EQUAL PAIRWISE GREATEST COMMON DIVISORS AND SUNFLOWERS

HRISHI SUNDER, SOURISH KUMRAWAT, AND KIREET CHERI

Abstract. Fix an integer $r \geq 3$. Let $f_r(N)$ be the largest size of a set $A \subseteq \{1, \dots, N\}$ with no r-element subset $\{a_1, \dots, a_r\}$ for which all pairwise greatest common divisors $\gcd(a_i, a_j)$ are equal. We encode each integer by the set of its prime-power divisibility layers and reduce the problem to the sunflower lemma for set systems. This gives

$$f_r(N) \geq \exp\left((\log(r-1) + o(1))\frac{\log N}{\log\log N}\right),$$
$$f_r(N) \leq \exp\left(O_r\left(\frac{\log N \, \log\log\log N}{\log\log N}\right)\right).$$

In particular, $f_r(N) = N^{o(1)}$.

1. Introduction

For a fixed integer $r \geq 3$, define $f_r(N)$ to be the largest cardinality of a set $A \subseteq \{1, \dots, N\}$ such that no r-element subset $\{a_1, \dots, a_r\} \subseteq A$ satisfies

$$\gcd(a_i, a_j) = d \qquad (1 \leq i < j \leq r)$$

for some integer d. Thus A is forbidden to contain r distinct elements whose pairwise greatest common divisors all have the same value.

The problem is naturally governed by sunflowers. Recall that a family $F_1, \dots, F_r$ of sets is an r-sunflower if all pairwise intersections $F_i \cap F_j$ are equal. Equivalently, there is a set K, called the kernel, such that

$$F_i \cap F_j = K \qquad (1 \leq i < j \leq r).$$

The bounds below do not determine the sharp asymptotic order, but they give an estimate $f_r(N) = N^{o(1)}$. The main estimate is the following.

Theorem 1.1. *Fix $r \geq 3$. As $N \to \infty$,*

$$f_r(N) \geq \exp\left((\log(r-1) + o(1))\frac{\log N}{\log\log N}\right),$$
$$f_r(N) \leq \exp\left(O_r\left(\frac{\log N \, \log\log\log N}{\log\log N}\right)\right).$$

Consequently,

$$f_r(N) = N^{o(1)}.$$

Date: April 2026.

2. Encoding Divisors as Sets

For a positive integer n, write

$$n = \prod_p p^{v_p(n)}.$$

Associate to n the finite set

$$S(n) = \{(p, j) : 1 \le j \le v_p(n)\}.$$

This encoding records prime-power divisibility with multiplicity. It is injective, and for all positive integers a, b one has

$$S(a) \cap S(b) = S(\gcd(a, b)).$$

Therefore distinct integers $a_1, \ldots, a_r$ have all pairwise greatest common divisors equal if and only if the sets

$$S(a_1), \ldots, S(a_r)$$

form an r-sunflower.

3. The Lower Bound

Let p_m denote the m-th prime. Partition the primes into consecutive blocks of size $r - 1$:

$$B_j = \{p_{(j-1)(r-1)+1}, \ldots, p_{j(r-1)}\}.$$

Let t be maximal subject to

$$\prod_{j=1}^{t} p_{j(r-1)} \le N.$$

By the prime number theorem,

$$\sum_{j=1}^{t} \log p_{j(r-1)} = (1 + o(1)) t \log t,$$

and hence

$$t = (1 + o(1)) \frac{\log N}{\log \log N}.$$

Define

$$A = \left\{ \prod_{j=1}^{t} q_j : q_j \in B_j \right\}.$$

Every element of A is at most

$$\prod_{j=1}^{t} p_{j(r-1)} \le N,$$

so $A \subseteq \{1, \ldots, N\}$. Moreover,

$$|A| = (r-1)^t = \exp\left((\log(r-1) + o(1)) \frac{\log N}{\log\log N} \right).$$

It remains to check that A is admissible. Suppose, to the contrary, that distinct elements $a_1, \ldots, a_r \in A$ have all pairwise greatest common divisors equal. Fix a block B_j. Each a_i contains exactly one prime from B_j.

If the common greatest common divisor contains a prime from B_j, then every pair a_i, a_ℓ shares that same prime. Since each a_i uses only one prime from B_j, all r elements choose the same prime from B_j. If the common greatest common divisor contains no prime from B_j, then no pair a_i, a_ℓ may share a prime from B_j. This is impossible, since r choices are being made from a block of only $r-1$ primes.

Thus in every block B_j, all a_i choose the same prime. Hence

$$a_1 = \cdots = a_r,$$

contrary to the assumption that the a_i are distinct. This proves the lower bound in Theorem 1.1.

4. The Upper Bound

We use the following consequence of Theorem 1 of Bell, Chueluecha, and Warnke [2], which sharpens the earlier sunflower bound of Alweiss, Lovett, Wu, and Zhang [1].

Lemma 4.1 (Sunflower lemma). *For each fixed $r \geq 3$, there is a constant $C_r > 0$ such that every family $\mathcal{F}$ of finite sets of size at most K containing no r-sunflower satisfies*

$$|\mathcal{F}| \leq (C_r \log K)^K$$

for all $K \geq 2$.

Proof. Let $C > 0$ be the absolute constant in Theorem 1 of [2]. That theorem says that every family of at least $(Cr \log K)^K$ distinct K-element sets contains an r-sunflower.

It remains only to pass from sets of size at most K to K-element sets. For each $S \in \mathcal{F}$, adjoin $K - |S|$ new dummy elements that are used for this set only, and let S' be the resulting K-element set. The padded family

$$\mathcal{F}' = \{S' : S \in \mathcal{F}\}$$

has $|\mathcal{F}'| = |\mathcal{F}|$. If $S'_1, \ldots, S'_r$ formed an r-sunflower, then no dummy element could lie in the intersection of two distinct padded sets. Removing the dummy elements would therefore show that the original sets $S_1, \ldots, S_r$ form an r-sunflower. Thus $\mathcal{F}'$ is also sunflower-free. Applying the theorem of Bell, Chueluecha, and Warnke and absorbing the fixed factor r into the constant gives the claimed bound. □

We also record a standard Rankin estimate in the special form needed below.

Lemma 4.2. *Let $L = \log N$. The number of L-smooth integers at most N is*

$$\exp\left(O\left(\frac{L}{\log L}\right)\right).$$

Proof. Let $\Psi(N, L)$ denote the number of L-smooth integers at most N, and take $\sigma = 1/\log L$. Rankin's method gives

$$\Psi(N, L) \leq N^\sigma \prod_{p \leq L} (1 - p^{-\sigma})^{-1}.$$

Here

$$N^\sigma = \exp\left(\frac{L}{\log L}\right).$$

It remains to bound the Euler product. For $p > \sqrt{L}$, each factor $(1-p^{-\sigma})^{-1}$ is bounded by an absolute constant, and the total contribution to the logarithm of the product is

$$O(\pi(L)) = O\left(\frac{L}{\log L}\right).$$

For $p \leq \sqrt{L}$, the inequality $1 - e^{-u} \gg u$ for $0 \leq u \leq 1$, applied with $u = \log p/\log L$, gives

$$(1 - p^{-\sigma})^{-1} \ll \frac{\log L}{\log p}.$$

Thus these primes contribute at most

$$O(\pi(\sqrt{L}) \log\log L) = O\left(\frac{\sqrt{L}\,\log\log L}{\log L}\right) = O\left(\frac{L}{\log L}\right)$$

to the logarithm of the product. Therefore

$$\prod_{p \leq L} (1 - p^{-\sigma})^{-1} \leq \exp\left(O\left(\frac{L}{\log L}\right)\right),$$

which proves the claim. ☐

Proof of the upper bound in Theorem 1.1. Let $A \subseteq \{1, \ldots, N\}$ be admissible, and put $L = \log N$. For each $n \in A$, write

$$n = s(n)h(n),$$

where every prime factor of $s(n)$ is at most L, and every prime factor of $h(n)$ is larger than L. Thus $s(n)$ is the L-smooth part of n, and $\gcd(s(n), h(n)) = 1$.

By Lemma 4.2, the number of possible values of $s(n)$ is at most

$$\exp\left(O\left(\frac{L}{\log L}\right)\right).$$

Fix one such value s, and consider the fiber

$$A_s = \{h : sh \in A,\ s(sh) = s\}.$$

Every prime factor of $h \in A_s$ is larger than L. Hence

$$h \geq L^{\Omega(h)}.$$

Here $\Omega(h)$ denotes the number of prime factors of h, counted with multiplicity. Since $h \leq N$, it follows that

$$\Omega(h) \leq \frac{\log N}{\log L} = \frac{L}{\log L}.$$

Set

$$K = \left\lfloor \frac{L}{\log L} \right\rfloor.$$

For all sufficiently large N, $K \geq 2$, and every set $S(h)$ with $h \in A_s$ has size at most K.

The family

$$\mathcal{H}_s = \{S(h) : h \in A_s\}$$

contains no r-sunflower. Indeed, if distinct $h_1, \ldots, h_r \in A_s$ gave an r-sunflower, then

$$S(h_i) \cap S(h_j)$$

would be independent of the pair $i < j$. Equivalently,

$$\gcd(h_i, h_j) = d \qquad (1 \leq i < j \leq r)$$

for some integer d. Since each h_i is coprime to s, this would imply

$$\gcd(sh_i, sh_j) = sd \qquad (1 \leq i < j \leq r),$$

producing a forbidden r-element subset of A. This contradicts the admissibility of A.

By Lemma 4.1,

$$|A_s| = |\mathcal{H}_s| \leq (C_r \log K)^K.$$

Summing over the possible smooth parts s, we obtain

$$|A| \leq \exp\left(O\left(\frac{L}{\log L}\right)\right)(C_r \log K)^K.$$

Since

$$K = \frac{L}{\log L} + O(1),$$

we have

$$\log(C_r \log K)^K = K \log(C_r \log K) = O_r\left(\frac{L \log\log L}{\log L}\right).$$

Therefore

$$|A| \leq \exp\left(O_r\left(\frac{L \log\log L}{\log L}\right)\right).$$

Substituting $L = \log N$ gives

$$|A| \leq \exp\left(O_r\left(\frac{\log N \ \log\log\log N}{\log\log N}\right)\right).$$

Since A was arbitrary, this proves the upper bound. $\square$

Proof of Theorem 1.1. The lower bound was proved in Section 3, and the upper bound was proved in Section 4. Since

$$\frac{\log N \ \log\log\log N}{\log\log N} = o(\log N),$$

the upper bound also implies $f_r(N) = N^{o(1)}$. □

Remark 4.3. The lower-bound construction uses only squarefree integers, while the upper bound needs the full prime-power encoding $S(n)$. This is why the divisor-layer representation is a convenient way to make the greatest-common-divisor condition exactly identical to the sunflower condition.

Works Cited

[1] R. Alweiss, S. Lovett, K. Wu, and J. Zhang, Improved bounds for the sunflower lemma, *Ann. of Math. (2)* **194** (2021), no. 3, 795–815. https://doi.org/10.4007/annals.2021.194.3.5.

[2] T. Bell, S. Chueluecha, and L. Warnke, Note on sunflowers, *Discrete Math.* **344** (2021), no. 7, Paper No. 112367. https://doi.org/10.1016/j.disc.2021.112367.