Mh. Math. 93, 63—74 (1982)

Monatshefte für
Mathematik

On Cubic Polynomials
I. Hua's Estimate of Exponential Sums

By

Wolfgang M. Schmidt*, Boulder, Colorado

(Received 14 July 1981)

Abstract. HUA and CHEN gave estimates of sums $\sum_{x=1}^{q} e(\mathfrak{F}(x))$ where $e(z) = e^{2\pi iz}$ and $\mathfrak{F}$ is a polynomial of the type $f(x)/q$ where $f(x) = a_k x^k + \cdots + a_1 x$ with integer coefficients having gcd $(q, a_k, \ldots, a_1) = 1$. But no good estimates hold for these sums when q is small in comparison to k. We therefore consider here a related but different class of polynomials. Special emphasis is given to the cubic case.

In subsequent papers of this series we shall deal with cubic exponential sums in many variables and with p-adic and rational zeros of systems of cubic forms.

1. Introduction. Let $A_k(q)$ be the set of polynomials $\mathfrak{F}(x) = f(x)/q$ where $f(x) = a_k x^k + \cdots + a_1 x$ has integer coefficients. Let $A_k^*(q)$ be the subset where gcd $(q, a_k, \ldots, a_1) = 1$. For a polynomial $\mathfrak{F} \in A_k^*(q)$, put

$$S(\mathfrak{F}) = q^{-1} \sum_{x=1}^{q} e(\mathfrak{F}(x)). \tag{1.1}$$

HUA [2] proved that

$$|S(\mathfrak{F})| \leqslant c(k)\, q^{-1/k}, \tag{1.2}$$

and CHEN [1] gave upper bounds for $c(k)$, e. g., $c(3) \leqslant e^{18.3}$ and $c(k) \leqslant e^{4k}$ when $k \geqslant 10$. It is not our intention here to improve upon the subtle estimates of HUA and of CHEN.

The trivial upper bound for $|S(\mathfrak{F})|$ is 1, and (1.2) is better than this trivial bound only if $q > c(k)^k$. It lies in the nature of the sums that for certain small values of q only the trivial bound holds. For example, if $k = q = p$, a prime, then $\mathfrak{F}(x) = (x^p - x)/p$ lies in $A_k^*(q)$, and $S(\mathfrak{F}) = 1$.

* Partially supported by NSF contract NSF-MCS-8015356.

0026—9255/82/0093/0063/$ 02.40

We believe that for certain applications the classes $A_k(q)$ and $A_k^*(q)$ are not the right ones, and we proceed to define new classes $B_k(q)$ and $B_k^*(q)$.

Only the values of $\mathfrak{F}(x)$ modulo 1 are of interest for the exponential sums. Let H be the factor group $\mathbb{Q}/\mathbb{Z}$ of the rationals modulo the integers. A *polynomial of degree* $\leqslant k$ for us will mean an expression

$$\mathfrak{F}(x) = x^k \alpha_k + \cdots + x\,\alpha_1$$

with coefficients $\alpha_k, \ldots, \alpha_1$ in H. Such a polynomial defines a map from $\mathbb{Z}$ into H. We shall say that $\mathfrak{F}$ *has period* q if $\mathfrak{F}(x+q) = \mathfrak{F}(x)$ for each $x \in \mathbb{Z}$. The smallest positive period of $\mathfrak{F}$ will be called its *order*. The periods of $\mathfrak{F}$ are then precisely the multiples of its order.

Write $B_k(q)$ for the class of polynomials of degree $\leqslant k$ with period q, and $B_k^*(q)$ for the subclass of polynomials of order q. For $\mathfrak{F} \in B_k(q)$ define $S(\mathfrak{F})$ by (1.1), and put

$$M_k(q) = \max_{\mathfrak{F} \in B_k^*(q)} |S(\mathfrak{F})|.$$

Theorem 1. *$M_k(q)$ is multiplicative in q, i.e. $M_k(q_1 q_2) = M_k(q_1) M_k(q_2)$ if q_1, q_2 are coprime.*

Theorem 2. *$M_k(q) \leqslant c(k) q^{-1/k}$, with the same constant $c(k)$ as in* (1.2).

It follows that $M_k(q) \leqslant q^{-1/(2k)}$ if $q \geqslant c(k)^{2k}$. A function $\mathfrak{F}$ in $B_k^*(q)$, where $q > 1$ is not a constant, hence has $|S(\mathfrak{F})| < 1$. There are only finitely many $q < c(k)^{2k}$, and it follows from (2.3) below that each set $B_k^*(q)$ contains only finitely many essentially different functions. It follows that there is a constant $\theta_k > 0$ such that

$$M_k(q) \leqslant q^{-\theta_k} \tag{1.3}$$

for all q. We will give a very crude estimate for θ_k.

Theorem 3. *We have* (1.3) *with $\theta_k = k^{-12k}$.*

The polynomials in $B_1^*(q)$ are linear and the corresponding exponential sums are character sums on the additive group $\mathbb{Z}/q\mathbb{Z}$. Hence $M_1(q) = 0$ if $q > 1$. On the other hand, the sums estimated by $M_2(q)$ are Gaussian sums. By the theory of these sums, or by Theorem 5 of [3], we have

$$M_2(q) \leqslant q^{-1/2}.$$

Hence we may take $\theta_2 = 1/2$. For subsequent application to p-adic cubic equations it will be important to estimate $M_3(q)$.

Theorem 4. *$M_3(q) \leqslant q^{-\theta_3}$ where $\theta_3 = 0.1142\ldots$ is given by*

$$2^{-\theta_3} = \cos(\pi/8). \tag{1.4}$$

The value θ_3 ist best possible, for $\mathfrak{F} = (3x^3/4) + (x^2/8) + (x/4)$ has period $q = 2$ and $|S(\mathfrak{F})| = \cos(\pi/8)$. Therefore $M_3(2) = 2^{-\theta_3}$.

The estimates for small values of q are cumbersome to get. I had thought that it could never happen to me, but I now have to admit that a few minutes on an Apple II computer were used to estimate $M_3(q)$ for certain small values of q.

2. The Multiplicativity of $M_k(q)$. Given polynomials $\mathfrak{F}, \mathfrak{G}$ in $B_k(q)$, write $\mathfrak{F} \sim \mathfrak{G}$ if $\mathfrak{F}(x) = \mathfrak{G}(x)$ for each $x \in \mathbb{Z}$. For example, the polynomials $\mathfrak{F} = \overline{(1/4)}\, x^2 + \overline{(1/4)}\, x$ (where the bar denotes the class in $H = \mathbb{Q}/\mathbb{Z}$) and $\mathfrak{G} = \overline{(3/4)}\, x^2 + \overline{(3/4)}\, x$ in $B_2(4)$ are equivalent. Let $C_k(q)$ and $C_k^*(q)$ respectively be the sets of equivalence classes in $B_k(q)$ and in $B_k^*(q)$.

Lemma 1. *$C_k(q)$ has cardinality $|C_k(q)| = q^k$.*

Proof. When $k = 1$, our polynomials are $x\alpha$, and period q means that $q\alpha = 0$ in H. So $\alpha = \overline{(a/q)}$ where $a = 0, 1, \ldots, q-1$. This gives q distinct polynomials.

Now if $\mathfrak{F}(x)$ is of degree $\leqslant k$ where $k > 1$, then

$$\mathfrak{G}(x) = \mathfrak{F}(x) - \mathfrak{F}(x-1)$$

is of degree $\leqslant k-1$ and lies in $B_{k-1}(q)$, or does it? Well, $B_{k-1}(q)$ contains only polynomials with constant term zero. So

$$\mathfrak{G}(x) = \mathfrak{G}_0(x) + \alpha,$$

where $\mathfrak{G}_0 \in B_{k-1}(q)$ and α is a constant. There are q^{k-1} possible equivalence classes for $\mathfrak{G}_0$. For $x > 0$ we have

$$\mathfrak{F}(x) = \sum_{j=1}^{x} \mathfrak{G}(j) = \sum_{j=1}^{x} \mathfrak{G}_0(j) + x\alpha. \tag{2.1}$$

The condition $\mathfrak{F}(x+q) = \mathfrak{F}(x)$ means that

$$\sum_{j=x+1}^{x+q} \mathfrak{G}_0(j) + q\alpha = 0.$$

Since $\mathfrak{G}_0$ has period q, this condition simply says that

$$\sum_{j=1}^{q} \mathfrak{G}_0(j) + q\alpha = 0. \tag{2.2}$$

This gives q possibilities for $\alpha \in H = \mathbb{Q}/\mathbb{Z}$. For each $\mathfrak{G}_0 \in B_{k-1}(q)$ and each α with (2.2), the polynomial of degree $\leqslant k$ defined by (2.1) has $\mathfrak{F}(x+q) = \mathfrak{F}(x)$ for $x > 0$. Since the polynomial, having coefficients in H, must have some period, it does in fact have the period q.

Hence $|C_k(q)| = q^{k-1} \cdot q = q^k$, and the lemma is established.

We remark that in view of

$$\sum_{d|q} |C_k^*(d)| = |C_k(q)| = q^k,$$

Moebius' inversion formula yields

$$|C_k^*(q)| = \sum_{d|q} \mu(d)(q/d)^k = q^k \prod_{p|q}(1 - p^{-k}). \tag{2.3}$$

Thus $|C_k(q)| = |A_k(q)|$ and $|C_k^*(q)| = |A_k^*(q)|$.

Lemma 2. *The values of polynomials $\mathfrak{F}$ in $C_k(q)$ are of the type $\overline{(a/q^k)}$.*

Proof. One may essentially repeat the argument of Lemma 1. In the induction step, we note that each value $\mathfrak{G}_0(j)$ is of the form $\overline{(b/q^{k-1})}$, and (2.2) shows that $\alpha = \overline{(c/q^k)}$. Thus by (2.1) the values of $\mathfrak{F}$ are of the type $\overline{(a/q^k)}$.

If $q = q_1 q_2$ with coprime q_1, q_2 and if $\mathfrak{F}_i \in C_k(q_i)$ $(i = 1, 2)$, then (with an obvious addition of polynomial classes)

$$\mathfrak{F}(x) = \mathfrak{F}_1(x) + \mathfrak{F}_2(x) \tag{2.4}$$

lies in $C_k(q)$, and may uniquely be written as such a sum of polynomial classes. Since $q^k = q_1^k q_2^k$, it follows that each polynomial class $\mathfrak{F}$ of $C_k(q)$ may uniquely be written in this way. Similarly, $\mathfrak{F}$ in $C_k^*(q)$ may uniquely be written as a sum (2.4) where $\mathfrak{F}_i \in C_k^*(q)$ $(i = 1, 2)$.

Now

$$S(\mathfrak{F}) = q^{-1} \sum_{x=1}^{q} e(\mathfrak{F}(x)) = q_1^{-1} q_2^{-1} \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e(\mathfrak{F}(a x_1 + b x_2))$$

where

$$a \equiv \begin{cases} 1 \pmod{q_1}, \\ 0 \pmod{q_2}, \end{cases} \qquad b \equiv \begin{cases} 0 \pmod{q_1}, \\ 1 \pmod{q_2}. \end{cases}$$

We obtain

$$S(\mathfrak{F}) = q_1^{-1} q_2^{-1} \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e(\mathfrak{F}_1(a x_1 + b x_2) + \mathfrak{F}_2(a x_1 + b x_2)) =$$

$$= (q_1^{-1} \sum_{x_1=1}^{q_1} e(\mathfrak{F}_1(a x_1)) \; (q_2^{-1} \sum_{x_2=1}^{q_2} e(\mathfrak{F}_2(b x_2))) =$$

$$= S(\mathfrak{F}_1) S(\mathfrak{F}_2).$$

Theorem 1 follows.

3. The Sets $B_k(p^l)$. In view of multiplicativity, we will restrict ourselves to the case when $q = p^l$, a prime power. Let $\hat{B}_k(p^l)$ consist of the polynomials of $B_k(p^l)$ whose coefficients have denominators which are powers of p, i. e. which are of the form $\overline{(a/p^n)}$. In particular, $\hat{B}_k(p^0)$ consists of the polynomials $\mathfrak{F}$ whose coefficients are of this form, and which have $\mathfrak{F}(x) = 0$ for $x \in \mathbb{Z}$. For example, $(1/2)x^2 + (1/2)x$ lies** in $\hat{B}_2(2^0)$.

Lemma 3. *Every element of $B_k(p^l)$ is equivalent to an element of $\hat{B}_k(p^l)$.*

Proof. Write $\mathfrak{F} \in B_k(p^l)$ in the form $\mathfrak{F}(x) = f(x)/m$ where f has integer coefficients. Say $m = p^n r$ where p does not divide r. Then

$$\mathfrak{F}(x) = \frac{f(x)/r}{p^n}.$$

By Lemma 2, the values of $\mathfrak{F}$ are of the form a/p^{lk}. Hence $f(x) \equiv 0 \pmod r$ for $x \in \mathbb{Z}$. Since p does not divide r, there is a polynomial $g(x)$ such that in $f(x) - r g(x)$ each coefficient is divisible by p^n, so that $f(x) \equiv r g(x) \pmod{p^n r = m}$ for $x \in \mathbb{Z}$. Thus $\mathfrak{F}$ is equivalent to $g(x)/p^n \in \hat{B}_k(p^l)$.

Lemma 4. *If $p > k$, then $\hat{B}_k(p^l)$ consists precisely of the polynomials $f(x)/p^l$ where f has integer coefficients.*

Therefore when $p > k$, the set $\hat{B}_k(p^l)$ is the same as the set of polynomials $A_k(p^l)$ considered by HUA and CHEN.

Proof. Since $p > k$, it is easily seen that if $f(x)/p^n \sim 0$, then each coefficient of f is $\equiv 0 \pmod{p^n}$, so that $f(x)/p^n = 0$. Therefore different

** For convenience we will omit bars such as in $\overline{(1/2)}$.

polynomials (they are different if their coefficients in $H = \mathbb{Q}/\mathbb{Z}$ are different) $f(x)/p^n$ lie in different equivalence classes. The p^{lk} polynomials $f(x)/p^l$ lie in $\hat{B}_k(p^l)$, and they represent all the p^{lk} classes in $C_k(p^l)$. Hence they constitute all the polynomials in $\hat{B}_k(p^l)$.

Lemma 5. *Suppose $p = k$. Then*

(i) $\hat{B}_k(p^0)$ *consists of the p polynomials*

$$(a/p)(x^p - x). \tag{3.1}$$

(ii) $\hat{B}_k(p^l)$ *where $l \geqslant 1$ consists of the p^{lk+1} polynomials*

$$(a_p/p^{l+1})x^p + (a_{p-1}/p^l)x^{p-1} + \cdots + (a_1/p^l)x. \tag{3.2}$$

Proof. The polynomials (3.1) certainly lie in $\hat{B}_k(p^0)$, but are they all? If $f(x)/p^n$ lies in $\hat{B}_k(p^0)$ and if $f(x) = a_p x^p + \ldots + a_1 x$, then $f(x) \equiv 0 \pmod{p^n}$ for $x \in \mathbb{Z}$, which implies $a_p + a_1 \equiv 0 \pmod{p}$ and $a_{p-1} \equiv \ldots \equiv a_2 \equiv 0 \pmod{p}$. When $n = 1$, this gives exactly the polynomials (3.1). When $n > 1$, then $f(p) \equiv 0 \pmod{p^2}$ yields $a_1 p \equiv \equiv 0 \pmod{p^2}$, so that $a_1 \equiv 0 \pmod{p}$ and hence each coefficient $a_j \equiv 0 \pmod{p}$. Therefore n may be replaced by $n - 1$, etc. Thus (i) is established.

As for (ii), it follows from Lemma 3 and from (i) that $|\hat{B}_k(p^l)| = p\,|C_k(p^l)| = p^{lk+1}$. But the polynomials (3.2) clearly do lie in $\hat{B}_k(p^l)$.

Finally we deal with the special case $k = 3$, $p = 2$:

Lemma 6. (i) $\hat{B}_3(2^0)$ *consists of the 2^2 polynomials*

$$(a/2)x^3 + (b/2)x^2 + (c/2)x \tag{3.3}$$

with $a + b + c \equiv 0 \pmod 2$.

(ii) $\hat{B}_3(2)$ *consists of the 2^5 polynomials*

$$(a/4)x^3 + (b/8)x^2 + (c/4)x \tag{3.4}$$

with $a \equiv b \equiv c \pmod 2$.

(iii) $\hat{B}_3(2^l)$ *where $l \geqslant 2$ consists of the 2^{3l+2} polynomials*

$$(a/2^{l+1})x^3 + (b/2^{l+2})x^2 + (c/2^l)x \tag{3.5}$$

with $a \equiv b \pmod 2$.

Proof. If $(ax^3 + bx^2 + cx)/2^n$ lies in $\hat{B}_3(2^0)$, then

$$ax^3 + bx^2 + cx \equiv 0 \pmod{2^n} \text{ for } x \in \mathbb{Z},$$

whence $a+b+c \equiv 0 \pmod 2$. When $n>1$, then the values $x=1,2,3$ yield $a+b+c \equiv 2c \equiv -a+b-c \pmod 4$, which gives $a \equiv b \equiv c \equiv 0 \pmod 2$, and n may be replaced by $n-1$. Hence the polynomials (3.3) are indeed all the polynomials belonging to $\hat{B}_3(2^0)$.

It is clear that $|\hat{B}_3(2)| = |\hat{B}_3(2^0)||C_3(2)| = 2^{2+3} = 2^5$. On the other hand it is easy to check that the polynomials (3.4) do belong to $\hat{B}_3(2)$: If $\mathfrak{F}$ is a polynomial (3.4), then for $x \in \mathbb{Z}$ the values in $H = \mathbb{Q}/\mathbb{Z}$ satisfy

$$\mathfrak{F}(x+2) = (a/4)(x+2)^3 + (b/8)(x+2)^2 + (c/4)(x+2) =$$
$$= \mathfrak{F}(x) + \tfrac{1}{2}(ax^2+bx) + \tfrac{1}{2}(b+c) = \mathfrak{F}(x).$$

The argument for (iii) is similar.

4. Proof of Theorems 2 and 3. A polynomial $\mathfrak{F}$ may be written as

$$\mathfrak{F}(x) = f(x)/m \tag{4.1}$$

where $f(x) = a_k x^k + \cdots + a_1 x$ has $\gcd(m, a_k, \ldots, a_1) = 1$. The function (4.1) has period m. Hence if $\mathfrak{F}$ has order q, then $q \mid m$. Thus for $\mathfrak{F} \in B_k^*(q)$ we have $q \mid m$ and

$$S(\mathfrak{F}) = q^{-1} \sum_{x=1}^{q} e(\mathfrak{F}(x)) = m^{-1} \sum_{x=1}^{m} e(f(x)/m).$$

HUA's estimate (1.2) yields

$$|S(\mathfrak{F})| \leqslant c(k) m^{-1/k} \leqslant c(k) q^{-1/k},$$

i. e. Theorem 2.

For the proof of Theorem 3 we may suppose that $k \geqslant 3$. We may restrict ourselves to prime powers. By the argument just given in the proof of Theorem 2, the estimates of CHEN and of HUA apply. CHEN [1, Theorem 1] gives

$$M_k(p^l) \leqslant p^{-l/k} \text{ if } p \geqslant (k-1)^{2k/(k-2)},$$
$$M_k(p^l) < k^2 p^{-l/k} \text{ for any } p.$$

The first inequality is certainly true if $p \geqslant k^4$. The second inequality yields

$$M_k(p^l) < p^{-l/3k}$$

if $p^l \geqslant k^{3k}$. We therefore are left with the cases when

$$p < k^4 \text{ and } p^l < k^{3k}. \tag{4.2}$$

By Lemma 2, the values of $\mathfrak{F}(x)$ where $\mathfrak{F} \in B_k(p)$ are of the form a/p^k. We have $\mathfrak{F}(0) = 0$, and for $\mathfrak{F} \in B_k^*(p)$ some value is $\neq 0$, i. e. is a/p^k with $a \not\equiv 0 \pmod{p^k}$. Therefore

$$M_k(p) \leqslant p^{-1}(p - 2 + |e(0) + e(a/p^k)|) \leqslant 1 - (2/p) + (2/p)\cos(\pi/p^k)$$
$$= 1 - (4/p)\sin^2(\pi/2p^k) \leqslant 1 - (4/p)(4/\pi^2)(\pi^2/4p^{2k}) = 1 - (4/p^{2k+1}).$$

Now if $\mathfrak{F} \in B_k^*(p^l)$, then

$$S(\mathfrak{F}) = \frac{1}{p^{l-1}} \sum_{j=1}^{p^{l-1}} \left(\frac{1}{p} \sum_{x=1}^{p} e(\mathfrak{F}_j(x)) \right)$$

where $\mathfrak{F}_j(x) = \mathfrak{F}(j + p^{l-1}x)$. Each $\mathfrak{F}_j$ has period p, and there must be some $\mathfrak{F}_j$ of order p. For this $\mathfrak{F}_j$, the estimate $|S(\mathfrak{F}_j)| \leqslant 1 - (4/p^{2k+1})$ holds. It follows that

$$|S(\mathfrak{F})| \leqslant (1/p^{l-1})(p^{l-1} - (4/p^{2k+1})) = 1 - (4/p^{2k+l}).$$

The conditions (4.2) yield

$$M_k(p^l) \leqslant 1 - (4/p^{2k+l}) \leqslant 1 - (4/k^{8k+3k}) <$$
$$< e^{-1/k^{11k}} < (k^{3k})^{-1/k^{12k}} < p^{-l/k^{12k}}.$$

5. $M_3(p^l)$ for $p \geqslant 3$. Define $\theta' = \theta(p)$ and $\theta'' = \theta''(p)$ by $M_3(p) = p^{-\theta'}$ and by $\theta'' = 2^{-1}(1 - (\log 2/\log p))$, and put

$$\theta = \theta(p) = \min(\tfrac{1}{3}, \theta', \theta''). \tag{5.1}$$

Lemma 7. $M_3(p^l) \geqslant p^{-\theta l}$.

Proof. The case $l = 1$ follows from the definition of θ'. For $l \geqslant 2$, a polynomial $\mathfrak{F} \in \hat{B}_3^*(p^l)$ is of the form

$$\mathfrak{F}(x) = p^{-l} f(x)$$

with $f(x) = ax^3 + bx^2 + cx$. Here when $p > 3$, the coefficients a, b, c are integers with $(p, a, b, c) = 1$ by Lemma 4. On the other hand when $p = 3$, then $3a, b, c$ are integers with $(3, 3a, b, c) = 1$ by Lemma 5. In either case, the derivative $f'(x) = 3ax^2 + 2bx + c$ has integer coefficients with $(p, 3a, 2b, c) = 1$.

We observe that

$$S(\mathfrak{F}) = p^{-l} \sum_{j=1}^{p^{l-1}} \sum_{x=1}^{p} e(\mathfrak{F}_j(x)) \tag{5.2}$$

where $\mathfrak{F}_j(x) = \mathfrak{F}(j + p^{l-1}x)$. Taylor expansion yields

$$\mathfrak{F}_j(x) = \mathfrak{F}(j) + \frac{f'(j)}{p}x + \tfrac{1}{2}p^{l-2}f''(j)x^2 + \tfrac{1}{6}p^{2l-3}f'''(j)x^3.$$

The coefficients of x^2 and of x^3 are integers, and therefore the inner sum in (5.2) vanishes unless $f'(j) \equiv 0 \pmod{p}$.

So let $\mathfrak{J}$ be the set of solutions of this congruence; clearly $|\mathfrak{J}| \leqslant 2$. Now

$$S(\mathfrak{F}) = p^{-1}\sum_{j\in\mathfrak{J}} S(\mathfrak{G}_j)$$

where $\mathfrak{G}_j(x) = \mathfrak{F}(j + p\,x)$. The expansion is

$$\mathfrak{G}_j(x) = \mathfrak{F}(j) + \frac{f'(j)}{p^{l-1}}x + \frac{2^{-1}f''(j)}{p^{l-2}}x^2 + \frac{6^{-1}f'''(j)}{p^{l-3}}x^3.$$

In the case when $|\mathfrak{J}| = 2$, each $j \in \mathfrak{J}$ has $f'(j) \equiv 0$ but $f''(j) \not\equiv 0 \pmod{p}$, and $\mathfrak{G}_j$ has order $\geqslant p^{l-2}$. An induction argument gives $|S(\mathfrak{G}_j)| \leqslant p^{-\theta(l-2)}$ and

$$|S(\mathfrak{F})| \leqslant (2/p)p^{-\theta(l-2)} = p^{-2\theta''-\theta(l-2)} \leqslant p^{-\theta l}.$$

In the case when $|\mathfrak{J}| = 1$, the only situation which might be different is when $f'(j) \equiv f''(j) \equiv 0 \pmod{p}$. But then $f'''(j) \not\equiv 0 \pmod{p}$. When $p > 3$, then $\mathfrak{G}_j$ is of order $\geqslant p^{l-3}$ by Lemma 4. In the case when $p = 3$, the coefficient of x^3 in $\mathfrak{G}_j$ is $2^{-1}f'''(j)/3^{l-2}$, and the order is $\geqslant p^{l-3}$ by Lemma 5. So the induction gives $|S(\mathfrak{G}_j)| \leqslant p^{-\theta(l-3)}$, and

$$|S(\mathfrak{F})| \leqslant p^{-1}p^{-\theta(l-3)} \leqslant p^{-\theta l}.$$

The proof of Lemma 7 is complete.

Lemma 8.

(i) $M_3(3^l) \leqslant 3^{-\theta(3)l}$ *where* $\theta(3) = 0.1543\ldots$,

(ii) $M_3(p^l) \leqslant p^{-l/5}$ *when* $p \geqslant 5$,

(iii) $M_3(p^l) \leqslant p^{-l/3}$ *when* $p > 64$.

Proof. By Lemma 5 the elements of $\hat{B}(3)$ are of the form $(a/9)x^3 + (b/3)x^2 + (c/3)x$. The 3^3 polynomials $(a/9)x^3 + (b/3)x^2$ with $0 \leqslant a < 9$, $0 \leqslant b < 3$ are a complete set of inequivalent polynomials. Either $a \not\equiv 0 \pmod 3$. Then

$$|S(\mathfrak{F})| \leqslant 3^{-1}(1 + |e(\mathfrak{F}(1)) + e(\mathfrak{F}(-1))|) =$$
$$= 3^{-1}(1 + 2|\cos(2a\pi/9)|) \leqslant 3^{-1}(1 + 2\cos(2\pi/9)).$$

Equality holds for $\mathfrak{F}(x) = x^3/9$. Or $a \equiv 0 \pmod 3$ and the values of $\mathfrak{J}$ are multiples of $1/3$. For $\mathfrak{F} \in \hat{B}_3^*(3)$ there is some value $d/3$ with $d \not\equiv 0 \pmod 3$. Therefore

$$|S(\mathfrak{J})| \leqslant 3^{-1}(1 + |e(0) + e(d/3)|) \leqslant 3^{-1}(1 + 2\cos(\pi/3)) <$$
$$< 3^{-1}(1 + 2\cos(2\pi/9)).$$

Hence $M_3(3) = 3^{-1}(1 + 2\cos(2\pi/9))$ and $\theta'(3) = 0.1543\ldots$. It follows that $\theta(3) = \theta'(3)$, and assertion (i) holds.

Similarly, one sees directly, or with short computer time, that

$$\theta'(5) = 0.201006\ldots \text{ (assumed for } (x^3 - x)/5),$$

$$\theta'(7) = 0.200253\ldots \text{ (assumed for } x^3/7).$$

Hence $\theta(5) = \theta'(5) > 1/5$ and $\theta(7) = \theta'(7) > 1/5$. For $p \geqslant 11$, the formula (5.1) reduces to $\theta = \min(\theta', 1/3)$. Since $M_3(p) \leqslant 2p^{-1/2}$ according to Weil, we have

$$\theta' \geqslant (1/2) - (\log 2/\log p) \geqslant (1/2) - (\log 2/\log 11) > 1/5.$$

This proves the second assertion of the lemma.

Finally, for $p > 64$, $\theta' > (1/2) - (\log 2/\log 64) = 1/3$, and $\theta(p) = 1/3$.

6. $M_3(2^l)$.

Lemma 9. *$M_3(2^l) \leqslant 2^{-\theta l}$, where $\theta = \theta(2) = 0.1142\ldots$ is given by $2^{-\theta} = \cos(\pi/8)$.*

Proof. We commence by showing that

$$M_3(2) = \cos(\pi/8). \tag{6.1}$$

By Lemma 6, the polynomials in $\hat{B}_3(2)$ are of the form $(a/4)x^3 + (b/8)x^2 + (c/4)x$ with $a \equiv b \equiv c \pmod 2$. For $\mathfrak{F} \in \hat{B}_3^*(2)$ we have $\mathfrak{F}(1) \neq 0$, hence $\mathfrak{F}(1) = d/8$ with $d \not\equiv 0 \pmod 8$. So $|S(\mathfrak{F})| = 2^{-1}|1 + e(d/8)| = |\cos(\pi d/8)| \leqslant \cos(\pi/8)$. Equality holds when $a = 3$, $b = c = 1$, and (6.1) is established.

By Lemma 6 again, $\hat{B}_3(2^3)$ consists of the 2^{11} polynomials $(a/16)x^3 + (b/32)x^2 + (c/8)x$ with $a \equiv b \pmod 2$. These are the polynomials

$$\mathfrak{F}(u, v, w, d; x) = d\left(\frac{x^3}{16} + \frac{x^2}{32}\right) + \frac{ux^3}{8} + \frac{vx^2}{16} + \frac{wx}{8} \tag{6.2}$$

with $0 \leqslant d < 2$, $0 \leqslant u < 8$, $0 \leqslant v < 16$, $0 \leqslant w < 8$. Modulo the 2^2

polynomials in $\hat{B}_3(2^0)$ we get $2^9 = |C_3(2^3)|$ inequivalent polynomials with

$$0 \leqslant d < 2, \quad 0 \leqslant u < 4, \quad 0 \leqslant v < 8, \quad 0 \leqslant w < 8. \tag{6.3}$$

The polynomial (6.2) lies in $\hat{B}_3(3)$ precisely if

$$d = 0 \text{ and } u \equiv 0 \pmod 2 \text{ and } u \equiv v \equiv w \pmod 4. \tag{6.4}$$

The $2^9 - 2^3$ inequivalent polynomials in $\hat{B}_3^*(2^2)$ and $\hat{B}_3^*(2^3)$ are the polynomials (6.2) with (6.3) but not (6.4). My son Hannes computed the maximum of $|S(\mathfrak{F})|$ for these polynomials on a computer. The maximum is $0.6932\ldots < 2^{-1/2}$ and is assumed e. g. for $\mathfrak{F}(3,5,2,0;x) \in \hat{B}_3^*(3^2)$. Thus $M_3(2^2), M_3(2^3) < 2^{-1/2}$, and the lemma is true for $l = 2, 3$.

Suppose now that $l \geqslant 4$. By Lemma 6, the polynomials of $\hat{B}_3(2^l)$ are

$$\mathfrak{F}(x) = 2^{-l} f(x) \text{ with } f(x) = \frac{a}{2}x^3 + \frac{b}{4}x^2 + cx,$$

where a, b, c are integers with $a \equiv b \pmod 2$. We note that

$$\begin{aligned} f'(x) &= \tfrac{1}{2}(3ax^2 + bx) + c, \\ f''(x) &= 3ax + \tfrac{1}{2}b, \\ f'''(x) &= 3a. \end{aligned}$$

We have

$$S(\mathfrak{F}) = 2^{-l} \sum_{j=1}^{2^{l-1}} \sum_{x=1}^{2} e(\mathfrak{F}_j(x)) \tag{6.5}$$

where $\mathfrak{F}_j(x) = \mathfrak{F}(j + 2^{l-1}x)$. Taylor expansion gives

$$\mathfrak{F}_j(x) = \mathfrak{F}(j) + \frac{f'(j)}{2}x + 2^{l-3}f''(j)x^2 + 2^{2l-4}3^{-1}f'''(j)x^3.$$

Since $l \geqslant 4$, the coefficients of x^2 and x^3 are integers. Thus the inner sum in (6.5) is zero unless $f'(j) \equiv 0 \pmod 2$, i. e.

$$3aj^2 + bj + 2c \equiv 0 \pmod 4. \tag{6.6}$$

Now if $a \equiv b \equiv 0 \pmod 2$, say if $a = 2a^*, b = 2b^*$, the congruence becomes $a^*j^2 + b^*j + c \equiv 0 \pmod 2$, or

$$(a^* + b^*)j + c \equiv 0 \pmod 2.$$

For $\mathfrak{F} \in \hat{B}_3^*(2^l)$ it cannot happen that $a^* + b^* \equiv c \equiv 0 \pmod 2$. Hence

there is at most one $j \pmod 2$ with $f'(j) \equiv 0 \pmod 2$. If there is such a j, then

$$S(\mathfrak{F}) = 2^{-1} \cdot 2^{1-l} \sum_{x=1}^{2^{l-1}} e(\mathfrak{G}(x)) = 2^{-1} S(\mathfrak{G})$$

where

$$\mathfrak{G}(x) = \mathfrak{F}(j + 2x) = \mathfrak{F}(j) + \frac{f'(j)}{2^{l-1}} x + \frac{f''(j)}{2^{l-1}} x^2 + \frac{3^{-1} f'''(j)}{2^{l-2}} x^3.$$

Now $a^* \equiv b^* \equiv 0 \pmod 2$ together with $f'(j) \equiv 0 \pmod 2$ would yield $c \equiv 0 \pmod 2$, which cannot happen. Hence not both a^* and b^* are $\equiv 0 \pmod 2$, and we cannot have both $f''(j) \equiv 0 \pmod 2$ and $f'''(j) \equiv 0 \pmod 4$. Comparing this fact with Lemma 6 we see that $\mathfrak{G}$ is of order $\geqslant 2^{l-4}$. By induction,

$$|S(\mathfrak{F})| \leqslant 2^{-1} 2^{-\theta(l-4)} < 2^{-\theta l}.$$

In the case when $a \equiv b \equiv 1 \pmod 2$, not both j and $j+2$ can be solutions of (6.6). So if $\mathfrak{J}$ is the set of numbers $j \pmod 4$ with (6.6), then $|\mathfrak{J}| \leqslant 2$. We have

$$S(\mathfrak{F}) = 2^{-l} \sum_{j \in \mathfrak{J}} \sum_{x=1}^{2^{l-2}} e(\mathfrak{G}_j(x)) = 2^{-2} \sum_{j \in \mathfrak{J}} S(\mathfrak{G}_j)$$

where

$$\mathfrak{G}_j(x) = \mathfrak{F}(j + 4x) = \mathfrak{F}(j) + \frac{f'(j)}{2^{l-2}} x + \frac{2f''(j)}{2^{l-2}} x^2 + \frac{3^{-1} f'''(j)}{2^{l-5}} x^3.$$

The assumption $b \equiv 1 \pmod 2$ yields $2f''(j) \equiv 1 \pmod 2$, so that $\mathfrak{G}_j$ has order $\geqslant 2^{l-4}$ by Lemma 6. By induction,

$$|S(\mathfrak{F})| \leqslant 2^{-2} \cdot 2 \cdot 2^{-\theta(l-4)} < 2^{-\theta l}.$$

References

[1] CHEN, JING R.: On Professor Hua's estimate of exponential sums. Sci. Sinica **20**, 711—719 (1977).

[2] HUA, L. K.: Additive prime number theory. (Chinese.) Peking: Science Press. 1957.

[3] SCHMIDT, W. M.: Simultaneous p-adic zeros of quadratic forms. Mh. Math. **90**, 45—65 (1980).

Prof. Dr. W. M. SCHMIDT
Mathematics Department, Box 426
University of Colorado
Boulder, CO 80309, U.S.A.