NUMBERS DIVISIBLE BY A LARGE SHIFTED PRIME AND LARGE TORSION SUBGROUPS OF CM ELLIPTIC CURVES

NATHAN MCNEW, PAUL POLLACK, AND CARL POMERANCE

Abstract. We sharpen a 1980 theorem of Erdős and Wagstaff on the distribution of positive integers having a large shifted prime divisor. Specifically, we obtain precise estimates for the quantity $N(x,y) := \#\{n \le x : \ell - 1 \mid n \text{ for some } \ell - 1 > y,\ \ell \text{ prime}\}$, in essentially the full range of x and y. We then present an application to a problem in arithmetic statistics. Let $T_{\mathrm{CM}}(d)$ denote the largest order of a torsion subgroup of a CM elliptic curve defined over a degree d number field. Recently, Bourdon, Clark, and Pollack showed that the set of d with $T_{\mathrm{CM}}(d) > y$ has upper density tending to 0, as $y \to \infty$. We quantify the rate of decay to 0, proving that the upper and lower densities of this set both have the form $(\log y)^{-\beta+o(1)}$, where $\beta = 1 - \frac{1+\log\log 2}{\log 2}$ (the *Erdős–Ford–Tenenbaum constant*).

1. Introduction

1.1. **Large shifted prime factors.** For any fixed y, no matter how large, the set of positive integers divisible by at least one prime $\ell > y$ has asymptotic density 1. Indeed, the set of integers made up only of primes in $[2, y]$ has counting function $O((\log x)^{\pi(y)})$, and so such numbers comprise a very sparse subset of the positive integers. It is perhaps somewhat surprising that replacing ℓ with $\ell - 1$ leads to a very different story; in fact, the set of n divisible by a shifted prime $\ell - 1 > y$ has upper density tending to 0, as $y \to \infty$. (Moreover, it is an easy consequence of Proposition 1.1 below that for each y, this set of n has a density, so that the adjective "upper" is not necessary; see, e.g., [21, Lemma 1].) The reason for this is that most integers m have about $\log\log y$ prime factors in $[1, y]$, as do shifted primes $\ell - 1$. Thus, integers of the form $(\ell - 1)m$ would tend to have considerably more than $\log\log y$ primes in $[1, y]$, which is abnormally large. Putting some rigor behind this heuristic, we have the following result, due to Erdős and Wagstaff [8, proof of Theorem 2, p. 107]. Put

$$N(x,y) := \#\{n \le x : (\ell - 1) \mid n \text{ for some } \ell - 1 > y\}.$$

In this definition, as in the rest of the paper, we adopt the convention that ℓ always denotes a prime.

Proposition 1.1. *There are positive constants c and δ such that the following holds. Whenever x and y are sufficiently large,*

$$N(x,y) \le c\frac{x}{(\log y)^{\delta}}.$$

In this paper, we obtain sigificantly more precise results about $N(x,y)$.

For the rest of this paper, we let

$$\beta = 1 - \frac{1 + \log\log 2}{\log 2}$$

2010 *Mathematics Subject Classification.* Primary 11N25, Secondary 11N64, 11G05.

(numerically, $\beta = 0.08607133205\ldots$). The constant β plays an important role in the study of the "anatomy of integers". As one example of its appearance, the asymptotic density of integers with a divisor in $(y, 2y]$ decays like $(\log y)^{-\beta+o(1)}$, as $y \to \infty$. That result was proved by Erdős in 1960 [7] and has been substantially extended and refined by later authors, notably Ford and Tenenbaum. See [9] for the state of the art on these problems.

Our first two theorems imply that as long as $y \to \infty$ and x/y is "fairly large", the *Erdős–Ford–Tenenbaum constant* β is the correct exponent on $\log y$ in the Erdős–Wagstaff result.

Theorem 1.2. *If $x, y \geq 3$, then*

$$N(x,y) \ll \frac{x}{(\log y)^{\beta}\sqrt{\log\log y}}.$$

Theorem 1.3. *Let $\epsilon > 0$. For a certain $\eta = \eta(\epsilon) > 0$ and all sufficiently large x and y (depending on ϵ) satisfying $y \leq x/\exp((\log x)^{1-\eta})$,*

$$N(x,y) \gg_{\epsilon,\eta} \frac{x}{(\log y)^{\beta+\epsilon}}.$$

Theorems 1.2 and 1.3 have the following immediate consequence.

Corollary 1.4. *If $x, y \to \infty$ with $y \leq x/\exp((\log x)^{1-o(1)})$, then*

$$N(x,y) = \frac{x}{(\log y)^{\beta+o(1)}}.$$

For values of y larger than allowed by Corollary 1.4, there is a change in behavior.

Theorem 1.5. *Suppose $x, y \geq 3$ and $y \geq x^{1-1/\log\log x}$. Assume that x/y exceeds a certain absolute constant. Define α by the equation $y = x/\exp((\log x)^{\alpha})$. If $\alpha \geq 1/\log 4$, then*

$$\frac{x}{(\log y)^{\beta+\alpha-1-\log\alpha/\log 2}} \cdot (\log\log(x/y))^{O(1)} \ll N(x,y) \ll \frac{x}{(\log y)^{\beta+\alpha-1-\log\alpha/\log 2}}.$$

If $\alpha \leq 1/\log 4$, then

$$\frac{x(\log\log(x/y))^{O(1)}}{(\log y)^{1-\alpha}} \ll N(x,y) \ll \frac{x}{(\log y)^{1-\alpha}}.$$

Remark 1.6. The assumption that x/y is large is a technical convenience in the proof. The theorem is true for large x if one assumes any condition of the form $x/y \geq 1+\epsilon$. In fact, in the domain where $\frac{x}{y} - 1$ is bounded above and below by positive constants, it is relatively easy to establish an asymptotic formula for $N(x,y)$, as $x \to \infty$. See the final remark at the end of §2.3.

As we now explain, Theorems 1.2 and 1.3 are closely connected to recent studies of the counting function of the range of Carmichael's λ-function.

Carmichael's function $\lambda(m)$ is defined as the exponent of the group $(\mathbb{Z}/m\mathbb{Z})^{\times}$. The values of λ at prime powers ℓ^{α} are discussed in Gauss's *Disquisitiones* [11, Articles 85–91], where it is shown that

$$\lambda(\ell^{\alpha}) = \begin{cases} \ell^{\alpha-1}(\ell-1) & \text{if } \ell \text{ is odd, or if } \ell = 2 \text{ and } \alpha \leq 2, \\ \ell^{\alpha-2}(\ell-1) & \text{if } \ell = 2 \text{ and } \alpha \geq 3. \end{cases}$$

To determine $\lambda(m)$ for an arbitrary m, one can factor m into prime powers and take advantage of the observation that $\lambda(ab) = \operatorname{lcm}[\lambda(a), \lambda(b)]$ when a and b are coprime.

It is clear from the above formulas that if m has a large prime factor, then $\lambda(m)$ is divisible by a large shifted prime. Thus, there is a close connection between the numbers we are trying to count in Theorems 1.2 and 1.3 and the values of the λ-function. In recent work of Luca–Pomerance [18] and Ford–Luca–Pomerance [10], a precise estimate is obtained for the counting function of the image of λ. Namely, as $x \to \infty$,

$$\#\{n \le x : n = \lambda(m) \text{ for some } m\} = x/(\log x)^{\beta+o(1)};$$

see [18, Theorem 1] for the upper bound and [10] for the lower bound. Our proofs of Theorems 1.2 and 1.3 are adaptations of the arguments from [18] and [10], respectively. Actually, our streamlined approach here actually yields a modest improvement over the upper bound of [18]. See the remark following the proof of Theorem 1.2.

1.2. **An application to arithmetic statistics.** If E is an elliptic curve defined over a degree d number field F, a deep theorem of Merel [19] asserts that $\#E(F)[\text{tors}]$ is bounded by a constant depending only on d. It is a folklore conjecture that this constant can be chosen to be a polynomial in d. However, all of the bounds that have so-far been exhibited grow superexponentially.

More reasonable bounds are available if we restrict to special classes of curves. The recent paper [6] presents a sharp result in the CM (complex multiplication) case. Let $T_{\rm CM}(d)$ denote the maximum size of $E(F)[\text{tors}]$ for a CM elliptic curve E over a degree d number field F. Then for $d \ge 3$,

$$T_{\rm CM}(d) \ll d \log\log d, \tag{1}$$

where the implied constant is absolute and effectively computable. (Note that when F does not contain the CM field, such a bound is contained in work of Silverberg [25, 26]; cf. [1, 22].) The result (1) cannot be improved apart from the value of the implied constant, as Breuer [3] has shown that $T_{\rm CM}(d) \gg d \log\log d$ along an infinite sequence of d.

Thus, $T_{\rm CM}(d)$ has upper order $d \log\log d$. What can be shown about its lower order? its average order? its normal order? Such statistical questions were investigated in [2]. Here we content ourselves with recalling only the normal order result. Using the Erdős–Wagstaff theorem, it was shown in [2] that $T_{\rm CM}(d)$ is *typically bounded*. By this, we mean that the set of d with $T_{\rm CM}(d) > y$ has upper density that tends to 0 as $y \to \infty$.

The methods of the present paper allow us to be much more precise. Put

$$D(x,y) = \#\{d \le x : T_{\rm CM}(d) > y\}.$$

The next two theorems provide $D(x,y)$-analogues of Theorem 1.2 and 1.3.

Theorem 1.7. *If $x, y \ge 3$, then*

$$D(x,y) \ll \frac{x}{(\log y)^{\beta}\sqrt{\log\log y}}.$$

Theorem 1.8. *Let $\epsilon > 0$. For a certain $\eta = \eta(\epsilon) > 0$ and all sufficiently large x and y (depending on ϵ) satisfying $y \le x/\exp((\log x)^{1-\eta})$,*

$$D(x,y) \gg_{\epsilon,\eta} \frac{x}{(\log y)^{\beta+\epsilon}}.$$

Thus, $D(x,y) = x/(\log y)^{\beta+o(1)}$ whenever $x, y \to \infty$ and $y \le x/\exp((\log x)^{1-o(1)})$. In analogy with Theorem 1.5, one can also ask about the frequency of still larger values of $T_{\rm CM}(d)$. Here

we only discuss what would seem to be the most interesting case, values close to the maximum possible size. We prove the following theorem by beefing up the arguments of [2] and [3].

Theorem 1.9. *For certain absolute constants $C, C' > 0$, the following statements hold:*

(i) *For all fixed real numbers $\alpha > 0$,*

$$\#\big\{d \in [x/2, x] : \frac{T_{\mathrm{CM}}(d)}{d \log\log d} > \alpha\big\} \le x/\exp((\log x)^{C\alpha + o(1)}), \quad \text{as } x \to \infty.$$

(ii) *For all sufficiently small and fixed $\alpha > 0$,*

$$\#\big\{d \in [x/2, x] : \frac{T_{\mathrm{CM}}(d)}{d \log\log d} > \alpha\big\} \ge x/\exp((\log x)^{C'\alpha + o(1)}), \quad \text{as } x \to \infty.$$

Remark 1.10. We do not know optimal values of the constants appearing in the statement of Theorem 1.9. (This is perhaps not so surprising for (i), since we do not know any explicit admissible value of the implied constant in (1).) Our proof shows that (ii) holds for all $\alpha < \frac{e^\gamma \pi}{\sqrt{3}}$ and $C' = \frac{\sqrt{3}}{e^\gamma \pi}$. So, in particular,

$$\limsup_{d \to \infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} \ge \frac{e^\gamma \pi}{\sqrt{3}}.$$

(This appears to be the first numerically explicit result of its kind.) The constant on the right-hand side is $3.2305\ldots$.

Notation. We remind the reader that ℓ always denotes a prime number. For positive integers n, we let $P(n)$ denote the largest prime factor of n, with the convention that $P(1) = 1$. We use $\omega(n)$ for the number of distinct prime factors of n and $\Omega(n)$ for the total number of prime factors of n, counted with multiplicity. We use $\omega_y(n)$ and $\Omega_y(n)$ to indicate the corresponding counts of prime factors not exceeding y. We let $\tau_k(n)$ denote the k-fold divisor function; we omit the subscript when $k = 2$. If K is a number field, h_K denotes the class number of K, w_K the number of roots of unity contained in K, and Δ_K the discriminant of K. We write $A = o(B)$ to indicate that $A/B \to 0$ and we write $A = O(B)$ when $|A| \le cB$ for some positive constant c; in particular, an expression of the form $O(1)$ may be negative. The notation $A = O(B)$ is synonymous with $A \ll B$. If $A \ll B$ and $B \ll A$, we write $A \asymp B$. Dependence of implied constants on additional parameters is indicated with subscripts.

2. Refinements of the Erdős–Wagstaff theorem: Proofs of Theorems 1.2–1.5

2.1. **Proof of Theorem 1.2.** The proof relies on counting those integers $n = (\ell - 1)m$ by the size of $\Omega_y(n)$. For $\alpha > 0$, let

$$Q(\alpha) = 1 - \alpha + \alpha \log \alpha.$$

Lemma 2.1 (Halász, Norton)**.** *Let $\epsilon > 0$. There is an absolute constant κ such that for $1 \le j \le (2 - \epsilon) \log\log y$ and $3 \le y \le x$, the number of integers $n \le x$ with $\Omega_y(n) = j$ is*

$$\ll_\epsilon \frac{x(\log\log y + \kappa)^j}{j! \log y}.$$

For $3 \le y \le x$ and $1 + \epsilon \le \alpha \le 2 - \epsilon$, the number of $n \le x$ with $\Omega_y(n) > \alpha \log\log y$ is

$$\ll_\epsilon \frac{x}{(\log y)^{Q(\alpha)} \sqrt{\log\log y}}.$$

The first result is in Halász [12] and the second is in Norton [20, Theorem 5.12]. Cf. [15, Theorems 08 and 09, pp. 5–6].

The next result proves Theorem 1.2 in the case when y is large.

Proposition 2.2. *Suppose that $x^{1/3} < y \le x$ and $y \ge 3$. Then*

$$N(x,y) \ll \frac{x}{(\log y)^\beta \sqrt{\log\log y}}.$$

Proof. Let $\alpha = 1/\log 2$ and let $k = \lfloor \alpha \log\log x \rfloor$. By Lemma 2.1 in the case $y = x$, we may assume that $n \le x$ has $\Omega(n) \le k$. Suppose that $n = (\ell-1)m$ with $\ell - 1 > y$. If $\omega(\ell-1) = i$ and $\omega(m) = j$, then we have $i + j \le k$. Using Timofeev [27, Theorem 1], the number of such integers n is at most

$$\sum_{\substack{i+j\le k\\ i\ge 1,\ j\ge 0}} \sum_{\substack{m\le x^{2/3}\\ \omega(m)=j}} \sum_{\substack{y<\ell\le x/m+1\\ \Omega(\ell-1)=i}} 1 \ll \sum_{\substack{i+j\le k\\ i\ge 1,\ j\ge 0}} \sum_{\substack{m\le x^{2/3}\\ \omega(m)=j}} \frac{(x/m)(\log\log(x/m)+\kappa')^{i-1}}{(i-1)!(\log(x/m))^2}$$
$$\ll \sum_{\substack{i+j\le k\\ i\ge 1,\ j\ge 0}} \sum_{\substack{m\le x^{2/3}\\ \omega(m)=j}} \frac{(x/m)(\log\log x+\kappa')^{i-1}}{(i-1)!(\log x)^2}.$$

Here κ' is an absolute constant. Now

$$\sum_{\substack{m\le x^{2/3}\\ \omega(m)=j}} \frac{1}{m} \le \frac{1}{j!}\left(\sum_{p\le x^{2/3}} 1/p + 1/p^2 + \dots\right)^j \le \frac{1}{j!}(\log\log x + \kappa'')^j$$

for an absolute constant κ''. So our count is

$$\ll \frac{x}{(\log x)^2} \sum_{\substack{i+j\le k\\ i\ge 1,\ j\ge 0}} \frac{(\log\log x+\kappa')^{i-1}(\log\log x+\kappa'')^j}{(i-1)!j!}$$
$$= \frac{x}{(\log x)^2} \sum_{0\le l\le k-1} \frac{1}{l!} \sum_{0\le i\le l} \binom{l}{i} (\log\log x+\kappa')^i (\log\log x+\kappa'')^{l-i}$$
$$= \frac{x}{(\log x)^2} \sum_{0\le l\le k-1} \frac{1}{l!} (2\log\log x + \kappa' + \kappa'')^l$$
$$\ll \frac{x(2\log\log x+\kappa'+\kappa'')^{k-1}}{(k-1)!(\log x)^2} \ll \frac{x}{(\log x)^\beta\sqrt{\log\log x}} \le \frac{x}{(\log y)^\beta\sqrt{\log\log y}}.$$

This completes our proof of the proposition. □

Proposition 2.3. *For $3 \le y \le x^{1/3}$, we have*

$$N(x,y) - N(x,y^2) \ll \frac{x}{(\log y)^\beta\sqrt{\log\log y}}.$$

Proof. Let $k = \lfloor \alpha \log\log y \rfloor$, where $\alpha = 1/\log 2$. By Lemma 2.1, we may assume that $n \le x$ has $\Omega_y(n) \le k$. Thus, writing $n = (\ell-1)m$ where $y < \ell - 1 \le y^2$, we have

$$N(x,y) - N(x,y^2) \le \sum_{i+j\le k} \sum_{\substack{\ell:\ y<\ell-1\le y^2\\ \Omega_y(\ell-1)=i}} \sum_{\substack{m\le x/(\ell-1)\\ \Omega_y(m)=j}} 1.$$

By the hypotheses, $x/(\ell-1) \geq x/y^2 \geq y$, so that the inner sum may be upper bounded using Lemma 2.1, getting

$$N(x,y) - N(x,y^2) \ll \sum_{i+j\leq k} \sum_{\substack{\ell:\ y<\ell-1\leq y^2 \\ \Omega_y(\ell-1)=i}} \frac{x(\log\log y+\kappa)^j}{j!\ell\log y}.$$

By partial summation with [27, Theorem 2], we have

$$N(x,y) - N(x,y^2) \ll \sum_{i+j\leq k} \frac{x(\log\log y+\kappa''')^i(\log\log y+\kappa)^j}{i!j!(\log y)^2},$$

with κ''' an absolute constant. As in the proof of Proposition 2.2, we get our result. □

Proof of Theorem 1.2. We may assume that $y \leq x$. We have

$$N(x,y) = \sum_{\nu\geq 0}(N(x,y^{2^\nu}) - N(x,y^{2^{\nu+1}})).$$

When $y^{2^\nu} > x^{1/3}$, there are at most 2 terms, and by Proposition 2.2, we have an acceptable estimate for them (in terms of our current value of y). And, by Proposition 2.3, we have

$$\sum_{y^{2^\nu}\leq x^{1/3}} (N(x,y^{2^\nu}) - N(x,y^{2^{\nu+1}})) \ll \sum_{\nu\geq 0} \frac{x}{(\log(y^{2^\nu}))^\beta\sqrt{\log\log y}} \ll \frac{x}{(\log y)^\beta\sqrt{\log\log y}}.$$

This completes the proof of the theorem. □

Remark 2.4. Theorem 1.2 implies a small improvement on the upper bound of [18] for the count of λ-values. Let $n \in \lambda(\mathbb{Z}^+)\cap[1,x]$, and put $y = x^{1/\log\log x}$. We will assume that $P(n) > y$, since otherwise standard results on the distribution of smooth numbers show that n is restricted to a set of size $O(x/\log x)$ (see [4]). Thus, writing $n = \lambda(m)$, the integer m must have a prime factor $\ell > y$. Then $\ell - 1 \mid n$, and so Theorem 1.2 restricts n to a set of size $O(\frac{x}{(\log y)^\beta\sqrt{\log\log y}})$. This improves the estimate of [18] by a factor of $(\log\log x)^{2.5-\beta}$. In particular, we obtain a clean bound $O(x/(\log x)^\beta)$ on the counting function of the range of λ.

2.2. **Proof of Theorem 1.3.** If $n = \lambda(m)$ for an integer $m > 1$, then $P(m) - 1 \mid n$, and so $P(m) \leq n + 1$. The next proposition asserts that many λ-values have a preimage m with $P(m)$ almost this large.

For each integer $k \geq 2$, define

$$\beta_k = 1 - \frac{k}{\log(2^k-1)}(1 + \log\log(2^k-1) - \log k).$$

Observe that $\beta_k \to \beta$ as $k \to \infty$.

Proposition 2.5. *Let $\epsilon \in (0,1)$. Let k be an integer with $k \geq 2$. There are numbers $\eta = \eta(\epsilon,k) \in (0,1)$ and $x_0 = x_0(\epsilon,k) > 0$ for which the following holds. For all $x > x_0$, there are*

$$\gg_{\epsilon,k} \frac{x}{(\log x)^{\beta_k+\epsilon}}$$

integers n in $(2^{-2k}x, x]$ that can be written in the form $\lambda(m)$, where m is squarefree with k prime factors each being in the residue class $1 \pmod 4$, and $P(m) > n/\exp((\log n)^{1-\eta})$.

Sketch of the proof of Proposition 2.5. We will deduce the proposition by slightly tweaking the construction of [10]. The proof there depends on estimating the sums

$$S_1 = \sum_{2^{-2k}<n\le x} \mu^2(n) r(n) \quad \text{and} \quad S_2 = \sum_{2^{-2k}<n\le x} \mu^2(n) r(n)^2, \tag{2}$$

the first from below and the second from above. Here $r(n)$ is defined on [10, pp. 2014–2015].

The only part of the argument that requires substantial amendment is the estimation of S_1 carried out in [10, §4]. In place of the definition of y in (3-1) on [10, p. 2014], we take

$$z = \exp\left(\frac{(\log x)^{1-\eta}}{28k \log\log x}\right).$$

We will determine η precisely later in the proof. Now proceeding as in [10], we find as a replacement for (4-4) on [10, p. 2016] that

$$b_1 \cdots b_{2^k-1} \le z' := \exp\left(\frac{1}{14k}(\log x)^{1-\eta}\right),$$

however, instead of merely having b_{2^k-1} even, we now require that $4 \mid b_{2^k-1}$. At this point in [10], one places the a_i in dyadic intervals $(A_i/2, A_i]$. There the A_i are powers of 2 exceeding $x^{1/2k}$. We relax this final inequality to the weaker requirement that each

$$A_i > z^9 z'^3.$$

We then resume the arguments of [10], continuing through the first paragraph at the top of p. 2018. The correct condition on D is now that D is a power of 2 with $D \le z'$. The first displayed estimate at the top of p. 2018 becomes

$$\sum_{\mathbf{A},\mathbf{b}} R(\mathbf{A},\mathbf{b}) \ll x \frac{(\log x)^{2^{k-1}-1}}{(\log z)^{k-1}} \sum_{D\le z'} \sum_{z^9 z'^3 < A_0 \le x/D} \frac{1}{A_0 D} \sum_{q \le z^3 z'} \tau_{2^{k-1}+3}(q) E^*(A_0 D; q).$$

Invoking [10, Corollary 1], we obtain enough savings from the innermost sum that — just as in [10] — the above works out to be $O(x/(\log x)^{\beta_k+1})$.

We deviate more substantially from [10] in our treatment of the main term. Given $b_1, \dots, b_{2^k-1}$, the product $A_0 \cdots A_{k-1}$ is the unique power of 2 satisfying

$$\frac{x}{2b_1 \cdots b_{2^k-1}} < A_0 \cdots A_{k-1} \le \frac{x}{b_1 \cdots b_{2^k-1}}.$$

This is so far exactly as in [10, p. 2018]. However, rather than consider all allowable choices for the A_i, we work only with $A_1, \dots, A_{k-1} \in (z^9 z'^3, z^9 z'^4]$. Note that once $A_1, \dots, A_{k-1}$ are selected, A_0 is uniquely determined and (for large x)

$$A_0 > \frac{x}{2b_1 \cdots b_{2^k-1} A_1 \cdots A_{k-1}} > \frac{x}{2z' \cdot z^{9k} z'^{4k}} > 2x \cdot z'^{-14k} = 2x/\exp((\log x)^{1-\eta}).$$

(The strange-seeming factor of 2 is included for reasons which will become clear later.) The number of choices for $A_1, \dots, A_{k-1}$ is $\gg (\log z')^{k-1}$. So in place of the middle display on p. 2018, we now find

$$\sum_{\mathbf{A},\mathbf{b}} M(\mathbf{A},\mathbf{b}) \gg \frac{x}{(\log z)^k} \frac{(\log z')^{k-1}}{(\log x)^k} \sum_{\mathbf{b}} \frac{1}{b_1 \cdots b_{2^k-1}}.$$

As in [10], the sum on $\mathbf{b}$ is $(\log z)^{k-\beta_k+1}(\log\log x)^{O(1)}$. Hence (using $z' \geq z$),

$$\sum_{\mathbf{A},\mathbf{b}} M(\mathbf{A},\mathbf{b}) \gg \frac{x}{(\log x)^k}(\log z)^{k-\beta_k}(\log\log x)^{O(1)}.$$

Recalling the definition of z, we see that if η is chosen sufficiently small in terms of ϵ and k, then this last expression is

$$\gg \frac{x}{(\log x)^{\beta_k+\frac{1}{3}\epsilon}}. \tag{3}$$

Combining this with our upper bound on $\sum_{\mathbf{A},\mathbf{b}} R(\mathbf{A},\mathbf{b})$, we see that (3) also serves a lower bound on our analogue of S_1 (for large x).

Can we write down a sum on n that represents our analogue of S_1, the same way that the sum in (2) represents the original S_1? There is no problem redefining $r(n)$ to use our value of z in place of the original value of y. But in addition, we must also account for the constraints we placed on the A_i. Because of these, S_1 is no longer the sum of terms $r(n)$ (even with z replacing y), but of terms $r'(n)$, where $r'(n)$ is defined like $r(n)$ but only counts representations where each $a_i \in (A_i/2, A_i]$. Then what our above arguments show is that

$$\sum_{2^{-2k}x<n\leq x} \mu(n)^2 r'(n)$$

is bounded below by (3).

To continue, we derive from [10] a corresponding upper bound for our $r'(n)$ in mean square, namely

$$\sum_{2^{-2k}x<n\leq x} \mu(n)^2 r'(n)^2 \ll \frac{x}{(\log x)^{\beta_k-\frac{1}{3}\epsilon}}. \tag{4}$$

In fact, we will argue that this upper bound holds even without considering our new restrictions on A_i; in other words, even if $r(n)$ is used in place of $r'(n)$. We follow the arguments of [10, §6] used to bound S_2 from above. With $r(n)$ defined in terms of the original value of y, those arguments give an upper bound on S_2 of

$$\frac{x}{(\log x)^{\beta_k}}(\log\log x)^{\beta_k}.$$

Unfortunately, we cannot use this upper bound directly, as several intermediate calculations in [10, §6] depend on the estimate

$$\log y = \log x(\log\log x)^{O(1)},$$

which no longer holds with z replacing y. But we do have $\log z = (\log x)(\log x)^{-\eta}$, with η at our disposal, and this is enough. Indeed, whenever $\log x$ appears in [10, §6], it appears to a power bounded in terms of k. So if η is chosen sufficiently small in terms of k, then the final estimate is affected by a factor bounded by an arbitrarily small power of $\log x$. In particular, we can ensure (4) by making η suitably small in terms of ϵ and k.

Applying Cauchy's inequality in the same manner as in [10], we deduce that the number of $n \in (2^{-2k}x, x]$ for which $r'(n) > 0$ is

$$\gg \frac{x}{(\log x)^{\beta_k+\epsilon}}.$$

Whenever $r'(n) > 0$, we have (in the notation of [10, eq. (3-2)])

$$n = \lambda\left(\prod_{i=0}^{k-1}(a_i B_i + 1)\right),$$

where the $a_i B_i + 1$ are k distinct primes. By our choice of A_0, the first of these primes satisfies

$$a_0 B_0 + 1 > a_0 > A_0/2 > x/\exp((\log x)^{1-\eta}) \geq n/\exp((\log n)^{1-\eta}).$$

This completes the proof. □

For $\eta \in (0,1)$, let $\mathcal{S}_\eta$ denote the set of integers n of the form $\lambda(m)$ where m is a squarefree integer with each prime factor in the residue class 1 (mod 4) and $P(m) > n/\exp((\log n)^{1-\eta})$.

Corollary 2.6. *For each $\epsilon > 0$, there are numbers $\eta = \eta(\epsilon) \in (0,1)$ and $x_0 = x_0(\epsilon) > 0$ such that for every $x > x_0$,*

$$\#\mathcal{S}_\eta \cap [1,x] \gg_\epsilon \frac{x}{(\log x)^{\beta+\epsilon}}.$$

Proof. This follows immediately from Proposition 2.5, since $\beta_k \to \beta$ as $k \to \infty$. □

Remark 2.7. By a simple modification of the proof of Proposition 2.5 we may replace the residue class 1 (mod 4) with 1 (mod M) for any fixed positive integer M.

For $x \geq e$ and $\nu \in (0,1)$, let $\xi_\nu(x) = x/\exp((\log x)^{1-\nu})$. It is straightforward to check that ξ_ν is strictly increasing. We let Ξ_ν denote the functional inverse of ξ_ν.

Proof of Theorem 1.3. Given $\epsilon > 0$, we choose a positive $\nu < \frac{1}{2}\eta(\epsilon)$, where $\eta(\cdot)$ is as in the statement of Corollary 2.6.

We take two cases according to the size of y.

Case I: $y \leq x^{1/6}$

Put $Y = (\Xi_\nu(y+1))^2$. We look at all integers $d \leq x$ whose Y-smooth component n is an integer in $(Y^{1/2}, Y]$ having the form $\lambda(m)$ for an m satisfying

$$P(m) > \xi_\nu(n). \tag{5}$$

For large x, we have $Y < x^{2/5}$. Now a lower bound sieve (such as [14, Theorem 1, p. 201]) implies that the number of d corresponding to a given n is $\asymp \frac{x}{n \log Y}$. We sum over allowable choices of $n \in (Y^{1/2}, Y]$. Since $\nu < \eta(\epsilon)$, Corollary 2.6 along with partial summation implies that the number of d obtained in this way is

$$\gg \frac{x}{(\log Y)^{\beta+\epsilon}} \gg \frac{x}{(\log y)^{\beta+\epsilon}}.$$

We claim that all of these integers d are divisible by an $\ell - 1$ with $\ell - 1 > y$. Let m be a λ-preimage of n satisfing (5), and let $\ell = P(m)$. Then $\ell - 1 \mid \lambda(m) = n \mid d$, and $\ell - 1 > \xi_\nu(n) - 1 > \xi_\nu(Y^{1/2}) - 1 = y$.

Case II: $x^{1/6} < y \leq \xi_\nu(x)$

We consider $d \in (\Xi_{2\nu}(y+1), x]$ of the form $\lambda(m)$ with $P(m) > \xi_{2\nu}(d)$. Since $2\nu < \eta(\epsilon)$, Corollary 2.6 applies, and shows that the number of these d is

$$\gg \frac{x}{(\log x)^{\beta+\epsilon}} \gg \frac{x}{(\log y)^{\beta+\epsilon}}.$$

(We use here that $\Xi_{2\nu}(y+1) \le \Xi_{2\nu}(\xi_\nu(x)+1) \le x/\exp((\log x)^{1-\nu+o(1)})$, as $x \to \infty$, so that discarding those $d \le \Xi_{2\nu}(y+1)$ does not change the estimate from Corollary 2.6.) Letting $\ell = P(m)$, we have $\ell - 1 > \xi_{2\nu}(d) - 1 > y$ and $\ell - 1 \mid \lambda(m) = d$. □

2.3. **Proof of Theorem 1.5.** We split the proof of Theorem 1.5 into two pieces. The next result completely handles the cases $\alpha \le 1/\log 4$ and yields the claimed lower bound when $\alpha \ge 1/\log 4$.

Theorem 2.8. *Suppose that $x, y \ge 3$, that $y \ge x^{1-1/\log\log x}$, and that x/y exceeds a certain absolute constant. Define α by the equation $y = x/\exp((\log x)^\alpha)$. Then for $\alpha \le 1/\log 4$, we have*

$$\frac{x(\log\log(x/y))^{O(1)}}{(\log y)^{1-\alpha}} \ll N(x,y) \ll \frac{x}{(\log y)^{1-\alpha}}.$$

Further, for $1/\log 4 \le \alpha < 1$, we have

$$N(x,y) \gg \frac{x(\log\log(x/y))^{O(1)}}{(\log y)^{\beta+\alpha-1-(\log\alpha)/\log 2}}.$$

Proof. Let $z = x/y = \exp((\log x)^\alpha) \le x^{1/\log\log x}$. Let $r(n)$ denote the number of representations of n in the form $m(\ell-1)$, where $\ell - 1 > y$. Note that if $n \le x$, then $m \le x/(\ell-1) < x/y = z$. We have

$$N(x,y) = \sum_{\substack{n\le x\\ r(n)>0}} 1 \le \sum_{n\le x} r(n). \tag{6}$$

This last sum is easy to estimate:

$$\sum_{n\le x} r(n) \le \sum_{m<z} \sum_{\ell \le x/m+1} 1 \ll \sum_{m\le z} \frac{x}{m\log x} \ll \frac{x\log z}{\log x} = \frac{x}{(\log x)^{1-\alpha}}. \tag{7}$$

Thus, we have an upper bound for $N(x,y)$, and we shall see that it is a fairly tight upper bound for $\alpha \le 1/\log 4$. To get a lower bound, we first replace $r(n)$ with $r_1(n)$, the number of representations of n as $m(\ell-1)$ where $\ell - 1 > y$, $\Omega(m) \le \log\log z$ and $\Omega_z(\ell-1) \le \log\log z$. We have

$$N(x,y) \ge \sum_{\substack{n\le x\\ r_1(n)>0}} 1.$$

Thus, by Cauchy's inequality,

$$N(x,y) \ge \frac{M_1^2}{M_2}, \quad \text{where } M_1 := \sum_{n\le x} r_1(n),\ M_2 := \sum_{n\le x} r_1(n)^2. \tag{8}$$

Using Timofeev [27, Theorem 3] and either Halász [12] or Sárközy [24], a simple calculation shows that

$$M_1 \asymp \frac{x}{(\log x)^{1-\alpha}}, \tag{9}$$

that is, the same estimate holds as with $r(n)$. (To obtain the lower bound here, we use our assumption that $z = x/y$ exceeds an appropriate absolute constant.)

Our task now is to establish an upper bound for M_2. Note that $r_1(n)^2$ is the number of solutions to

$$n = m_1(\ell_1 - 1) = m_2(\ell_2 - 1),\ \Omega(m_i) \le \log\log z,\ \ell_i - 1 > y,\ \Omega_z(\ell_i - 1) \le \log\log z,\ i = 1, 2.$$

We have already counted those cases where $m_1 = m_2$, so assume now that $m_1 \ne m_2$. Given such a dual representation of n, write $a = \gcd(m_1, m_2)$, $m_1 = ab$, $m_2 = ac$. Thus $b \mid \ell_2 - 1$ and $c \mid \ell_1 - 1$. With $g = \gcd(\ell_1 - 1, \ell_2 - 1)$, we have $\ell_1 - 1 = cg$ and $\ell_2 - 1 = bg$. We let d be the largest divisor of g with $P(d) \le z$, and write $g = dh$, so that all of the primes dividing h are larger than z. We thus have

$$n = abcdh, \quad m_1 = ab,\ m_2 = ac,\ \ell_1 - 1 = cdh,\ \ell_2 - 1 = bdh.$$

We may assume that $d \le x^{1/3}$. Indeed, the set $\mathcal{E}$ of $n \le x$ with a z-smooth divisor larger than $x^{1/3}$ has size $O(x/(\log x)^{100})$ (say); see [15, bottom of p. 9]. Noting that $r_1(n) \le \tau(n)$, the contribution of these n to M_2 does not exceed

$$\sum_{n\in\mathcal{E}} \tau(n)^2 \le (\#\mathcal{E})^{1/2} \cdot \left(\sum_{n\le x} \tau(n)^4\right)^{1/2} \ll (x(\log x)^{-100})^{1/2}(x(\log x)^{15})^{1/2} \le x/(\log x)^{40},$$

which will be negligible for us. Thus, we may assume that $h > x^{1/3}$. We have

$$M_2 \le M_1 + \sum_{a,b,c,d,h} 1 = M_1 + \sum_{a,b,c,d} \sum_{h\le x/abcd} 1.$$

Here, we have a, b, c, d all z-smooth, $\Omega(ab), \Omega(ac), \Omega(bd), \Omega(cd) \le \log\log z$, h is not divisible by any prime $\le z$, and both $bdh + 1$ and $cdh + 1$ are prime. Since we are assuming that $m_1 \ne m_2$, this implies that $b \ne c$, so that $bdh + 1 \ne cdh + 1$. By the sieve (see [13, Theorem 2.2, p. 68]), we thus have

$$M_2 \le M_1 + \sum_{a,b,c,d} \frac{x(\log\log z)^{O(1)}}{abcd(\log x)^2 \log z}. \tag{10}$$

We have that $\Omega(a) + \Omega(b)$, $\Omega(a) + \Omega(c)$, $\Omega(b) + \Omega(d)$, $\Omega(c) + \Omega(d)$ are all $\le \log\log z$, which implies that $\omega(abcd) \le \Omega(abcd) \le 2\log\log z$. Thus, letting $m = abcd$,

$$\sum_{a,b,c,d} \frac{1}{abcd} \le \sum_{\substack{m:\ P(m)\le z \\ \omega(m)\le 2\log\log z}} \frac{\tau_4(m)}{m} \le \sum_{j\le 2\log\log z} \frac{S^j}{j!},$$

where

$$S := \sum_{p\le z} \left(\frac{\tau_4(p)}{p} + \frac{\tau_4(p^2)}{p^2} + \dots\right).$$

Since $S = \sum_{p\le z}(\frac{4}{p} + O(1/p^2)) = 4\log\log z + O(1)$,

$$\sum_{a,b,c,d} \frac{1}{abcd} \le \sum_{j\le 2\log\log z} \frac{1}{j!}(4\log\log z + O(1))^j \ll \frac{(4\log\log z + O(1))^{\lfloor 2\log\log z\rfloor}}{\lfloor 2\log\log z\rfloor!}$$
$$\ll \frac{\exp(2\log\log z(\log 4 - \log 2 + 1))}{\sqrt{\log\log z}} = \frac{(\log z)^{2+2\log 2}}{\sqrt{\log\log z}}.$$

Using this in the prior estimate, we have

$$M_2 \ll M_1 + \frac{x(\log\log z)^{O(1)}}{(\log x)^{2+\alpha(-1-2\log 2)}}.$$

We thus conclude, with (9), that $M_2 \ll M_1(\log\log z)^{O(1)}$ when $\alpha \le 1/\log 4$ and

$$M_2 \ll \frac{x(\log\log z)^{O(1)}}{(\log x)^{2-\alpha(1+\log 4)}},$$

when $1/\log 4 \le \alpha < 1$. In particular, from (6), (7), and (8), we have

$$\frac{x(\log\log z)^{O(1)}}{(\log x)^{1-\alpha}} \le N(x,y) \ll \frac{x}{(\log x)^{1-\alpha}} \quad \text{when } 0 < \alpha \le 1/\log 4. \tag{11}$$

We can use (8) to get a lower bound for $N(x,y)$ when $1/\log 4 \le \alpha < 1$, but we will go directly towards a sharper bound. This can be done by counting certain restricted representations of n as $m(\ell-1)$. Let $0 < \gamma \le 1$ and let $r_\gamma(n)$ be the number of representations of n as $m(\ell-1)$, where $\ell - 1 > y$, $\Omega(m) \le \gamma \log\log z$, and $\Omega_z(\ell-1) \le \gamma \log\log z$. (So, the case $\gamma = 1$ has already been handled.) We now take

$$M_1(\gamma) := \sum_{n\le x} r_\gamma(n), \;\; M_2(\gamma) := \sum_{n\le x} r_\gamma(n)^2,$$

and so,

$$N(x,y) \ge M_1(\gamma)^2/M_2(\gamma).$$

Using [12], [24], and [27], we have (once z exceeds a certain absolute constant)

$$M_1(\gamma) \ll \frac{x}{\log x(\log z)^{1+2\gamma\log\gamma-2\gamma}}$$

and

$$M_1(\gamma) \gg \frac{x}{\log x(\log z)^{1+2\gamma\log\gamma-2\gamma}\log\log z} = \frac{x}{(\log x)^{1+\alpha(1+2\gamma\log\gamma-2\gamma)}\log\log z}.$$

(In fact, the lower bound gives the correct order of $M_1(\gamma)$ when $1-\gamma \gg 1$.) Using the same ideas we used for $\gamma = 1$, we have

$$M_2(\gamma) \le M_1 + \frac{x(\log\log z)^{O(1)}}{(\log x)^2(\log z)^{1+2\gamma\log\frac{\gamma}{2}-2\gamma}} = M_1 + \frac{x(\log\log z)^{O(1)}}{(\log x)^{2+\alpha(1+2\gamma\log\gamma-2\gamma\log 2-2\gamma)}}.$$

Ignoring double logarithmic factors, the M_1 term dominates for $\alpha\gamma \le 1/\log 4$. We shall actually take γ so that $\alpha\gamma = 1/\log 4$, and in this case we get the lower bound

$$N(x,y) \gg M_1(1/(\alpha\log 4))\cdot(\log\log z)^{O(1)}.$$

Note that we are assuming that $\alpha \ge 1/\log 4$, so $1/(\alpha\log 4) \le 1$. Doing the calculation, we arrive at

$$N(x,y) \ge \frac{x(\log\log z)^{O(1)}}{(\log x)^{\beta+\alpha-1-\log\alpha/\log 2}}. \tag{12}$$

Finally note that $\log y \sim \log x$ as $x \to \infty$ in our range. The theorem now follows from (6), (7), (11), and (12). □

It remains to establish the upper bound of Theorem 1.5 when $\alpha \ge 1/\log 4$. This requires one more preliminary "anatomical" lemma. In the following, $\Omega(n,\mathcal{P})$ denotes the number of prime factors of n from the set $\mathcal{P}$, counted with multiplicity.

Lemma 2.9. *Let $\mathcal{P}$ be a nonempty set of primes with smallest element p_0. Let $\epsilon > 0$, and assume $0 < t \le p_0 - \epsilon$. For $x \ge 3$,*

$$\sum_{n \le x} t^{\Omega(n,\mathcal{P})} \ll_{\epsilon, p_0} x \cdot \exp\left((t-1)\sum_{\substack{p \le x \\ p \in \mathcal{P}}} \frac{1}{p}\right).$$

Proof. This estimate appears explicitly on [15, p. 7]. It is also contained in [20, Lemma 3.11 and eq. (3.15)]. □

We can now prove the missing upper bound.

Theorem 2.10. *Let $\epsilon > 0$. Suppose that $x, y \ge 3$ with $x > y \ge x^{1-1/\log\log x}$. Define α by the equation $y = x/\exp((\log x)^\alpha)$. Then for $1/\log 4 \le \alpha < 1$, we have*

$$N(x,y) \ll \frac{x}{(\log y)^{\beta+\alpha-1-\log\alpha/\log 2}}.$$

Proof. Let $z = x/y$, so $\log z = (\log x)^\alpha \sim (\log y)^\alpha$ as $x \to \infty$, and let $\gamma = \frac{1}{\alpha \log 2}$. Note that because $\alpha \ge 1/\log 4$, we have $1/\log 2 < \gamma \le 2$. Suppose n is counted by $N(x,y)$, so that $n = m(\ell-1)$ with $\ell - 1 > y$ (and hence $m < z$). We begin by discarding those n where

$$\omega_z(\ell-1) + \omega(m) > \gamma \log\log z. \tag{13}$$

Let us analyze the number of n this forces us to exclude. Let $\mathcal{P}$ be the set of odd primes not exceeding z. If (13) holds,

$$\begin{aligned}\Omega(n,\mathcal{P}) &= \Omega(m,\mathcal{P}) + \Omega(\ell-1,\mathcal{P}) \\ &\ge (\omega(m)-1) + (\omega_z(\ell-1)-1) > \gamma\log\log z - 2.\end{aligned}$$

Applying Lemma 2.9 with $t = \gamma$, we find that

$$\begin{aligned}\#\{n \le x : \Omega(n,\mathcal{P}) \ge \gamma\log\log z - 2\} &\ll \gamma^{-\gamma\log\log z}\sum_{n\le x}\gamma^{\Omega(n,\mathcal{P})} \\ &\ll x\cdot\gamma^{-\gamma\log\log z}\cdot(\log z)^{\gamma-1} = x/(\log z)^{Q(\gamma)}.\end{aligned}$$

Since $\log z = (\log x)^\alpha \ge (\log y)^\alpha$, it follows that the number of n we exclude here is

$$\ll \frac{x}{(\log y)^{\alpha-\alpha\gamma+\alpha\gamma\log\gamma}} = \frac{x}{(\log y)^{\beta+\alpha-1-\log\alpha/\log 2}},$$

which is acceptable for us.

Thus, we can restrict to those $n = m(\ell-1)$ with $\omega_z(\ell-1) + \omega(m) \le \gamma\log\log z$. Let $k = \lfloor \gamma\log\log z \rfloor$. Writing $\omega_z(\ell-1) = i$ and $\omega(m) = j$, the number of such integers n is at most

$$\sum_{i+j\le k}\sum_{\substack{m\le z \\ \omega(m)=j}}\sum_{\substack{y+1<\ell\le x/m+1 \\ \omega_z(\ell-1)=i}} 1. \tag{14}$$

We use the upper bound sieve to estimate the innermost sum. Write $\ell - 1 = ab$, where a is z-smooth and all prime divisors of b exceed z. We can assume that $a < x^{1/3}$, since otherwise $n = m(\ell-1)$ has a z-smooth divisor exceeding $x^{1/3}$, which — keeping in mind that $z \le x^{1/\log\log x}$ — places n in a set of size $O(x/(\log x)^{100})$ (say). (Again, see [15, p. 9].) Then

$$b \le \frac{x}{am}, \quad b \text{ has no prime factors} \le z, \quad ab+1 \text{ is prime.}$$

Moreover, $x/am > x^{1/2}$. For each a, the upper bound sieve shows that the number of possible b is

$$\ll \frac{1}{\varphi(a)} \frac{x}{m \log x \cdot \log z}.$$

Summing on z-smooth values of a with $\omega(a) = i$ gives an upper bound that is

$$\ll \frac{x}{m \log x \cdot \log z} \cdot \frac{1}{i!} \left(\sum_{p \le z} \left(\frac{1}{\varphi(p)} + \frac{1}{\varphi(p^2)} + \dots \right) \right)^i$$
$$\le \frac{x}{m \log x \cdot \log z} \cdot \frac{1}{i!} \left(\log \log z + O(1) \right)^i.$$

Now bounding the sum of $1/m$ as $(\log \log z + O(1))^j / j!$, we find that the triple sum in (14) is

$$\ll \frac{x}{\log x \cdot \log z} \sum_{i+j \le k} \frac{(\log \log z + O(1))^{i+j}}{i! j!} = \frac{x}{\log x \cdot \log z} \sum_{l=0}^{k} \frac{(2 \log \log z + O(1))^l}{l!}. \tag{15}$$

Since $\gamma \le 2$, the sum on l is bounded above by

$$\left(\frac{2}{\gamma} \right)^k \cdot \sum_{l=0}^{k} \frac{(\gamma \log \log z + O(1))^l}{l!} \ll \left(\frac{2}{\gamma} \right)^k \cdot \exp(\gamma \log \log z). \tag{16}$$

Putting this back in above, we find that our count of n is

$$\ll \frac{x (2/\gamma)^{\lfloor \gamma \log \log z \rfloor}}{(\log z)^{1-\gamma} \log x} \ll \frac{x}{(\log z)^{1-\gamma-\gamma \log(2/\gamma)} \log x}$$
$$\le \frac{x}{(\log x)^{\alpha - \alpha\gamma - \alpha\gamma \log(2/\gamma) + 1}} \le \frac{x}{(\log y)^{\beta + \alpha - 1 - \log \alpha / \log 2}}.$$

This completes the proof of Theorem 2.10. □

Remarks 2.11. Theorem 1.5 can be sharpened at the cost of slightly more elaborate arguments.

(i) In the range $\alpha \le \frac{1}{\log 4}$, the factor $(\log \log (x/y))^{O(1)}$ can be removed in the lower bound. Thus, $N(x, y) \asymp x/(\log y)^{1-\alpha}$ in this range. Here the main idea is to deal with the "singular series" factors from the sieve in the sum (10), rather than to crudely estimate them away as $(\log \log z)^{O(1)}$.

(ii) In the range $\alpha \ge \frac{1}{\log 4} + \epsilon$, one can show that

$$\frac{x}{(\log y)^{\beta + \alpha - 1 - \log \alpha / \log 2} (\log \log z)^{3/2 + o(1)}} \le N(x, y) \ll_\epsilon \frac{x}{(\log y)^{\beta + \alpha - 1 - \log \alpha / \log 2} (\log \log z)^{1/2}},$$

as $x \to \infty$. (As usual, $z = x/y$ here.) The improved lower bound is obtained by a careful treatment of the singular series terms, as in (i).

To obtain the upper bound, we revisit the proof of Theorem 2.10. If $\alpha \ge \frac{1}{\log 4} + \epsilon$, then γ is bounded away from 2, and now Lemma 2.1 allows us to save an extra factor of $\sqrt{\log \log z}$ for our count of exceptions to (13). We then continue with the argument, but bound the final sum in (15) by its largest term, rather than following (16). This leads to a savings of $\sqrt{\log \log z}$ in the final estimate.

Remark 2.12. We say a word about the case when $z = x/y$ is very small. Here we can use the same second moment method employed in Theorem 2.8, but applied to $r(n)$ instead of $r_1(n)$. Working this out, we find that for each fixed $\epsilon > 0$,

$$N(x,y) \sim \frac{x}{\log x} \int_1^z \frac{\lfloor v \rfloor}{v^2}\, dv,$$

as $x \to \infty$, uniformly throughout the region $x/\exp((\log x)^{1/2-\epsilon}) \le y \le (1-\epsilon)x$.

3. Torsion subgroups of CM elliptic curves: Proofs of Theorems 1.7–1.9

3.1. **Proof of Theorem 1.7.** We will deduce Theorem 1.7 directly from Theorem 1.2. In order to relate the occurrence of large torsion subgroups to divisibility by large shifted primes, we draw on some recent algebraic results from [2].

For each natural number m, we introduce a set $\Lambda(m)$ defined as follows. If ℓ^α is a prime power with $\alpha \ge 2$, we put

$$\Lambda(\ell^\alpha) = \{\ell^{\alpha-2}(\ell^2-1), \ell^{\alpha-2}(\ell-1)^2, \ell^{\alpha-1}(\ell-1)\}.$$

For each prime ℓ, let

$$\Lambda(\ell) = \{\ell^2-1, (\ell-1)^2, \ell-1\}.$$

For a general m, we let $\Lambda(m)$ be the set of integers A that can be written in the form

$$A = \prod_{\ell^\alpha \| m} A_{\ell^\alpha},$$

with each $A_{\ell^\alpha} \in \Lambda(\ell^\alpha)$. The following result is contained in [2, Theorem 2.4].

Theorem 3.1. *Let E be a CM elliptic curve over a degree d number field F. Suppose that E has CM by an order in the imaginary quadratic field K, and that $F \supset K$. If $\#E(F)[\mathrm{tors}] = m$, then there is an $A \in \Lambda(m)$ for which $A \mid 6d$.*

Proof of Theorem 1.7. We can assume that y exceeds any convenient absolute constant, since otherwise the upper bound claimed in the theorem is trivial.

Suppose $d \le x$ is such that $T_{\mathrm{CM}}(d) > y$. Choose a CM elliptic curve E over a degree d number field F_0 with $\#E(F_0)[\mathrm{tors}] > y$. With K the corresponding CM field, let $F = KF_0$. Then $m := \#E(F)[\mathrm{tors}] > y$, and $[F:\mathbb{Q}] = d$ or $2d$. So by Theorem 3.1, there is an $A \in \Lambda(m)$ for which $A \mid 12d$.

Suppose first that m is divisible by a prime $\ell > y^{1/100}$. From the definition of $\Lambda(m)$,

$$\ell - 1 \mid A \mid 12d.$$

So by Theorem 1.2 (with y replaced by $\frac{1}{2}y$ and x by $12x$), the number of possibilities for d is

$$\ll \frac{x}{(\log y)^\beta \sqrt{\log\log y}},$$

as desired.

We will show that the remaining cases for m correspond to a negligible set of values of d. By Lemma 2.1, we may assume that $\Omega_y(d) \le 1.9 \log\log y$. Since $A \mid 12d$, we have (crudely)

$$\Omega_y(A) \le \Omega_y(d) + 3 \le 1.95 \log\log y.$$

Suppose $\ell^\alpha \parallel m$. Each element of $\Lambda(\ell^\alpha)$ has at least α prime factors, counted with multiplicity, except possibly when $\ell = 2$, when each has at least $\alpha - 2$ prime factors. Since $\ell \le y$, the prime factors of the elements of $\Lambda(\ell^\alpha)$ are also at most y. Thus, $\Omega_y(A) = \Omega(A)$, and

$$\Omega(m) - 2 \le \Omega(A) \le 1.95 \log\log y.$$

Hence, $\Omega(m) \le 2 \log\log y$, and

$$\prod_{\substack{\ell^\alpha \| m \\ \ell \le y^{\frac{1}{10\log\log y}}}} \ell^\alpha \le (y^{\frac{1}{10\log\log y}})^{\Omega(m)} \le y^{1/5}.$$

Since $m > y$,

$$\prod_{\substack{\ell^\alpha \| m \\ \ell > y^{\frac{1}{10\log\log y}}}} \ell^\alpha > y^{4/5}. \tag{17}$$

We can assume that $\alpha = 1$ for each exponent α on the left-hand side of (17). To see this, observe that $12d$ is divisible by an element of $\Lambda(\ell^\alpha)$ for each ℓ^α exactly dividing m. Now $\#\Lambda(\ell^\alpha) = O(1)$, and each element of $\Lambda(\ell^\alpha)$ is $\gg \ell^\alpha$. Thus, the number of $d \le x$ corresponding to having some $\alpha > 1$ is

$$\ll \sum_{\substack{\ell > y^{\frac{1}{10\log\log y}} \\ \alpha > 1}} \frac{x}{\ell^\alpha} \ll x/y^{\frac{1}{10\log\log y}},$$

which is negligible. Looking back at (17), and remembering that m is $y^{1/100}$-smooth, we see that there must be more than 80 primes ℓ dividing m with $\ell > y^{1/10\log\log y}$. Since $\prod_{\ell | m}(\ell - 1) \mid A \mid 12d$,

$$\sum_{\substack{\ell | m \\ \ell > y^{1/10\log\log y}}} \Omega(\ell - 1) \le \sum_{\ell | m} \Omega(\ell - 1) \le \Omega(A) \le 1.95 \log\log y.$$

Hence, there is a prime $\ell \mid m$ with $\ell > y^{1/10\log\log y}$ and $\Omega(\ell - 1) < \frac{1.95}{80} \log\log y < \frac{1}{40} \log\log \ell$. Since $\ell - 1 \mid 12d$, this puts d in a set of size

$$\le \sum_{\substack{\ell > y^{1/10\log\log y} \\ \Omega(\ell-1) < \frac{1}{40}\log\log\ell}} \frac{12x}{\ell - 1}.$$

By [27, Theorem 1], the count of $\ell \le T$ with $\Omega(\ell - 1) \le \frac{1}{40} \log\log \ell$ is $\ll T/(\log T)^{1+Q(1/40)} \ll T/(\log T)^{1.88}$. By partial summation, the last displayed sum is $\ll x/(\log y)^{0.87}$, which is again negligible. □

3.2. **Proof of Theorem 1.8.** The following result is the special case $\mathcal{O} = \mathcal{O}_K$ of [5, Theorem 3(a)].

Lemma 3.2. *Let ℓ be an odd prime that splits in the imaginary quadratic field K. There is an $\mathcal{O}_K$-CM elliptic curve E defined over a number field F of degree $2(\ell - 1)\frac{h_K}{w_K}$ for which $E(F)$ has a point of order ℓ.*

Since we can base change E to any extension of F, we have the following useful consequence of Lemma 3.2: If the odd prime ℓ splits in the imaginary quadratic field K, then

$$(\forall\ d \in \mathbb{Z}^+) \qquad 2(\ell-1)\frac{h_K}{w_K} \mid d \Longrightarrow T_{\mathrm{CM}}(d) \geq \ell.$$

For each odd prime ℓ, we let n_ℓ denote the least positive quadratic nonresidue modulo ℓ. Observe that if $\ell \equiv 1 \pmod 4$, then it splits in $\mathbb{Q}(i)$, while if $\ell \equiv 3 \pmod 4$, then ℓ splits in $\mathbb{Q}(\sqrt{-n_\ell})$.

We are now in a position to prove Theorem 1.8. The argument is more complicated than for Theorem 1.7; rather than appeal directly to Theorem 1.3, it is necessary to revisit its proof.

Proof of Theorem 1.8. Keeping the notation of Corollary 2.6 and just following, choose a positive number $\nu < \frac{1}{2}\eta(\epsilon/2)$. We again take two cases according to the size of y.

Case I: $y \leq x^{1/6}$

Let $Y = \Xi_\nu(y)^2$. We consider numbers $d \leq x$ whose Y-smooth component has the form nL, where

$$L = \lfloor (\log\log y)^{0.8} \rfloor !, \tag{18}$$

and where n runs over the integers in $(Y^{1/2}, Y]$ having the form $\lambda(m)$ with

$$P(m) > \xi_\nu(n), \quad P(m) \equiv 1 \pmod 4. \tag{19}$$

Since $Y \leq x^{2/5}$,

$$nL \leq x^{2/5}\lfloor (\log\log y)^{0.8} \rfloor ! < x^{3/7}.$$

(Here and below, we assume x and y are sufficiently large.) Now the sieve yields

$$\#\{d \leq x : d \text{ has } Y\text{-smooth part } nL\} \asymp \frac{x}{nL\log Y}. \tag{20}$$

Summing over $n \in (Y^{1/2}, Y]$, keeping in mind the result of Corollary 2.6 (and $\nu < \eta(\epsilon/2)$), shows that the number of d obtained in this way is

$$\gg \frac{x}{L(\log Y)^{\beta+\epsilon/2}} \gg \frac{x}{L(\log y)^{\beta+\epsilon/2}}. \tag{21}$$

We now argue that $T_{\mathrm{CM}}(d) > y$ for all of these d. By construction, d has Y-smooth part nL. If m is a λ-preimage of n satisfying (19), then

$$\ell := P(m) \geq \xi_\nu(n) > \xi_\nu(Y^{1/2}) = y, \quad \ell \equiv 1 \pmod 4.$$

We apply Lemma 3.2 with $K = \mathbb{Q}(i)$. Observe that

$$2(\ell-1)\frac{h_K}{w_K} = \frac{\ell-1}{2} \mid \lambda(m) = n \mid nL \mid d.$$

So from Lemma 3.2, $T_{\mathrm{CM}}(d) \geq \ell > y$, as desired.

Case II: $x^{1/6} < y \leq \xi_\nu(x)$

We take $d = nL$ where L is as in (18), and where $n \in (\Xi_{2\nu}(y), x/L]$ has the form $\lambda(m)$ with $P(m) > \xi_{2\nu}(n)$ and $P(m) \equiv 1 \pmod 4$. Since $2\nu < \eta(\epsilon/2)$, Corollary 2.6 implies that the

number of these d is

$$\gg \frac{x/L}{\log(x/L)^{\beta+\epsilon/2}} \gg \frac{x}{L(\log x)^{\beta+\epsilon/2}}.$$

Then $\ell := P(m) > \xi_{2\nu}(\Xi_{2\nu}(y)) = y$. We can now prove that $T_{\mathrm{CM}}(d) \geq \ell > y$ exactly as in Case I. □

3.3. **Proof of Theorem 1.9.** Before proving Theorem 1.9, we require one more "anatomical" lemma. The following estimate appears as [15, Exercise 05, p. 12]. For the details of the proof, see [17, Lemmas 12 and 13].

Lemma 3.3. *For all $x \geq 3$ and all positive integers k, the number of $n \leq x$ with $\Omega(n) \geq k$ is*

$$\ll \frac{k}{2^k} x \log x.$$

Proof of Theorem 1.9(i). Noting that $\log\log \frac{x}{2} > \frac{1}{2}\log\log x$ for $x \geq 10$, each d counted here satisfies $T_{\mathrm{CM}}(d) > Zd$, where $Z := \frac{1}{2}\alpha \log\log x$. Let E be a CM elliptic curve over a degree d number field F having $\#E(F)[\mathrm{tors}] > Zd$, and let K be the corresponding CM field. Writing N for the exponent of the group $E(FK)[\mathrm{tors}]$, equation (7) in [6] shows that

$$Zd < \#E(F)[\mathrm{tors}] \leq \#E(FK)[\mathrm{tors}] \leq 6\frac{d}{h_K} \prod_{\mathfrak{p}\mid N} \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{-1},$$

where h_K denotes the class number of K, the product is over prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ dividing N, and $|\cdot|$ denotes the norm. Let w denote the number of prime ideal divisors of N in $\mathcal{O}_K$. Then

$$\prod_{\substack{\mathfrak{p}\mid N \\ |\mathfrak{p}|>w}} \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{-1} \leq \left(1 - \frac{1}{w}\right)^{-w} \ll 1,$$

so that

$$\prod_{\mathfrak{p}\mid N} \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{-1} \ll \prod_{|\mathfrak{p}|\leq w} \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{-1} \ll h_K \log w,$$

where the final implied constant is absolute. (See [6, eq. (4)] for the form of Mertens' theorem used here.) Inserting this above, we find that $\log w \gg Z$, and so $w \gg (\log x)^{C\alpha}$ for a certain absolute constant $C > 0$. It follows that

$$\omega(N) \geq \frac{w}{2} \gg (\log x)^{C\alpha}.$$

Putting $n = \#E(FK)[\mathrm{tors}]$, we have that $N \mid n$. From Theorem 3.1, there is an $A \in \Lambda(n)$ with $A \mid 6[FK : \mathbb{Q}] \mid 12d$. By an argument appearing in the proof of Theorem 1.7 above, each element of $\Lambda(n)$ has at least $\Omega(n) - 2$ prime factors, counted with multiplicity. Thus,

$$\Omega(12d) \geq \Omega(A) \geq \Omega(n) - 2 \geq \Omega(N) - 2 \geq \omega(N) - 2.$$

Hence (for large x),

$$\Omega(d) \gg (\log x)^{C\alpha}.$$

By Lemma 3.3, the number of such $d \leq x$ is at most $x/\exp((\log x)^{C\alpha+o(1)})$, as $x \to \infty$. □

Proof of Theorem 1.9(ii). Consider the curve $E\colon Y^2 = X^3+1$, which has CM by the maximal order of $K = \mathbb{Q}(\sqrt{-3})$. For each prime p, CM theory shows that $K(E[p])/K$ is an abelian extension whose degree divides

$$\#(\mathcal{O}_K/(p))^\times = p^2(1-1/p)(1-\left(\tfrac{-3}{p}\right)/p).$$

(See, for instance, [23, Corollary 5.5]. Here $\left(\frac{-3}{p}\right)$ is to be understood as a Kronecker symbol, so that $\left(\frac{-3}{2}\right) = -1$.) When $p = 2$ or $p = 3$, this degree bound is not sharp: $[K(E[2]) : K] = 1$ and $[K(E[3]) : K] = 3$, reflecting that all of the 2-torsion of E is K-rational and that K contains a 3-torsion point of E (but not the full 3-torsion). We apply these observations to bound the degree of the m-torsion field when m is the product of the first several primes. Given $z \geq 3$, we put $m = \prod_{p\leq z} p$ and

$$D = \frac{1}{6}m^2 \prod_{p\leq z}(1-1/p)(1-\left(\tfrac{-3}{p}\right)/p).$$

Since $K(E[m])$ is the compositum of the fields $K(E[p])$, for $p \leq z$, and each extension $K(E[p])/K$ is Galois,

$$[K(E[m]) : K] \mid \prod_{p\leq z}[K(E[p]) : K] \mid D.$$

We will take $z = (\log x)^\delta$, where $0 < \delta < 1$ is a parameter to be chosen in terms of α, in a way to be made precise shortly. Let $\ell \equiv 1 \pmod 3$ be a prime with

$$\frac{1}{3}x/D < \ell \leq \frac{1}{2}x/D.$$

Now $D = \exp((\log x)^{\delta+o(1)})$, and so by the prime number theorem for progressions, the number of ℓ allowed here is at least

$$x/\exp((\log x)^{\delta+o(1)}), \tag{22}$$

as $x \to \infty$. Since ℓ splits in K, there is an abelian extension of K of degree dividing $\ell - 1$ in which E has an ℓ-torsion point. (Again, this follows from [23, Corollary 5.5].) Taking the compositum of this extension with $K(E[m])$, and passing to a suitable further extension if necessary, we obtain an extension M_ℓ/K with

$$[M_\ell : K] = (\ell-1)D$$

over which E has full m-torsion and a point of order ℓ. In particular, both m^2 and ℓ divide $\#E(M_\ell)[\mathrm{tors}]$, so that

$$\#E(M_\ell)[\mathrm{tors}] \geq m^2\ell.$$

Putting $d_\ell = [M_\ell : \mathbb{Q}]$, so that

$$d_\ell = 2[M_\ell : K] = 2(\ell-1)\cdot D,$$

we see that $d_\ell \in [x/2, x]$, and (as $x \to \infty$)

$$\begin{aligned} T_{\mathrm{CM}}(d_\ell) \geq m^2\ell &\geq 3d_\ell \prod_{p\leq z}(1-1/p)^{-1}\left(1-\left(\tfrac{-3}{p}\right)/p\right)^{-1} \\ &\geq (1+o(1))\cdot 3d_\ell(e^\gamma\delta\log\log x)\cdot L(1,\left(\tfrac{-3}{\cdot}\right)) \\ &\geq \left(\frac{e^\gamma\pi}{\sqrt{3}}\delta + o(1)\right) d_\ell \log\log d_\ell, \end{aligned}$$

where we used in the last step that $L(1, \left(\frac{-3}{\cdot}\right)) = \frac{\pi}{3\sqrt{3}}$.

It is now straightforward to conclude. Assume that $\alpha < e^{\gamma}\pi/\sqrt{3}$. Let δ be any real number with $\alpha e^{-\gamma}\sqrt{3}/\pi < \delta < 1$. Then (for large x), each d_ℓ constructed above satisfies $T_{\mathrm{CM}}(d_\ell) > \alpha \cdot d_\ell \log\log d_\ell$. Now d_ℓ assumes distinct values for distinct ℓ, and the number of ℓ to work with is bounded below by (22). Since we can choose any $\delta < 1$ with $\delta > \alpha e^{-\gamma}\sqrt{3}/\pi$, Theorem 1.9(ii) follows with $C' = e^{-\gamma}\sqrt{3}/\pi$. □

Remark 3.4. The use in the above argument of the particular curve E and the particular sequence of fields M_ℓ may appear somewhat arbitrary. Actually, one can show that these choices are optimal in the following restricted sense: Let E be a fixed elliptic curve defined over a number field F, and suppose E has CM by the maximal order of the imaginary quadratic field K. For any sequence of fields M containing FK with $[M : \mathbb{Q}] \to \infty$,

$$\limsup \frac{\#E(M)[\mathrm{tors}]}{[M : \mathbb{Q}] \log\log[M : \mathbb{Q}]} \leq e^{\gamma}\pi/\sqrt{3}.$$

Acknowledgements

We are heavily indebted to Abbey Bourdon and Pete L. Clark for many enlightening conversations on the theory of CM elliptic curves. We owe to Kevin Ford the suggestion that we consider very large values of $T_{\mathrm{CM}}(d)$. We thank the referees for several helpful comments. The second author (P.P.) is supported by NSF award DMS-1402268.

References

[1] N. Aoki, *Torsion points on abelian varieties with complex multiplication*, Algebraic cycles and related topics (Kitasakado, 1994), World Sci. Publ., River Edge, NJ, 1995, pp. 1–22.
[2] A. Bourdon, P. L. Clark, and P. Pollack, *Anatomy of torsion in the CM case*, submitted, preprint online as `arXiv:1506.00565 [math.NT]`.
[3] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules*, J. Number Theory **130** (2010), 1241–1250.
[4] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free prime factors $> y$. II*, Indag. Math. **28** (1966), 239–247.
[5] P. L. Clark, B. Cook, and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), 447–479.
[6] P. L. Clark and P. Pollack, *The truth about torsion in the CM case*, C. R. Math. Acad. Sci. Paris **353** (2015), 683–688.
[7] P. Erdős, *An asymptotic inequality in the theory of numbers*, Vestnik Leningrad Univ. **15** (1960), 41–49 (Russian).
[8] P. Erdős and S. S. Wagstaff, Jr., *The fractional parts of the Bernoulli numbers*, Illinois J. Math. **24** (1980), 104–112.
[9] K. Ford, *The distribution of integers with a divisor in a given interval*, Ann. of Math. (2) **168** (2008), 367–433.
[10] K. Ford, F. Luca, and C. Pomerance, *The image of Carmichael's λ-function*, Algebra Number Theory **8** (2014), 2009–2025.
[11] C. F. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986.
[12] G. Halász, *Remarks to my paper "On the distribution of additive and the mean value of multiplicative functions"*, Acta Math. Acad. Sci. Hungar. **23** (1972), 425–432.
[13] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, vol. 4, Academic Press, 1974.
[14] H. Halberstam and K. F. Roth, *Sequences*, second ed., Springer-Verlag, New York-Berlin, 1983.
[15] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.

[16] H. W. Lenstra, Jr. and C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), 483–516.
[17] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler function chains*, Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 351–361; Integers **7** (2007), no. 2, #A25.
[18] ———, *On the range of Carmichael's universal-exponent function*, Acta Arith. **162** (2014), 289–308.
[19] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.
[20] K. K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. **20** (1976), 681–705.
[21] C. Pomerance and A. Sárközy, *On homogeneous multiplicative hybrid problems in number theory*, Acta Arith. **49** (1988), 291–302.
[22] D. Prasad and C. S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can. **23** (2001), 1–5.
[23] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 167–234.
[24] A. Sárközy, *Remarks on a paper of G. Halász*, Period. Math. Hungar. **8** (1977), 135–150.
[25] A. Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), 241–249.
[26] ———, *Points of finite order on abelian varieties*, p-adic methods in number theory and algebraic geometry, Contemp. Math., vol. 133, Amer. Math. Soc., Providence, RI, 1992, pp. 175–193.
[27] N. M. Timofeev, *Hardy-Ramanujan and Halasz inequalities for shifted prime numbers*, Math. Notes **57** (1995), 522–535.

Department of Mathematics, Towson University, Towson, MD 21252, USA
E-mail address: nmcnew@towson.edu

Department of Mathematics, University of Georgia, Athens, GA 30602, USA
E-mail address: pollack@uga.edu

Department of Mathematics, Dartmouth College, Hanover, NH 03755, USA
E-mail address: carl.pomerance@dartmouth.edu