ON LINKED BINARY REPRESENTATIONS OF PAIRS OF INTEGERS: SOME THEOREMS OF THE ROMANOV TYPE

BY G. J. RIEGER

Communicated by P. T. Bateman, March 7, 1963

1. Introduction. Let us denote by \( N \) the sequence \{1, 2, 3, \ldots \}, by \( p \) a prime, by \((a, b)\) the greatest common divisor of \( a \) and \( b \), by \([a, b]\) the least common multiple of \( a \) and \( b \), by \( \{*: \ldots \} \) resp. \( \mathcal{A}\{*: \ldots \} \) the set resp. number of * with the properties \( \ldots \), by \( \mu \) the Moebius function, by \( C \) an absolute positive constant and by \( C(*) \) a positive constant depending on * only.

Suppose \( N\subset N \) (\( j=1, 2, 3, 4 \)) and denote by \( y_1\sim y_2 \) an arbitrary relation (\( = \) linking) with \( y_{1,2}\in N \). For instance, \([y_1\sim y_2]= [y_1, y_2]= 1\) resp. \([y_1\sim y_2]= [y_1= y_2]\) can be considered a weak resp. strong linking. By a linked binary representation of a pair \( m, n \) with \( m\in N \) and \( n\in N \) we mean a solution \( #1, #2, #3, #4 \) of the Diophantine system \( x_1+x_2=m\wedge x_3+x_4=n \wedge x_j\in N_j \) (\( j=1, 2, 3, 4 \)) \( \forall x_j\sim x_4 \). Various generalizations are obvious (more summands, triples, etc.). We do not intend to give a detailed and general study of the questions arising in this context. We rather prefer to investigate two special problems of this type with \( \sim \) being \( = \); they are inspired by the following two well-known results of Romanov:

\[
E_a: = \{m: m = p + v^a \wedge p\text{ prime } \wedge v \in N\} \quad (1 < a \in N)
\]

and

\[
F_a: = \{m: m = p + a^v \wedge p\text{ prime } \wedge v \in N\} \quad (a \in N)
\]

have positive asymptotic density [1, pp. 63–70].

2. On Romanov's first theorem. Generalizing the result for \( E_a \), we show that the set \( \{m, n: m=p_1+v^a \wedge n=p_2+v^a \wedge p_{1,2}\text{ prime } \wedge v \in N\} \), considered as a set of lattice points in the plane, has positive asymptotic density in the plane:

**Theorem 1.** For \( 1 < a \in N \) there exist constants \( C_1(a) \) and \( C_2(a) \) such that \( x > C_1(a) \) implies

\[
A_1(x, a): = A \{m, n: m < x \wedge n < x \wedge m = p_1 + v^a \wedge n = p_2 + v^a \wedge p_{1,2}\text{ prime } \wedge v \in N\} > C_2(a) x^2.
\]

\[\text{1 With support from NSF grant G-16305 to Purdue University.}\]
Proof. Let \( f_1(m, n; a) := A \{ p_1, p_2, v; p_1 + v^a = m \land p_2 + v^a = n \} \); since \( A_1(x, a) = A \{ m, n; m < x \land n < x \land f_1(m, n; a) > 0 \} \), the Schwarz inequality yields

\[
(1) \quad \left( \sum_{m < a} \sum_{n < a} f_1(m, n; a) \right)^2 \leq A_1(x, a) \sum_{m < a} \sum_{n < a} f_1^2(m, n; a).
\]

On the one hand, we find

\[
\sum_{m < a} \sum_{n < a} f_1(m, n; a) = A \{ p_1, p_2, v; p_1 + v^a < x \land p_2 + v^a < x \}
\]

\[
\geq A \left\{ p_1; p_1 < \frac{x}{2} \right\} A \left\{ p_2; p_2 < \frac{x}{2} \right\} A \left\{ v; v^a < \frac{x}{2} \right\}
\]

\[
> C_4 \left( \frac{x}{\log x} \right)^2 \left( \frac{x}{2} \right)^{1/a} \quad (x > C_8(a)).
\]

On the other hand, we find

\[
S_1(x, a) := \sum_{m < a} \sum_{n < a} f_1^2(m, n; a)
\]

\[
= A \{ p_1, p_2, p_3, p_4, v_1, v_2; p_1 + v_1 = p_2 + v_2 < x \land p_3 + v_1 = p_4 + v_2 < x \}
\]

\[
\leq \sum_{v_1 < x^{1/a}} \sum_{v_2 < x^{1/a}} A \{ p_1, p_2, p_3, p_4; p_1 - p_2 = p_3 - p_4 \}
\]

\[
= v_2 - v_1 \land p_1,2,3,4 < x \}.
\]

In case of \( v_1 = v_2 \) resp. \( v_1 \neq v_2 \) we use

\[
A \{ p; p < x \} < C_6 \frac{x}{\log x} \quad (x > 2)
\]

resp. Brun's sieve method \([2, 2, \text{Satz 4.2}]\) and obtain

\[
S_1(x, a) < C_7 \left( \frac{x}{\log x} \right)^2 x^{1/a} + 2 \sum_{x_1 < x^{1/a}} \sum_{x_2 < x^{1/a}} \left( C_8 \frac{x}{\log^2 x} g(v_1 - v_2) \right)^2
\]

\[
(x > C_6)
\]

where

\[
g(b) := \prod_{p | b} \left( 1 + \frac{1}{p} \right) = \sum_{d | b; \nu(d) = 0} \frac{1}{d}.
\]

It follows

\[
S_1(x, a) < C_7 \left( \frac{x}{\log x} \right)^2 x^{1/a} + C_9 \frac{x^2}{\log^4 x} \sum_{u < x} F(u; x, a) g^2(u) \quad (x > C_6)
\]
where
\[ F(u; x, a) = A \{ v_1, v_2 : v_2 < v_1 < x^{1/a} ∧ v_1 - v_2 = u \}. \]

Writing \( g(u) \) as a sum and changing the order of summation gives
\[
\sum_{u < x} F(u; x, a) g^2(u) = \sum_{d_1 < x} \sum_{d_2 < x} \sum_{\mu(d_1) \neq 0} \sum_{\mu(d_2) \neq 0} \frac{1}{d_1 d_2} B([d_1, d_2]; x, a)
\]

where
\[ B(k; x, a) = \sum_{u < x; u \equiv 0 \mod k} F(u; x, a) < 2x^{2/a} k^{-1/a} a^w(k) \quad (\mu(k) \neq 0) \]

[1, p. 66] with
\[ w(k) = A \{ p : p | k \} < C_{10} \frac{\log k}{\log \log k}. \]

Since \( \mu(d_1) \neq 0 \land \mu(d_2) \neq 0 \) imply \( \mu([d_1, d_2]) \neq 0 \), we obtain
\[
S_1(x, a) < C_7 \frac{x^{2+1/a}}{\log^2 x} + \frac{x^{2+2/a}}{\log^4 x} C_{11}(a) \sum_{d_1 < x} \sum_{d_2 < x} (d_1 d_2)^{-1} [d_1, d_2]^{-1/2a} (x > C_6).
\]

Using \( [d_1, d_2]^2 \geq d_1 d_2 \), we find
\[ S_1(x, a) < C_{12}(a) \frac{x^{2+2/a}}{\log^4 x} \quad (x > C_6). \]

(1), (2), and (3) give the desired result.

It is not difficult to determine a dependence of \( C_{12}(a) \) on \( a \) explicitly. Since \( A_1(x, a) \leq A \{ m, n : m < x ∧ n < x \} \), Theorem 1 is best possible with respect to the order of magnitude in \( x \). Theorem 1 is also correct for \( a = 1 \) but of no interest.

3. On Romanov's second theorem. In a similar way we generalize the result for \( F_a \).

**Theorem 2.** For \( 1 < a \leq N \) there exist constants \( C_{13}(a) \) and \( C_{14}(a) \) such that \( x > C_{13}(a) \) implies
\[ A_2(x, a) = A \{ m, n : m < x ∧ n < x ∧ m = p_1 + a^n ∧ n = p_2 + a^n \land p_{1,2} \text{ prime} \land v \in N \} > C_{14}(a) \frac{x^2}{\log x}. \]

**Proof.** Let \( f_2(m, n; a) = A \{ p_1, p_2, v : p_1 + a^n = m \land p_2 + a^n = n \} \). As
in the preceding proof, we find

\[ \sum_{m<n} \sum_{n<s} f_2(m, n; a) > C_{16} \left( \frac{x}{\log x} \right)^2 \frac{\log x/2}{\log a} \quad (x > C_{16}(a)) \]

and

\[ S_2(x, a) := \sum_{m<n} \sum_{n<s} f_3(m, n; a) \]

\[ < C_{18} \left( \frac{x}{\log x} \right)^2 \frac{\log x}{\log a} + 2 \sum_{s_1 < s_2 < \log x/\log a} \left( C_8 \frac{x}{\log^2 x} g(a^{s_1} - a^{s_2}) \right)^2 \]

\[ (x > C_{17}). \]

For \( v_1 > v_2 \) we have

\[ g(a^{v_1} - a^{v_2}) = g(a)g(a^{v_1-v_2} - 1); \]

with \( h := v_1 - v_2 \) we get

\[ S_2(x, a) < C_{19}(a) \frac{x^2}{\log x} + 2 \left( C_8 \frac{x}{\log^2 x} \right)^2 \frac{\log x}{\log a} \sum_{h<\log x/\log a} g^2(a^h - 1) \quad (x > C_{17}). \]

For \((a, d) = 1\), let \( e(a, d) \) denote the exponent of \( a \mod d \) (i.e., the certainly existing smallest \( t \in \mathbb{N} \) with \( a^t \equiv 1 \mod d \)); then \( d \mid (a^h - 1) \) implies \((a, d) = 1 \land e(a, d) \mid h\). Therefore,

\[ \sum_{h<\log x/\log a} g^2(a^h - 1) = \sum_{h<\log x/\log a} \sum_{\mu(d_1) \neq 0} \frac{1}{d_1} \sum_{\mu(d_2) \neq 0} \frac{1}{d_2} \sum_{h<\log x/\log a} \frac{1}{d_1 d_2 \left[ e(a, d_1), e(a, d_2) \right]} \]

\[ \leq \frac{\log x}{\log a} \sum_{\mu(d_1) \neq 0} \sum_{\mu(d_2) \neq 0} \frac{1}{d_1 d_2} \sum_{\mu(d_2) \neq 0} \frac{1}{d_1 d_2 \left[ e(a, d_1), e(a, d_2) \right]} \]

\[ \leq \frac{\log x}{\log a} \left( \sum_{d<z} d^{-1} \frac{1}{d \log d} \right)^2 \leq C_{20}(a) \log x, \]

since \([a, b] \leq ab\) and since, for an arbitrary positive increasing function \( f \),
implies

\[ \sum_{d=1}^{\infty} \frac{1}{df(d)} < \infty \]

\[ \sum_{(d,a)=1; \mu(d) \neq 0} \frac{1}{d f(e(a, d))} < C_{21}(a, f) \]

[3, Satz 3]. Hence, we have

\[ S_2(x, a) < C_{22}(a) \frac{x^2}{\log x} \quad (x > C_{17}). \]

(4), (5), and (1) with index 2 instead of 1 give the desired result.

It is not difficult to give an explicit dependence of \( C_{1b}(a) \) and \( C_{14}(a) \) on \( a \). Again, since

\[ A_1(x, a) \leq A\{ p_1, p_2, \nu: p_{1,2} < x \land a^* < x \} \]

\[ < \left( C_6 \frac{x}{\log x} \right)^2 \frac{\log x}{\log a} \quad (x > 2), \]

Theorem 2 is best possible in \( x \).

4. Generalization to algebraic number fields \( K \). For convenience, let \( K \) be a totally real algebraic number field. Denote by \( n \) the degree of \( K \), by \( J(K) \) the ring of all integers of \( K \), by small Greek letters elements of \( J(K) \), by \( \xi^{(1)}, \ldots, \xi^{(n)} \) the conjugates of \( \xi \), and by \( \xi < x \) the system \( |\xi^{(j)}| < x \) \( (j = 1, \ldots, n) \). \( \pi \) is called a prime if \( \pi \) generates a prime ideal of \( J(K) \). Combining the method used above with ideas of [4], we arrive at direct generalizations of Theorem 1 and Theorem 2:

**Theorem 1'.** For \( 1 < a \in \mathbb{N} \) there exist constants \( C_{28}(K, a) \) and \( C_{24}(K, a) \) such that \( x > C_{28}(K, a) \) implies

\[ A\{ \sigma, \tau: \sigma = \pi_1 + \nu^a \land \tau = \pi_2 + \nu^a \land \pi_{1,2} \text{ prime} \land \pi_{1,2} < x \land \nu < x^{1/\alpha} \} \]

\[ > C_{24}(K, a) x^{2n}. \]

**Theorem 2'.** For \( 0 \neq \alpha \in J(K) \) and not a root of unity there exist constants \( C_{28}(K, \alpha) \) and \( C_{26}(K, \alpha) \) such that \( x > C_{26}(K, \alpha) \) implies

\[ A\{ \sigma, \tau: \sigma = \pi_1 + \alpha^a \land \tau = \pi_2 + \alpha^a \land \pi_{1,2} \text{ prime} \land \pi_{1,2} \]

\[ < x \land \nu \in \mathbb{N} \land \alpha^a < x \}

\[ > C_{26}(K, \alpha) \frac{x^{2n}}{\log x}. \]

Again, the estimates are best possible in \( x \).
THE COHOMOLOGY OF CERTAIN ORBIT SPACES

By P. A. Smith

Communicated by Deane Montgomery, March 11, 1963

Let \((G, X)\) be a topological transformation group—or action—in which \(G\) is finite and \(X\) is locally compact. An important part of the cohomology of the orbit space \(X/G\) lies, so to speak, in the free part \(f\) of the action (i.e. the union of orbits of cardinality \([G:1]\)). The cohomology of \(f/G\) can be regarded as an \(H(G)\)-module. We shall exhibit a complete set of generators and relations for this module assuming \(G\) to be the direct product of cyclic groups of prime order \(p\) and \(X\) to be a generalized sphere over \(Z_p\) (see [4, p. 404]). \(H\) will always denote cohomology with values in \(Z_p\). A useful device consists in relating the generators of \(H(G)\) to those of \(G\).

Dimension functions. From now on let \(G=Z_p \times \cdots \times Z_p\), \(r\) factors, and let \(g_i\) be the collection of subgroups of order \(p^i\); \(g_0\) consists of the identity only. Let \(g, h, \cdots\) always denote subgroups of \(G\) and \(g_i, h_i, \cdots\) elements of \(g_i\). In particular \(g_0=\{1\}\) and \(g_r=G\).

By a dimension function of the pair \((G, p)\) we shall mean an integer-valued function \(n(g)\) of constant parity with values \(\geq -1\) and such that for each \(g\) different from \(G\)

\[
n(g) = n(G) + \sum_h (n(h) - n(G))
\]

summed over those \(h\)'s which lie in \(g_{r-1}\) and contain \(g\); when \(p=2\), constant parity is not required.

For a given dimension function \(n(g)\) let \(\Omega\) be the totality of se-

---

1 This work has been supported by the Office of Naval Research.