ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 5, 2006

CONGRUENCES AND RATIONAL EXPONENTIAL SUMS WITH THE EULER FUNCTION

WILLIAM D. BANKS AND IGOR E. SHPARLINSKI

ABSTRACT. We give upper bounds for the number of solutions to congruences with the Euler function $\varphi(n)$ modulo an integer $q \geq 2$. We also give nontrivial bounds for rational exponential sums with $\varphi(n)/q$.

1. Introduction. Let $\varphi(n)$ denote the Euler function:

$$\varphi(n) = \#\{1 \leq a \leq n \mid \gcd(a, n) = 1\}.$$

For any integer $q \geq 2$, let $\mathbf{e}_q(z)$ denote the exponential function $\exp(2\pi i z/q)$, which is defined for all $z \in \mathbf{R}$.

In this paper, we give upper bounds for rational exponential sums of the form

$$S_a(x, q) = \sum_{n \leq x} \mathbf{e}_q(a\varphi(n)),$$

where $\gcd(a, q) = 1$, and x is sufficiently large. Our results are nontrivial for a wide range of values for the parameter q. In the special case where $q = p$ is a prime number, however, stronger results have been obtained in [**1**].

One of the crucial ingredients of [**1**] is an upper bound on the number solutions of a congruence with the Euler function. To be more precise, let $T(x, q)$ denote the number of positive integers $n \leq x$ such that $\varphi(n) \equiv 0 \pmod{q}$. The results of [**1**] are based on the bound

$$T(x, p) = O\left(\frac{x \log\log x}{p}\right) \tag{1}$$

which is a partial case of [**4**, Theorem 3.5].

Here we obtain an upper bound on $T(x, q)$, albeit weaker than (1), and we follow the approach of [**1**] to estimate the sums $S_a(x, q)$.

Received by the editors on December 19, 2003, and in revised form on March 22, 2004.

As in [**1**], we expect that our methods can be suitably modified to obtain nontrivial bounds for more general exponential sums. For instance, one should be able to estimate sums of the form

$$S_f(x,q) = \sum_{n\le x} \mathbf{e}_q(f(\varphi(n))),$$

where $f(X)$ is a polynomial with integer coefficients and positive degree.

Throughout the paper, the implied constants in the symbols "O," "$\gg$" and "$\ll$" are absolute (we recall that the notations $U \ll V$ and $V \gg U$ are equivalent to the statement that $U = O(V)$ for positive functions U and V). We also use the symbol "o" with its usual meaning: the statement $U = o(V)$ is equivalent to $U/V \to 0$.

As usual, p always denotes a prime number.

2. Preliminary estimates. The following estimate is well known, see [**8**, Chapter 1, Theorem 5.1]:

$$\frac{n}{\log\log n} \ll \varphi(n) \le n. \tag{2}$$

Let $\tau_w(n)$ be the number of representations of n as a product of w positive integers:

$$\tau_w(n) = \#\{(n_1,\dots,n_w) \in \mathbf{N}^w \mid n = n_1 n_2 \cdots n_w\}.$$

In particular, $\tau(n) = \tau_2(n)$ is the number of positive integer divisors of n. If $\omega(n)$ denotes the number of distinct prime divisors of n, then clearly

$$\tau(n) \ge 2^{\omega(n)}. \tag{3}$$

Let $N(x,w)$ be the number of positive integers $n \le x$ such that $\omega(n) > w$. Very precise results about the asymptotic behavior of $N(x,w)$ have been derived in [**5**]; for our purposes, however, the following estimate is sufficient:

$$N(x,w) \ll 2^{-w} x \log x. \tag{4}$$

To see this, we first observe that (3) implies

$$N(x,w) = \sum_{\substack{n\le x\\ \omega(n)>w}} 1 < \sum_{\substack{n\le x\\ \omega(n)>w}} \frac{\tau(n)}{2^w} \le 2^{-w}\sum_{n\le x}\tau(n).$$

The estimate (4) then follows from the well-known expansion, see [**9**, Section I.3.2, Theorem 2]:

$$\sum_{n\le x}\tau(n) = x(\log x + 2\gamma - 1) + O(x^{1/2}),$$

where γ is the Euler-Mascheroni constant.

We also need the following upper bound from [**10**]:

$$\tau_w(n) \le \exp\left(\frac{(\log n)(\log w)}{\log\log n}\left(1 + O\left(\frac{\log\log\log n + \log w}{\log\log n}\right)\right)\right), \tag{5}$$

which is valid for all $n, w \ge 2$.

For any integer $n \ge 2$, let $P(n)$ denote the largest prime divisor of n, and put $P(1) = 1$. As usual, we say that an integer $n \ge 1$ is Y-smooth if and only if $P(n) \le Y$. Let

$$\psi(X,Y) = \#\{1 \le n \le X \mid n \text{ is } Y\text{-smooth}\}.$$

The following estimate is a substantially relaxed and simplified version of Corollary 1.3 of [**6**]; see also [**3**].

Lemma 1. *Let $u = (\log X)/(\log Y)$. For any $u \to \infty$ with $u \le Y^{1/2}$, we have*

$$\psi(X,Y) \ll X u^{-u+o(u)}.$$

Now let $T(x,w,q)$ denote the number of positive integers $n \le x$ such that $\omega(n) \le w$ and $\varphi(n) \equiv 0 \pmod q$.

Lemma 2. *The bound*

$$T(x,w,q) \ll x(c\,\log\log x)^{w-1}\left(\frac{\tau_w(q)\tau(q)}{q}\right)^{1/2}$$

holds for some absolute constant $c > 0$.

Proof. Let $T(x,y,w,q)$ denote the number of positive integers $n \le x$ such that $\omega(n) \le w$, $\varphi(n) \equiv 0 \pmod q$, and if $n = s^2 m$, then $s \le y$. Clearly,

$$T(x,w,q) \le T(x,y,w,q) + \sum_{s>y} \sum_{\substack{n \le x \\ s^2 \mid n}} 1 = T(x,y,w,q) + O(x/y). \tag{6}$$

Let $R(x,w,q)$ denote the number of positive *squarefree* integers $m \le x$ such that $\omega(m) \le w$ and $\varphi(m) \equiv 0 \pmod q$.

If $n \le x$, $n = s^2 m$, $\varphi(n) \equiv 0 \pmod q$ and m is squarefree, then it follows that $\varphi(m) \equiv 0 \pmod d$ for some divisor $d \mid q$ with $d \ge q/s^2$. Indeed, put $d = \gcd(\varphi(m), q)$. Since m is squarefree, we see that $\varphi(m) \mid \varphi(n)$; hence, $\operatorname{lcm}(\varphi(m), q) \mid \varphi(n)$, and thus

$$\frac{\varphi(m)\, q}{d} = \operatorname{lcm}(\varphi(m), q) \le \varphi(n) = s^2 m \prod_{p \mid sm} (1 - 1/p) \le s^2 \varphi(m).$$

This shows that $d \ge q/s^2$, as claimed. As a consequence, we now derive that

$$T(x,y,w,q) \le \sum_{s \le y} \sum_{\substack{d \mid q \\ d \ge q/s^2}} R(x/s^2, w, d). \tag{7}$$

It is therefore sufficient to estimate $R(x,w,q)$ for all integers $w, q \ge 1$ and all $x > 0$.

Now, fix a factorization of q into $\nu \le w$ factors:

$$q = q_1 \cdots q_\nu. \tag{8}$$

We proceed to estimate the number $Q(x; q_1, \ldots, q_\nu)$ of squarefree $m \le x$ of the form $m = p_1 \cdots p_\nu$, where p_j is prime with $p_j \equiv 1 \pmod{q_j}$, $j = 1, \ldots, \nu$.

By the bound (3.1) from [**4**] (see also [**2**, Lemma 1]) and estimate (2), it follows that for any positive integer r and any real number $y \ge r$, the bound

$$\sum_{\substack{p \le y \\ p \equiv 1 \pmod r}} \frac{1}{p} \le \frac{c\,(\log\log y)^2}{r} \tag{9}$$

holds for some absolute constant $c > 0$, and it also holds when $r > y \geq 1$ since, in that case, the sum on the left-hand side is empty.

We now prove by induction on ν that, with the same constant $c > 0$, the bound

$$Q(x; q_1, \ldots, q_\nu) \leq \frac{x(c \log\log x)^{2(\nu-1)}}{q_1 \cdots q_\nu} \tag{10}$$

holds. For $\nu = 1$, this is obvious since

$$Q(x; q_1) \leq \frac{x}{q_1}.$$

We also have

$$Q(x; q_1, \ldots, q_\nu) \leq \sum_{\substack{p_\nu \leq x \\ p_\nu \equiv 1 \pmod{q_\nu}}} Q(x/p_\nu; q_1, \ldots, q_{\nu-1}).$$

Then, using the inductive hypothesis for $\nu - 1 \geq 1$, we obtain that

$$Q(x; q_1 \cdots q_\nu) \leq \frac{x(c \log\log x)^{2(\nu-2)}}{q_1 \cdots q_{\nu-1}} \sum_{\substack{p_\nu \leq x \\ p_\nu \equiv 1 \pmod{q_\nu}}} \frac{1}{p_\nu},$$

hence the estimate (9) yields the bound (10).

Considering all possible factorizations (8), we derive from (10) the following bound:

$$R(x, w, q) \leq \tau_w(q) \, \frac{x(c \log\log x)^{2(w-1)}}{q}. \tag{11}$$

Finally, after applying the estimate (11), with appropriate changes in the parameters, to the bound (7), we see that

$$\begin{aligned} T(x, y, w, q) &\leq x(c \log\log x)^{2(w-1)} \sum_{s \leq y} \sum_{\substack{d \mid q \\ d \geq q/s^2}} \frac{\tau_w(d)}{s^2 d} \\ &\leq \frac{xy\,(c \log\log x)^{2(w-1)} \tau_w(q) \tau(q)}{q}. \end{aligned}$$

Choosing

$$y = \left(\frac{q}{(c \log\log x)^{2(w-1)} \tau_w(q) \tau(q)} \right)^{1/2}$$

in order to balance both terms in (6), we obtain the stated result. $\square$

Finally, our principal tool is the following bound for exponential sums over prime numbers, which follows immediately from [**11**, Theorem 2] by partial summation, see also [**1**].

Lemma 3. *For any $X \ge 2$, the following bound holds*:

$$\max_{\gcd(c,q)=1} \left| \sum_{p \le X} \mathbf{e}_q(cp) \right| \ll (q^{-1/2} + X^{-1/4} q^{1/8} + q^{1/2} X^{-1/2}) X \log^3 X.$$

3. Congruences with the Euler function. As before, we denote by $T(x,q)$ the number of positive integers $n \le x$ such that $\varphi(n) \equiv 0 \pmod{q}$.

Theorem 1. *For some absolute constant $\delta > 0$, the bound*

$$T(x,q) \ll x\, 2^{-(\log q)^{\delta}}$$

holds for all $q \ge \exp((\log\log x)^{2/\delta})$ provided that x is sufficiently large.

Proof. Using (4) and Lemma 2, we have for any $w \ge 1$:

$$(12) \qquad \begin{aligned} T(x,q) &\le T(x,w,q) + N(x,w) \\ &\ll x (c \log\log x)^{(w-1)} \left(\frac{\tau_w(q)\tau(q)}{q} \right)^{1/2} + 2^{-w} x \log x. \end{aligned}$$

According to (5), for some absolute constant $c_0 > 0$, the bound

$$\tau_w(q) \le \exp\left(\frac{(\log q)(\log w)}{\log\log q} \left(1 + c_0 \left(\frac{\log\log\log q + \log w}{\log\log q} \right) \right) \right)$$

holds for all $q, w \geq 2$. Choose δ such that $\delta(1 + c_0\delta) = 1/2$, say, and put $w = \lfloor 2(\log q)^{\delta} \rfloor$; it follows that $\tau_w(q) \leq q^{1/2+o(1)}$. Remarking that

$$(w - 1) \log(c \log\log x) = o(\log q),$$

we see that the first term in (12) is bounded by $xq^{-1/4+o(1)}$; since $w = o(\log q)$, this term is dominated by $2^{-w} x \log x$. For q in the specified range, we also have

$$\log\log x \leq (\log q)^{\delta/2} = o(w),$$

and the result follows. $\square$

On the other hand, we remark that by [**7**, Lemma 2], almost all values of $\varphi(n)$, $1 \leq n \leq x$, are divisible by all prime powers p^r with

$$p^r \ll \frac{\log\log x}{\log\log\log x}.$$

Therefore, for some constant $\alpha > 0$ and all q with

$$q \leq \exp\left(\alpha \frac{\log\log x}{\log\log\log x}\right),$$

one has $T(x, q) = x + o(x)$.

4. Exponential sums with the Euler function. We now show that the same arguments used in [**1**] combined with the bound of Lemma 2 can be used to estimate exponential sums with the Euler function.

Theorem 2. *For some absolute constant $\delta > 0$, the bound*

$$\max_{\gcd(a,q)=1} |S_a(x, q)| \ll x\Big(v^{-2v/5+o(v)} + 2^{-(\log q)^{\delta}}\Big)$$

holds with $v = (\log x)/(\log q)$ provided that

$$v \leq \frac{\log x}{(\log\log x)^{2/\delta}}.$$

Proof. Let $\delta > 0$ be the constant from Theorem 1; replacing δ by a smaller value if necessary, we can assume that $\delta < 1/(8 \log 2)$. Without loss of generality, we can also assume that $q \geq \log^8 x$ since the bound is trivial otherwise. Throughout the proof, fix a with $\gcd(a, q) = 1$. We define $y = q^{5/2}$ and denote by $\mathcal{E}_1$ the set of $n \leq x$ which are y-smooth. Let

$$u = \frac{\log x}{\log y} = 2v/5.$$

It is easy to see that, if $v \geq q$, then $q \leq \log x$ and the bound is trivial; thus, we can assume that $u \leq q \leq y^{1/2}$. Hence, by Lemma 1, we have that

$$\#\mathcal{E}_1 \ll x u^{-u+o(u)}.$$

Denote by $\mathcal{E}_2$ the set of $n \leq x$ for which $P(n) > y$ and $P(n)^2 \mid n$. Then

$$\#\mathcal{E}_2 \ll \sum_{p \geq y} x/p^2 \ll x/y = xq^{-5/2}.$$

Put $w = \lfloor 5(\log q)^\delta \rfloor$ and denote by $\mathcal{E}_3$ the set of $n \leq x$ with $\omega(n) \geq w + 1$. By (4), we see that

$$\#\mathcal{E}_3 \ll 2^{-w} x \log x.$$

Finally, let $\mathcal{N} = \{1, \ldots, N\} \backslash (\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3)$, where $N = \lfloor x \rfloor$.

From the preceding bounds, it follows that

$$S_a(x, q) = \sum_{n \in \mathcal{N}} \mathbf{e}_q(a\varphi(n)) + O\Big(xu^{-u+o(u)} + xq^{-5/2} + 2^{-w} x \log x\Big). \tag{13}$$

For the remainder of the proof, we denote by $\mathcal{P}$ the set of all prime numbers, $\mathcal{P}[Y, X]$ the set of $p \in \mathcal{P}$ with $Y < p \leq X$, and $\mathcal{P}[X] = \mathcal{P}[1, X]$.

Now every integer $n \in \mathcal{N}$ has a unique representation of the form $n = mp$, where $p \in \mathcal{P}[y, x]$ and $p > P(m)$. Conversely, if $\mathcal{M}$ is the set of $m \leq x/y$ such that $\omega(m) \leq w$ and $L_m = \max\{y, P(m)\}$, then for any $m \in \mathcal{M}$ and any $p \in \mathcal{P}[L_m, x/m]$, we have $n = mp \in \mathcal{N}$. Then, observing that $\varphi(n) = \varphi(m)(p-1)$, we obtain

$$\begin{aligned}\sum_{n\in\mathcal{N}} \mathbf{e}_q(a\varphi(n)) &= \sum_{m\in\mathcal{M}} \sum_{p\in\mathcal{P}[L_m,x/m]} \mathbf{e}_q(a\varphi(mp)) \\ &= \sum_{m\in\mathcal{M}} \mathbf{e}_q(-a\varphi(m)) \sum_{p\in\mathcal{P}[L_m,x/m]} \mathbf{e}_q(a\varphi(m)p).\end{aligned}$$

For any divisor $d \mid q$, denote by $\mathcal{M}_d$ the set of $m \in \mathcal{M}$ with $\gcd(q,\varphi(m)) = d$. Then

$$\sum_{n\in\mathcal{N}} \mathbf{e}_q(a\varphi(n)) \ll \sum_{d\mid q} \sum_{m\in\mathcal{M}_d} \left| \sum_{p\in\mathcal{P}[L_m,x/m]} \mathbf{e}_q(a\varphi(m)p)\right|. \tag{14}$$

Write

$$\begin{aligned}&\sum_{p\in\mathcal{P}[L_m,x/m]} \mathbf{e}_q(a\varphi(m)p) \\ &\qquad = \sum_{p\in\mathcal{P}[x/m]} \mathbf{e}_q(a\varphi(m)p) - \sum_{p\in\mathcal{P}[L_m]} \mathbf{e}_q(a\varphi(m)p),\end{aligned}$$

and observe that the right-hand side of the bound in Lemma 3 is a monotonically increasing function of X. Then, since $m \le x/y$ for all $m \in \mathcal{M}$, it follows that for all $m \in \mathcal{M}_d$,

$$\begin{aligned}&\sum_{p\in\mathcal{P}[L_m,x/m]} \mathbf{e}_q(a\varphi(m)p) \\ &\ll \frac{x}{m}\Big((q/d)^{-1/2} + x^{-1/4}m^{1/4}(q/d)^{1/8} + (q/d)^{1/2}x^{-1/2}m^{1/2}\Big)\log^3 x \\ &\ll \frac{x}{m}\Big((q/d)^{-1/2} + (q/d)^{1/8}y^{-1/4} + (q/d)^{1/2}y^{-1/2}\Big)\log^3 x \\ &\ll \frac{x}{m}\Big(q^{-1/2}d^{1/2} + q^{1/8}y^{-1/4} + q^{1/2}y^{-1/2}\Big)\log^3 x.\end{aligned}$$

Recalling the definition of y, we see that the first term always dominates; therefore,

$$\sum_{p\in\mathcal{P}[L_m,x/m]} \mathbf{e}_q(a\varphi(m)p) \ll \frac{xd^{1/2}\log^3 x}{mq^{1/2}}.$$

We now derive that

$$\sum_{m\in\mathcal{M}_d}\left|\sum_{p\in\,\mathcal{P}[L_m,x/m]}\mathbf{e}_q(a\varphi(m)p)\right| \ll \frac{xd^{1/2}\log^3 x}{q^{1/2}}\sum_{m\in\mathcal{M}_d}\frac{1}{m}.$$

By Lemma 2 and partial summation, we have

$$\begin{aligned}\sum_{m\in\mathcal{M}_d}\frac{1}{m} &\ll \sum_{1\le m\le x/y}\left(\frac{1}{m}-\frac{1}{m+1}\right)T(m,w,d)+\frac{y}{x}\,T(x/y,w,d)\\ &\ll \sum_{1\le m\le x/y}\frac{1}{m}\,(c\,\log\log m)^{w-1}\left(\frac{\tau_w(d)\tau(d)}{d}\right)^{1/2}\\ &\quad+\ (c\,\log\log x)^{w-1}\left(\frac{\tau_w(d)\tau(d)}{d}\right)^{1/2}\\ &\ll (c\,\log\log x)^{w-1}\left(\frac{\tau_w(q)\tau(q)}{d}\right)^{1/2}\log x.\end{aligned}$$

Hence,

$$\sum_{m\in\mathcal{M}_d}\left|\sum_{p\in\,\mathcal{P}[L_m,x/m]}\mathbf{e}_q(a\varphi(m)p)\right| \ll xq^{-1/2}(c\,\log\log x)^{w-1}(\tau_w(q)\tau(q))^{1/2}\log^4 x.$$

Summing up over all divisors $d \mid q$ and recalling (14), we obtain

$$\sum_{m\in\mathcal{M}}\left|\sum_{p\in\,\mathcal{P}[L_m,x/m]}\mathbf{e}_q(a\varphi(m)p)\right| \ll xq^{-1/2}(c\,\log\log x)^{w-1}\tau_w(q)^{1/2}\tau(q)^{3/2}\log^4 x.$$

Now, from (13) we derive

$$\begin{aligned}S_a(x,q) \ll x\Big(&u^{-u+o(u)}+2^{-w}\log x\\ &+q^{-1/2}(c\,\log\log x)^{w-1}\tau_w(q)^{1/2}\tau(q)^{3/2}\log^4 x\Big).\end{aligned}$$

Recalling the choice of w, we see (as in the proof of Theorem 1) that under the condition of the theorem, both the second and the third terms inside the parentheses are dominated by $2^{-(\log q)^{\delta}}$, which finishes the proof. $\square$

5. Remarks. Sums with multiplicative characters might also be considered; in principle, our methods should provide nontrivial bounds in certain ranges, similar to those of Theorem 2.

Finally, we mention that our methods can be applied to the sum of divisors function $\sigma(n)$. However, it is still not clear how to estimate exponential sums with the Carmichael function $\lambda(n)$, even given its close relationship to the Euler function. We recall that $\lambda(n)$ is defined as the largest possible order of elements of the unit group in the residue ring modulo n. More explicitly, for a prime power p^k we define

$$\lambda(p^k) = \begin{cases} p^{k-1}(p-1) & \text{if } p \geq 3 \text{ or } k \leq 2; \\ 2^{k-2} & \text{if } p = 2 \text{ and } k \geq 3; \end{cases}$$

and finally,

$$\lambda(n) = \operatorname{lcm}\left(\lambda(p_1^{k_1}), \dots, \lambda(p_\nu^{k_\nu})\right),$$

where

$$n = p_1^{k_1} \cdots p_\nu^{k_\nu}$$

is the prime number factorization of m.

REFERENCES

1. W. Banks and I.E. Shparlinski, *Congruences and exponential sums with the Euler function*, in *High primes and misdemeanours*: *Lectures in honour of the 60th birthday of Hugh Cowie Williams*, Amer. Math. Soc., Providence, 2004, pp. 49–59.

2. N.L. Bassily, I. Kátai and M. Wijsmuller, *On the prime power divisors of the iterates of the Euler-ϕ function*, Publ. Math. Debrecen **55** (1999), 17–32.

3. B.C. Berndt, H.G. Diamond, H. Halberstam and A. Hildebrand, *On a problem of Oppenheim concerning "Factorisatio Numerorum"*, J. Number Theory **17** (1983), 1–28.

4. P. Erdős, A. Granville, C. Pomerance and C. Spiro, *On the normal behaviour of the iterates of some arithmetic functions*, in *Analytic number theory*, Birkhäuser, Boston, 1990, pp. 165–204.

5. A. Hildebrand and G. Tenenbaum, *On the number of prime factors of an integer*, Duke Math. J. **56** (1988), 471–501.

6. ———, *Integers without large prime factors*, J. Théor. Nombres Bordeaux **5** (1993), 411–484.

7. F. Luca and C. Pomerance, *On some problems of Mąkowski-Schinzel and Erdős concerning the arithmetical functions φ and σ*, Colloq. Math. **92** (2002), 111–130.

8. K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

9. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, University Press, Cambridge, UK, 1995.

10. L.P. Usol'tsev, *On an estimate for a multiplicative function*, in *Additive problems in number theory*, Kuybyshev. Gos. Ped. Inst., Kuybyshev, 1985, pp. 34–37 (in Russian).

11. R.C. Vaughan, *Mean value theorems in prime number theory*, J. London Math. Soc. **10** (1975), 153–162.

Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
E-mail address: bbanks@math.missouri.edu

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au