CONSTRAINED TERNARY INTEGERS

FLORIAN LUCA, PIETER MOREE, ROBERT OSBURN, SUMAIA SAAD EDDIN AND ALISA SEDUNOVA

Abstract. An integer n is said to be ternary if it is composed of three distinct odd primes. In this paper, we asymptotically count the number of ternary integers $n \leq x$ with the constituent primes satisfying various constraints. We apply our results to the study of the simplest class of (inverse) cyclotomic polynomials that can have coefficients that are greater than 1 in absolute value, namely to the n^{th} (inverse) cyclotomic polynomials with ternary n. We show, for example, that the corrected Sister Beiter conjecture is true for a fraction ≥ 0.925 of ternary integers.

1. Introduction

Let $\omega(n)$ denote the number of distinct prime factors in the prime factorisation of n and let $\Omega(n)$ be the total number of prime factors. Put

$$\pi(x,k) = \sum_{n\leq x,\, \omega(n)=k} 1 \quad \text{and} \quad N(x,k) = \sum_{n\leq x,\, \Omega(n)=k} 1.$$

Note that $\pi(x,1)$ counts the number of primes $p \leq x$. As is usual, we will write $\pi(x)$ instead of $\pi(x,1)$.

In [22] Landau, confirming a conjecture of Gauss, showed that as $x \to \infty$

$$\pi(x,k) \sim N(x,k) \sim \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}. \tag{1}$$

This result is a generalization of the Prime Number Theorem, which is the case $k = 1$. Nowadays, using the Selberg-Delange method, much more precise estimates can be given (see e.g. Tenenbaum [26, pp. 200–206]). In particular, we have

$$\pi(x,k) = \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\left(1 + o_k\left(\frac{1}{\log\log x}\right)\right), \tag{2}$$

and a similar estimate holds for $N(x,k)$. Various authors considered the related problem where k is allowed to vary to some extent with x. For a nice survey, see Hildebrand [17].

In this paper, we establish some variations of the result of Landau in case $k = 3$ (see Section 2), which might be of some interest for cryptography, but certainly have some applications in the theory of coefficients of cyclotomic polynomials (see Section 7). Here, in particular, *ternary integers* are of importance.

Definition. *An integer n is said to be ternary if it is of the form $n = pqr$ with $3 \leq p < q < r$ primes. It is constrained if on at least one of p, q and r a constraint is imposed.*

Date: September 21, 2018.
Mathematics Subject Classification (2010). 11R09, 11C08

Let $N_T(x)$ denote the number of ternary $n \le x$, that is the number of integers up to x consisting of exactly 3 different odd prime factors. It is an easy consequence (see Corollary 1) of the validity of the estimate in (2) for $N(x,k)$ that asymptotically

$$N_T(x) = \frac{x(\log\log x)^2}{2\log x}\Big(1 - \frac{(1+o(1))}{\log\log x}\Big). \tag{3}$$

2. Results on constrained ternary integers

The theory of ternary (inverse) cyclotomic coefficients naturally leads to some questions in analytic number theory. For the sake of brevity we consider only a few of those. Their applications are discussed in Section 7.4.

Theorem 1. *Let p, q, r be primes. Put*

$$\mathcal{T}(x) = \left\{pqr \le x : 3 \le p < q < r < \left(\frac{p-1}{p-2}\right)(q-1),\ r \equiv q \equiv \pm 1 (\operatorname{mod} p)\right\}.$$

We have

$$|\mathcal{T}(x)| = C_1 \frac{x}{(\log x)^2} + O\left(\frac{x \log\log x}{(\log x)^3}\right),$$

where

$$C_1 = 4 \sum_{p\ge 3} \frac{1}{p(p-1)^2} \log\left(\frac{p-1}{p-2}\right) = 0.249029016616718\ldots \tag{4}$$

The terms of the sum C_1 are $O(p^{-4})$ and this allows one to obtain C_1 with the indicated precision by truncation at a sufficient large p.

Theorem 1 can be applied to obtain analytic results on ternary inverse cyclotomic coefficients, see Theorem 9 in Section 7.4.1. Note that for $x \ge 561$ the smallest integer in $\mathcal{T}(x)$ is 561, which is also the smallest Carmichael number.

Theorem 2. *Let a be a non-zero integer and p, q, r be distinct odd primes. Define*

$$\mathcal{T}_a(x) = \{pqr \le x :\ 3 \le p < q < r,\ r \equiv a (\operatorname{mod} pq)\}.$$

Then

$$|\mathcal{T}_a(x)| = C_2 \frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2}\right),$$

where

$$C_2 = \left(\sum_p \frac{1}{p(p-1)}\right)^2 = 0.597771234896174\ldots \tag{5}$$

Here the convergence of the prime sum is much poorer. However, it is easily related to zeta values at integer arguments, see [10, p. 230], and in this way one obtains

$$\sum_p \frac{1}{p(p-1)} = \sum_{k=1}^{\infty} \frac{(\varphi(k) - \mu(k))}{k} \log\zeta(k) = 0.77315666904975\ldots.$$

Theorem 2 allows one to deduce asymptotic results on the flatness of ternary cyclotomic polynomials, see Theorem 10 in Section 7.4.2.

Theorem 3. *For every odd prime $p \geq 3$ let*

$$M(p) = \{(a_i(p), b_i(p)) \ : \ 1 \leq a_i(p), b_i(p) \leq p-1\}$$

be a set of mutually distinct pairs $(a_i(p), b_i(p))$ of cardinality

$$|M(p)| = \alpha p^2 + O(p), \qquad as \quad p \to \infty,$$

with $0 < \alpha < 1$. Put

$$\mathcal{T}_M = \{pqr \ : \ 3 \leq p < q < r, \ (q,r) \equiv (a_i(p), b_i(p)) \ (\mathrm{mod}\, p), \ 1 \leq i \leq |M(p)|\},$$

where p, q and r are distinct odd primes. Then

$$\mathcal{T}_M(x) = \frac{\alpha x (\log\log x)^2}{2\log x}\left(1 + O\left(\frac{1}{\log\log\log x}\right)\right).$$

Finally, Theorem 3 can be used to provide further evidence of the truth of the corrected Sister Beiter conjecture, see Theorem 11 in Section 7.4.3.

3. Auxiliary results

For a positive integer k and a positive real number x we write $\log_k x$ for the iteratively defined function given by $\log_1 x = \max\{1, \log x\}$, where $\log x$ is a natural logarithm of x, and for $k \geq 2$, $\log_k x = \max\{1, \log_{k-1} x\}$.

We first briefly recall some standard tools.

Chebychev showed that

$$\pi(x) \asymp \frac{x}{\log x}. \tag{6}$$

Since the times of Chebychev our understanding of $\pi(x)$ has much improved:

Theorem 4 (Prime Number Theorem in strongest form)**.** *There exists $c > 0$ such that*

$$\pi(x) = \mathrm{li}(x) + O\left(x e^{-c(\log x)^{3/5}(\log\log x)^{-1/5}}\right),$$

where $\mathrm{li}(x)$ denotes the logarithmic integral

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}.$$

The error term above was established in [12] using the strongest available version of the zero-free region for ζ-function due to Vinogradov and Korobov. It was shown by Trudgian [28] that one can take $c = 0.2098$.

Theorem 5 (Mertens)**.** *We have*

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + c_0 + O\left(\frac{1}{\log x}\right),$$

valid for all $x \geq 3$ with some constant c_0.

Theorem 6 (Siegel-Walfisz)**.** *Given any $A > 0$, there exists a constant $c_1(A)$ such that if $d \leq \log^A x$, then*

$$\pi(x; d, a) = \frac{\mathrm{Li}(x)}{\varphi(d)} + O(x e^{-c_1(A)\sqrt{\log x}}),$$

where $\pi(x; d, a) = |\{p \leq x : p \equiv a (\mathrm{mod}\, d)\}|$.

Lemma 1. *Put* $y := \exp(\log x/\log_2 x)$ *and* $z_1 := \exp((\log x)^{1/\log_3 x})$. *Then there exists a positive constant* A *such that if* $z_1 < p$ *and* $p^{\log_2 x} < t \le y$, *then*

$$\pi(t;p,a) = \frac{\pi(t)}{p-1}\left(1 + O\left(\frac{1}{(\log t)^A}\right)\right) \tag{7}$$

holds for all residue classes $a \in \{1,\ldots,p-1\}$ *and all* t *except for at most* $2\log_2 x$ *exceptional primes* p *each of which exceeds* $\log_2 x$.

Remark. Observe that since $t > z_1$, it follows that $(\log t)^A > \log_2 x$ holds for all x sufficiently large. Thus, we may assume that also the error in the estimate of the above lemma (uniformly in our range for t), is larger than $\log_2 x$.

Proof. We follow the proof of Linnik's theorem from page 54 in [7]. Let $p \in (z_1, y^{1/\log_2 x})$ be fixed and let $t > p^{\log_2 x}$. There it is shown that if $p \le T$ is any modulus then

$$\sum_{\substack{q\le t\\ q\equiv a (\bmod p)}} \log q = \frac{t}{\varphi(p)} + E + O\left(t^{1/2} + \frac{t\log t}{T}\right),$$

and

$$E = -\chi_1(a)\frac{t^{\beta_1}}{\beta_1} + O\left(\frac{F}{\varphi(p)}\right),$$

with both E and F certain sums over zeros of L functions $L(s,\chi)$, where χ runs over the characters modulo p. The term $-\chi_1(a)t^{\beta_1}/\beta_1$ appears only if there exists an exceptional zero relative to the pair (T,c_1). For us, we put $T := t^{2/\log_2 x}$ and take any c_1. Then $p \le T^{1/2}$. If there is an exceptional zero with respect to the pair (T,c_1), then it is unique. Further, it is also exceptional for the pair $(T',c_1/2)$ for any $T' \in [T,T^2]$, and the prime p satisfies

$$p > (\log(T^{1/2}))^{c_2} = (\log T)^{c_2/2}.$$

Since $p > z_1$, we have that $t > z_1^{\log_2 x}$, so

$$\log t > (\log_2 x) z_1 = (\log_2 x)(\log x)^{1/\log_3 x} > (\log_2 x)^2 \qquad \text{for} \qquad x > x_0.$$

Hence,

$$\log T = \frac{2\log t}{\log_2 x} > (\log t)^{1/2}$$

uniformly for all our t when $x > x_0$, so $p > (\log T)^{c_2/2} > (\log t)^{c_2/4}$. Note that since $t > p^{\log_2 x} > z_1^{\log_2 x}$, it follows easily that

$$(\log t)^{c_2/2} > ((\log_2 x)(\log x)^{1/\log_3 x})^{c_2/2} > \log_2 x$$

for all $x > x(c_1)$. Let us give an upper bound on the number k of exceptional primes of this type. Since we just said that if there is some exceptional prime for T, then it is also the exceptional prime for all $T' \in [T,T^2]$, it follows that if we take $t_1 := z_1^{\log_2 x}$, $t_2 := t_1^2$, $t_3 := t_2^2$, $\ldots$, $t_k := t_{k-1}^2$, where k is the smallest positive integer such that $t_k \ge y$, then there can be at most k exceptional primes altogether. Clearly, from the above recurrence we have $t_j = t_1^{2^j}$. Hence,

$$y \le t_1^{2^k} = (z_1^{2\log_2 x})^{2^k},$$

and upon taking logarithms we get

$$\frac{\log x}{\log_2 x} \le 2^k (\log_2 x)(\log x)^{1/\log_3 x},$$

and taking logarithms once again we get

$$k \log 2 - \frac{\log_2 x}{\log_3 x} \geq \log_2 x - 2\log_3 x.$$

Hence,

$$k = \left(\frac{1}{\log 2} + O\left(\frac{1}{\log_3 x} \right) \right) \log_2 x,$$

so clearly, $k < 2\log_2 x$ for all x large enough. From now on, we discard the exceptional primes and work with the remaining ones. For them,

$$E = O\left(\frac{F}{\varphi(p)} \right),$$

where by arguments from the middle of page 55 in [7] together with the fact that we are under the assumption that there is no exceptional zero, F is bounded as

$$F \ll t^{1/2} T^5 + \frac{(\log t) t^{1-c_1/\log T}}{\log(t/T^{c_3})} \quad \text{if} \quad t > T^{c_3}.$$

For us, the inequality $t > T^{2c_3}$ holds for all $x > x_0$, so $\log(t/T^{c_3}) \gg \log t$. Further, since in fact $\log T \leq 2\log t/\log\log x \leq 2\log t/\log\log t$, it follows that $1 - c_1/\log T \geq 1 - 2c_1(\log\log t)/\log t$, therefore the second term on the right above is

$$\ll \frac{t}{(\log t)^{2c_1+1}}.$$

Putting everything together, we get that

$$\sum_{\substack{q \leq t \\ q \equiv a (\bmod p)}} \log q = \frac{t}{\log q} + O\left(t^{1/2} + \frac{t \log t}{T} + \frac{t^{1/2} T^5}{\varphi(p)} + \frac{t}{\varphi(p)(\log t)^{2c_1+1}} \right). \tag{8}$$

Since $\varphi(p) < p \leq T^{1/2} = t^{o(1)}$, the first and third terms above are all dominated by the fourth term, while the second one is

$$\frac{t \log t}{T}.$$

It remains to show that this is also dominated by the fourth one. Since $T^{1/2} \geq p > \varphi(p)$, it suffices to show that

$$T^{1/2} > (\log t)^{2c_1+2}.$$

This is equivalent to

$$\frac{\log t}{\log_2 x} > (2c_1 + 1)\log_2 t, \qquad \text{or} \qquad \frac{\log t}{\log_2 t} > (2c_1+1)\log_2 x.$$

The function $t \mapsto \log t/\log_2 t$ is increasing for $t > e^e$, and since for us $t > z_1^{\log_2 x} > z_1$, we have

$$\frac{\log t}{\log_2 t} > \frac{(\log x)^{1/\log_3 x}}{((\log_2 x)/\log_3 x)}$$

and the function on the right hand side exceeds any multiple of $\log_2 x$ for x sufficiently large. Hence, the four contributions to the error term in (8) are dominated by the fourth one, and so

$$\sum_{\substack{q \leq t \\ q \equiv a (\bmod p)}} \log q = \frac{t}{\varphi(p)} \left(1 + O\left(\frac{1}{(\log t)^A} \right) \right),$$

where we can take $A = 2c_1$. This is uniform for all t in our range, and now the desired conclusion follows by Abel summation. $\square$

Let $k \geq 1$. Put

$$M(x,k) = \sum_{n \leq x,\ \Omega(n)=k} \mu(n)^2.$$

Using elementary analytic number theory an asymptotic for $M(x,k)$ can be derived (cf. Hardy and Wright [16, Theorem 437]). We will need a slightly stronger result.

Lemma 2. *We have*

$$M(x,k) = \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\left(1 + o_k\left(\frac{1}{\log\log x}\right)\right).$$

Proof. As remarked in the introduction one has the estimate

$$N(x,k) = \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\left(1 + o_k\left(\frac{1}{\log\log x}\right)\right). \tag{9}$$

For $k = 1$ the result is merely a weaker variant of Theorem 4, the Prime Number Theorem. For $k \geq 2$ the idea of the proof is to relate $M(x,k)$ to $N(x,k)$ and use the estimate (9). Noting that $M(x,2) = N(x,2) - \sum_{p \leq \sqrt{x}} 1$ and using (9) with $k = 2$, the claim follows for $k = 2$ and so we may assume that $k \geq 3$.

Observe that if $\Omega(n) = k$, then either n is square-free or $n = p^2 m$ with $\Omega(m) = k-2$ and p a prime. It follows that

$$M(x,k) = N(x,k) + O\Big(\sum_{p \leq \sqrt{x}} N(\frac{x}{p^2}, k-2)\Big).$$

Using the trivial estimate $N(x,k-2) = O(x)$ in the range $x^{1/3} \leq p \leq \sqrt{x}$ and the non-trivial estimate (9) in the range $p < x^{1/3}$, the proof is easily completed. $\square$

Corollary 1. *The counting function $N_T(x)$ satisfies the asymptotic estimate* (3).

Proof. Note that $N_T(x) = M(x,3) - M(x/2,2) + \pi(x/4) + O(1)$ and use the lemma for $k = 3$ and $k = 2$. $\square$

4. The proof of Theorem 1

Proof of Theorem 1. We observe that for ternary n,

$$p^3 < n \leq x, \quad \text{therefore} \quad p < x^{1/3},$$

and similarly

$$pq^2 < n \leq x, \quad \text{therefore} \quad q < \sqrt{x/p}.$$

Thus,

$$|\mathcal{T}(x)| = \sum_{3 \leq p < x^{\frac{1}{3}}} \sum_{\substack{p < q < \sqrt{x/p} \\ q \equiv \pm 1 (\bmod p)}} \sum_{\substack{q < r \leq \frac{p-1}{p-2}(q-1) \\ pqr \leq x \\ r \equiv q (\bmod p)}} 1. \tag{10}$$

Denote the inner sum over r by σ_r. We start with a lower bound on $|\mathcal{T}(x)|$. Take $p = 3$. Then $r \equiv q (\bmod 3)$ and $q < r < 2q - 2$. Thus, by Theorem 6, $\sigma_r \gg \frac{q}{\log q}$ for $q \geq q_0$. Note also that any such r leads to a legitimate choice for $n \in \mathcal{T}(x)$ provided that $3q(2q) \le x$, that is, whenever $q \le \sqrt{x/6}$. Thus, for $x \ge x_0$

$$|\mathcal{T}(x)| \gg \sum_{q_0 \le q \le \sqrt{x/6}} \frac{q}{\log q} \gg \int_{q_0}^{\sqrt{x/6}} \frac{t d\pi(t)}{\log t} \gg \frac{t^2}{(\log t)^2}\Big|_{t=2}^{\sqrt{x/6}} \gg \frac{x}{(\log x)^2}.$$

We now determine an asymptotic for $\mathcal{T}(x)$ and show that $x/(\log x)^2$ is indeed the correct order of magnitude.

Neglecting the primality condition on r we obtain

$$\sigma_r \le \pi\left(q-1+\frac{q-1}{p-2}; p; q\right) - \pi(q;p,q) \le \frac{1}{p}\left(\frac{q-1}{p-2}-1\right)+1 \ll \frac{q}{p^2}+1. \tag{11}$$

We now sum up over all q forgetting the congruence condition on q. It follows that for a fixed p, the number of constrained ternary integers under scrutiny is of order at most

$$\frac{1}{p^2}\left(\sum_{q\le\sqrt{x/p}} q\right) + \pi\left(\sqrt{\frac{x}{p}}\right). \tag{12}$$

For us $p < x^{1/3}$, therefore $\log(x/p) \gg \log x$, and thus the second term in (12) is, by the Chebychev estimates (6),

$$\pi\left(\sqrt{\frac{x}{p}}\right) \ll \frac{\sqrt{x}}{\sqrt{p}\log(x/p)} \ll \frac{\sqrt{x}}{\sqrt{p}\log x}.$$

For the first term in (12) above, we can also use the Chebychev estimates and get that

$$\sum_{q\le\sqrt{x/p}} q \ll \int_2^{\sqrt{x/p}} t d\pi(t) \ll \frac{t^2}{\log t}\Big|_{t=2}^{t=\sqrt{x/p}} \ll \frac{x}{p\log(x/p)} \ll \frac{x}{p\log x}.$$

Thus, for a fixed p, the number of choices for n is at most of order

$$\ll \frac{x}{p^3\log x} + \frac{\sqrt{x}}{\sqrt{p}\log x}. \tag{13}$$

We now sum up over p. We deal first with the second term in (13). There, even forgetting that p is prime, we get that this term contributes at most

$$\frac{\sqrt{x}}{\log x}\sum_{p\le x^{1/3}} \frac{1}{\sqrt{p}} \ll \frac{\sqrt{x}}{\log x}\int_2^{x^{1/3}} \frac{dt}{\sqrt{t}} \ll \frac{x^{\frac{1}{2}+\frac{1}{6}}}{\log x} = \frac{x^{2/3}}{\log x}$$

to $\mathcal{T}(x)$. Next we deal with the first term in (13), when summed up over all $p > \log x$. There we get, even forgetting the condition that p is prime, that this term contributes

$$\frac{x}{\log x}\sum_{p>\log x}\frac{1}{p^3} \ll \frac{x}{\log x}\int_{\log x}^{\infty}\frac{dt}{t^3} \ll \frac{x}{\log x}\left(-\frac{1}{t^2}\Big|_{t=\log x}^{t=\infty}\right) \ll \frac{x}{(\log x)^3}. \tag{14}$$

Thus, (12) is small compared to $|\mathcal{T}(x)|$ when $p > \log x$. We see that the main contribution comes from $p \le \log x$ and from now on, we work under this assumption. Let us now go back to (11) and assume in addition that $q < \sqrt{x}/\log x$. Summing up over all primes $q \le \sqrt{x}/\log x$ of this type, we get instead of (12) the number of integers $n \in \mathcal{T}(x)$ of size at most

$$\frac{1}{p^2}\sum_{q \le \sqrt{x}/\log x} q + \pi\left(\sqrt{x/p}\right) \ll \frac{x}{p^2(\log x)^3},$$

since $p \le \log x$. Summing up over all p, we get a contribution of $O\left(x/(\log x)^3\right)$ to $|\mathcal{T}(x)|$, which is small.

So, from now on we work in the range $p \le \log x$ and $\sqrt{x}/\log x < q < \sqrt{x/p}$. One can rewrite (10) as follows

$$|\mathcal{T}(x)| = \sum_{3<p\le \log x}\ \sum_{\substack{\frac{\sqrt{x}}{\log x}<q<\sqrt{x/p}\\ q\equiv \pm 1 \pmod p}}\ \sum_{\substack{q<r\le \min\left(\frac{p-1}{p-2}(q-1),\frac{x}{pq}\right)\\ r\equiv q \pmod p}} 1 + O\left(\frac{x}{(\log x)^3}\right).$$

Write σ_r' for the inner sum. It clearly makes sense for large x and $p \le \log x$ to write q_p for the solution q of

$$\frac{x}{pq} = q - 1 + \frac{q-1}{p-2} = \left(\frac{p-1}{p-2}\right)(q-1).$$

Hence,

$$q - \frac{1}{2} = \sqrt{\frac{x(p-2)}{p(p-1)} + O(1)} = \sqrt{\frac{x(p-2)}{p(p-1)}\left(1 + O\left(\frac{p}{x}\right)\right)} = \sqrt{\frac{x(p-2)}{p(p-1)}} + O(1),$$

which gives

$$q_p = \sqrt{\frac{x(p-2)}{p(p-1)}} + O(1). \tag{15}$$

Suppose first that $q \le q_p$. Then, by Theorem 6, we have

$$\sigma_r' = \frac{\pi(q-1+(q-1)/(p-2)) - \pi(q)}{\varphi(p)} + O\left(qe^{-c_0\sqrt{\log q}}\right)$$

for some constant $c_0 > 0$. For us, $\log q = (1/2 + o(1))\log x$. Further, by Theorem 4 we have that

$$\pi\left(q - 1 + \frac{q-1}{p-2}\right) - \pi(q) = \int_q^{q-1+\frac{q-1}{p-2}} \frac{dt}{\log t} + O\left(qe^{-c_1(\log q)^{3/5}(\log_2 q)^{-1/5}}\right)$$

for some constant $c_1 > 0$. Putting everything together, we get that when $p,\ q \le q_p$ are fixed

$$\sigma_r' = \frac{1}{p-1}\int_q^{q-1+\frac{q-1}{p-2}} \frac{dt}{\log t} + O\left(qe^{-c_2\sqrt{\log q}}\right)$$

for some constant $c_2 > 0$. We split the integral as

$$\int_q^{q-1+\frac{q-1}{p-2}} \frac{dt}{\log t} = \int_q^{q+\frac{q}{p-2}} \frac{dt}{\log t} + \int_{q+\frac{q}{p-2}}^{q-1+\frac{q-1}{p-2}} \frac{dt}{\log t}.$$

In the second integral, the length of the interval is $O(1)$ and the integral is of size $O(1/\log x)$. Thus,

$$\sigma_r' = \frac{1}{p-1}\int_q^{q+\frac{q}{p-2}} \frac{dt}{\log t} + O\left(qe^{-c_2\sqrt{\log q}}\right).$$

Now we estimate the latter integral. We make the substitution $t = qu$ for which $dt = qdu$. We get

$$\begin{aligned}\int_q^{q+\frac{q}{p-2}} \frac{dt}{\log t} &= \int_1^{1+\frac{1}{p-2}} \frac{qdu}{\log q + \log u} \\ &= \frac{q}{\log q}\int_1^{1+\frac{1}{p-2}} du - \frac{q}{\log q}\int_1^{1+\frac{1}{p-2}} \frac{\log u}{\log q + \log u} du \\ &= \frac{q}{(p-2)\log q} + O\left(\frac{q}{p^2(\log x)^2}\right).\end{aligned}$$

In the last inequality above, we used the fact that

$$0 \le \log u \le \log\left(1 + \frac{1}{p-2}\right) \le \frac{1}{p-2}$$

for all $u \in [1, 1 + 1/(p-2)]$. Further, notice that since $\sqrt{x}/\log x < q < \sqrt{x/p}$, we have that $\log q = \frac{1}{2}\log x + O(\log\log x)$ and hence,

$$\frac{1}{\log q} = \frac{2}{\log x}\left(1 + O\left(\frac{\log_2 x}{\log x}\right)\right)^{-1} = \frac{2}{\log x} + O\left(\frac{\log_2 x}{(\log x)^2}\right).$$

Thus,

$$\sigma_r' = \frac{2q}{(p-1)(p-2)\log x} + O\left(\frac{q\log_2 x}{p^2(\log x)^2}\right). \tag{16}$$

Next consider $q > q_p$. Then certainly $x/(pq) \asymp q$ (in fact, $q_p > \sqrt{x/(4p)}$ for large enough x). So, by the same argument and using Theorems 4 and 6, we have

$$\begin{aligned}\sigma_r' &= \frac{\pi(x/(pq)) - \pi(q)}{\varphi(p)} + O\left(qe^{-c_3\sqrt{\log x}}\right) = \frac{x/(pq) - q}{(p-1)\log q} + O\left(\frac{q}{p(\log x)^2}\right) \\ &= \frac{2}{(p-1)\log x}\left(\frac{x}{pq} - q\right) + O\left(\frac{q\log_2 x}{p(\log x)^2}\right).\end{aligned} \tag{17}$$

Combining (16) and (17), we get

$$\sigma_r' = \frac{2a_{p,q}(x)}{(p-1)\log x} + O\left(\frac{q\log_2 x}{p(\log x)^2}\right), \quad \text{where} \quad a_{p,q}(x) = \begin{cases} \frac{q}{p-2} & \text{if} \quad q \le q_p; \\ \frac{x}{pq} - q & \text{if} \quad q > q_p. \end{cases}$$

We sum up over q and first deal with the error term. Since

$$\begin{aligned}\sum_{p\le\log x}\ \sum_{\substack{q\le\sqrt{x/p} \\ q\equiv\pm1 \pmod p}} \frac{q}{p} &\ll \sum_{p\ge3}\frac{1}{p}\int_3^{\sqrt{x/p}} t\, d\pi(t;p,\pm1) \\ &\ll \sum_{p\ge3}\left(\frac{t^2}{p(p-1)\log t}\Big|_2^{\sqrt{x/p}}\right) \ll \frac{x}{\log x},\end{aligned}$$

then the error term coming from σ_r is $O\left(x(\log x)^{-3}\log_2 x\right)$. Thus, we have

$$|\mathcal{T}(x)| = \sum_{p\le\log x}\ \sum_{\substack{\frac{\sqrt{x}}{\log x}<q\le\sqrt{x/p} \\ q\equiv\pm1 \pmod p}} \frac{2a_{p,q}(x)}{(p-1)\log x} + O\left(\frac{x\log_2 x}{(\log x)^3}\right). \tag{18}$$

It remains to deal with the main term. We let $\varepsilon \in \{\pm 1\}$ and sum over all q in the interval $\sqrt{x}/\log x < q < q_p$ such that $q \equiv \varepsilon (\bmod\, p)$. By Abel's summation formula, one gets

$$\sum_{\substack{\frac{\sqrt{x}}{\log x} < q \le q_p \\ q \equiv \varepsilon (\bmod\, p)}} q \quad = \quad q_p \pi(q_p; p, \varepsilon) - \frac{\sqrt{x}}{\log x} \pi\left(\frac{\sqrt{x}}{\log x}; p, \varepsilon\right) - \int_{\frac{\sqrt{x}}{\log x}}^{q_p} \pi(t; p, \varepsilon) dt. \tag{19}$$

By combining Theorem 4 and Theorem 6, we obtain that

$$\pi(t; p, \varepsilon) = \frac{t}{(p-1)\log t} + O\left(\frac{t}{p(\log t)^2}\right) \quad \text{uniformly in} \quad t \in \left[\frac{\sqrt{x}}{\log x}, \sqrt{\frac{x}{p}}\,\right].$$

Thus, one can check that

$$\sum_{\substack{\frac{\sqrt{x}}{\log x} < q \le q_p \\ q \equiv \varepsilon (\bmod\, p)}} q = \frac{q_p^2}{(p-1)\log x} + O\left(\frac{x \log_2 x}{p(\log x)^2}\right).$$

This was for a fixed $\varepsilon \in \{\pm 1\}$ and for $q \le q_p$. It remains to deal with the contribution of q in the range $q_p < q \le \sqrt{x/p}$. For this, we need to compute

$$\sum_{\substack{q_p < q \le \sqrt{x/p} \\ q \equiv \varepsilon (\bmod\, p)}} \left(\frac{x}{pq} - q\right) = \frac{x}{p} \sum_{\substack{q_p < x \le \sqrt{x/p} \\ q_p \equiv \varepsilon (\bmod\, p)}} \frac{1}{q} - \sum_{\substack{q_p \le q \le \sqrt{x/p} \\ q \equiv \varepsilon (\bmod\, p)}} q.$$

The second sum is, by the above arguments,

$$\sum_{\substack{q_p < q \le \sqrt{x/p} \\ q \equiv \varepsilon (\bmod\, p)}} q = \frac{x}{p(p-1)\log x} - \frac{q_p^2}{(p-1)\log x} + O\left(\frac{x \log_2 x}{p(\log x)^2}\right).$$

Accounting for the fact that we have two values of ε and inserting the above estimates into (18), we get

$$|\mathcal{T}(x)| = \sum_{p \le \log x} \left(\frac{2x}{p(p-1)\log x} \sum_{\substack{q_p \le q \le \sqrt{x/p} \\ q \equiv \pm 1 (\bmod\, p)}} \frac{1}{q} + \frac{4f(x, p, q_p)}{(p-1)(\log x)^2}\right) + O\left(\frac{x \log_2 x}{(\log x)^3}\right),$$

where

$$f(x, p, q_p) = \frac{q_p^2}{(p-2)(p-1)} - \frac{x}{p(p-1)} + \frac{q_p^2}{p-1}.$$

Using (15), we see that

$$q_p^2 = \frac{x(p-2)}{p(p-1)} + O(q_p) = \frac{x(p-2)}{p(p-1)} + O(\sqrt{x}),$$

and hence

$$f(x, p, q_p) \quad = \quad \frac{x}{p(p-1)^2} - \frac{x}{p(p-1)} + \frac{x(p-2)}{p(p-1)^2} + O\left(\frac{\sqrt{x}}{p}\right) = O\left(\frac{\sqrt{x}}{p}\right).$$

Thus, the contribution coming from the sum over p to $\mathcal{T}(x)$ of the term that contains $f(x, p, q_p)$, is

$$O\left(\frac{\sqrt{x}}{(\log x)^2} \sum_{p \le \log x} \frac{1}{p(p-1)}\right),$$

which is small. We conclude that

$$|\mathcal{T}(x)| = \frac{2x}{\log x}\sum_{p\le \log x}\frac{1}{p(p-1)}\sum_{\substack{q_p\le q\le\sqrt{x/p}\\ q\equiv\pm 1 (\bmod p)}}\frac{1}{q} + O\left(\frac{x\log_2 x}{(\log x)^3}\right).$$

Using again the Abel summation formula we get (after a short computation) that for a fixed $\varepsilon\in\{\pm1\}$,

$$\sum_{\substack{q_p\le q\le\sqrt{x/p}\\ q\equiv\varepsilon (\bmod p)}}\frac{1}{q} = \frac{1}{p-1}\frac{\log(\frac{p-1}{p-2})}{\log x} + O\left(\frac{\log_2 x}{p(\log x)^2}\right).$$

Since there are two values for ε, the contribution of a fixed p to the number of elements of $\mathcal{T}(x)$ is

$$\frac{4}{p(p-1)^2(\log x)^2}\log\left(\frac{p-1}{p-2}\right) + O\left(\frac{x\log_2 x}{p^3(\log x)^2}\right).$$

We now sum over $3\le p\le\log x$, getting

$$\frac{4}{(\log x)^2}\left(\sum_{p\le\log x}\frac{1}{p(p-1)^2}\log\left(\frac{p-1}{p-2}\right)\right) + O\left(\frac{x\log_2 x}{(\log x)^3}\sum_{p\ge 3}\frac{1}{p^3}\right).$$

The error term is $O(x\log_2 x/(\log x)^3)$. As for the main term, we can take the sum of the series to infinity introducing a tail of size

$$\sum_{p>\log x}\frac{1}{p(p-1)^2}\log\left(\frac{p-1}{p-2}\right) \ll \sum_{m>\log x}\frac{1}{m^4} \ll \frac{1}{(\log x)^3}.$$

The result is therefore proved. □

5. Proof of Theorem 2

Proof of Theorem 2. We proceed as in the proof of Theorem 1. Since $p^3 < pqr \le x$, it follows that $p < x^{\frac{1}{3}}$ and similarly $pq^2 < pqr \le x$ implies $q < \sqrt{x/p}$. Thus, we want to count

$$|\mathcal{T}_a(x)| = \sum_{p\le x^{\frac{1}{3}}}\ \sum_{p<q<\sqrt{x/p}}\ \sum_{\substack{q<r\le x/(pq)\\ r\equiv a (\bmod pq)}} 1. \tag{20}$$

Let $p=3$ and $q=5$. Then r runs over some arithmetic progression modulo 15 in the range $5<r\le x/15$. By Theorem 6, it follows that $|\mathcal{T}_a(x)| \gg x/\log x$.

We denote the inner sum over r in (20) by σ_r. By neglecting the condition of r being prime we obtain

$$\sigma_r = \sum_{\substack{q<r\le x/(pq)\\ r\equiv a (\bmod pq)}} 1 \le \frac{1}{pq}\left(\frac{x}{pq}-q\right) = \frac{x}{(pq)^2} - \frac{1}{p}.$$

Thus,

$$|\mathcal{T}_a(x)| = x\sum_{p\le x^{\frac{1}{3}}}\frac{1}{p^2}\sum_{p<q<\sqrt{x/p}}\frac{1}{q^2} - \sum_{p\le x^{\frac{1}{3}}}\frac{1}{p}\sum_{p<q<\sqrt{x/p}} 1.$$

Define

$$\mathcal{T}_a'(x) = \{pqr\le x:\ 3\le p<q<r,\ r\equiv a (\bmod pq),\ g\ge(\log x)^2\}.$$

Let $\mathcal{T}_a'(x)$ count the integers counted by $\mathcal{T}_a(x)$ with the additional requirement that $q \geq (\log x)^2$. We then have

$$\left|\mathcal{T}_a'(x)\right| < \frac{x}{(\log x)^2} \sum_{p \leq x^{\frac{1}{3}}} \frac{1}{p^2} \sum_{p<q<\sqrt{x/p}} \frac{1}{q} < \frac{x \log_2 x}{(\log x)^2} \sum_{p \leq x^{\frac{1}{3}}} \frac{1}{p^2} \ll \frac{x \log_2 x}{(\log x)^2},$$

where we used Theorem 5. Similarly if $p \geq (\log x)^2$, then we can improve the bound to

$$\left|\mathcal{T}_a'(x)\right| \ll \frac{x \log_2 x}{(\log x)^4}.$$

By the above we get

$$|\mathcal{T}_a(x)| = \sum_{p<(\log x)^2} \sum_{\substack{p<q<\sqrt{x/p} \\ q<(\log x)^2}} \sigma_r + O\left(\frac{x \log_2 x}{(\log x)^2}\right).$$

On noticing that $\pi(q; a, pq) = \pi(q)$, we obtain

$$\sum_{p<(\log x)^2} \sum_{p<q<(\log x)^2} \pi\left(q\right) \ll \sum_{p<(\log x)^2} \int_p^{(\log x)^2} t d\pi(t) \ll \frac{(\log x)^6}{(\log_2 x)^2}.$$

We then write

$$\sigma_r = \pi\left(\frac{x}{pq}; a, pq\right) - \pi(q; a, pq),$$

and get

$$|\mathcal{T}_a(x)| = \sum_{p<(\log x)^2} \sum_{p<q<(\log x)^2} \pi\left(\frac{x}{pq}; a, pq\right) + O\left(\frac{x \log_2 x}{(\log x)^2}\right).$$

Since $\log(x/pq) = \log x + O(\log_2 x)$, the main term above equals

$$\begin{aligned} & x \sum_{p<(\log x)^2} \frac{1}{p(p-1)} \sum_{p<q<(\log x)^2} \frac{1}{q(q-1)} \frac{1}{\log\left(\frac{x}{pq}\right)} \\ = & \frac{x}{\log x} \sum_{p<(\log x)^2} \frac{1}{p(p-1)} \sum_{p<q<(\log x)^2} \frac{1}{q(q-1)} + O\left(\frac{x \log_2 x}{(\log x)^2}\right). \end{aligned}$$

We complete the sums above to infinity with an error of a suitable size and get

$$|\mathcal{T}_a(x)| = C_2 \frac{x}{\log x} + O\left(\frac{x \log_2 x}{(\log x)^2}\right),$$

thus concluding the proof.

□

6. The proof of Theorem 3

Note that there are $(p-1)^2$ possible pairs of residue classes (a, b) modulo p with $1 \leq a, b \leq p-1$. Recall that

$$N_T(x) = |\{n = pqr \leq x : 3 \leq p < q < r\}| \sim \frac{x(\log_2 x)^2}{2 \log x}. \tag{21}$$

Hence, by restricting for each p the number of possibilities of the pair (q, r) modulo p to a fraction α of the total number of possibilities, we end up with a set of positive integers the cardinality of which, if we count them up to x, is asymptotic to α times the total number of positive integers $n \le x$ with exactly three prime factors $p < q < r$. Notice that a comparison of Theorem 3 with (21) shows that this simple heuristic idea is actually true.

For ease of exposition in the proof of Theorem 3, we now let

$$y := \exp\left(\frac{\log x}{\log_2 x}\right), \ z_1 := \exp\left(\exp\left(\frac{\log_2 x}{\log_3 x}\right)\right), \ y_1 := \exp\left(\frac{\log x}{\exp((\log_3 x)^2)}\right).$$

The proof of Theorem 3. Let $n = pqr \le x$ with $p < q < r$. Then

$$p^3 < x \quad \text{and} \quad pq^2 < x,$$

and so

$$p < x^{1/3} \quad \text{and} \quad q < \sqrt{x/p}.$$

We may also assume that $n > x/\log x$, since otherwise there are at most $O(x/\log x)$ integers $n \le x$, regardless of the number of their prime factors. Thus,

$$\frac{x}{pq\log x} < r \le \frac{x}{pq}.$$

Furthermore, $r^3 > n > x/\log x$, so $r > (x/\log x)^{1/3}$. Fix p and q. Since $r \le x/(pq)$, the number of possibilities for r (disregarding the congruence conditions on (q, r) modulo p) is less or equal than

$$\pi\left(\frac{x}{pq}\right) \ll \frac{x}{pq\log(x/pq)} \ll \frac{x}{pq\log x}, \tag{22}$$

where for the last inequality we used the fact that

$$\frac{x}{pq} \ge r > \left(\frac{x}{\log x}\right)^{1/3} \gg x^{1/4}, \quad \text{so} \quad \log(x/pq) \gg \log x.$$

Assume $q \in [y, x]$. Then for a fixed p, the number of $n \le x$ with such q is by Theorem 5 of order at most

$$\frac{x}{p\log x}\sum_{y<q<x}\frac{1}{q} \ll \frac{x}{p\log x}(\log_2 x - \log_2 y + o(1)) \ll \frac{x\log_3 x}{p\log x}. \tag{23}$$

Summing up (23) over all $p \le x^{1/3}$, we get an upper bound of

$$\frac{x\log_3 x}{\log x}\sum_{p\le x^{1/3}}\frac{1}{p} \ll \frac{x\log_2 x\log_3 x}{\log x} = O\left(N_T(x)\frac{\log_3 x}{\log_2 x}\right)$$

on the set of such $n \le x$. So, from now on we may assume that $q \le y$. Assume that $p \le z_1$. Then summing up (22) over all $p \le z_1$ but q fixed, we get a number of $n \le x$ of order

$$\frac{x}{q\log x}\sum_{p\le z_1}\frac{1}{p} \ll \frac{x}{q\log x}(\log_2 z_1 + O(1)) \ll \frac{x}{q\log x}\frac{\log_2 x}{\log_3 x}.$$

Summing up the above inequality over all $q \le \sqrt{x}$, we get an upper bound of order

$$\frac{x}{\log x}\frac{\log_2 x}{\log_3 x}\sum_{q\le\sqrt{x}}\frac{1}{q} \ll \frac{x}{\log x}\frac{(\log_2 x)^2}{\log_3 x} = O\left(\frac{N_T(x)}{\log_3 x}\right)$$

on the set of such $n \le x$, so we can ignore such n. So, from now on $z_1 < p < q < y$. Assume next that $q < p^{\log_2 x}$. Then $p < q < p^{\log_2 x}$. Keeping p fixed and summing up inequality (22) over all such q we get that the number of integers $n \le x$ is of order at most

$$\frac{x}{p \log x} \sum_{p<q<p^{\log_2 x}} \frac{1}{q} \ll \frac{x}{p \log x}(\log_2(p^{\log_2 x}) - \log_2 p + O(1)) \ll \frac{x \log_3 x}{p \log x}.$$

Summing up over all $p \le x^{1/3}$, we get that the total number of $n \le x$ is of order at most

$$\frac{x \log_3 x}{\log x} \sum_{p \le x^{1/3}} \frac{1}{p} \ll \frac{x \log_2 x \log_3 x}{\log x} = O\left(N_T(x) \frac{\log_3 x}{\log_2 x}\right),$$

and this is negligible for us. So, we can ignore such integers n from our argument. So, from now on, we may assume that $p^{\log_2 x} < q$. Since also $q < y$, it follows that $p < y^{1/\log_2 x} = \exp(\log x/(\log_2 x)^2)$. In fact, we will do better. We assume that n is such that $y_1 \le p < x^{1/3}$. Then keeping q fixed and summing over such p, we get a number of such n of order at most

$$\frac{x}{q \log x} \sum_{y_1 \le p \le x^{1/3}} \frac{1}{p} \ll \frac{x}{q \log x}(\log_2 x^{1/3} - \log_2 y_1) \ll \frac{x(\log_3 x)^2}{q \log x}.$$

Summing up the above bound over all $q \le y$, we get a bound of

$$\frac{x(\log_3 x)^2}{\log x} \sum_{q \le y} \frac{1}{q} \ll \frac{x(\log_2 x)(\log_3 x)^2}{\log x} = O\left(N_T(x) \frac{(\log_3 x)^2}{\log_2 x}\right)$$

for the number of such $n \le x$, and this is negligible for us. So, we may assume that $p \in [z_1, y_1]$.

We plan to apply Lemma 1. We deal first with the exceptional primes. Let P_E be the set of such primes. Recall that $p > \log_2 x$ and $\#P_E \le 2 \log_2 x$ by Lemma 1. Fixing $p \in P_E$, the remaining $qr \le x/p$ can be chosen in at most

$$\pi_2\left(\frac{x}{p}\right) \ll \frac{x}{p} \frac{\log_2(x/p)}{\log(x/p)} \ll \frac{x \log_2 x}{p \log x}$$

ways. Here we used the fact that $p^{\log_2 x} < y < x$ and so $p < x^{1/\log_2 x}$, which implies that $\log(x/p) \gg \log x$. Now p is in a set of at most $2 \log_2 x$ elements each larger than $\log_2 x$. We now sum up over $p \in P_E$. Discarding the information that they are primes and keeping only the information about their sizes and the number of them, we get a contribution of at most

$$\frac{x \log_2 x}{\log x} \sum_{\substack{p \in P_E \\ \log_2 x < p \\ \#P_E \le 2 \log_2 x}} \frac{1}{p} \ll \frac{x \log_2 x}{\log x} \left(\frac{\#P_E}{\log_2 x}\right) \ll \frac{x \log_2 x}{\log x} = O\Big(\frac{N_T(x)}{\log_2 x}\Big)$$

ternary integers, and we are done.

Now we are in a situation were we can apply Lemma 1. We may assume that the estimate (7) holds for all $p \in [z_1, y_1]$ and all t such that $p^{\log_2 x} < t \le y$. So, we fix p in our range. We fix pair of residue classes $(a, b) \in \{1, \ldots, p-1\}$ such that $(a, b) \in M(p)$. We also fix q in the interval $(p^{\log_2 x}, y]$ such that $q \equiv a (\bmod\, p)$. So, we need to count the number of primes

$$r \in \left[\frac{x}{pq(\log x)}, \frac{x}{pq}\right]$$

which are congruent to $b (\bmod\, p)$. Then we need to sum up this over all b modulo p such that $(a, b) \in M(p)$, then over all q which are a modulo p, then over all $a (\bmod\, p)$ such that there exist b with $(a,b) \in M(p)$ and finally over all p. Since (7) applies, the first step gives

$$\frac{\pi(x/pq)}{\varphi(p)}\left(1+O\left(\frac{1}{\log_2 x}\right)\right) - \frac{\pi(x/pq(\log x))}{\varphi(p)}\left(1+O\left(\frac{1}{\log_2 x}\right)\right),$$

which equals

$$\frac{x}{pq\varphi(p)\log(x/pq)}\left(1+O\left(\frac{1}{\log_2 x}\right)\right). \tag{24}$$

Note that

$$\log(x/pq) = \log x + O(\log y) = (\log x)\left(1+O\left(\frac{1}{\log_2 x}\right)\right),$$

so because of the presence of the error term we can replace the factor $\log(x/pq)$ in the denominator in (24) by $\log x$. Thus, the count so far is

$$\frac{x}{\varphi(p)pq\log x}\left(1+O\left(\frac{1}{\log_2 x}\right)\right).$$

Now we sum up over all $q \in [p^{\log_2 x}, y]$ which are $q \equiv b(\bmod p)$. By the Abel summation formula, we infer that

$$\begin{aligned}
\sum_{\substack{p^{\log_2 x} \le q \le y \\ q \equiv b(\bmod p)}} \frac{1}{q} &= \left(\frac{\pi(t;p,b)}{t}\Big|_{t=p^{\log_2 x}}^{t=y}\right) + \int_{p^{\log_2 x}}^{y} \frac{\pi(t;p,b)}{t^2}dt \\
&= \frac{1+O(1/\log_2 x)}{\varphi(p)} \int_{p^{\log_2 x}}^{y} \frac{\pi(t)}{t^2}dt \\
&= \frac{1+O(1/\log_2 x)}{\varphi(p)} \int_{p^{\log_2 x}}^{y} \frac{1}{t\log t}\left(1+O\left(\frac{1}{\log t}\right)\right)dt \\
&= \frac{1+O(1/\log_2 x)}{\varphi(p)}\left(\log_2 y - \log_2(p^{\log_2 x}) + O(1)\right).
\end{aligned}$$

Note that

$$\log_2 y - \log_2(p^{\log_2 x}) = \log_2 x - \log_2 p + O(\log_3 x).$$

Since $p \le z_1$, it follows that

$$\log_2 x - \log_2 p \ge (\log_3 x)^2.$$

Thus,

$$\log_2 y - \log_2(p^{\log_2 x}) = (\log_2 x - \log_2 p)\left(1+O\left(\frac{1}{\log_3 x}\right)\right).$$

Thus, we get

$$\sum_{\substack{p^{\log_2 x} \le q \le y \\ q \equiv b(\bmod p)}} \frac{1}{q} = \frac{1}{\varphi(p)}(\log_2 x - \log_2 p)\left(1+O\left(\frac{1}{\log_3 x}\right)\right).$$

Hence, we get that for fixed p, a and b, the number of such n is

$$\frac{x}{p\varphi(p)^2(\log x)}(\log_2 x - \log_2 p)\left(1+O\left(\frac{1}{\log_3 x}\right)\right).$$

Now we sum up over all $n(a)$ which, by definition, is the number of $b \in \{1,\ldots,p-1\}$ such that $(a,b) \in M(p)$, then over all the a such that $n(a) > 0$. Keeping in mind that

$$\sum_{1 \le a \le p-1} n(a) = |M(p)| = \alpha p^2 + O(p),$$

we obtain a contribution of

$$\frac{\alpha x}{p\log x}(\log_2 x - \log_2 p)\left(1+O\left(\frac{1}{\log_3 x}\right)\right)\left(1+O\left(\frac{1}{p}\right)\right).$$

Now we sum the latter expression up over all $p \in [z_1, y_1]$ and on using that

$$1+O\left(\frac{1}{p}\right) = 1+O\left(\frac{1}{\log_3 x}\right)$$

in that range and the fact that

$$\sum_{p\le t}\frac{\log_2 p}{p} = \frac{1}{2}(\log_2 t)^2\left(1+O\left(\frac{1}{\log_2 t}\right)\right),$$

we get that the number of r we are after is

$$\alpha\left(\frac{x\log_2 x}{\log x}\sum_{z_1\le p\le y_1}\frac{1}{p} - \frac{x}{\log x}\sum_{z_1\le p\le y_1}\frac{\log_2 p}{p}\right)\left(1+O\left(\frac{1}{\log_3 x}\right)\right). \tag{25}$$

The first sum in (25) above asymptotically equals

$$\log_2 y_1 - \log_2 z_1 + o(1) = \log_2 x\left(1+O\left(\frac{1}{\log_3 x}\right)\right).$$

The second sum in (25) is

$$\frac{1}{2}\big((\log_2 y_1)^2 - (\log_2 z_1)^2 + O(\log_2 x)\big) = \frac{(\log_2 x)^2}{2}\left(1+O\left(\frac{1}{(\log_3 x)^2}\right)\right).$$

On putting everything together, the result is proved. $\square$

7. Applications

7.1. Cyclotomic polynomials. We define the *height* of a polynomial f in $\mathbb{Z}[x]$, $h(f)$, to be the maximum of absolute value of the coefficients of f. A polynomial of height one is said to be *flat*.

The n^{th} cyclotomic polynomial Φ_n is defined by

$$\Phi_n(x) = \prod_{\substack{1\le j\le n\\ (j,n)=1}}(x-\zeta_n^j) = \sum_{k=0}^{\varphi(n)} a_n(k)x^k,$$

where φ is Euler's totient function and ζ_n a primitive n^{th} root of unity. For a very readable introduction to the properties of coefficients of cyclotomic polynomials, the reader is referred to Thangadurai [27].

The coefficients $a_n(k)$ are integers that tend to be small. For example, for $n \le 104$ we have $|a_n(k)| \le 1$, but $a_{105}(7) = -2$. Note that 105 is the smallest ternary integer. It can be shown that if $|a_n(k)| > 1$, then n must have at least three distinct odd prime factors (see [23]). For a more recent reproof see, e.g., Lam and Leung [21].

Gallot and Moree [13] showed that the set $\{a_n(k) : 0 \le k \le \varphi(n)\}$ consists of a string of consecutive integers in case n is ternary. Different proofs of this fact were given by Bachmann [4] and Bzdęga [8]. In all three papers [4, 8, 13] this was achieved by establishing that, in case n is ternary, $|a_n(k) - a_n(k-1)| \le 1$. Thus, neighboring coefficients differ by at most one. In 2014 Bzdęga [9] went beyond this and characterized all k such that $|a_{pqr}(k) - a_{pqr}(k-1)| = 1$ and determined the number of k's for which this equality holds. There are various papers devoted to ternary cyclotomic polynomials, e.g. [1, 2, 3, 6, 14, 15, 19, 29].

For a long time the main conjecture on ternary cyclotomic polynomials was one made by Sister Marion Beiter in 1968.

Conjecture 1 (Sister Beiter conjecture [5])**.** *Let $p < q < r$ be primes. The cyclotomic coefficient $a_{pqr}(k)$ satisfies $|a_{pqr}(k)| \leq (p+1)/2$.*

Sister Beiter herself established her conjecture for $p = 3$ and $p = 5$ [6]. Zhao and Zhang [29] proved it for $p = 7$. However, for every $p \geq 11$ the conjecture is false as was shown by Gallot and Moree [14]. They put forward the following conjecture.

Conjecture 2 (Corrected Sister Beiter conjecture, Gallot and Moree [14])**.** *Let $p < q < r$ be primes. The cyclotomic coefficient $a_{pqr}(k)$ satisfies $|a_{pqr}(k)| \leq 2p/3$.*

This conjecture is sharp as it becomes false if the ratio $2/3$ is replaced by any smaller number [14]. It has been shown to hold if the ratio $2/3$ is replaced by $3/4$ [1].

7.2. **Flat cyclotomic polynomials.** Cyclotomic polynomials Φ_n are called flat if $h(\Phi_n) = 1$. The main challenge here is to find all n such that Φ_n is flat. For contributions, see [3, 11, 19, 20]. In particular, Broadhurst made a far reaching conjecture here, cf. [20]. Kaplan [19] found the following family of cyclotomic polynomials.

Theorem 7 (Kaplan [19])**.** *If $p < q$ are primes and $r \equiv \pm 1 (\mathrm{mod}\, pq)$, then Φ_{pqr} is flat.*

Elder [11] conjectured that if n has five or more odd prime factors, then Φ_n is not flat. It thus seems that flat polynomials are quite sparse.

7.3. **Inverse cyclotomic polynomials.** We define $\Psi_n(x) = (x^n - 1)/\Phi_n(x)$ to be the n^{th} *inverse* cyclotomic polynomial. Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$, we find that $\Psi_n = \prod_{d|n, d<n} \Phi_d$. Thus, Ψ_n is of degree $n - \varphi(n)$ and has integer coefficients $c_n(k)$ which, like those of the cyclotomic polynomials, tend to be small. For example Ψ_n has coefficients that are ≤ 1 in absolute value for $n \leq 560$. Moreover, $c_p(k) \in \{-1, 1\}$ and $c_{pq}(k) \in \{-1, 0, 1\}$ (compare [24, Lemma 5]).

We now recall two results on heights of cyclotomic and inverse cyclotomic polynomials due to Sister Beiter [6] and Moree [24]. By the following result and the Prime Number Theorem for Arithmetic Progressions (a weaker form of Theorem 6), one infers that the analogues of both the original and the corrected Sister Beiter conjecture for the ternary (inverse) cyclotomic polynomials are true for $p = 3$ and false for every $p \geq 5$.

Theorem 8 (Moree [24])**.** *Let $p < q < r$ be odd primes. Then $h(\Psi_n) = p - 1$ if and only if*

$$q \equiv r \equiv \pm 1 (\mathrm{mod}\ p) \text{ and } r < \frac{(p-1)}{(p-2)}(q-1). \tag{26}$$

In the remaining cases, $h(\Psi_n) < p - 1$.

We say that a ternary cyclotomic polynomial Ψ_n is *coefficient optimal* if $h(\Psi_n) = P(n) - 1$, where $P(n)$ denote the smallest prime factor of n. Thus, a ternary integer $n = pqr$ is coefficient optimal if and only if q and r satisfy (26).

7.4. **Analytic results.**

7.4.1. *An analytic result related to ternary inverse cyclotomic coefficients.* On combining Theorem 8 with Theorem 1, the following result is obtained.

Theorem 9. *The number $N_{CO}(x)$ of ternary $n = pqr \le x$ such that Ψ_n is coefficient optimal satisfies*

$$N_{CO}(x) = C_1 \frac{x}{(\log x)^2} + O\left(\frac{x \log\log x}{(\log x)^3}\right),$$

with C_1 as in (4).

Corollary 2. *We have*

$$\frac{N_{CO}(x)}{N_T(x)} \sim \frac{2C_1}{(\log x)(\log\log x)^2}.$$

In particular, Ψ_n is not coefficient optimal for almost all ternary n.

Proof. Combine Corollary 1 and Theorem 9. □

7.4.2. *Flatness.* On combining Theorem 2 and Theorem 7, the following result is obtained.

Theorem 10. *Let $F(x)$ denote the number of ternary $n \le x$ such that Φ_n is flat. Then*

$$F(x) \ge (2C_2 + o(1)) \frac{x}{\log x},$$

with C_2 as in (5).

7.4.3. *The corrected Sister Beiter conjecture.* The next result provides some evidence towards the corrected Sister Beiter conjecture.

Theorem 11. *The number $N_{CB}(x)$ of ternary $n \le x$ such that $h(\Phi_n) \le 2P(n)/3$ satisfies*

$$N_{CB}(x) \ge \Big(\frac{25}{27} + o(1)\Big) \frac{x(\log\log x)^2}{2\log x}.$$

Corollary 3. *The relative density of ternary integers for which the correct Sister Beiter conjecture holds true is at least* 0.925.

The proof of Theorem 11 makes use of the following estimate due to Bzdęga [8]. For completeness, we also consider what would happen if one would use an older estimate (2003) due to Bachman [1]. In that case we obtain Theorem 11 and Corollary 3 with 25/27 replaced by 8/9 and 0.925 by 0.888, respectively.

Theorem 12. *Let $3 \le p < q < r$ be primes. Let q^* and r^* be inverses of q and r modulo p, respectively that satisfy $1 \le q^*, r^* \le p-1$. Set $a = \min(q^*, r^*, p-q^*, p-r^*)$ and let $1 \le d \le p-1$ be defined by the relation $adqr \equiv 1 (\bmod\, p)$. Then we have (G. Bachman)*

$$-\min\Big(\frac{p-1}{2} + a, d\Big) \le a_{pqr}(k) \le \min\Big(\frac{p-1}{2} + a, p-d\Big),$$

and (B. Bzdęga)

$$-\min\Big(p + 2a - d, d\Big) \le a_{pqr}(k) \le \min\Big(2a + d, p - d\Big).$$

It is not difficult to show that

$$d = \min(\max(q^*, r^*), \max(p - q^*, p - r^*)).$$

Corollary 4. *Put* $d_1 = \min(d, p-d)$. *We have (G. Bachman)*

$$|a_{pqr}(k)| \le \min\Big(\frac{p-1}{2} + a, p - d_1\Big),$$

and (B. Bzdęga)

$$|a_{pqr}(k)| \le \min\Big(2a + d_1, p - d_1\Big).$$

Let $1 \le j, k \le p-1$ be integers. Put

$$\alpha = \min(j, k, p-j, p-k),\ \ \delta = \min(\max(j,k), \max(p-j, p-k)),$$

and $\delta_1 = \min(\delta, p-\delta)$. Put

$$GB(j,k) = \min\Big(\frac{p-1}{2} + \alpha, p - \delta_1\Big) \text{ and } BB(j,k) = \min(2\alpha + \delta_1, p - \delta_1).$$

We can reformulate the latter corollary in the following way.

Corollary 5. *If* $q^* \equiv j(\operatorname{mod} p)$ *and* $r^* \equiv k(\operatorname{mod} p)$, *then* $|a_{pqr}(k)| \le GB(j,k)$ *and* $|a_{pqr}(k)| \le BB(j,k)$.

Definition. *Put*

$$GB(p) = \{(j,k) : 1 \le j, k \le p-1,\ GB(j,k) \le 2p/3\},$$

and

$$BB(p) = \{(j,k) : 1 \le j, k \le p-1,\ BB(j,k) \le 2p/3\}.$$

The cardinality of $GB(p)$ *and* $BB(p)$ *we denote by* $N_{GB}(p)$, *respectively* $N_{BB}(p)$.

It is an elementary, but quite tedious, exercise to evaluate these quantities.

Proposition 1. *Let* $p > 3$ *be a prime. Then*

$$N_{GB}(p) = \begin{cases} \frac{8}{9}p^2 - \frac{16}{9}p + \frac{8}{9} & \text{if } p \equiv 1(\operatorname{mod} 3); \\ \frac{8}{9}p^2 - \frac{8}{9}p - \frac{16}{9} & \text{if } p \equiv 2(\operatorname{mod} 3). \end{cases}$$

and

$$N_{BB}(p) = \begin{cases} \frac{25}{27}p^2 - (\frac{8}{27}(\frac{p}{3}) + 2)p + \frac{73}{27} & \text{if } p \equiv \pm 2(\operatorname{mod} 9); \\ \frac{25}{27}p^2 - (\frac{8}{27}(\frac{p}{3}) + 2)p + \frac{37}{27} & \text{otherwise.} \end{cases}$$

Proof. We give a sketch. Note that if $(j,k) \in BB(p)$, then also $(k,j) \in BB(p)$. It thus follows that

$$N_{BB}(p) = 2 \sum_{\substack{1 \le j < k \le p-1 \\ (j,k) \in BB(p)}} 1 + \sum_{\substack{1 \le j \le p-1 \\ (j,j) \in BB(p)}} 1.$$

Let us concentrate on the first sum as it is more complicated to evaluate. We divide up the (j,k) region $1 \le j < k \le p-1$ into pieces on which $BB(j,k)$ takes on a value not involving a minimum or maximum anymore and compare this value with $2p/3$. Each of these contributions turns out to be a polynomial in p that is at most quadratic and has coefficients that depend at most on the residue of p modulo 9. Working out each of these contributions and summing gives the required result. Alternatively, after one has established that the final answer is a quadratic polynomial depending at most on the residue of p modulo 9, one finds the formula for $N_{BB}(p)$ be evaluting it for various values of p and inferring the coefficients of the polynomial from this.

For $N_{GB}(p)$ we find similarly that the result should be a quadratic polynomial depending at most on the residue of p modulo 3. $\square$

Proof of Theorem 11. Given an integer a coprime to p, we write a^* for the inverse of a modulo p satisfying $1 \le a^* \le p-1$. If $n = pqr$ satisfies $3 \le p < q < r$ with $q \equiv j^* (\mathrm{mod}\, p)$ and $r \equiv k^* (\mathrm{mod}\, p)$ and $(j,k) \in BB(p)$, then n satisfies the corrected Sister Beiter conjecture by Corollary 5. By Proposition 1, we have $N_{BB}(p) = 25p^2/27 + O(p)$. Now apply Theorem 3 with $\alpha = 25/27$ and $M(p) = \{(j^*, k^*) : (j,k) \in BB(p)\}$. □

7.5. **Applications in cryptography.** In [10] by Camburu et al., there is a ternary counting problem that is related to attempts of Hong et al. [18] to provide a simple and exact formula for the minimum Miller loop length in the Ate_i pairing arising in elliptic curve cryptography. The problem there is to estimate

$$\{pqr \le x : p < q < r,\ 4(p-1) > q,\ p^2 > r\}.$$

Also various other ternary counting problems are considered in Camburu et al. [10].

Acknowledgments

The first author was supported in part by NRF (South Africa) Grants CPRR160325161141 and an A-rated researcher award and by CGA (Czech Republic) Grant 17-02804S. Part of this work was done when this author visited the Max Planck Institute for Mathematics in Bonn from January to July, 2017.

The fourth author is supported by the Austrian Science Fund (FWF) : Project F5507-N26, which is part of the special Research Program "Quasi Monte Carlo Methods : Theory and Application". Part of this work was done while the author was supported by the Japan Society for the Promotion of Science (JSPS) "Overseas researcher under Postdoctoral Fellowship of JSPS".

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, *J. Number Theory* **100** (2003), 104–116.
[2] G. Bachman, Ternary cyclotomic polynomials with an optimally large set of coefficients, *Proc. Amer. Math. Soc.* **132** (2004), 1943–1950 (electronic).
[3] G. Bachman, Flat cyclotomic polynomials of order three, *Bull. London Math. Soc.* **38** (2006), 53–60.
[4] G. Bachman, On ternary inclusion-exclusion polynomials, *Integers* **10** (2010), 623–638.
[5] Sister M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.
[6] Sister M. Beiter, Coefficients of the cyclotomic polynomial $F_{3qr}(x)$, *Fibonacci Quart.* **16** (1978), 302–306.
[7] E. Bombieri, Le grand crible dans la théorie analytique des nombres, *Astérisque* **18** (1987), 103 pp.
[8] B. Bzdęga, Bounds on ternary cyclotomic coefficients, *Acta Arith.* **144** (2010), 5–16.
[9] B. Bzdęga, Jumps of ternary cyclotomic coefficients, *Acta Arith.* **163** (2014), 203–213.
[10] O.-M. Camburu, E.-A. Ciolan, F. Luca, P. Moree and I.E. Shparlinski, Cyclotomic coefficients: gaps and jumps, *J. Number Theory* **163** (2016), 211–237.
[11] S. Elder, Flat cyclotomic polynomials: a new approach, arXiv:1207.5811.
[12] K. Ford, Vinogradov's integral and bounds for the Riemann zeta function, *Proc. London Math. Soc.* (3) **85** No 3 (2002), 565–633.
[13] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), 235–248.
[14] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math.* **632** (2009), 105–125.
[15] Y. Gallot and P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, *Involve* **4** (2011), 317–341.
[16] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Sixth edition, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles, Oxford University Press, Oxford, 2008.

[17] A. Hildebrand, On the number of prime factors of an integer, *Ramanujan revisited* (Urbana-Champaign, Ill., 1987), 167–185, Academic Press, Boston, MA, 1988.
[18] H. Hong, E. Lee, H.-S. Lee and C.-M. Park, Maximum gap in (inverse) cyclotomic polynomial, *J. Number Theory* **132** (2012), 2297–2315.
[19] N. Kaplan, Flat cyclotomic polynomials of order three, *J. Number Theory* **127** (2007), 118–126.
[20] N. Kaplan, Flat cyclotomic polynomials of order four and higher, *Integers* **10** (2010), A30, 357–363.
[21] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996), 562–564.
[22] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Chelsea Publishing Co., New York, 1953.
[23] A. Migotti, Zur Theorie der Kreistheilungsgleichung, Z. B. der Math.-Naturwiss, Class der Kaiserlichen Akademie der Wissenschaften, Wien **87** (1883), 7–14.
[24] P. Moree, Inverse cyclotomic polynomials, *J. Number Theory* **129** (2009), 667–680.
[25] P. Moree and S. Saad Eddin, Products of two proportional primes, *Int. J. Number Theory* **13** (2017), 2583–2596.
[26] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics **46**. Cambridge University Press, Cambridge, 1995.
[27] R. Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic fields and related topics* (Pune, 1999), 311–322, Bhaskaracharya Pratishthana, Pune, 2000.
[28] T. Trudgian, Updating the error term in the prime number theorem, *Ramanujan J.* **39** (2016), 225–234.
[29] J. Zhao and X. Zhang, Coefficients of ternary cyclotomic polynomials, *J. Number Theory* **130** (2010), 2223–2237.

School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, South Africa;

Department of Mathematics, Faculty of Sciences, University of Ostrava, 30. dubna 22, 701 03 Ostrava 1, Czech Republic;

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.

e-mail: `florian.luca@wits.ac.za`

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.

e-mail: `moree@mpim-bonn.mpg.de`

School of Mathematics and Statistics, University College Dublin, Belfield, Dublin 4, Ireland.

e-mail: `robert.osburn@ucd.ie`

Institute of Financial Mathematics and Applied Number Theory, JKU Linz, Altenbergerstrae 69, 4040 Linz, Austria.

e-mail: `sumaia.saad_eddin@jku.at`

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.

e-mail: `alisa.sedunova@phystech.edu`