9

Waring's problem: the number $G(k)$

The number $G(k)$ was defined (by Hardy and Littlewood) to be the least value of s with the property that every sufficiently large integer N is representable as a sum of s positive integral kth powers. We already know, from Theorems 4.1 and 5.1, that $G(k) \leq 2^k + 1$. In the opposite direction, it is easily deduced from considerations of density that $G(k) \geq k + 1$; in fact the number of sets of integers $x_1, \ldots, x_k$ satisfying

$$x_1^k + \cdots + x_k^k \leq X, \quad 0 < x_1 \leq x_2 \leq \cdots \leq x_k$$

is easily seen to be asymptotic to γX as $X \to \infty$, where $\gamma < 1$ (by comparison with a multiple integral), and consequently there are many numbers not representable by k kth powers. A better lower bound is often deducible from congruence conditions; we have $G(k) \geq \Gamma(k)$, where $\Gamma(k)$ is the number defined in Chapter 4.

There are better upper bounds available for $G(k)$ when k is large. In 1934 Vinogradov proved that $G(k) < (6 + \delta)k \log k$ for $k > k_0(\delta)$, where δ is any small positive number [92]. We shall now give an exposition of the proof.[1] The numerical coefficient 6 was subsequently improved to 3 by Vinogradov in 1947 [93], but the proof is somewhat more difficult.

It will be recalled that in Chapter 4 we divided the range of integration for α into major arcs and minor arcs, the major arcs comprising those α that admit a rational approximation a/q with

$$q \leq P^\delta, \quad |\alpha - a/q| < P^{-k+\delta}.$$

Compared with what is usually needed in work on Waring's problem, these major arcs were exceptionally few in number and short in length. It was possible to make the choice because of the very effective estimate of Hua (Lemma 3.2), which 'saves' almost P^k in the estimation of

[1] We base this mainly on Heilbronn's account [44].

$\int |T(\alpha)|^{2^k}\ d\alpha$. In the present treatment we cannot include as much of the integral of α in the minor arcs. We therefore need a more effective method of approximation to $T(\alpha)$ on the major arcs than the very crude one used in the proof of Lemma 4.2. The question is essentially one of replacing a sum by an integral, and we shall use the following lemma of van der Corput, which is of independent interest.

Lemma 9.1. (van der Corput) *Suppose $f(x)$ is a real function which is twice differentiable for $A \le x \le B$. Suppose further that, in this interval,*

$$0 \le f'(x) \le \tfrac{1}{2}, \quad f''(x) \ge 0.$$

Then

$$\sum_{A \le n \le B} e(f(n)) = \int_A^B e(f(x))\ dx + O(1).$$

Proof. It will suffice to prove the result when A, B are integers with $A < B$, and when the end terms $n = A$, $n = B$ in the sum are counted with factors $\frac{1}{2}$. By replacing $f(x)$ with $f(x) + c$, which is equivalent to multiplying both the sum and the integral by $e^{2\pi i c}$, we can ensure that the difference between the sum and the integral is real, and this allows us to replace $e(f(x))$ by $\cos(2\pi f(x))$ on both sides.

Let $\Psi(x) = x - [x] - \frac{1}{2}$. Then, for any integer m and any differentiable $F(x)$, we hae

$$\int_m^{m+1} \Psi(x) F'(x)\ dx = \tfrac{1}{2}\{F(m+1) + F(m)\} - \int_m^{m+1} F(x)\ dx.$$

Summing this for $m = A, A+1, \ldots, B-1$, we obtain

$$\sum_{n=A}^{B}{}' F(n) = \int_A^B F(x)\ dx + \int_A^B \Psi(x) F'(x)\ dx,$$

where the accent means that the end terms are counted with factors $\frac{1}{2}$. Thus the question is reduced to proving that

$$I = \int_A^B \Psi(x)\left(\cos(2\pi f(x))\right)'\ dx$$

is bounded in absolute value.

We recall that, for any x which is not an integer,

$$\Psi(x) = -\sum_{\nu=1}^{\infty} \frac{\sin 2\pi\nu x}{\pi\nu}.$$

Hence

$$\begin{aligned} I &= -\sum_{\nu=1}^{\infty} \frac{1}{\nu\pi} \int_A^B (\sin 2\pi\nu x) \left(\cos(2\pi f(x))\right)' \, dx \\ &= 2\sum_{\nu=1}^{\infty} \frac{1}{\nu} \int_A^B (\sin 2\pi\nu x) \left(\sin(2\pi f(x))\right) f'(x) \, dx \\ &= \sum_{\nu=1}^{\infty} \frac{1}{\nu} \int_A^B f'(x) \left\{\cos\left(2\pi\left(\nu x - f(x)\right)\right) - \cos\left(2\pi\left(\nu x + f(x)\right)\right)\right\} \, dx. \end{aligned}$$

The interchange of summation and integration on the first line is easily justified by appealing to the bounded convergence of the series for $\Psi(x)$. We shall prove that

$$\left| \int_A^B f'(x) \cos\left(2\pi\left(\nu x \pm f(x)\right)\right) \, dx \right| < \frac{1}{\pi(2\nu - 1)}$$

and this will imply

$$|I| < \frac{1}{\pi} \sum_{\nu=1}^{\infty} \frac{1}{\nu(2\nu-1)} < \frac{2}{\pi},$$

giving the desired result.

We write the integral as

$$\frac{1}{2\pi} \int_A^B \frac{f'(x)}{\nu \pm f'(x)} \phi'(x) \, dx,$$

where

$$\phi(x) = \sin(2\pi(\nu x \pm f(x))),$$

and appeal to the mean value theorem. The second factor, $\phi'(x)$, has the property that its integral between any two limits has absolute value at most 2. The first factor is monotonic (for each positive integer ν), its derivative being

$$\frac{\nu f''(x)}{(\nu \pm f'(x))^2} \geq 0.$$

The maximum of the first factor is at most $1/(2\nu - 1)$. Hence

$$\left| \frac{1}{2\pi} \int_A^B \frac{f'(x)}{\nu \pm f'(x)} \phi'(x) \, dx \right| \leq \frac{1}{\pi(2\nu - 1)},$$

as asserted above. Thus the proof of Lemma 9.1 is complete. □

We define the major arcs $\mathfrak{M}_{a,q}$ for the purpose of the present chapter, to consist of the intervals

$$(a,q)=1, \quad 1 \le a \le q, \quad q \le P^{1/2}, \quad |q\alpha - a| < \frac{1}{2kP^{k-1}}. \tag{9.1}$$

As in Chapter 2, we define

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k).$$

The more precise result, which takes the place of Lemma 4.2, is as follows.

Lemma 9.2. *For α in $\mathfrak{M}_{a,q}$, we have*

$$T(\alpha) = q^{-1} S_{a,q} I(\beta) + O(q), \tag{9.2}$$

with the notation of Chapter 4.

Proof. Putting $x = qy + z$, as in the proof of Lemma 4.2, we obtain

$$T(\alpha) = \sum_{z=1}^{q} e(az^k/q) \sum_{y} e\left(\beta(qy+z)^k\right),$$

the summation for y being over $0 < qy + z \le P$. If

$$f(y) = \beta(qy+z)^k,$$

then (for $\beta > 0$),

$$f'(y) = k\beta q(qy+z)^{k-1} < k(2kP^{k-1})^{-1}P^{k-1} = \tfrac{1}{2},$$

by (9.1). Also $f''(y) \ge 0$. Hence Lemma 9.1 is applicable, and is equally applicable if $\beta < 0$ to the complex conjugate sum. Hence we can replace the inner sum over y by

$$\int e\left(\beta(q\eta+z)^k\right)\, d\eta + O(1),$$

and this leads to (9.2). □

Note. It will be seen that the condition $q \le P^{1/2}$ in (9.1) has not been used in the proof, though of course the result loses its value if q is allowed to be almost as large as P.

There is a still more effective method of approximating to $T(\alpha)$. If it is assumed that $q \le P^{1-\delta}$ and $|q\alpha - a| < P^{-k+1-\delta}$, then[1]

$$T(\alpha) = q^{-1} S_{a,q} I(\beta) + O\left(q^{\frac{3}{4}+\varepsilon}\right).$$

It is remarkable that the exponent in the error term here should be independent of k.

Lemma 9.3. *Suppose $s \ge 4k$. Then, for*

$$\tfrac{1}{5} P^k \le M \le P^k, \tag{9.3}$$

we have

$$\int_{\mathfrak{M}} T(\alpha)^s e(-M\alpha)\, d\alpha \gg P^{s-k}, \tag{9.4}$$

where $\mathfrak{M}$ denotes the totality of the major arcs $\mathfrak{M}_{a,q}$.

Note. The reason why we want the result for a range of values of M, instead of a single number, will appear later; it will spare us from having to approximate to a somewhat complicated exponential sum on the major arcs.

Proof. For α on a particular interval $\mathfrak{M}_{a,q}$, we have (9.2), and the first step is to raise the approximation to the power s. We have

$$q^{-1} |S_{a,q}| \ll q^{-1/k}$$

by Lemma 6.4; also

$$I(\beta) \ll \min(P, |\beta|^{-1/k}).$$

The first estimate, P, is trivial, and the second comes from writing $I(\beta)$ as

$$\frac{1}{k} |\beta|^{-1/k} \int_0^{P^k |\beta|} e(\pm\eta) \eta^{-1+1/k}\, d\eta$$

and observing that the last integral is bounded. Hence the main term in (9.2) has absolute value

$$\ll q^{-1/k} \min\left(P, |\beta|^{-1/k}\right).$$

The error term q does not exceed this, since

$$q^{1+1/k} < P \quad \text{and} \quad q^{1+1/k} < |\beta|^{-1/k}$$

[1] See [18, Lemmas 8 and 9].

by (9.1). Hence

$$\begin{aligned} T(\alpha)^s &= (q^{-1}S_{a,q}I(\beta))^s \\ &\quad + O\left\{q\, q^{-(s-1)/k}\left(\min\left(P, |\beta|^{-1/k}\right)\right)^{s-1}\right\}. \end{aligned}$$

The error term here, when integrated with respect to β (the range of β is immaterial — one can take $(-\infty, \infty)$) becomes

$$\ll q^{1-(s-1)/k} P^{s-1-k}.$$

When this is summed over a (at most q values) and over $q \leq P^{1/2}$, it gives a final error term

$$\ll P^{s-1-k} \sum_q q^{2-(s-1)/k} \ll P^{s-k-1},$$

since the series is convergent $(s-1 > 3k)$.

The contribution of the main term to the integral in (9.4) is

$$\sum_q \sum_a (q^{-1}S_{a,q})^s e(-Ma/q) \int I^s(\beta) e(-M\beta)\, d\beta,$$

where the conditions of summation and integration are determined by (9.1). We can extend the integration over β to $(-\infty, \infty)$, since by the estimate for $|I(\beta)|$ the resulting error is

$$\begin{aligned} &\ll \sum_q q q^{-s/k} \int_{(2kq)^{-1}P^{1-k}}^{\infty} \beta^{-s/k}\, d\beta \\ &\ll \sum_q q^{1-s/k} q^{s/k-1} P^{(k-1)(s/k-1)} \\ &\ll P^{s-k-s/k+3/2} \ll P^{s-k-1}. \end{aligned}$$

By a simple change of variable,

$$I(\beta) = Pk^{-1} \int_0^1 e(\beta P^k \eta) \eta^{-1+1/k}\, d\eta = Pk^{-1} I_1(\beta P^k),$$

say. Putting $\beta = P^{-k}\gamma$, we obtain

$$\int_{-\infty}^{\infty} I^s(\beta) e(-M\beta)\, d\beta = P^{s-k} k^{-s} \int_{-\infty}^{\infty} I_1^s(\gamma) e(-\theta\gamma)\, d\gamma,$$

where $\theta = M/P^k$, so that $\frac{1}{5} \leq \theta \leq 1$. As in the proof of Theorem 4.1, it follows from Fourier's integral theorem that the integral

$$\int_{-\infty}^{\infty} I_1^s(\gamma) e(-\theta\gamma)\, d\gamma$$

is equal to

$$\int_0^1 \cdots \int_0^1 \{\zeta_1 \cdots \zeta_{s-1}(\theta - \zeta_1 - \cdots - \zeta_{s-1})\}^{-1+1/k} \; d\zeta_1 \cdots \; d\zeta_{s-1},$$

where the integral is taken over $\zeta_1, \dots, \zeta_{s-1}$ for which $\zeta_1 + \cdots + \zeta_{s-1} < \theta$. Hence

$$\int_{-\infty}^{\infty} I_1^s(\gamma) e(-\theta\gamma) \; d\gamma = \theta^{s/k-1} \frac{\Gamma(1/k)^s}{\Gamma(s/k)},$$

and since $\theta \geq 1/5$, we obtain, on substitution,

$$\int_{-\infty}^{\infty} I^s(\beta) e(-M\beta) \gg P^{s-k}.$$

It suffices now to obtain a positive lower bound for

$$\sum_{q \leq P^{1/2}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} (q^{-1} S_{a,q})^s e(-Ma/q).$$

This series can be continued to infinity with an error which is bounded by a negative power of P; this follows from Lemma 6.4 since $s \geq 4k > 2k+1$. It then becomes $\mathfrak{S}(M)$, and this has a positive lower bound independent of M by Theorem 6.1. Thus Lemma 9.3 is proved. □

We now come to the main idea of the proof. This is: to consider the representations of a large number N in the form

$$N = x_1^k + \cdots + x_{4k}^k + u_1 + u_2 + y^k v, \tag{9.5}$$

where

(i) $1 \leq x_j \leq P$;
(ii) u_1 and u_2 run through all the different numbers less than $\frac{1}{4}P^k$ that are representable as sums of ℓ positive integral kth powers;
(iii) $1 \leq y \leq P^{1/2k}$;
(iv) v runs through the different numbers less than $\frac{1}{4}P^{k-1/2}$ that are representable as sums of ℓ positive integral kth powers.

Thus we shall be representing N as a sum of $4k + 3\ell$ positive integral kth powers. In order to prove that a representation exists, we shall have to choose ℓ in terms of k later. We shall choose

$$P = [N^{1/k}] + 1;$$

this will ensure that

$$\tfrac{1}{5}P^k < N - u_1 - u_2 - y^k v < P^k. \tag{9.6}$$

It is vital to have a lower bound for the number of u_1, u_2, v, and such a lower bound is provided by the following lemma.

Lemma 9.4. (Hardy and Littlewood) *Let $U_\ell(X)$ denote the number of different numbers up to X that are representable as sums of ℓ positive integral kth powers. Then, provided $X > X_0(k,\ell)$, we have*

$$U_\ell(X) \gg X^{1-\lambda^\ell}, \quad \lambda = 1 - \tfrac{1}{k}. \tag{9.7}$$

Proof. The result holds when $\ell = 1$, since then the number is $[X^{1/k}]$, and the number on the right of (9.7) is $X^{1/k}$. The general result is proved by induction on ℓ. Consider numbers of the form $x^k + z$, where

$$\left(\tfrac{1}{4}X\right)^{1/k} < x < \left(\tfrac{1}{2}X\right)^{1/k}$$

and

$$0 < z < \tfrac{1}{2}X^{1-1/k},$$

and z is expressible as a sum of $\ell - 1$ positive integral kth powers. These numbers are all distinct, for if

$$x_1^k + z_1 = x_2^k + z_2, \quad x_1 > x_2,$$

we get

$$x_1^k - x_2^k > kx_2^{k-1} > k(\tfrac{1}{4}X)^{1-1/k} > \tfrac{1}{2}X^{1-1/k},$$

whereas

$$z_2 - z_1 < z_2 < \tfrac{1}{2}X^{1-1/k},$$

a contradiction. The number of possibilities for x is $\gg X^{1/k}$, and the number for z is $U_{\ell-1}\left(\tfrac{1}{2}X^{1-1/k}\right)$, so we have

$$U_\ell(X) \gg X^{1/k} U_{\ell-1}\left(\tfrac{1}{2}X^{1-1/k}\right).$$

If the analogue of (9.7) with $\ell - 1$ in place of ℓ holds, we get

$$U_\ell(X) \gg X^{1/k} X^{(1-1/k)(1-\lambda^{\ell-1})} = X^{1-\lambda^\ell},$$

so (9.7) itself holds. This proves the result. □

Note. Nothing substantially better than (9.7) is known for general k, and any real improvement would be of interest. Better results are known for small k (see the paper of Davenport [19]).

Corollary. *Let*

$$R(\alpha) = \sum_{u<\frac{1}{4}P^k} e(\alpha u) \tag{9.8}$$

where u runs through different numbers that are sums of ℓ kth powers. Then

$$\int_0^1 |R(\alpha)|^2 \, d\alpha = R(0) \ll P^{-k(1-\lambda^\ell)} R^2(0). \tag{9.9}$$

Proof. The first result is immediate, being valid for any exponential sum $\sum e(\alpha u)$ in which u runs through a set of different integers. The second result follows from the fact that

$$R(0) = U_\ell\left(\tfrac{1}{4}P^k\right) \gg P^{k(1-\lambda^\ell)}.$$

$\square$

Note. It is convenient to use $R(0)$ as a means of indicating the number of terms in the exponential sum $R(\alpha)$, in order to avoid introducing new symbols. The trivial estimate for the integral in (9.9) would be $R^2(0)$, and it will be seen that in comparison with this we have saved an amount $k(1-\lambda^\ell)$ in the exponent of P. We shall ultimately choose ℓ so that λ^ℓ (that is, $(1-1/k)^\ell$) is about $1/Ck^2$, so that the saving will be about $k - 1/Ck$. It will be necessary to save a further amount, more than $1/Ck$, when α is in the minor arcs $\mathfrak{m}$, and this will be attained by an estimate for the exponential sum corresponding to the last term $y^k v$ in (9.5). The estimate depends on the following very general lemma, the principle of which plays a large part in most of Vinogradov's work.

Lemma 9.5. (Vinogradov) *Let x run through a set of X_0 distinct integers contained in an interval of length X, and let y run through a set of Y_0 distinct integers contained in an interval of length Y. Suppose $\alpha = a/q + O(q^{-2})$, where $(a,q) = 1$, $q > 1$. Then*

$$\left| \sum_x \sum_y e(\alpha x y) \right|^2 \ll X_0 Y_0 \frac{\log q}{q} (q+X)(q+Y). \tag{9.10}$$

Proof. Denoting the sum by S, we have

$$|S|^2 \le \left(\sum_x 1 \right) \left(\sum_x \left| \sum_y e(\alpha x y) \right|^2 \right)$$

$$\leq X_0 \sum_{x=x_1}^{x_1+X} \sum_y \sum_{y'} e(\alpha x(y-y')),$$

where now x runs through *all* integers of the interval containing the original set, whereas y, y' are still restricted. Carrying out the summation over x, we obtain

$$|S|^2 \ll X_0 \sum_y \sum_{y'} \min(X, \|\alpha(y-y')\|^{-1}).$$

Now $|y-y'| \leq Y$, and each value of $y-y'$ arises from at most Y_0 pairs y, y'. Hence

$$|S|^2 \ll X_0 Y_0 \sum_{\substack{t \\ |t| \leq Y}} \min(X, \|\alpha t\|^{-1}).$$

The rest of the argument is essentially the same as that in the proof of Lemma 3.1. The sum over t is divided into blocks of q consecutive terms, the number of blocks being $\ll Y/q+1$. The sum of the terms in any one block is of the form

$$\sum_{t=t_1+1}^{t_1+q} \min\left(X, \left\| \frac{at}{q} + \tau + O\left(\frac{1}{q}\right)\right\|^{-1}\right)$$
$$\ll X + \sum_{1 \leq u \leq \frac{1}{2}q} \frac{q}{u} \ll X + q\log q.$$

Hence

$$|S|^2 \ll X_0 Y_0 \left(Y/q+1\right)\left(X + q\log q\right),$$

and this implies (9.10). □

Corollary. *Let*

$$S(\alpha) = \sum_y \sum_v e(\alpha y^k v), \tag{9.11}$$

where the conditions of summation are those in (iii) and (iv) earlier. Then, if $\alpha = a/q + O(q^{-2})$, and

$$P^{1/2} < q \leq 2kP^{k-1},$$

we have

$$|S(\alpha)| \ll S(0) P^{-\frac{1}{4k} + \frac{1}{2}(k-\frac{1}{2})\lambda^{\ell}}. \tag{9.12}$$

Proof. The sum is an instance of that of the lemma, with

$$X = \tfrac{1}{4}P^{k-\frac{1}{2}}, \quad X_0 = U_\ell\left(\tfrac{1}{4}P^{k-\frac{1}{2}}\right),$$
$$Y = P^{1/2}, \qquad Y_0 = P^{\frac{1}{2k}}.$$

Hence

$$\begin{aligned} |S(\alpha)|^2 &\ll X_0 P^{\frac{1}{2k}} \frac{\log q}{q}\left(q + \tfrac{1}{4}P^{k-\frac{1}{2}}\right)\left(q + P^{1/2}\right) \\ &\ll X_0 P^{\frac{1}{2k}} (\log P) P^{k-\frac{1}{2}}. \end{aligned}$$

Since

$$S(0) \gg P^{\frac{1}{2k}} X_0,$$

we obtain

$$\left|\frac{S(\alpha)}{S(0)}\right|^2 \ll P^{-\frac{1}{2k}+(k-\frac{1}{2})+\varepsilon} X_0^{-1},$$

and since

$$X_0 \gg P^{(k-\frac{1}{2})(1-\lambda^\ell)}$$

by Lemma 9.4, we obtain (9.12). □

Note. It will be seen that (9.12) represents a saving over the trivial estimate of almost $1/4k$ in the exponent of P, provided λ^ℓ is small.

Lemma 9.6. *Let $\mathfrak{m}$ denote the minor arcs, that is, the complement of the intervals $\mathfrak{M}_{a,q}$ in (9.1). Then provided $\ell \geq 2k \log 3k$, we have*

$$\int_{\mathfrak{m}} |T(\alpha)|^{4k} |R(\alpha)|^2 |S(\alpha)|\, d\alpha \ll P^{3k} R^2(0) S(0) P^{-\delta}$$

for some fixed $\delta > 0$.

Proof. For every α there exist a, q such that

$$(a,q) = 1, \quad 1 \leq q \leq 2kP^{k-1}, \quad \left|\alpha - \frac{a}{q}\right| < \frac{1}{2kqP^{k-1}},$$

and if α is not in any $\mathfrak{M}_{a,q}$, we must have $q > P^{1/2}$. Note that $|\alpha - a/q| < 1/(2kqP^{k-1})$. By the Corollary to Lemma 9.5,

$$|S(\alpha)| \ll S(0) P^{-\frac{1}{4k}+\frac{1}{2}(k-\frac{1}{2})\lambda^\ell}.$$

By the Corollary to Lemma 9.4,

$$\int_0^1 |R(\alpha)|^2\, d\alpha \ll R^2(0)P^{-k+k\lambda^\ell}.$$

Using the trivial estimate $|T(\alpha)| \le P$, we see that the integral in the enunciation is

$$\ll P^{3k}R^2(0)S(0)P^{-\frac{1}{4k}+\frac{3}{2}k\lambda^\ell}.$$

If $\ell \ge 2k\log 3k$, then

$$\log\lambda^\ell = \ell\log\left(1-\frac{1}{k}\right) < -\frac{\ell}{k} < -2\log 3k,$$

whence $\lambda^\ell < (3k)^{-2}$ and

$$\frac{3}{2}k\lambda^\ell < \frac{1}{6k}.$$

Hence the result. □

Theorem 9.1. *$G(k) < 4k + 6k\log 3k + 3$.*

Proof. Let $r_1(N)$ denote the number of representation of N in the special form (9.5), subject to the conditions given there. Then

$$r_1(N) = \int_0^1 T^{4k}(\alpha)R^2(\alpha)S(\alpha)e(-N\alpha)\, d\alpha.$$

By Lemma 3.1, the contribution of the minor arcs $\mathfrak{m}$ to the integral is of lower order than $P^{3k}R^2(0)S(0)$, provided $\ell \ge 2k\log 3k$.

We write the contribution of the major arcs as

$$\sum_{u_1}\sum_{u_2}\sum_{y}\sum_{v}\int_{\mathfrak{M}} T^{4k}(\alpha)e\left(\alpha(-N+u_1+u_2+y^kv)\right)\, d\alpha.$$

The number of terms in the outside sum is $R^2(0)S(0)$, and for any choice of these we have

$$\tfrac{1}{5}P^k < N - u_1 - u_2 - y^kv < P^k,$$

as noted earlier. Thus, by Lemma 9.3, the integral over $\mathfrak{M}$ is $\gg P^{3k}$, since now $s = 4k$. Hence $r_1(N) \gg P^{3k}R^2(0)S(0)$, so that $r_1(N) \to \infty$ as $N \to \infty$. It follows that

$$G(k) \le 4k + 3\ell \le 4k + 3(2k\log 3k + 1),$$

giving the result. □