

MORDELL'S EXPONENTIAL SUM ESTIMATE REVISITED

J. BOURGAIN

1. SUMMARY

The main result of this paper is

Theorem 1. *Let p be prime. Given $r \in \mathbb{Z}_+$ and $\varepsilon > 0$, there is $\delta = \delta(r, \varepsilon) > 0$ satisfying the following property: If*

$$f(x) = \sum_{i=1}^r a_i x^{k_i} \in \mathbb{Z}[x] \text{ and } (a_i, p) = 1$$

where the exponents $1 \leq k_i < p-1$ satisfy

$$(1.1) \quad (k_i, p-1) < p^{1-\varepsilon} \text{ for all } 1 \leq i \leq r,$$

$$(1.2) \quad (k_i - k_j, p-1) < p^{1-\varepsilon} \text{ for all } 1 \leq i \neq j \leq r,$$

then there is an exponential sum estimate

$$(1.3) \quad \left| \sum_{x=1}^{p-1} e_p(f(x)) \right| < p^{1-\delta}$$

(denoting $e_p(y) = e^{2\pi iy/p}$).

Remarks. (1) The result for $r = 1$ (Gauss sums) was obtained in [B-K]. Thus

$$(1.4) \quad \left| \sum_{x=1}^{p-1} e_p(ax^k) \right| < p^{1-\delta} \text{ if } a \in \mathbb{F}_p^* \text{ and } (k, p-1) < p^{1-\varepsilon}.$$

More precisely, it was shown in [B-K] that if $G \triangleleft \mathbb{F}_p^*$ and $|G| > p^\varepsilon$, then

$$(1.5) \quad \left| \sum_{x \in G} e_p(ax) \right| < |G|^{1-\delta} \text{ for } a \in \mathbb{F}_p^*.$$

See also [B] for further extensions to exponential sums of the form

$$(1.6) \quad \sum_{s=1}^{t_1} e_p(a\theta^s)$$

and

$$(1.7) \quad \sum_{s, s'=1}^{t_1} e_p(a\theta^s + b\theta^{ss'})$$

where $a, \theta \in \mathbb{F}_p^*$ and θ is of multiplicative order t , $t \geq t_1 > p^\delta$.

Received by the editors July 16, 2004.

2000 *Mathematics Subject Classification.* Primary 11L07; Secondary 11T23.

The methods involved here are closely related to those used in [B-K] and [B] (while the results in [K-S] and [C-P2] depend on Stepanov’s method).

(2) Theorem 1 improves upon the results from [C-P1] and [C-P2] when the exponents $\{k_i\}$ are large. Notice that the recent paper [C-P1] already contains a substantial improvement over Mordell’s original paper [Mor].

(3) The role of condition (1.2) above is made clear by the following example from [C-P1] (see Example 1.1 in [C-P1]). Let r be even and let

$$(1.8) \quad f(x) = \sum_{i=1}^{r/2} (x^{\frac{r-1}{2}+i} - x^i).$$

Then

$$(1.9) \quad \left| \sum_{x=1}^{p-1} e_p(f(x)) - \frac{p-1}{2} \right| \leq r\sqrt{p}.$$

(4) As mentioned above, our argument follows the same pattern as in [B-K] and [B]. The key combinatorial ingredient in [B-K] is a ‘sum-product’ theorem for subsets A of the field \mathbb{F}_p (see also [B-K-T]).

Proposition 1. *Given $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{F}_p$ and*

$$(1.10) \quad 1 < |A| < p^{1-\varepsilon},$$

then

$$(1.11) \quad |A + A| + |A.A| > C|A|^{1+\delta}.$$

We denote here $A + A = \{x + y | x, y \in A\}$ and $A.A = \{x.y | x, y \in A\}$ for the sum and product sets (and will use the same notation if, more generally, A is a subset of a commutative ring \mathcal{R}).

Given $G \subset \mathbb{F}_p^*$, consider the probability measure ν on \mathbb{F}_p defined by

$$(1.12) \quad \nu = \frac{1}{|G|} \sum_{x \in G} \delta_x.$$

As shown in [B-K], one may then derive from Proposition 1 uniform bounds on the convolution powers

$$\nu^{(k)} = \underbrace{\nu * \dots * \nu}_{k\text{-fold}}$$

denoting

$$(\nu * \mu)(x) = \sum_{y \in \mathbb{F}_p} \nu(x - y)\mu(y)$$

and those bounds translate in exponential sum estimates such as (1.5).

It turns out that in order to establish Theorem 1 for general r , it suffices to treat the monomial ($r = 1$) and the binomial case ($r = 2$). Thus we are left with the problem for $r = 2$. Following the scheme used for $r = 1$, we need to establish a sum-product theorem for subsets A of the product $\mathbb{F}_p \times \mathbb{F}_p$. Clearly if A is a subset of the form

$$A = \{a\} \times \mathbb{F}_p, A = \mathbb{F}_p \times \{a\} \text{ or } A = \{(x, ax) | x \in \mathbb{F}_p\},$$

one has $|A| = |A + A| = |A.A| = p$. It turns out that these are essentially the only ‘exceptions’ to be taken into account when reformulating Proposition 1 for $\mathbb{F}_p \times \mathbb{F}_p$.

Proposition 2. *Let $A \subset \mathbb{F}_p \times \mathbb{F}_p$ satisfying for some $\varepsilon_0 > 0$*

$$(1.13) \quad |A| > p^{\varepsilon_0}.$$

Assume that

$$(1.14) \quad |A + A| + |A \cdot A| < p^\varepsilon |A|.$$

Then one of the following cases occurs:

$$(1.15) \quad |A| > p^{2-\varepsilon'}.$$

(1.16) There is $a \in \mathbb{F}_p$ such that either

$$|A \cap (\{a\} \times \mathbb{F}_p)| > p^{-\varepsilon'} |A|$$

or

$$|A \cap (\mathbb{F}_p \times \{a\})| > p^{-\varepsilon'} |A|.$$

(1.17) There is $a \in \mathbb{F}_p^*$ such that

$$|A \cap \{(x, ax) | x \in \mathbb{F}_p\}| > p^{-\varepsilon'} |A|$$

where $\varepsilon' = \varepsilon'(\varepsilon) \rightarrow 0$ for $\varepsilon \rightarrow 0$ with ε_0 in (1.13) fixed.

Moreover, in cases (1.16), (1.17)

$$(1.18) \quad p^{1-\varepsilon'} < |A| < p^{1+\varepsilon'}.$$

(5) Theorem 1 has the following reformulation.

For $\theta \in \mathbb{F}_p^*$, denote by $0(\theta)$ the multiplicative order of θ in \mathbb{F}_p^* .

Corollary. *Let $\theta_1, \dots, \theta_r \in \mathbb{F}_p^*$ satisfy for some $\varepsilon > 0$*

$$(1.19) \quad 0(\theta_i) > p^\varepsilon \text{ for all } i = 1, \dots, r,$$

$$(1.20) \quad 0(\theta_i \theta_j^{-1}) > p^\varepsilon \text{ for all } 1 \leq i \neq j \leq r.$$

Then

$$(1.21) \quad \max_{a_i \in \mathbb{F}_p^*} \left| \sum_{s=1}^{p-1} e_p \left(\sum_{i=1}^r a_i \theta_i^s \right) \right| < p^{1-\delta}$$

with $\delta = \delta(\varepsilon)$.

Indeed, let ψ be a generator of \mathbb{F}_p^* and write $\theta_i = \psi^{k_i}$, where thus

$$(1.22) \quad 0(\theta_i) = \frac{p-1}{(p-1, k_i)},$$

$$(1.23) \quad 0(\theta_i \theta_j^{-1}) = \frac{p-1}{(p-1, k_i - k_j)}.$$

Clearly

$$\sum_{s=1}^{p-1} e_p \left(\sum_{i=1}^r a_i \psi^{s k_i} \right) = \sum_{x \in \mathbb{F}_p^*} e_p \left(\sum_{i=1}^r a_i x^{k_i} \right).$$

Since (1.19), (1.20), (1.22), and (1.23) ensure conditions (1.1), (1.2) on the exponents k_i , (1.21) is equivalent to (1.3).

The corollary remains valid for incomplete sums (the case $r = 1$ appears in [B]).

Theorem 2. *Let $\varepsilon > 0$ and $\theta_1, \dots, \theta_r \in \mathbb{F}_p^*$ satisfy (1.19), (1.20). Then for $t > p^\varepsilon$*

$$(1.24) \quad \max_{a_i \in \mathbb{F}_p^*} \left| \sum_{s=1}^t e_p \left(\sum_{i=1}^r a_i \theta_i^s \right) \right| < p^{-\delta} t$$

where $\delta = \delta(\varepsilon)$.

(6) The paper is organized as follows. We will prove Proposition 2 in the next section. Section 3 contains the proof of Theorem 1 for $f(x) = ax^k + bx^\ell$ a binomial. The general case (r arbitrary) is treated in Section 4. In Section 5, we point out the modifications to obtain Theorem 2.

Sections 6 and 7 illustrate applications to uniform distribution issues for power generators in cryptography, in the spirit of [F-S] and [F-P-S]. Since in this context the module is assumed to be a product of two distinct primes (a Blum integer), we first show in Section 6 how to extend Theorem 2 to composite moduli which factor in distinct large primes.

2. SUM-PRODUCT ESTIMATES

We denote for $k \in \mathbb{Z}_+$

$$\begin{aligned} kA &= A + A + \dots + A && (k\text{-fold}), \\ A^k &= A.A \dots A && (k\text{-fold}) \end{aligned}$$

where sum and product sets are defined as

$$\begin{aligned} A + B &= \{x + y | x \in A, y \in B\}, \\ A.B &= \{x.y | x \in A, y \in B\}. \end{aligned}$$

Lemma 1. (i) *Let $S \subset \mathbb{F}_p, |S| > p^{3/4}$. Then*

$$(2.1) \quad \mathbb{F}_p = 3S.S.$$

(ii) *Let $S \subset \mathbb{F}_p, |S| > p^\varepsilon$. Then*

$$(2.2) \quad \mathbb{F}_p = k.S^k \text{ for } k \geq k(\varepsilon).$$

Proof. (1) We may of course assume $S \subset \mathbb{F}_p^*$. Introduce the function

$$(2.3) \quad f(x) = \frac{1}{|S|} \sum_{y \in S^{-1}} \chi_S(x.y)$$

satisfying $\text{supp } f \subset S.S$.

If $\xi \in \mathbb{F}_p$, we have

$$\hat{f}(\xi) \equiv \sum_{x \in \mathbb{F}_p} e_p(x\xi) f(x) = \frac{1}{|S|} \sum_{y \in S} \hat{\chi}_s(y\xi)$$

and for $\xi \in \mathbb{F}_p^*$

$$(2.4) \quad |\hat{f}(\xi)| \leq |S|^{-1/2} \left(\sum_{y \in S} |\hat{\chi}_s(y\xi)|^2 \right)^{1/2} \leq |S|^{-1/2} \left(\sum_{\eta \in \mathbb{F}_p} |\hat{\chi}_s(\eta)|^2 \right)^{1/2} = p^{1/2}.$$

Write $(f * f)(x) = \sum_{y \in \mathbb{F}_p} f(x - y) f(y)$ and

$$(f * f * f)(x) = \frac{1}{p} \hat{f}(0)^3 + \frac{1}{p} \sum_{\xi \in \mathbb{F}_p^*} \hat{f}(\xi)^3 e_p(x\xi).$$

Hence for all $x \in \mathbb{F}_p$

$$(2.5) \quad \left| (f * f * f)(x) - \frac{1}{p} |S|^3 \right| \stackrel{(2.4)}{\leq} \frac{1}{\sqrt{p}} \sum |\hat{f}(\xi)|^2 = \sqrt{p} \|f\|_2^2 \stackrel{(2.3)}{\leq} \sqrt{p} |S|.$$

Since $\frac{1}{p} |S|^3 > \sqrt{p} |S|$ from assumption on S ,

$$\mathbb{F}_p = \text{supp}(f * f * f) \subset 3 \text{supp } f \subset 3S.S$$

proving (2.1). □

(ii) From the sum-product theorem in \mathbb{F}_p (Proposition 1), there is $k_1 = k_1(\varepsilon)$ such that $|k_1 \cdot S^{k_1}| > p^{3/4}$. Here we just iterate (1.11) using the fact that $(A+A) \cdot (A+A) \subset 4A^2$. Next apply part (i) to get $\mathbb{F}_p = 3(k_1 S^{k_1})(k_1 S^{k_1}) \subset 3k_1^2 S^{2k_1}$.

Lemma 2. *If $S \subset \mathbb{F}_p \times \mathbb{F}_p$ satisfies*

$$|S| > p^{1+\varepsilon},$$

then

$$(2.6) \quad kS^k = \mathbb{F}_p \times \mathbb{F}_p \text{ for } k \in \mathbb{Z}_+, k \geq k(\varepsilon).$$

Proof. Denote by $\pi_i : \mathbb{F}_p \times \mathbb{F}_p \rightarrow \mathbb{F}_p$ the coordinate projections. From the assumption, there are $a_1, a_2 \in \mathbb{F}_p$ so that

$$S_i = \{x \in S | \pi_i(x) = a_i\}$$

satisfies

$$|S_i| = |\pi_{3-i}(S_i)| > p^\varepsilon \quad (i = 1, 2).$$

From Lemma 1, there is $k_1 = k_1(\varepsilon) \in \mathbb{Z}_+$ s.t.

$$\mathbb{F}_p = k_1 \pi_2(S_1)^{k_1} = \pi_2(k_1 S_1^{k_1})$$

and

$$\mathbb{F}_p = k_1 \pi_1(S_2)^{k_1} = \pi_1(k_1 S_2^{k_1}).$$

Writing then

$$2k_1 S^{k_1} \supset k_1 S_1^{k_1} + k_1 S_2^{k_1} = (\{k_1 a_1^{k_1}\} \times \mathbb{F}_p) + (\mathbb{F}_p \times \{k_1 a_2^{k_1}\}) = \mathbb{F}_p \times \mathbb{F}_p,$$

(2.6) follows. □

Lemma 3. *Let $A \subset \mathbb{F}_p^* \times \mathbb{F}_p^*$ satisfy for some $\varepsilon > 0$*

$$(2.7) \quad |\pi_1(A)| > p^\varepsilon \text{ and } |\pi_2(A)| > p^\varepsilon.$$

Then either

$$(2.8) \quad A \subset \{(x, ax) | x \in \mathbb{F}_p\} \text{ for some } a \in \mathbb{F}_p^*$$

or

$$(2.9) \quad kA^k = \mathbb{F}_p \times \mathbb{F}_p \text{ for some } k = k(\varepsilon) \in \mathbb{Z}.$$

Proof. Applying Lemma 1 to $S = \pi_1(A) \subset \mathbb{F}_p$, we have for some $k_0 \in \mathbb{Z}_+$

$$(2.10) \quad \pi_1(k_0 A^{k_0}) = k_0 S^{k_0} = \mathbb{F}_p$$

and similarly

$$(2.11) \quad \pi_2(k_0 A^{k_0}) = \mathbb{F}_p.$$

Clearly (2.10), (2.11) remain valid for $k \geq k_0$. In particular

$$(2.12) \quad |kA^k| \geq p \text{ for } k \geq k_0.$$

Assume $k \geq k_0$ and $|kA^k| > p$. Then $\pi_1|_{kA^k}$ is not one-to-one and there are $z, w \in kA^k$ such that $z_1 = w_1$ and $z_2 \neq w_2$. Hence

$$\begin{aligned} 2kA^{2k} - (z - w)(kA^k) &= \{(x_1, x_2 - (z_2 - w_2)y_2) \mid \\ &\quad x = (x_1, x_2) \in 2kA^{2k}, y = (y_1, y_2) \in kA^k\} \\ &= \mathbb{F}_p \times \mathbb{F}_p \end{aligned}$$

since $\pi_1(2kA^{2k}) = \mathbb{F}_p = \pi_2(kA^k)$. Thus

$$\mathbb{F}_p \times \mathbb{F}_p = 2kA^{2k} - (kA^k - kA^k)(kA^k)$$

and

$$(2.13) \quad \mathbb{F}_p \times \mathbb{F}_p = k_1A^{k_1} - k_1A^{k_1} \text{ for } k_1 = 3k^2.$$

From the Plünnecke-Ruzsa sumset inequalities (see [Na]) applied in the additive group $\mathbb{F}_p \times \mathbb{F}_p$ and (2.13)

$$p^2 = |k_1A^{k_1} - k_1A^{k_1}| \leq \left(\frac{|2k_1A^{k_1}|}{|k_1A^{k_1}|} \right)^3 |k_1A^{k_1}|$$

and hence by (2.12)

$$(2.14) \quad |2k_1A^{k_1}| \geq p^{4/3}.$$

We may then apply Lemma 2 to $S = 2k_1A^{k_1} \subset \mathbb{F}_p \times \mathbb{F}_p$ and get $k_2 \in \mathbb{Z}_+$ s.t. $k_2A^{k_2} = \mathbb{F}_p \times \mathbb{F}_p$, hence (2.9).

Fix $z \in k_0A^{k_0}$ and let $P = k_0A^{k_0} - z$. Thus $0 \in P \subset P + P$ and $|P| \geq p$ by (2.12). If $|P + P| = |2k_0A^{k_0}| > p$, it follows from the preceding that we are in alternative (2.9). Assume thus $|P + P| = p = |P|$, so that $P = P + P$ and P is closed under addition. Since $\pi_1(P) = \mathbb{F}_p$ by (2.10), there is $c \in \mathbb{F}_p$ s.t. $(1, c) \in P$ and

$$(2.15) \quad \begin{aligned} P &= \{(t, ct) \mid t \in \mathbb{F}_p\}, \\ k_0A^{k_0} &= \{(z_1 + t, z_2 + ct) \mid t \in \mathbb{F}_p\} = \{(t, ct + d) \mid t \in \mathbb{F}_p\} \end{aligned}$$

with $d = z_2 - cz_1 \in \mathbb{F}_p$. By (2.11), $c \neq 0$. Assume $d \neq 0$. Writing

$$(k_0A^{k_0}) \cdot (k_0A^{k_0}) = \{(t_1t_2, c^2t_1t_2 + cd(t_1 + t_2) + d^2) \mid t_1, t_2 \in \mathbb{F}_p\},$$

it follows that

$$(2.16) \quad |k_0^2A^{2k_0}| \geq |\{(t_1t_2, t_1 + t_2) \mid t_1, t_2 \in \mathbb{F}_p\}| \geq \frac{p^2}{2}$$

putting us again in alternative (2.9).

Assume $d = 0$ in (2.15), i.e., $k_0A^{k_0} = \{(t, ct) \mid t \in \mathbb{F}_p\}$. Fix an element $w = (w_1, w_2) \in k_0A^{k_0-1}$ with $w_2 \neq 0$. Then, for all $x = (x_1, x_2) \in A, wx \in k_0A^{k_0}$ and $w_2x_2 = cw_1x_1$, implying that $A \subset \{(t, at) \mid t \in \mathbb{F}_p\}$ with $a = cw_1w_2^{-1}$. This is alternative (2.8). \square

Lemma 4. *Let $A \subset \mathbb{F}_p^* \times \mathbb{F}_p^*$ satisfying*

$$(2.17) \quad |A| > p^{\varepsilon_0},$$

$$(2.18) \quad \begin{aligned} |A + A| + |A \cdot A| &< p^\varepsilon |A| \\ (\varepsilon &\ll \varepsilon_0). \end{aligned}$$

Fix $k \in \mathbb{Z}_+$. There is a subset $A_1 \subset A$ such that

$$(2.19) \quad |A_1| > p^{-\delta} |A|,$$

$$(2.20) \quad |kA_1^k| < p^\delta |A_1|$$

where $\delta = \delta_k(\varepsilon)$ and $\delta_k(\varepsilon) \xrightarrow{\varepsilon \rightarrow 0} 0$ for given k .

(Observe that $|kA_1^k|$ is nondecreasing in k).

Lemma 4 may be proven by an adjustment of the argument in [B-K-T] for subsets of \mathbb{F}_p (the main point in the present context is to avoid problems due to zero-divisors). We give a different argument, in particular not relying on Gowers' proof of the Balog-Szemerédi theorem.

Lemma 5. Let A_1, A_2, A_3 be finite subsets of an additive group, satisfying

$$(2.21) \quad |A_1 \cap A_3| > \frac{1}{K} |A_1|,$$

$$(2.22) \quad |A_2 \cap A_3| > \frac{1}{K} |A_2|,$$

$$(2.23) \quad |A_i + A_i| < K |A_i| \quad (i = 1, 2, 3).$$

Then

$$(2.24) \quad |A_1 + A_2| < K^9 |A_3|.$$

Proof of Lemma 5. Write for $i = 1, 2$

$$(2.25) \quad \chi_{A_i} \leq \frac{1}{|A_i \cap A_3|} \sum_{y \in A_i - (A_i \cap A_3)} \chi_{y + (A_i \cap A_3)}.$$

Hence

$$\chi_{A_1 + A_2} \leq \frac{1}{|A_1 \cap A_3| |A_2 \cap A_3|} \sum_{\substack{y_i \in A_i - (A_i \cap A_3) \\ i=1,2}} \chi_{y_1 + y_2 + (A_1 \cap A_3) + (A_2 \cap A_3)}$$

and therefore

$$|A_1 + A_2| \leq \frac{|A_1 - A_1| |A_2 - A_2| |A_3 + A_3|}{|A_1 \cap A_3| |A_2 \cap A_3|} < \frac{K^7 |A_1| |A_2| |A_3|}{K^{-2} |A_1| |A_2|} = K^9 |A_3|$$

from (2.21)–(2.23) and the sum-difference inequalities; (see [Na]). □

Remark. One could alternatively have invoked ‘Ruzsa’s triangle inequality’ $|A - B| \cdot |C| \leq |A - C| |B - C|$ to derive a similar estimate.

Proof of Lemma 4. Recall that $A \subset \mathbb{F}_p^* \times \mathbb{F}_p^*$. Write

$$|A|^2 = \sum_{x \in A} |xA| \leq |A \cdot A|^{1/2} \left[\sum_{x, x' \in A} |xA \cap x'A| \right]^{1/2}$$

and by (2.18)

$$(2.26) \quad \sum_{x, x' \in A} |xA \cap x'A| > p^{-\varepsilon} |A|^3.$$

From (2.26), we may specify $\bar{x} \in A$ such that

$$(2.27) \quad A_1 = \left\{ x \in A \mid |xA \cap \bar{x}A| > \frac{1}{2} p^{-\varepsilon} |A| \right\}$$

satisfies

$$|A_1| > p^{-\varepsilon}|A|.$$

If $x_1, x_2 \in A_1$, apply Lemma 5 with $A_1 = x_1A, A_2 = x_2A, A_3 = \bar{x}A$ and $K = 2p^\varepsilon$. From (2.24)

$$(2.28) \quad |x_1A + x_2A| < p^{10\varepsilon}|A|.$$

Next, let $x_1, x_2, x_3, x_4 \in A_1$. Since

$$|x_1x_3A \cap x_1\bar{x}A| = |x_3A \cap \bar{x}A| > \frac{1}{2}p^{-\varepsilon}|A|,$$

$$|x_2x_4A \cap x_2\bar{x}A| > \frac{1}{2}p^{-\varepsilon}|A|,$$

we may apply Lemma 5 with $A_1 = x_1x_3A, A_2 = x_2x_4A, A_3 = x_1\bar{x}A \cup x_2\bar{x}A$ and $K = p^{10\varepsilon}$, from (2.28). Hence

$$(2.29) \quad |x_1x_3A + x_2x_4A| < p^{90\varepsilon}|A|.$$

Straightforward iteration implies that

$$(2.30) \quad |y_1A + y_2A| < p^{C\varepsilon}|A|$$

whenever $y_1, y_2 \in A_2^k$ and with $C = C_k$ in (2.30).

The same statement holds clearly also if $y_1, y_2 \in A_1^{-1}A_1^k$.

Write now

$$(2.31) \quad \chi_{A_1^k} \leq \frac{1}{|A_1|} \sum_{y \in A_1^{-1}A_1^k} \chi_{yA_1},$$

$$\chi_{A_1^k + A_1^k} \leq \frac{1}{|A_1|^2} \sum_{y_1, y_2 \in A_1^{-1}A_1^k} \chi_{y_1A_1 + y_2A_1}$$

and using (2.30)

$$(2.32) \quad |A_1^k + A_1^k| \leq \frac{|A_1^{-1}A_1^k|^2}{|A_1|^2} p^{c\varepsilon}|A| < p^{c\varepsilon} \frac{|A^{-1}A^k|^2}{|A|}.$$

From (2.18) and the Plünnecke-Ruzsa inequalities applied multiplicatively in the group $\mathbb{F}_p^* \times \mathbb{F}_p^*$, we have $|(A \cup A^{-1})^k| < p^{c\varepsilon}|A|$. Thus (2.32) gives

$$(2.33) \quad |A_1^k + A_1^k| < p^{c\varepsilon}|A|$$

and (2.30) follows from (2.33), applying again the sumset inequalities. □

Proof of Proposition 2. Decomposing A as $(A \cap (\mathbb{F}_p^* \times \mathbb{F}_p^*)) \cup (A \cap (\{0\} \times \mathbb{F}_p)) \cup (A \cap (\mathbb{F}_p \times \{0\}))$, we may, in view of alternative (1.16), assume $|A \cap (\mathbb{F}_p^* \times \mathbb{F}_p^*)| > \frac{1}{2}|A|$ and hence $A \subset \mathbb{F}_p^* \times \mathbb{F}_p^*$. Fix $\varepsilon' > 0$ small and $k \in \mathbb{Z}_+$ (to be specified). Take ε in (2.14) small enough to obtain from Lemma 4 a subset $A_1 \subset A$ satisfying

$$(2.34) \quad |A_1| > p^{-\varepsilon'}|A|,$$

$$(2.35) \quad |kA_1^k| < p^{\varepsilon'}|A_1|.$$

Next, apply Lemma 3 to the set A_1 with $\varepsilon = \varepsilon'$.

If (2.7) fails, say $|\pi_1(A_1)| \leq p^{\varepsilon'}$, obviously for some $a \in \mathbb{F}_p$

$$|A \cap (\{a\} \times \mathbb{F}_p)| \geq |A_1 \cap (\{a\} \times \mathbb{F}_p)| \geq p^{-\varepsilon'}|A_1| > p^{-2\varepsilon'}|A|$$

and hence (2.16) holds.

Otherwise, either (2.8) or (2.9) holds. If (2.9) and assuming $k \geq k(\varepsilon')$ (= the integer in (2.9)), we get

$$p^2 = |kA_1^k| \stackrel{(2.35)}{<} p^{\varepsilon'} |A_1|$$

and hence

$$|A_1| > p^{2-\varepsilon'}$$

and (1.15) holds.

Assume (2.8). Since then

$$A_1 \subset \{(x, ax) | x \in \mathbb{F}_p\} \text{ for some } a \in \mathbb{F}_p^*,$$

$$|A \cap \{(x, ax) | x \in \mathbb{F}_p\}| \geq |A_1| \stackrel{(2.34)}{>} p^{-\varepsilon'} |A| \text{ and (1.17) holds.}$$

Assuming (1.16) or (1.17), the upperbound in (1.18) is clear and the lower bound follows from Proposition 1.

This proves Proposition 2. □

3. PROOF OF THE BINOMIAL ESTIMATE

In this section, we prove Theorem 1 for $r = 2$. The case $r = 1$ was treated in [B-K]. First we recall a few results from combinatorics and harmonic analysis.

Lemma 6 (The Balog-Szemerédi-Gowers theorem; see [Go]). *Let A be a finite subset of an additive group, $|A| = N$, and assume for some $0 < \delta < \frac{1}{10}$ that*

$$(3.1) \quad |\{(x_1, x_2, x_3, x_4) \in A^4 | x_1 + x_2 = x_3 + x_4\}| > \delta N^3.$$

Then there is a subset $A_1 \subset A$ satisfying

$$(3.2) \quad |A_1| > \delta^C N$$

and

$$(3.3) \quad |A_1 + A_1| < \delta^{-C} |A_1|$$

where C is an absolute constant.

See [Go].

Later on we will apply this result in the additive group $\mathbb{F}_p \times \mathbb{F}_p$ and also in the multiplicative group $\mathbb{F}_p^* \times \mathbb{F}_p^*$ (both cases may in fact be derived from the statement for subsets of \mathbb{Z} , +).

Next, we give an elementary fact about the Fourier transform of probability measures.

Lemma 7. *Let ν be a probability measure on an Abelian group G and assume $\gamma_1, \dots, \gamma_m \in \Gamma$ (= dual group) such that*

$$\sum_{i=1}^m |\hat{\nu}(\gamma_i)| > \delta m.$$

Then

$$\sum_{i,j=1}^m |\hat{\nu}(\gamma_i - \gamma_j)| > \delta^2 m^2.$$

Proof. Take $a_i \in \mathbb{C}$, $|a_i| = 1$, such that $a_i \hat{\nu}(\gamma_i) = |\hat{\nu}(\gamma_i)|$. Hence, identifying γ_i with the character function $G \rightarrow \{z \in \mathbb{C} \mid |z| = 1\}$,

$$\begin{aligned} \delta m &< \int_G \left| \sum_{i=1}^m a_i \gamma_i(x) \right| \nu(dx), \\ \delta^2 m^2 &< \int_G \left| \sum_{i=1}^m a_i \gamma_i(x) \right|^2 \nu(dx) \\ &\leq \sum_{i,j=1}^m \left| \int (\gamma_i \bar{\gamma}_j)(x) \nu(dx) \right| = \sum_{i,j=1}^m |\hat{\nu}(\gamma_i - \gamma_j)|. \quad \square \end{aligned}$$

Returning to the exponential sum estimate, assume $1 \leq k_1 < k_2 < p-1$ satisfying

$$(3.4) \quad (k_i, p-1) < p^{1-\gamma} \quad (i = 1, 2)$$

and

$$(3.5) \quad (k_1 - k_2, p-1) < p^{1-\gamma}$$

for some $\gamma > 0$. Let $a_1, a_2 \in \mathbb{F}_p^*$ and assume

$$(3.6) \quad \left| \sum_1^{p-1} e_p(a_1 x^{k_1} + a_2 x^{k_2}) \right| > p^{1-\varepsilon}.$$

Our purpose is to get a contradiction for $\varepsilon < \varepsilon(\gamma), \varepsilon(\gamma) > 0$ in (3.6).

Consider the multiplicative subgroup $H \triangleleft \mathbb{F}_p^* \times \mathbb{F}_p^*$ defined by

$$H = \{(x^{k_1}, x^{k_2}) \mid x \in \mathbb{F}_p^*\}.$$

Hence

$$(3.7) \quad |H| = \frac{p-1}{d} \text{ with } d = (k_1, k_2, p-1).$$

Define the probability measures μ, μ_- on $\mathbb{F}_p \times \mathbb{F}_p$ by

$$\begin{aligned} \mu &= \frac{1}{|H|} \sum_{y \in H} \delta_y, \\ \mu_- &= \frac{1}{|H|} \sum_{y \in H} \delta_{(-y)} \end{aligned}$$

where δ_y stands for the Dirac measure at y . Rephrase (3.6) as

$$(3.8) \quad |\hat{\mu}(a)| > p^{-\varepsilon}.$$

Notice that by invariance, $\hat{\mu}(\xi) = \hat{\mu}(y\xi)$ for $y \in H$.

Let $\ell \in \mathbb{Z}_+$. From (3.8)

$$(3.9) \quad \sum_{y \in H} |\hat{\mu}(ya)|^{2\ell} > |H| p^{-2\varepsilon\ell}.$$

Since $|\hat{\mu}(\xi)|^{2\ell} = (\mu^{(\ell)} * \mu_-^{(\ell)})(\xi)$, iterated application of Lemma 7 with $\nu = \mu^{(\ell)} * \mu_-^{(\ell)}$ implies

$$(3.10) \quad \frac{1}{|H|^{2r}} \sum_{y_1, \dots, y_{2r} \in H} |\hat{\mu}((y_1 - y_2 + \dots - y_{2r})a)|^{2\ell} > p^{-4\varepsilon r\ell}$$

assuming $r \in \mathbb{Z}_+$ to be a power of 2.

Hence

$$\begin{aligned}
 (3.11) \quad p^{-4\epsilon r \ell} &< \sum_{y \in \mathbb{F}_p^2} |\hat{\mu}(ya)|^{2\ell} (\mu^{(r)} * \mu_-^{(r)})(y) \\
 &\leq (\mu^{(r)} * \mu_-^{(r)})(0) \sum_{\xi \in \mathbb{F}_p^2} |\hat{\mu}(\xi)|^{2\ell} \\
 (3.12) \quad &= p^2 (\mu^{(r)} * \mu_-^{(r)})(0) \cdot (\mu^{(\ell)} * \mu_-^{(\ell)})(0).
 \end{aligned}$$

Taking $r = \ell$, it follows that

$$(3.13) \quad (\mu^{(r)} * \mu_-^{(r)})(0) > p^{-1-2\epsilon r^2}.$$

On the other hand, there is the upperbound

$$\begin{aligned}
 (\mu^{(r)} * \mu_-^{(r)})(0) &= |H|^{-2r} |\{(y_1, \dots, y_{2r}) \in H^{2r} | y_1 - y_2 + \dots - y_{2r} = 0\}| \\
 &= (p-1)^{-2r} \left| \left\{ (x_1, \dots, x_{2r}) \in (\mathbb{F}_p^*)^{2r} \begin{cases} x_1^{k_1} - x_2^{k_1} + \dots - x_{2r}^{k_1} = 0 \\ x_1^{k_2} - x_2^{k_2} + \dots - x_{2r}^{k_2} = 0 \end{cases} \right\} \right| \\
 (3.14) \quad &\leq (p-1)^{-2r} \left| \left\{ (x_1, \dots, x_{2r}) \in (\mathbb{F}_p^*)^{2r} | x_1^{k_1} - x_2^{k_1} + \dots - x_{2r}^{k_1} = 0 \right\} \right|
 \end{aligned}$$

to which the Gauss sum estimate applies. Write

$$(3.14) = (p-1)^{-2r} p^{-1} \sum_{\xi \in \mathbb{F}_p^*} \left| \sum_{x=1}^{p-1} e_p(\xi x^{k_1}) \right|^{2r} < \left(\frac{p}{p-1} \right)^{2r} p^{-1} + (p-1)^{-2r} \max_{\xi \in \mathbb{F}_p^*} \left| \sum_{x=1}^{p-1} e_p(\xi x^{k_1}) \right|^{2r}.$$

In view of assumption (3.4), by (1.4), there is $\delta_0 = \delta(\gamma) > 0$ such that

$$(3.15) \quad \max_{\xi \in \mathbb{F}_p^*} \left| \sum_{x=1}^{p-1} e_p(\xi x^{k_i}) \right| < p^{1-\delta_0} \quad (i = 1, 2).$$

Taking $r \geq r_0$,

$$(3.16) \quad r_0 = \left\lceil \frac{1}{\delta_0} \right\rceil$$

and it follows that (3.14) $< \frac{2}{p}$.

Summarizing

$$(3.17) \quad p^{-1-2\epsilon r^2} < (\mu^{(r)} * \mu_-^{(r)})(0) < \frac{2}{p} \text{ for } r \geq r_0.$$

Define the sets

$$\Omega_\delta = \{\xi \in \mathbb{F}_p^2 \mid |\hat{\mu}(\xi)| > p^{-\delta}\}$$

and

$$\Lambda_{r,\delta} = \{y \in \mathbb{F}_p^2 \mid (\mu^{(r)} * \mu_-^{(r)})(y) > p^{-1-\delta}\}.$$

From (3.17) with $r = r_0$

$$(3.18) \quad \sum_{\xi} |\hat{\mu}(\xi)|^{2r_0} < p^2 \frac{2}{p} = 2p.$$

Hence

$$(3.19) \quad |\Omega_\delta| < p^{1+2r_0\delta}.$$

Obviously

$$(3.20) \quad |\Lambda_{r,\delta}| < p^{1+\delta}.$$

Apply (3.11) with $\ell = 1, r = r_0$. Thus

$$p^{-4\epsilon r_0} < \sum_{y \in \mathbb{F}_p^2} |\hat{\mu}(ya)|^2 (\mu^{(r_0)} * \mu_-^{(r_0)})(y)$$

implying

$$\frac{1}{2} p^{-4\epsilon r_0} < \sum_{ay \in \Omega_{3\epsilon r_0}} (\mu^{(r_0)} * \mu_-^{(r_0)})(y) \stackrel{(3.17)}{<} \frac{2}{p} |\Omega_{3\epsilon r_0}|$$

and

$$(3.21) \quad |\Omega_\delta| > p^{1-5\epsilon r_0} \text{ for } \delta > 3\epsilon r_0.$$

Next, writing (3.11) with $\ell = r_0$

$$(3.22) \quad p^{-4\epsilon r r_0} < \sum_{y \in \mathbb{F}_p^2} |\hat{\mu}(ya)|^{2r_0} (\mu^{(r)} * \mu_-^{(r)})(y) = \sum_{y \in \Lambda_{r,\delta}} + \sum_{y \notin \Lambda_{r,\delta}}.$$

Since

$$\sum_{y \notin \Lambda_{r,\delta}} < p^{-1-\delta} \sum_{\xi \in \mathbb{F}_p^2} |\hat{\mu}(\xi)|^{2r_0} \stackrel{(3.18)}{<} 2p^{-\delta},$$

it follows from (3.22) that for $\delta > 4\epsilon r r_0$

$$|\Lambda_{r,\delta}| (\mu^{(r)} * \mu_-^{(r)})(0) > p^{-4\epsilon r r_0}$$

and hence

$$(3.23) \quad |\Lambda_{r,\delta}| > p^{1-4\epsilon r r_0} \text{ if } r \geq r_0, \delta > 4\epsilon r r_0.$$

Notice also that, by (3.15), if $\delta < \delta_0$,

$$\Omega_\delta \setminus (\mathbb{F}_p^* \times \mathbb{F}_p^*) = \{(0, 0)\};$$

hence $\Omega_\delta = \Omega_\delta^* \cup \{(0, 0)\}$, denoting

$$\Omega_\delta^* = \Omega_\delta \cap (\mathbb{F}_p^* \times \mathbb{F}_p^*).$$

Put

$$(3.24) \quad \delta_1 = 5\epsilon r_0$$

and let $\xi \in \Omega_{\delta_1}^*$. Replacing in (3.11) a by ξ and ϵ by δ_1 ,

$$(3.25) \quad p^{-4\delta_1 r \ell} < \sum_{y \in \mathbb{F}_p^2} |\hat{\mu}(y\xi)|^{2\ell} (\mu^{(r)} * \mu_-^{(r)})(y).$$

Taking $\ell = 1$ in (3.25),

$$(3.26) \quad \frac{1}{2} p^{-4\delta_1 r} < \sum_{y \xi \in \Omega_{2\delta_1 r}} (\mu^{(r)} * \mu_-^{(r)})(y).$$

Since $|\Omega_{2\delta_1 r}| < p^{1+4\delta_1 r_0 r}$ by (3.19), in (3.26) we may further restrict the y -summation to $\Lambda_{r,5\delta_1 r_0 r}$ and conclude that

$$(3.27) \quad |\Lambda_{r,5\delta_1 r_0 r} \cap (\xi^{-1} \Omega_{2\delta_1 r})| > \frac{1}{4} p^{1-4\delta_1 r} \text{ for } r \geq r_0.$$

From (3.19), (3.21)

$$(3.28) \quad p^{1-\delta_1} < |\Omega_{\delta_1}| < p^{1+2r_0 \delta_1}.$$

Inequality (3.27) is valid for all $\xi \in \Omega_{\delta_1}^*$. Taking $r = r_0$, (3.27), (3.28) imply

$$\sum_{\xi \in \Omega_{\delta_1}^*} |(\xi^{-1}\Omega_{2\delta_1 r_0}) \cap \Lambda_{r_0, 5\delta_1 r_0^2}| > p^{2-5\delta_1 r_0}$$

and the left side is bounded by

$$|\Lambda_{r_0, 5\delta_1 r_0^2}|^{1/2} \left(\sum_{\xi_1, \xi_2 \in \Omega_{\delta_1}^*} |(\xi_1^{-1}\Omega_{2\delta_1 r_0}^*) \cap (\xi_2^{-1}\Omega_{2\delta_1 r_0}^*)| \right)^{1/2}.$$

Therefore

$$\begin{aligned} p^{3-15\delta_1 r_0^2} &< \sum_{\xi_1, \xi_2 \in \Omega_{\delta_1}^*} |(\xi_1^{-1}\Omega_{2\delta_1 r_0}^*) \cap (\xi_2^{-1}\Omega_{2\delta_1 r_0}^*)| \\ (3.29) \qquad &\leq |\{(\xi_1, \xi_2, \xi_3, \xi_4) \in (\Omega_{2\delta_1 r_0}^*)^4 \mid \xi_1 \xi_3 = \xi_2 \xi_4\}|. \end{aligned}$$

With ε sufficiently small, we may make δ_1 in (3.24) arbitrarily small. Applying Lemma 6 to the set $\Omega_{2\delta_1 r_0}^*$ in the multiplicative group $\mathbb{F}_p^* \times \mathbb{F}_p^*$, there is a subset $\Omega \subset \Omega_{2\delta_1 r_0}^*$ satisfying

$$(3.30) \qquad |\Omega| > p^{1-Cr_0^2\delta_1}$$

and

$$(3.31) \qquad |\Omega.\Omega| < p^{1+Cr_0^2\delta_1}.$$

We reduce Ω further to also obtain a small additive doubling set. From Lemma 7

$$(3.32) \qquad \sum_{\xi_1, \xi_2 \in \Omega} |\hat{\mu}|^2(\xi_1 - \xi_2) > p^{-8\delta_1 r_0} |\Omega|^2$$

implying

$$|\{(\xi_1, \xi_2) \in \Omega^2 \mid \xi_1 - \xi_2 \in \Omega_{5\delta_1 r_0}\}| > \frac{1}{2} p^{-8\delta_1 r_0} |\Omega|^2$$

and since $|\Omega_{5\delta_1 r_0}| < p^{1+10r_0^2\delta_1}$, it also holds that

$$(3.33) \qquad |\{(\xi_1, \xi_2, \xi_3, \xi_4) \in \Omega^4 \mid \xi_1 - \xi_2 = \xi_3 - \xi_4\}| > p^{3-Cr_0^2\delta_1}.$$

Now applying Lemma 6 to Ω in the additive group $\mathbb{F}_p \times \mathbb{F}_p$ gives a subset $A \subset \Omega$ such that

$$(3.34) \qquad p^{1+4r_0^2\delta_1} > |A| > |\Omega| p^{-Cr_0^2\delta_1} > p^{1-Cr_0^2\delta_1},$$

$$(3.35) \qquad |A + A| < p^{Cr_0^2\delta_1} |A|$$

(here we use C to denote various numerical constants).

By (3.31), it also holds that

$$(3.36) \qquad |A.A| < p^{Cr_0^2\delta_1} |A|.$$

Since A satisfies (3.35), (3.36), we may apply Proposition 2. Notice that by (3.24), $\varepsilon' = \varepsilon'(\delta_1) = \varepsilon'(\varepsilon) \xrightarrow{\varepsilon \rightarrow 0} 0$. Either (1.16) or (1.17) holds. Assume (1.16), say for some $b \in \mathbb{F}_p$

$$(3.37) \quad |\Omega \cap (\{b\} \times \mathbb{F}_p)| \geq |A \cap (\{b\} \times \mathbb{F}_p)| > p^{-\varepsilon'} |A| \stackrel{(3.34)}{>} p^{1-2\varepsilon'}.$$

Applying (3.32) with Ω replaced by $\Omega \cap (\{b\} \times \mathbb{F}_p)$, we obtain

$$|\{(\xi_1, \xi_2) \in \mathbb{F}_p^2 | (0, \xi_1 - \xi_2) \in \Omega_{5\delta_1 r_0}\}| > p^{2-4\varepsilon' - 9\delta_1 r_0} > p^{3/2}$$

contradicting the fact that $\Omega_{5\delta_1 r_0} = \Omega_{5\delta_1 r_0}^* \cup \{(0, 0)\}$.

Assume (1.17). Thus there is $c \in \mathbb{F}_p^*$ s.t. if

$$(3.38) \quad A_1 = A \cap \{(t, ct) | t \in \mathbb{F}_p\},$$

then

$$(3.39) \quad |A_1| > p^{-\varepsilon'} |A| > p^{1-2\varepsilon'}.$$

Recalling that $A_1 \subset \Omega_{2\delta_1 r_0}^*$, write

$$(3.40) \quad \sum_{t=0}^{p-1} |\hat{\mu}(t, ct)|^2 \geq |A_1| p^{-4\delta_1 r_0} \stackrel{(3.39)}{>} p^{1-3\varepsilon'}$$

where

$$\hat{\mu}(t, ct) = \frac{1}{p-1} \sum_{z=1}^{p-1} e_p(t(z^{k_1} + cz^{k_2})).$$

Hence (3.40) implies

$$(3.41) \quad |\{(z, w) \in \mathbb{F}_p^* \times \mathbb{F}_p^* | z^{k_1} + cz^{k_2} = w^{k_1} + cw^{k_2}\}| > p^{2-3\varepsilon'}.$$

Writing $w = v.z$, there is $v \in \mathbb{F}_p^*$ such that

$$(3.42) \quad v^{k_2} \neq 1$$

and the equation

$$(3.43) \quad z^{k_2-k_1} = \frac{1 - v^{k_1}}{c(v^{k_2} - 1)}$$

has at least $p^{1-3\varepsilon'}$ solutions in $z \in \mathbb{F}_p$.

To ensure (3.42), we used that $x^{k_2} \equiv 1$ has $(k_2, p-1) \stackrel{(3.4)}{<} p^{1-\gamma} < p^{1-3\varepsilon'}$ solutions in \mathbb{F}_p . By (3.5), (3.43) has at most $(k_2 - k_1, p-1) < p^{1-\gamma}$ solutions, a contradiction for ε' (hence ε in (3.6)) small enough.

This completes the proof of Theorem 1 in the binomial case.

4. PROOF OF THEOREM 1 IN GENERAL

Let $1 \leq k_i < p-1$ ($1 \leq i \leq r$) satisfy (1.1) and (1.2).

We prove that

$$(4.1) \quad \max_{(a_1, \dots, a_r, p)=1} \left| \sum_{x=1}^{p-1} e_p(a_1 x^{k_1} + \dots + a_r x^{k_r}) \right| < p^{1-\delta_r}$$

for some $\delta_r > 0$, by induction on r .

The case $r = 1$ appears in [B-K] and $r = 2$ was treated in the previous section.

Thus assume $r \geq 3$.

Let

$$(4.2) \quad H = \{(x^{k_1}, \dots, x^{k_r}) \mid x \in \mathbb{F}_p^*\} \triangleleft (\mathbb{F}_p^*)^r$$

with

$$|H| = \frac{p-1}{d}, d = (k_1, \dots, k_r, p-1).$$

Consider again the probability measures on \mathbb{F}_p^r

$$\begin{aligned} \mu &= \frac{1}{|H|} \sum_{y \in H} \delta_y, \\ \mu_- &= \frac{1}{|H|} \sum_{y \in H} \delta_{-y} \end{aligned}$$

where δ_y is Dirac at $y \in \mathbb{F}_p^r$.

To establish (4.1), we may assume all $a_i \in \mathbb{F}_p^*$ ($1 \leq i \leq r$), since otherwise the problem reduces to $r-1$ terms. Assume

$$(4.3) \quad \frac{1}{p} \left| \sum_1^{p-1} e_p(a_1 x^{k_1} + \dots + a_r x^{k_r}) \right| = |\hat{\mu}(a)| > p^{-\delta}.$$

The same argument leading to (3.13) (now applied on \mathbb{F}_p^r) implies

$$(4.4) \quad (\mu^{(\ell)} * \mu_-^{(\ell)})(0) > p^{-\frac{r}{2} - 2\delta\ell^2}.$$

On the other hand, letting $\frac{r}{2} < r_1 < r$ ($r \geq 3$), proceeding as in the binomial case, we estimate

$$(4.5) \quad \begin{aligned} (\mu^{(\ell)} * \mu_-^{(\ell)})(0) &= (p-1)^{-2\ell} |\{(x_1, \dots, x_{2\ell}) \in (\mathbb{F}_p^*)^{2\ell} \mid x_1^{k_i} - x_2^{k_i} + \dots - x_{2\ell}^{k_i} = 0 \ (1 \leq i \leq r)\}| \\ &\leq (p-1)^{-2\ell} |\{(x_1, \dots, x_{2\ell}) \in (\mathbb{F}_p^*)^{2\ell} \mid x_1^{k_i} - x_2^{k_i} + \dots - x_{2\ell}^{k_i} = 0 \ (1 \leq i \leq r_1)\}|. \end{aligned}$$

To bound (4.5), express the quantity by exponential sums that may be estimated nontrivially from the induction hypothesis, since $r_1 < r$. Thus clearly

$$(4.6) \quad \begin{aligned} (4.5) &= (p-1)^{-2\ell} p^{-r_1} \sum_{\xi_1, \dots, \xi_{r_1} \in \mathbb{F}_p} \left| \sum_{x=1}^{p-1} e_p(\xi_1 x^{k_1} + \dots + \xi_{r_1} x^{k_{r_1}}) \right|^{2\ell} \\ &< p^{-r_1} + (p-1)^{-2\ell} p^{2\ell(1-\delta_{r_1})} < p^{-r_1} + 2p^{-2\ell\delta_{r_1}}. \end{aligned}$$

Taking

$$(4.7) \quad \ell = \left\lceil \frac{r_1}{\delta_{r_1}} \right\rceil,$$

(4.4), (4.6) imply

$$p^{-\frac{r}{2} - 2\delta\ell^2} < 2p^{-r_1};$$

hence, from the choice of r_1

$$\delta > \frac{1}{4\ell^2} > \frac{\delta_{r_1}^2}{4r_1^2}.$$

Taking $r_1 = \lfloor \frac{r}{2} \rfloor + 1$, we proved that

$$(4.8) \quad \delta_r > \frac{\delta_{\lfloor \frac{r}{2} \rfloor + 1}^2}{4r^2}$$

implying Theorem 1 with

$$(4.9) \quad \delta_r > \left(\frac{\delta_2}{4r}\right)^{4r}$$

where $\delta_2 = \delta_2(\varepsilon)$.

5. FURTHER COMMENTS

(1) We comment on how δ in (1.3) according to the preceding argument depends on ε in (1.1), (1.2). For $r = 1$ (the monomial case) it was shown in [B-K] that we may take

$$(5.1) \quad \delta_1 > \exp(-C_1\varepsilon^{-C_2})$$

for some constants C_1, C_2 (see [B-K, Theorem 4]).

A more careful analysis of the proof of Proposition 2 and the binomial case gives a similar lower bound for δ_2 . Therefore (4.8) implies

$$(5.2) \quad \delta_r > \exp(-C_3r(\varepsilon^{-C_2} + \log r)).$$

(2) Next we indicate the proof of Theorem 2. As already mentioned, the case $r = 1$ appears in [B] (these and related exponential sums have their importance in issues related to cryptography, such as the Diffie-Hellman distributions; see [B] and related references).

We first treat the case $r = 2$. The general case is then obtained using the same strategy as described in Section 4.

Also the proof of the $r = 2$ case is almost identical.

Let $\gamma > 0$ and assume

$$(5.3) \quad 0(\theta_1) > p^\gamma, 0(\theta_2) > p^\gamma, 0(\theta_1\theta_2^{-1}) > p^\gamma.$$

Take

$$(5.4) \quad t = [p^\gamma].$$

Introduce

$$(5.5) \quad H = \{(\theta_1^s, \theta_2^s) | s = 1, \dots, t\} \subset \mathbb{F}_p^* \times \mathbb{F}_p^*.$$

H is not a subgroup of $\mathbb{F}_p^* \times \mathbb{F}_p^*$ (but an ‘approximative’ subgroup in the sense of [B]).

Clearly $|H| = t$. Define μ, μ_- as in Section 3 and assume $a \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ such that

$$(5.6) \quad |\hat{\mu}(a)| > p^{-\varepsilon}$$

with $\varepsilon > 0$ small enough. Justifying (3.9) requires an additional argument, since there is no true invariance under H -multiplication. Let $t_1 = \frac{t}{10}p^{-\varepsilon}$ and write for $1 \leq s_1 \leq t_1$

$$|\hat{\mu}(\theta_1^{s_1} a_1, \theta_2^{s_1} a_2) - \hat{\mu}(a_1, a_2)| \leq \frac{2s_1}{t} < \frac{1}{5}p^{-\varepsilon};$$

hence

$$(5.7) \quad |\hat{\mu}(\theta_1^{s_1} a_1, \theta_2^{s_1} a_2)| > \frac{1}{2}p^{-\varepsilon}.$$

Therefore

$$(5.8) \quad \sum_{y \in H} |\hat{\mu}(ya)|^{2\ell} \geq \sum_{s_1=1}^{t_1} |\hat{\mu}(\theta_1^{s_1} a_1, \theta_2^{s_1} a_2)|^{2\ell} > t_1 4^{-\ell} p^{-2\ell\epsilon} < |H| p^{-3\epsilon\ell}$$

providing (3.9).

Inequality (3.15) is substituted by the $r = 1$ case of Theorem 2 (established in [B]); thus

$$(5.9) \quad \max_{\xi \in \mathbb{F}_p^*} \left| \sum_{s=1}^t e_p(\xi \theta_i^s) \right| < t p^{-\delta_0} \quad (r = 1, 2)$$

where $\delta_0 = \delta_0(\gamma) > 0$.

We establish (3.17) again and continue verbatim the argument until invoking Proposition 2.

Assuming alternative (1.17), we obtain instead of (3.41) that

$$(5.10) \quad |\{s, s' = 1, \dots, t | \theta_1^s + c\theta_2^s = \theta_1^{s'} + c\theta_2^{s'}\}| > t^2 p^{-3\epsilon'}$$

for some $c \in \mathbb{F}_p^*$. Writing $s' = s + \bar{s}$, the equation becomes

$$(5.11) \quad (\theta_2 \theta_1^{-1})^s = c^{-1} \frac{\theta_1^{\bar{s}} - 1}{1 - \theta_2^{\bar{s}}}.$$

Since $s, \bar{s} \leq t < \min(0(\theta_1), 0(\theta_2), 0(\theta_2 \theta_1^{-1}))$, equation (5.11) has at most t solutions, contradicting (5.10).

6. THE CASE OF COMPOSITE MODULUS

The combinatorial methods introduced here (sum-product theorems) permit us to extend the results from [B-G-K] (in particular estimates on Gauss sums) and the results from this paper for sparse polynomials to the case of certain composite moduli q . More precisely, we assume the factorization of q involves only a bounded number of prime factors. Details will appear in [B-C].

If q factors as a (simple) product of a bounded number of distinct prime factors, i.e., $q = p_1 \cdots p_r$, the residue ring \mathbb{Z}_q identifies with $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$ and the argument simplifies significantly. It is basically an easy variant of the methods described earlier in the paper. In view of cryptographical applications (some of which are discussed in the next section), the special case where $q = p\ell$ with p, ℓ distinct primes, $p \sim \ell$, is of particular interest (such q are called Blum integers). Our first aim is to extend the proof of Theorem 2 to such moduli. The argument extends easily to products of several (boundedly many) distinct primes involving only notational complications.

Proposition 3. *Let $q = p.\ell$ with p, ℓ as above and $\theta_1, \dots, \theta_r \in \mathbb{Z}_q^*$ where \mathbb{Z}_q^* denotes the multiplicative group of \mathbb{Z}_q . Assume for some $\delta > 0$*

$$(6.1) \quad O_p(\theta_i) > q^\delta, O_\ell(\theta_i) > q^\delta \quad (1 \leq i \leq r),$$

$$(6.2) \quad O_p(\theta_i \theta_j^{-1}) > q^\delta, O_\ell(\theta_i \theta_j^{-1}) > q^\delta \quad (1 \leq i \neq j \leq r).$$

Then for $J > q^\delta$

$$(6.3) \quad \max_{a_1, \dots, a_r \neq 0 \pmod{p\ell}} \left| \sum_{j=1}^J e_q(a_1 \theta_1^j + \dots + a_r \theta_r^j) \right| < Jq^{-\delta'}$$

where $\delta' = \delta'(r, \delta) > 0$.

We first specify the identification of $\mathbb{Z}_{p\ell}$ and the product $\mathbb{Z}_p \times \mathbb{Z}_\ell$. Take $\alpha \in \mathbb{Z}_p$ s.t. $\alpha\ell = 1 \pmod{p}$ and $\beta \in \mathbb{Z}_\ell$ s.t. $\beta p = 1 \pmod{\ell}$. Denote by $\pi_p : \mathbb{Z}_{p\ell} \rightarrow \mathbb{Z}_p, \pi_\ell : \mathbb{Z}_{p\ell} \rightarrow \mathbb{Z}_\ell$ the quotient maps. If $a \in \mathbb{Z}_{p\ell}$, clearly

$$(6.4) \quad a = \pi_p(a)\ell\alpha + \pi_\ell(a)p\beta \pmod{p\ell}$$

providing a factorization of the identity on $\mathbb{Z}_{p\ell}$ as $\varphi \circ (\pi_p \times \pi_\ell)$ where $\varphi : \mathbb{Z}_p \times \mathbb{Z}_\ell \rightarrow \mathbb{Z}_{p\ell}$ is the ring isomorphism given by $\varphi(A, B) = A\ell\alpha + Bp\beta$. Writing $\frac{a}{p\ell} = \frac{\alpha A}{p} + \frac{\beta B}{\ell}$ ($A = \pi_p(a), B = \pi_\ell(a)$), we get for the exponential sum

$$(6.5) \quad \sum_{j \leq J} e_{p\ell} \left(\sum_{s=1}^r a_s \theta_s^j \right) = \sum_j e_p \left(\sum_s (\alpha A_s) \theta_s^j \right) e_\ell \left(\sum_s (\beta B_s) \theta_s^j \right).$$

Let us outline the proof of Proposition 3.

In order to treat the binomial case, we also need the sum-product result in $\mathbb{Z}_p \times \mathbb{Z}_\ell$, p, ℓ distinct primes. It turns out that the situation is even simpler than for $p = \ell$.

Lemma 8. *Let $S \subset \mathbb{Z}_p \times \mathbb{Z}_\ell$, where p, ℓ are distinct primes as above. Assume*

$$(6.6) \quad p^\delta < |S| < (p\ell)^{1-\delta}$$

and ($\varepsilon > 0$ assumed small enough depending on δ)

$$(6.7) \quad |S + S| + |S \cdot S| < |S|^{1+\varepsilon}$$

(addition and multiplication refer to the $\mathbb{Z}_p \times \mathbb{Z}_\ell$ (product) ring structure).

Then one of the following two alternatives holds:

$$(6.8) \quad |S \cap (\mathbb{Z}_p \times \{a\})| > p^{-\varepsilon'} |S| \text{ for some } a \in \mathbb{Z}_\ell,$$

$$(6.9) \quad |S \cap (\{a\} \times \mathbb{Z}_\ell)| > p^{-\varepsilon'} |S| \text{ for some } a \in \mathbb{Z}_p$$

where $\varepsilon' = \varepsilon'(\varepsilon) \rightarrow 0$ with $\varepsilon \rightarrow 0$.

Moreover, in case (6.8) (resp. (6.9)), $p^{1-\varepsilon'} < |S| < p^{1+\varepsilon'}$ (resp. $\ell^{1-\varepsilon'} < |S| < \ell^{1+\varepsilon'}$).

Notice that if $p \neq \ell$, we do not have to consider alternative (1.17) in Proposition 2.

Sketch of the proof. We follow essentially the same argument as when $p = \ell$ (see Section 2). Assume (6.8), (6.9) do not hold. We may in particular assume $S \subset \mathbb{Z}_p^* \times \mathbb{Z}_\ell^*$.

By (6.7), there is a subset $S_1 \subset S$ s.t. $|S_1| > p^{-C\varepsilon} |S|$ and

$$(6.10) \quad |kS_1^k| < p^{C\varepsilon} |S_1| < p^{C\varepsilon} (p\ell)^{1-\delta} < (p\ell)^{1-\delta+C\varepsilon} < (p\ell)^{1-\frac{\delta}{2}}$$

(here k is specified, depending on ε' , and the constant C depends on k).

Denote by $\pi_p : \mathbb{Z}_p \times \mathbb{Z}_\ell \rightarrow \mathbb{Z}_p$ and $\pi_\ell : \mathbb{Z}_p \times \mathbb{Z}_\ell \rightarrow \mathbb{Z}_\ell$ the projections. If (6.8) fails, $\max_a |S_1 \cap (\mathbb{Z}_p \times \{a\})| < p^{-\varepsilon'} |S| < p^{-\varepsilon'+C\varepsilon} |S_1| < p^{-\varepsilon'/2} |S_1|$ and hence $|\pi_\ell(S_1)| > p^{\varepsilon'/2}$. Similarly $|\pi_p(S_1)| > p^{\varepsilon'/2}$.

By the sum-product theorem in prime fields and Lemma 1 we may thus (replacing S_1 by $k_0 S_1^{k_0} = S_2$ for some $k_0 \in \mathbb{Z}_+$, depending on ϵ') assume

$$(6.11) \quad \pi_p(S_2) = \mathbb{Z}_p \text{ and } \pi_\ell(S_2) = \mathbb{Z}_\ell.$$

Suppose $|S_2| \geq p > \ell$. There are distinct elements $x_0 \neq x_1$ in S_2 s.t. $\pi_\ell(x_0) = \pi_\ell(x_1)$. Then by (6.11)

$$(6.12) \quad \begin{aligned} S_2^2 + (S_2 - S_2)S_2 &\supset S_2^2 + (x_0 - x_1)S_2 = S_2^2 + (\pi_p(x_0 - x_1)\pi_p(S_2) \times \{0\}) \\ &= S_2^2 + (\mathbb{Z}_p \times \{0\}) = \mathbb{Z}_p \times \mathbb{Z}_\ell \end{aligned}$$

and therefore

$$|2S_2^2 - S_2^2| = p\ell$$

contradicting (6.10).

Also, if (6.8), it follows from (6.7) and $|S| > p^\delta$ that $|S \cap (\mathbb{Z}_p \times \{a\})| > p^{1-\epsilon'}$; hence $p^{1-\epsilon'} < |S| < p^{1+\epsilon'}$.

This proves Lemma 8.

With Lemma 8 at hand, we obtain the exponential sum estimate.

Lemma 9. *Let p, ℓ be as above, $p \neq \ell$. Let $\theta \in \mathbb{Z}_p^*, \psi \in \mathbb{Z}_\ell^*$ satisfying for some $\delta > 0$*

$$\begin{aligned} O_p(\theta) &> p^\delta, \\ O_\ell(\psi) &> p^\delta. \end{aligned}$$

If $J > p^\delta, a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_\ell^*$, then

$$(6.13) \quad \left| \sum_{j=0}^J e_p(a\theta^j) e_\ell(b\psi^j) \right| < Jp^{-\delta'}$$

for some $\delta' = \delta'(\delta) > 0$.

The proof is similar to the argument explained in Section 3 but no condition on $\frac{\theta}{\psi}$ is involved, since (1.17) is not an issue here.

More generally, following the argument in Section 4, we get

Lemma 10. *Let p, ℓ be as above, $p \neq \ell$. Let $\theta_1, \dots, \theta_r \in \mathbb{Z}_p^*, \psi_1, \dots, \psi_s \in \mathbb{Z}_\ell^*$ satisfy for some $\delta > 0$*

$$(6.14) \quad O_p(\theta_i) > p^\delta \quad (1 \leq i \leq r), \quad O_p(\theta_i \theta_j^{-1}) > p^\delta \quad (1 \leq i \neq j \leq r)$$

and

$$(6.15) \quad O_\ell(\psi_i) > p^\delta \quad (1 \leq i \leq s), \quad O_p(\psi_i \psi_j^{-1}) > p^\delta \quad (1 \leq i \neq j \leq s).$$

Let $a_1, \dots, a_r \in \mathbb{Z}_p^*$ and $b_1, \dots, b_s \in \mathbb{Z}_\ell^*$. Let $J > p^\delta$. Then

$$(6.16) \quad \left| \sum_{j=1}^J e_p(a_1 \theta_1^j + \dots + a_r \theta_r^j) e_\ell(b_1 \psi_1^j + \dots + b_s \psi_s^j) \right| < Jp^{-\delta'}$$

with $\delta' = \delta'_{r+s}(\delta) > 0$.

As in the proof of Theorems 1 and 2 we proceed by induction on $r + s$. Again the case $r + s = 1$ follows from [B-G-K]. Let $r + s = 2$. There are three cases. If $r = 2$ or $s = 2$, we are in the situation $p = \ell$ discussed in Section 3. If $r = s = 1$, apply Lemma 9. The case $r + s \geq 3$ is treated inductively as in Section 4.

From the identification of $\mathbb{Z}_{p\ell}$ and $\mathbb{Z}_p \times \mathbb{Z}_\ell$, in particular (6.5), Proposition 3 follows from Lemma 10.

7. SOME APPLICATIONS TO UNIFORM DISTRIBUTION PROPERTIES OF POWER GENERATORS IN CRYPTOGRAPHY

We now discuss a few cryptographical applications related to the works [F-S], [F-P-S].

Let $q = p\ell$ with $p \neq \ell, p \sim \ell$ prime, be a Blum integer. Fix $e \in \mathbb{Z}_q^*$ and consider the sequence $\bar{u} = \{u_n\}$ defined by

$$u_{n+1} = u_n^e \text{ with initial } u_0 = \theta \in \mathbb{Z}_q^*.$$

If $e = 2$, \bar{u} is the Blum-Blum-Shub generator.

If $(e, (p-1)(\ell-1)) = 1$, \bar{u} is called an RSA generator.

Let $\lambda(q)$ be the smallest common multiple of $p-1, \ell-1$ (the Carmichael function). Denote $T = O_q(\theta)$ and $\tau = O_T(e)$. Thus $T|\lambda(q)$. Recall the result from [F-P-S] stating that almost surely in p, ℓ, θ, e we have

$$(7.1) \quad \tau \gg q^{1-\varepsilon}$$

for any fixed $\varepsilon > 0$.

From (7.1) and the results from [F-P-S], the authors deduce in [F-S] the uniform distribution of $\{u_0, \dots, u_{\tau-1}\} \pmod{q}$. Using Proposition 3, we establish also the joint distribution, i.e., the uniform distribution of $(u_n, u_{n+1}, \dots, u_{n+J-1})$ in \mathbb{Z}_q^J , for any fixed $J \geq 1$.

This will be an immediate consequence of the corresponding exponential sum estimate.

Proposition 4. *Assume p, ℓ, θ, e satisfy (7.1). Then for some $\delta > 0$*

$$(7.2) \quad \left| \sum_{n=0}^{\tau-1} e_q(a_0 u_n + a_1 u_{n+1} + \dots + a_{J-1} u_{n+J-1}) \right| < \tau q^{-\delta}$$

for all $(a_0, \dots, a_{J-1}) \in \mathbb{Z}_q^J \setminus \{0\}$.

Proof. Denote $A = \{u_n | n = 0, 1, \dots, \tau-1\} \subset G = \{\theta^j | 0 \leq j < T\} \subset \mathbb{Z}_q^*$ and denote by \mathcal{X}_A the indication function of A . Let $1 < V < \tau$ be an integer to specify and let $v = 0, 1, \dots, V$. Write

$$\begin{aligned} \sum_{n=0}^{\tau-1} e_q(\dots) &= \sum_{n=0}^{\tau-1} e_q(a_0 u_{n+v} + \dots + a_{J-1} u_{n+v+J-1}) + 0(V) \\ &= \frac{1}{V} \sum_{v=0}^{V-1} \sum_{n=0}^{\tau-1} e_q(a_0 u_n^{e^v} + \dots + a_{J-1} u_n^{e^{v+J-1}}) + 0(V) \\ (7.3) \quad &= \frac{1}{V} \sum_{v=0}^{V-1} \sum_{x \in G} e_q(a_0 x^{e^v} + \dots + a_{J-1} x^{e^{v+J-1}}) \mathcal{X}_A(x) + 0(V). \end{aligned}$$

In order to remove the restriction $x \in A$ in the first term of (7.3), proceed in the usual way. Thus estimate by

$$\frac{1}{V} |A|^{1/2} \left(\sum_{x \in G} \left| \sum_{v=0}^{V-1} e_q(\dots) \right|^2 \right)^{1/2} \leq \frac{1}{V} |A|^{1/2} (V|G| + (7.4))^{1/2}$$

where

$$(7.4) = \sum_{v_1 \neq v_2 < V} \left| \sum_{x \in G} e_q(a_0 x^{e^{v_1}} + \dots + a_{J-1} x^{e^{v_1+J-1}} - a_0 x^{e^{v_2}} - \dots - a_{J-1} x^{e^{v_2+J-1}}) \right|.$$

Rewrite the inner sum in (7.4) as

$$(7.5) \quad \sum_{s=0}^{T-1} e_q(a_0(\theta_0^s - \psi_0^s) + \dots + a_{J-1}(\theta_{J-1}^s - \psi_{J-1}^s))$$

where

$$(7.6) \quad \theta_j = \theta^{e^{v_1+j}} \text{ and } \psi_j = \theta^{e^{v_2+j}}.$$

In order to apply Proposition 3 to (7.5), we need to ensure that for some $\gamma > 0$

$$(7.7) \quad O_p(\theta_i), O_p(\psi_i) > p^\gamma \quad (\text{for all } i),$$

$$(7.8) \quad O_p(\theta_i \theta_j^{-1}), O_p(\psi_i \psi_j^{-1}) > p^\gamma \quad (i \neq j),$$

$$(7.9) \quad O_p(\theta_i \psi_j^{-1}) > p^\gamma \quad (\text{for all } i, j)$$

and similarly replacing p by ℓ .

By (7.6), these conditions are equivalent to

$$(7.10) \quad (e^{v_1+j}, p-1) < p^{1-\gamma},$$

$$(7.11) \quad (e^{v_2+j}, p-1) < p^{1-\gamma},$$

$$(7.12) \quad (e^{v_1+i} - e^{v_1+j}, p-1) < p^{1-\gamma} \quad (i \neq j),$$

$$(7.13) \quad (e^{v_1+i} - e^{v_2+j}, p-1) < p^{1-\gamma}$$

and similarly with p replaced by ℓ .

Conditions (7.10), (7.11) are obviously satisfied since $(e, p-1) = 1 = (e, \ell-1)$.

Also (7.12), (7.13) are equivalent to

$$(7.14) \quad (e^j - 1, p-1) < p^{1-\gamma} \quad (0 < j \leq J)$$

and

$$(7.15) \quad (e^{v_1-v_2+j} - 1, p-1) < p^{1-\gamma} \quad (|j| \leq J).$$

If $(e^w - 1, p-1) = \xi > p^{1-\gamma}, w \neq 0$, clearly

$$\#\{e^u \pmod{p-1}\} \leq |w| \cdot \frac{p-1}{\xi}$$

and recalling (7.1)

$$(7.16) \quad q^{1-\varepsilon} < O_T(e) \leq \#\{e^u \pmod{(p-1)(\ell-1)}\} < \left| \frac{w}{\xi} \right| q.$$

Therefore $|\xi| < q^\varepsilon |w|$ and $|w| > q^{\frac{1-\gamma}{2}-\varepsilon}$.

Take $\gamma = \frac{1}{2}$.

Thus (7.14) holds, since $j = w < J < q^{\frac{1}{4}-\varepsilon}$. Since

$$|v_1 - v_2 + j| \leq V + J,$$

choosing $V = \lceil q^{\frac{1}{5}} \rceil$ will also ensure (7.15) if $|v_1 - v_2| > J$.

Returning to (7.4), it follows from Proposition 3

$$(7.4) < V^2 |G|^{1-\delta'} + J.V |G|$$

where $\delta' = \delta'(\gamma) = \delta'(\frac{1}{4})$. Therefore

$$\begin{aligned}
 (7.3) &< \frac{1}{V} \tau^{1/2} (JV|G| + V^2|G|^{1-\delta'})^{1/2} + O(V) \\
 (7.17) \quad &\lesssim V^{-1/2} (\tau T)^{1/2} + \tau^{\frac{1}{2}} T^{\frac{1-\delta'}{2}} + O(V). \\
 &\lesssim q^{9/10} + q^{1-\frac{\delta'}{2}} < \tau q^{\varepsilon - (\frac{\delta'}{2} \wedge \frac{1}{10})}.
 \end{aligned}$$

This proves (7.2). □

Remark. Let us point out that instead of (7.1) it clearly suffices to assume that $T > q^\gamma$ for some $\gamma > 0$ and

$$\tau > T^{1-\varepsilon}$$

provided we may ensure (7.10)–(7.11) for ‘most’ pairs v_1, v_2 .

Next, we aim to establish an unconditional result for the Blum-Blum-Shub generator. First, we choose appropriate primes p, ℓ . Fix r and let p, ℓ be distinct primes of the form

$$(7.18) \quad p = 1 + c3^r,$$

$$(7.19) \quad \ell = 1 + d3^r$$

with $c, d \in \mathbb{Z}+$ and

$$(7.20) \quad p \sim \ell < 3^{20r}$$

(which exist by Linnik’s theorem).

Clearly $3^r | \lambda(q), q = p\ell$ and we take $\theta = u_0 \in \mathbb{Z}_q^*$ s.t.

$$(7.21) \quad O_q(\theta) = T = 3^r > q^{\frac{1}{20}}.$$

Hence

$$(7.22) \quad \tau = O_T(2) \sim T.$$

We verify conditions (7.10)–(7.13).

From (7.18)–(7.20)

$$(2^{v_1+j}, p-1) = (2^{v_1+j}, c3^r) = (2^{v_1+j}, c) < \frac{p}{3^r} < p^{19/20}.$$

Condition (7.14) is obviously satisfied. We verify (7.15).

Let $(2^w - 1, p-1) = \xi > p^{1-\gamma}, w \neq 0$. Again

$$(7.23) \quad 3^r \lesssim \{2^u \pmod{3^r}\} < \#\{2^u \pmod{p-1}\} < |w| \frac{p-1}{\xi} < p^\gamma |w|;$$

hence

$$|w| > p^{\frac{1}{20} - \gamma}.$$

The same holds with p replaced by ℓ .

It suffices thus to choose $\gamma = \frac{1}{40}$ and $V = [q^{\frac{1}{50}}]$ in (7.17). We proved

Proposition 5. *Take p, ℓ distinct primes as in (7.18)–(7.20) and let $u_0 = \theta$ satisfy (7.22). Thus the Blum-Blum-Shub generator $\{u_n\}$ satisfies (7.2) (for any fixed J) and hence \bar{u} is jointly uniformly distributed.*

REFERENCES

- [B] J. Bourgain, *Estimates on exponential sums related to the Diffie–Hellman distributions*, to appear in GAFA.
- [B-C] J. Bourgain, M.-C. Chang, *Exponential sum estimates over subgroups and almost subgroups of \mathbb{Z}_q^* where q is composite with few prime factors*, submitted to Geom. Funct. Anal.
- [B-G-K] J. Bourgain, A. Glibichuk, S. Konyagin, *Estimate for the number of sums and products and for exponential sums in fields of prime order*, submitted to J. London Math. Soc.
- [B-K] J. Bourgain, S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, CR Acad. Sci., Paris 337 (2003), no 2, 75–80. MR1998834 (2004g:11067)
- [B-K-T] J. Bourgain, N. Katz, T. Tao, *A sum-product theorem in finite fields and applications*, Geom. Funct. Anal. 14 (2004), no. 1, 27–57. MR2053599
- [C-P1] T. Cochrane, C. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. 133 (2005), no. 2, 313–320 (electronic). MR2093050
- [C-P2] ———, *Stepanov’s method applied to binomial exponential sums*, Quart. J. Math. 54 (2003), No 3, 243–255. MR2013138 (2004k:11136)
- [F-P-S] J. Friedlander, C. Pomerance, I. Shparlinsky, *Period of the power generator and small values of the Carmichael function*, Math. Comp. 70 (2001), no. 236, 1591–1605. MR1836921 (2002g:11112)
- [F-S] J. Friedlander, I. Shparlinsky, *On the distribution of the power generator*, Math. Comp., Vol. 70, No. 236, (2001), 1575–1589. MR1836920 (2002f:11107)
- [Go] T. Gowers, *A new proof of Szemerédi’s theorem for arithmetic progressions of length 4*, GAFA 8 (1998), no. 3, 529–551. MR1631259 (2000d:11019)
- [K-S] S. Konyagin, I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge UP, Cambridge (1999). MR1725241 (2000h:11089)
- [Mor] L.J. Mordell, *On a sum analogous to a Gauss sum*, Quart. J. Math. 3 (1932), 161–162.
- [Na] M. Nathanson, *Additive Number Theory*, Springer-Verlag, NY, 1996. MR1395371 (97e:11004); MR1477155 (98f:11011)

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540