1) = 1$, and (3.1) with $b = 3$ gives $c(7) \leq 1 + 126 \cdot 2185 = 275311 < 7^7 = 823543$. For $n = 5$, Lemma 5.2 gives $c(5) \leq 2925 < 5^5$. $\square$

Corollary 5.1 (Logarithmic form). *For every odd $n \geq 3$,*

$$\log c(n) \leq \frac{1}{2}n \log n + n \log 4 + \frac{1}{2}\sqrt{n} \quad \text{and} \quad \log c(n) \leq \frac{1}{2}n \log n + n \log \frac{2\pi}{\sqrt{6}} + O(\sqrt{n} \log n).$$

Proof. By Theorem A, $c(n) < (4\sqrt{n} + 2)^n = (4\sqrt{n})^n(1 + x)^n$ with $x = 1/(2\sqrt{n})$, and $n \log(1 + x) \leq nx = \frac{1}{2}\sqrt{n}$. The second bound follows from $c(n) < (2M_n)^n$ and $M_n = (\pi/\sqrt{6})\sqrt{n} + O(\log n)$, since $\log M_n = \frac{1}{2} \log n + \log(\pi/\sqrt{6}) + O(n^{-1/2} \log n)$. $\square$

Lemma 5.2 (Five-dimensional decompositions). *Every integer $K \geq 2925$ belongs to $\mathcal{D}(5)$, that is, $c(5) \leq 2925$.*

Proof. The grid of side 2 gives $32 \in \mathcal{D}(5)$, with increment $2^5 - 1 = 31$. In $[0, 3]^5$ keep $[0, 2]^5$ as one cube and tile the rest by unit cubes, which is possible because $[0, 3]^5 \setminus [0, 2]^5$ is a union of unit cells of the integer grid. This tiling has $1 + 3^5 - 2^5 = 212$ cubes, with increment 211. For $j \in \{1, 2, 4\}$ define

$$A_j = [0, 3]^j \times [0, 6]^{5-j}, \quad B_j = [0, 4]^j \times [0, 6]^{5-j}.$$

Tile A_j by 2^{5-j} cubes of side 3. Tile $[0, 6]^5 \setminus B_j$ by cubes of side 2, of which there are $3^5 - 2^j 3^{5-j}$, since B_j is a union of cells of the grid of side 2 because 4 and 6 are even. Tile $B_j \setminus A_j$ by $(4^j - 3^j)6^{5-j}$ unit cubes. The three regions have pairwise disjoint interiors and union $[0, 6]^5$, so they give a tiling of $[0, 6]^5$ by

$$K_j = 2^{5-j} + 3^5 - 2^j 3^{5-j} + (4^j - 3^j)6^{5-j}$$

cubes, with $K_1 = 1393$, $K_2 = 1655$ and $K_4 = 1247$, and with increments 1392, 1654 and 1246. The maps $x \mapsto x/6$, $x \mapsto x/3$ and $x \mapsto x/2$ carry the tilings of $[0, 6]^5$, $[0, 3]^5$ and $[0, 2]^5$ to cubical decompositions of the unit cube with the same numbers of cubes, and by Lemma 2.1 the set Γ_5 contains the additive semigroup S generated by 31, 211, 1246, 1392 and 1654.

Since $211 \equiv 25 \pmod{31}$ is prime to 31, the residues of $211t$ for $0 \leq t \leq 30$ exhaust $\mathbb{Z}/31\mathbb{Z}$, and $1392 \equiv 28 \equiv 16 \cdot 211$, $1654 \equiv 11 \equiv 24 \cdot 211$ and $1246 \equiv 6 \equiv 30 \cdot 211 \pmod{31}$. The integers

$$w_t = \begin{cases} 211t & \text{for } 0 \leq t \leq 14, \\ 1392 + 1246 = 2638 & \text{for } t = 15, \\ 1392 + 211(t - 16) & \text{for } 16 \leq t \leq 23, \\ 1654 + 211(t - 24) & \text{for } 24 \leq t \leq 30 \end{cases}$$

belong to S , and $w_t \equiv 211t \pmod{31}$, since $16 + 30 \equiv 15 \pmod{31}$. Their maxima on the four ranges are 2954, 2638, 2869 and 2920, so every residue class modulo 31 contains an element of S at most 2954. Let $s \geq 2924$ be an integer, and let t be the index with $s \equiv w_t \pmod{31}$. If $s < w_t$, then $s \leq w_t - 31 \leq 2923$, which is not the case, so $s - w_t$ is a nonnegative multiple of 31 and $s \in S$, as in the proof of [Proposition 3.1](#). Every integer $K \geq 2925$ therefore belongs to $1 + \Gamma_5 = \mathcal{D}(5)$, and $c(5) \leq 2925 < 5^5 = 3125$. The proof uses no computation beyond the arithmetic displayed. $\square$

Proof of Theorem B. The first assertion is [Theorem 4.4](#). Let $p = P(n)$. For $2 \leq b < p$ every $m \leq b$ is prime to p , and $p - 1 \mid n$ gives $p \mid m^n - 1$ by Fermat's theorem, so the list through b has the common divisor p and $h(n) \geq p$. Let $B = \max\{p, M_n\}$. Then $N(B) \geq N(M_n) > n$, because N is nondecreasing, and no prime $q > B$ has $q - 1 \mid n$, because p is the largest such prime. The product in [Theorem 4.4](#) with $M = B$ is therefore empty, the list through B has greatest common divisor 1, and $h(n) \leq B$. If $p \geq M_n$, then $p \leq h(n) \leq B = p$. The bound $M_n \leq \lceil 2\sqrt{n} \rceil$ is in [Lemma 4.1](#), which completes (1.6), and (1.7) is [Corollary 3.2](#) with $b = h(n)$. $\square$

Proof of Corollary C. (i) The bounds $M_n \leq n$ of [Lemma 4.1](#) and $P(n) \leq n + 1$ give $h(n) \leq n + 1$ in (1.6), and (1.7) gives $c(n) < (2n + 2)^n$. Since $2^n - 1 > 1$, $h(n) \geq 3$, and $\gcd(2^n - 1, 3^n - 1) = 1$ means $h(n) = 3$, in which case $c(n) < 6^n$ by (1.7).

(ii) If $n + 1$ is prime, then $P(n) = n + 1 \geq M_n$ and $h(n) = n + 1$ by [Theorem B](#). Conversely, $M_n \leq n < n + 1$, so $h(n) = n + 1$ forces $P(n) = n + 1$ in (1.6), and $n + 1$ is prime.

(iii) This is the equality case of [Theorem B](#), and $P(n) \geq 2\sqrt{n}$ gives $P(n) \geq \lceil 2\sqrt{n} \rceil \geq M_n$.

(iv) If $n + 1$ is composite, every prime p with $p - 1 \mid n$ has $p - 1$ a proper divisor of n , so $p - 1 \leq n/2$ and $P(n) \leq n/2 + 1$. For $n \geq 5$ the integer $M = \lfloor n/2 \rfloor + 1 \geq 3$ has $N(M) \geq 2M + 1 = 2\lfloor n/2 \rfloor + 3 \geq n + 2 > n$ by [Lemma 4.1](#), so $M_n \leq n/2 + 1$. By (1.6), $h(n) \leq n/2 + 1$, and (1.7) gives $c(n) < (2h(n))^n \leq (n + 2)^n = n^n(1 + 2/n)^n < e^2 n^n$.

(v) By (1.7), $c(n) < (2h(n))^n \leq n^n$ when $2h(n) \leq n$. For $n \geq 8$, [Lemma 4.1](#) gives $M_n \leq \lfloor n/2 \rfloor$, and $P(n) \leq n/2$ then gives $h(n) \leq n/2$ in (1.6). $\square$

Proof of Theorem D. Define $\mathcal{A}_0 = \{m^n - 1 : 2 \leq m \leq M_n\}$, whose greatest common divisor is D by [Theorem B](#), and let C_0 be the conductor of $\mathcal{A}_0/D$. The least and largest elements of $\mathcal{A}_0/D$ are $(2^n - 1)/D$ and $(M_n^n - 1)/D$, so [Proposition 3.1](#) gives

$$DC_0 \leq D \left(\frac{2^n - 1}{D} - 1 \right) \left(\frac{M_n^n - 1}{D} - 1 \right) = \frac{(2^n - 1 - D)(M_n^n - 1 - D)}{D}.$$

Let $p_1 < \dots < p_t$ be the prime divisors of D , define $d_i = p_{i+1} \dots p_t$ for $0 \leq i \leq t$, so that $d_0 = D$ and $d_t = 1$, and define $\mathcal{A}_i = \mathcal{A}_{i-1} \cup \{p_i^n - 1\}$ for $1 \leq i \leq t$. The greatest common divisor of $\mathcal{A}_i$ is d_i , because $p_i^n - 1 \equiv -1 \pmod{p_i}$ and every p_j with $j \neq i$ divides $p_i^n - 1$ by Fermat's theorem, since $p_j - 1 \mid n$ and $p_j \nmid p_i$. Let C_i be the conductor of $\mathcal{A}_i/d_i$. The set $\mathcal{A}_{i-1}/d_i$ has greatest common divisor $d_{i-1}/d_i = p_i$, the integer $(p_i^n - 1)/d_i$ is prime to p_i , and $(\mathcal{A}_{i-1}/d_i)/p_i = \mathcal{A}_{i-1}/d_{i-1}$ has conductor C_{i-1} , so [Proposition 3.3](#) gives

$$C_i \leq (p_i - 1) \left(\frac{p_i^n - 1}{d_i} - 1 \right) + p_i C_{i-1}, \quad d_i C_i \leq (p_i - 1)(p_i^n - 1) - (d_{i-1} - d_i) + d_{i-1} C_{i-1}.$$

Adding the second inequality over $1 \leq i \leq t$ gives

$$C_t \leq DC_0 + \sum_{i=1}^t (p_i - 1)(p_i^n - 1) - (D - 1).$$

Every integer $S \geq C_t$ belongs to $\Gamma(\mathcal{A}_t) \subseteq \Gamma_n$ by Lemma 2.2, so $c(n) \leq 1 + C_t$, which is (1.8). For $D = 1$ the bound (1.8) is (3.1) with $b = M_n$.

Assume that $n + 1$ is composite and $n \geq 5$. For odd n the inequality $c(n) < n^n$ is Theorem A, so let $n \geq 8$ be even. Every prime p with $p - 1 \mid n$ has $p - 1$ a proper divisor of n , so $p - 1 \leq n/2$, and Lemma 4.1 gives $M_n \leq n/2$. If $D = 1$, then (1.8) gives $c(n) \leq 1 + (2^n - 2)((n/2)^n - 2) < n^n$. If $D > 1$, then $D \geq 3$, and the first two terms of (1.8) are less than $(2^n - 1)(M_n^n - 1)/3 < (2M_n)^n/3 \leq n^n/3$. Each prime $p \mid D$ contributes $(p-1)(p^n-1) < (n/2)(n/2+1)^n < e^2(n/2)^{n+1}$, because $(1+2/n)^n < e^2$, and there are at most $n/2$ of them, since $p - 1$ is a divisor of n at most $n/2$. The sum in (1.8) is therefore less than $e^2 n^{n+2}/2^{n+2}$, which is at most $e^2 \cdot 64 n^n/1024 < 0.47 n^n$ for $n \geq 8$, because $n^2/2^{n+2}$ decreases for $n \geq 3$. Altogether $c(n) < n^n/3 + 0.47 n^n < n^n$.

Assume that $n + 1$ is prime. Then $n + 1 > M_n$ and $n \mid n$, so $n + 1$ divides D , and the term $p = n + 1$ of (1.8) is $n((n + 1)^n - 1) < n(n + 1)^n$. The other primes $p \mid D$ have $p \leq n/2 + 1$, and their terms sum to less than $e^2 n^{n+2}/2^{n+2}$ as before. The first two terms of (1.8) are less than $(2^n - 1)(M_n^n - 1)/(n + 1) < (2M_n)^n$. This proves (1.9). Finally $n(n + 1)^n = n^{n+1}(1 + 1/n)^n$ with $(1 + 1/n)^n \rightarrow e$, while $(2M_n)^n \leq (4\sqrt{n} + 2)^n$ and $e^2 n^{n+2}/2^{n+2}$ are $o(n^{n+1})$, so the right-hand side of (1.9) is $(e + o(1))n^{n+1}$. $\square$

Proposition 5.3 (The congruence obstruction). *Let $n \geq 2$ and $M \geq 2$ be integers, and let $D = \gcd(2^n - 1, \dots, M^n - 1)$. Every tiling of a cube of integer side $m \leq M$ by cubes of integer sides has a number of cubes $K \equiv 1 \pmod{D}$, and every cubical decomposition obtained from the unit cube by finitely many replacements of a cube by a scaled copy of such a tiling has $K \equiv 1 \pmod{D}$.*

Proof. Let the tiling consist of K cubes of sides $s_1, \dots, s_K$. Then $1 \leq s_i \leq m \leq M$, so $s_i^n \equiv 1 \pmod{D}$, trivially for $s_i = 1$ and by the definition of D otherwise, and in the same way $m^n \equiv 1 \pmod{D}$. The volume identity $m^n = \sum_{i=1}^K s_i^n$ gives $1 \equiv m^n \equiv K \pmod{D}$. The unit cube alone has $K = 1$, and each replacement of a cube by a scaled copy of a tiling with K' cubes adds $K' - 1 \equiv 0 \pmod{D}$ to the count, by Lemma 2.1. $\square$

When $N(M) > n$, Theorem 4.4 identifies D with the product of the primes $q > M$ with $q - 1 \mid n$, so for even n and a prime $p > M$ with $p - 1 \mid n$, no composition of tilings of grids of side at most M reaches a count outside the class 1 modulo p . This is the obstruction behind $h(n) \geq P(n)$, and behind the rows $n = 6$ and $n = 8$ of Table 4, where the tilings of the grids of side less than $P(6) = 7$ and $P(8) = 5$ contribute only to the class 1 modulo $P(n)$.

For $n = 3$ the question is open, since $c(3) \geq 15$ is proven [3] and $c(3) = 48$ is the conjecture of Meier. By Theorems A and D, $c(n) < n^n$ for every $n \geq 5$ with $n + 1$ composite, so the question (1.1) is confined to the dimensions in which $n + 1$ is prime. There the bound (1.9) has the order n^{n+1} of the bounds of Burgess and Erdős and of Connor and Marmorino [3], whose constant 1.8 is smaller than e , and the expectation of Erdős that $c(n) > n^n$ in these dimensions is neither confirmed nor refuted here. The proofs above use no computation, and Appendix A enters only through Theorem E.

APPENDIX A. EXACT COMPUTATIONS

Proposition A.1 (Values of $h(n)$). *Table 1 lists $h(n)$, $P(n)$ and M_n for $2 \leq n \leq 61$, and Figure 1 plots $h(n)$ for $n \leq 300$. For every $2 \leq n \leq 1000$ the values satisfy $P(n) \leq h(n) \leq \max\{P(n), M_n\}$, with $h(n) = P(n)$ whenever $P(n) \geq M_n$, as Theorem B requires. In this range $h(n) = P(n)$ for 490 values of n and $h(n) = 3$ for 429 values. The even n with $h(n) > P(n)$ are*

$$86, 146, 214, 338, 386, 428, 602, 734, 794, 926,$$

with $h(n) \in \{5, 7\}$ and $P(n) \in \{3, 5\}$, and the largest value of $h(n)$ at an odd n is $h(779) = 17$. The threshold takes the values $M_3 = 3$, $M_{19} = 6$, $M_{100} = 13$ and $M_{1000} = 41$, against $\lceil 2\sqrt{1000} \rceil = 64$.

Proof. The accompanying program computes $h(n)$ by successive greatest common divisors of the integers $m^n - 1$, $P(n)$ by trial division, and $N(M)$ by counting coprime pairs, all in exact integer arithmetic, and checks the inequalities for every $n \leq 1000$. $\square$

n	h	P	M_n	n	h	P	M_n	n	h	P	M_n
2	3	3	2	22	23	23	6	42	43	43	8
3	3	2	3	23	5	2	7	43	5	2	9
4	5	5	3	24	13	13	7	44	23	23	9
5	3	2	3	25	3	2	7	45	3	2	9
6	7	7	3	26	3	3	7	46	47	47	9
7	3	2	4	27	3	2	7	47	3	2	9
8	5	5	4	28	29	29	7	48	17	17	9
9	3	2	4	29	3	2	7	49	3	2	9
10	11	11	4	30	31	31	7	50	11	11	9
11	5	2	5	31	3	2	7	51	3	2	9
12	13	13	5	32	17	17	7	52	53	53	9
13	3	2	5	33	5	2	7	53	3	2	9
14	3	3	5	34	3	3	7	54	19	19	9
15	3	2	5	35	7	2	8	55	5	2	10
16	17	17	5	36	37	37	8	56	29	29	10
17	3	2	5	37	3	2	8	57	3	2	10
18	19	19	5	38	3	3	8	58	59	59	10
19	3	2	6	39	3	2	8	59	3	2	10
20	11	11	6	40	41	41	8	60	61	61	10
21	3	2	6	41	3	2	8	61	3	2	10

TABLE 1. The least grid size $h(n)$ with $\gcd(2^n - 1, \dots, h(n)^n - 1) = 1$, the largest prime $P(n)$ with $P(n) - 1 \mid n$, and the threshold M_n , for $2 \leq n \leq 61$. In every row $P(n) \leq h(n) \leq \max\{P(n), M_n\}$.

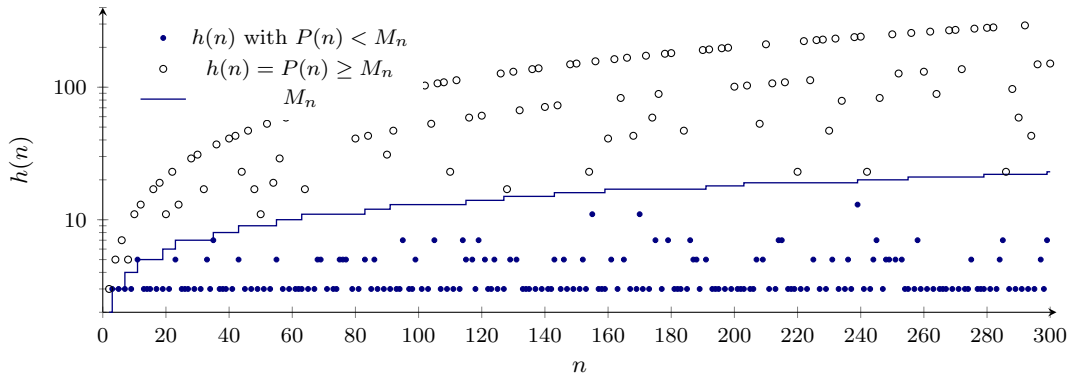


FIGURE 1. The values $h(n)$ for $2 \leq n \leq 300$ on a logarithmic scale. The circles are the dimensions with $P(n) \geq M_n$, where $h(n) = P(n)$ lies on one of the lines $n + 1$, $n/2 + 1$, $n/3 + 1$ and below. The dots are the other dimensions, where $h(n) \leq M_n$, and the step function is M_n .

Proposition A.2 (The refinement semigroups). *For $2 \leq n \leq 12$, Table 2 lists the exact value of $1 + \text{cond}\{m^n - 1 : 2 \leq m \leq h(n)\}$, which is the least count from which the chains of refinements (2.3) with grids of size at most $h(n)$ realise every integer, against the bound $1 + (2^n - 2)(h(n)^n - 2)$ of Corollary 3.2. The two agree exactly when $h(n) = 3$.*

Proof. The conductor is computed from the minimum representatives of the residue classes modulo $2^n - 1$, by shortest paths in the graph on $\mathbb{Z}/(2^n - 1)\mathbb{Z}$ whose edges $r \rightarrow r + u$ have weight u for each generator u , as in Proposition 3.1. The equality for two generators is the theorem of Sylvester. $\square$

n	$h(n)$	$1 + \text{cond}\{m^n - 1 : 2 \leq m \leq h(n)\}$	$1 + (2^n - 2)(h(n)^n - 2)$
2	3	15	15
3	3	151	151
4	5	2 643	8 723
5	3	7 231	7 231
6	7	711 651	7 294 115
7	3	275 311	275 311
8	5	1 890 243	99 218 243
9	3	10 037 311	10 037 311
10	11	259 379 677 395	26 508 047 940 179
11	5	1 089 805 531	99 902 339 659
12	13	279 661 050 002 883	95 382 360 491 429 027

TABLE 2. The exact cutoff of the refinement method with grids of size at most $h(n)$, against the bound of Corollary 3.2.

Proposition A.3 (Guillotine decompositions). *For $2 \leq n \leq 8$ let S_n be the additive semigroup generated by the integers $K - 1$ with $K \in G(m, \dots, m)$ and $2 \leq m \leq m_n$, where m_n is the grid size in Table 4. Then $1 + S_n \subseteq \mathcal{D}(n)$, and $1 + \text{cond } S_n$ is the bound on $c(n)$ in the table. In particular $c(2) = 6$, $c(3) \leq 48$, $c(4) \leq 719$, $c(5) \leq 1891$, $c(6) \leq 279864$, $c(7) \leq 67375$ and $c(8) \leq 1564913$, and the elements of $1 + S_3$ below 48 are*

$$1, 8, 15, 20, 22, 27, 29, 34, 36, 38, 39, 41, 43, 45, 46.$$

Proof of Proposition A.3 and of Theorem E. The program computes the sets $G(l)$ by the recursion of Lemma 2.3 over the multisets of side lengths at most m_n , storing each set of counts as a bit vector, and $1 + S_n \subseteq \mathcal{D}(n)$ by Lemmas 2.1 and 2.3. The conductor is computed as in Proposition A.2. For every generator that occurs in a minimum representative of a residue class the program reconstructs an explicit guillotine tiling of an m -cube with that number of cubes, lists its cubes with integer corners and sides, and verifies that the cubes lie in the m -cube and cover each of its m^n unit cells exactly once. For $n = 2$ the elements of $1 + S_2$ below 6 are 1 and 4, and $c(2) = 6$ is the classical value.

For $n = 4$ the modulus is $a = 2^4 - 1 = 15$, and Table 3 lists the modulus and the thirteen further generators that occur in the minimum representatives, each with the size of the grid that it tiles, and the fifteen representatives w_r . Every positive representative except $w_{14} = 434 = 65 + 369$ is a generator. The largest is $w_{12} = 732$, so by Proposition 3.1 every integer $S \geq 732 - 15 + 1 = 718$ lies in S_4 , and every $K \geq 719$ is the number of cubes of a decomposition of $[0, 1]^4$. The count $733 = 1 + 732$ is realised by a single guillotine tiling of the grid of size 12. $\square$

The list for $n = 3$ is the known list of numbers of cubes in a decomposition of the cube below 48 (sequence A014544 of the OEIS), and the equality $\mathcal{D}(3) = 1 + S_3$ would imply the conjecture of Meier. In dimensions 6 and 8 every tiling of a grid of size less than $P(n)$ has a number of cubes congruent to 1 modulo $P(n)$ by Proposition 5.3, and the bounds there are governed by the primes

$K-1$	15	65	130	319	369	498	516	533	551	598	601	722	727	732
m	2	3	6	5	5	10	12	10	9	10	9	10	10	12
r	0	1	2	3	4	5	6	7	8	9	10	11	12	13
w_r	0	601	722	498	319	65	516	727	533	369	130	551	732	598

TABLE 3. Dimension four. Above, the modulus 15 and the thirteen increments $K-1$ of guillotine tilings of m -cubes that occur in the minimum residue representatives. Below, the minimum representative w_r of each residue r modulo 15 in S_4 . The maximum 732 gives $c(4) \leq 719$.

n	m_n	generators	$1 + \text{cond } S_n$	(1.7)	earlier bound
2	16	245	6	15	6
3	12	1 620	48	151	48
4	12	18 967	719	8 723	734
5	8	28 188	1 891	7 231	1 891
6	8	44 839	279 864	7 294 115	246 964
7	6	95 026	67 375	275 311	67 375
8	5	774	1 564 913	99 218 243	123 967 790

TABLE 4. Upper bounds on $c(n)$ from guillotine tilings of the grids of size at most m_n : the number of generators $K-1$, the bound $1 + \text{cond } S_n$, the bound (1.7), and the earlier bound: classical for $n = 2, 3$, Hudelson [8] for $n = 5$, Prather (arXiv:1910.06206) for $n = 4, 6, 7$, and $\lfloor e^2 n^n \rfloor$ of Connor and Marmorino [3] for $n = 8$.

7 and 5. The bounds for $n = 5$ and $n = 7$ reproduce the earlier ones, the bound for $n = 6$ is weaker than Prather's, the bound for $n = 8$ improves the general bound of Connor and Marmorino, and the bound for $n = 4$ improves the earlier one and refutes the conjectured value $c(4) = 734$. Grids of size at most 16 for $n = 4$, 12 for $n = 5$ and 9 for $n = 6$ do not lower the bounds.

The accompanying programs verify every inequality of Proposition A.1 for $n \leq 1000$, compute the conductors of Propositions A.2 and A.3, and reconstruct and verify the tilings behind Tables 3 and 4. Their inputs and recorded outputs are provided with the source.

REFERENCES

- [1] A. Brauer, On a problem of partitions, *Amer. J. Math.* **64** (1942), 299–312.
- [2] A. Brauer and J. E. Shockley, On a problem of Frobenius, *J. Reine Angew. Math.* **211** (1962), 215–220.
- [3] P. Connor and P. Marmorino, Decomposing cubes into smaller cubes, *J. Geom.* **109** (2018), no. 1, Paper No. 19, 11 pp.
- [4] M. Dehn, Über die Zerlegung von Rechtecken in Rechtecke, *Math. Ann.* **57** (1903), 314–332.
- [5] P. Erdős, Remarks on some problems in number theory, *Math. Balkanica* **4** (1974), 197–202.
- [6] N. J. Fine and I. Niven, Problem E724, *Amer. Math. Monthly* **53** (1946), 271; solution, **54** (1947), 41–42.
- [7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, Oxford, 2008.
- [8] M. Hudelson, Dissecting d -cubes into smaller d -cubes, *J. Combin. Theory Ser. A* **81** (1998), no. 2, 190–200.
- [9] C. Meier, Decomposition of a cube into smaller cubes, *Amer. Math. Monthly* **81** (1974), 630–631.
- [10] J. L. Ramírez Alfonsín, *The Diophantine Frobenius Problem*, Oxford Lecture Series in Mathematics and its Applications 30, Oxford University Press, Oxford, 2005.

LONDON, UNITED KINGDOM

Email address: budden@pingyou.com