Bull. Math. Soc. Sci. Math. Roumanie
Tome 56(104) No. 3, 2013, 267–279

Congruences Characterizing the Bicrossproduct of Cyclic Groups

by
N.C. Bonciocat, M. Cipu, M.-T. Tsai, and A. Zaharescu

Dedicated to Professors Toma Albu and Constantin Năstăsescu on the occasion of their 70th birthdays

Abstract

We study congruences characterizing the matching of cyclic groups by automorphisms, obtain necessary and sufficient conditions such that the congruences have non-trivial solutions in both symmetric and general cases, and discuss various properties of some related congruences.

Key Words: Prime number, congruence, bicrossproduct.
2010 Mathematics Subject Classification: Primary: 11A07; Secondary: 11A41, 11A51.

1 Introduction

In 1981, Takeuchi [7] introduced the matched pair concept and the corresponding bicrossproduct, characterizing in terms of group actions the groups which can be expressed as internal products of two subgroups with trivial intersection. In [2], necessary and sufficient conditions for a pair of groups to be matched by automorphisms were obtained, and the following number-theoretical equivalent condition for a pair of finite cyclic groups to be matched by automorphisms was derived.

Proposition 1 ([2, Prop. 2.6])**.** *Let H and K be cyclic groups of orders n and m, respectively. The pair (H,K) can be matched by automorphisms if and only if there exist two integers $a \in [1,n)$ and $b \in [1,m)$ such that:*

$$\begin{cases} b^n \equiv 1 \pmod m, a^m \equiv 1 \pmod n, \\ b^{a-1} \equiv 1 \pmod m, a^{b-1} \equiv 1 \pmod n. \end{cases} \tag{1.1}$$

More precisely, each pair of automorphisms that match the two groups corresponds to a pair (a,b) which is a solution to the system of congruences (1.1). Clearly, for any orders n and m, a trivial solution $a = b = 1$ always exists. Furthermore, if one of them, say $a = 1$, then

the only equation yet to be solved is $b^n \equiv 1 \pmod{m}$, and it is clear that a solution $b > 1$ exists if and only if $\gcd(n, \varphi(m)) > 1$. So a natural thing to do is to focus on the solutions where both a and b are greater than 1, which would be referred to as the non-trivial solutions of congruence (1.1). The goal of this paper is to derive conditions such that congruence (1.1) has a non-trivial solution, and some related problems.

First in Section 2, we consider a special case of congruence (1.1), where we have $n = m$ and $a = b$. If that case, we say that (H, K) may be symmetrically matched by automorphisms if and only if

$$\begin{cases} a^n \equiv 1 \pmod{n}, \\ a^{a-1} \equiv 1 \pmod{n}, \end{cases} \tag{1.2}$$

has a solution $a \in [1, n)$. Again $a = 1$ is considered as the trivial solution. We will give a characterization for those numbers n that bear a non-trivial solution. Surprisingly those are exactly the numbers such that the first line of congruence (1.2) has a non-trivial solution. Therefore, it is worth considering the second line of congruence (1.2) independently, and in Section 3 we shall see that this congruence has the curious property that the absence of nontrivial solutions forces n to be a prime number.

Then in Section 4, we will derive a characterization for those pairs of numbers (n, m) for which congruence (1.1) has a non-trivial solution, and finally, in Section 5, we discuss results related to the existence of non-trivial solutions to the second line of congruence (1.1).

2 Cyclic groups symmetrically matched by automorphisms

In this section we study the system of equations (1.2). It turns out that the system of two equations (1.2) has such a solution, if and only if the first equation

$$a^n \equiv 1 \pmod{n} \tag{2.1}$$

has such a solution. Recall that a number n is called a cyclic number if any of the following equivalent characterizations holds:

(1) Congruence (2.1) has no solution $a \in (1, n)$.

(2) $\gcd(n, \varphi(n)) = 1$.

(3) n is square-free, and for any prime factors p, q of n, we have $p \nmid q - 1$.

Szele [6] proved that a number n is a cyclic number if and only if there is only one group (which is cyclic) up to isomorphism with order n. Erdős [5] showed that the number of cyclic numbers up to x is

$$(1 + o(1)) \frac{xe^{-\gamma}}{\log\log\log x}.$$

We shall prove the following theorem.

Theorem 1. *Congruence* (1.2) *has a solution* $a \in (1, n)$ *if and only if* n *is not a cyclic number.*

Proof: (Necessity) By characterization (1), if congruence (1.2) has a solution $a \in (1, n)$, then n must not be a cyclic number.

(Sufficiency) We will use characterization (3) to construct a particular solution. First assume that n is not square-free, say $n = p^k m$ where p is a prime, $k \geq 2$ and $(m, p) = 1$. Then we take $a = p^{k-1}m + 1$. It follows that $3 \leq a \leq n/2 + 1 \leq n - 1$ since $n \geq 4$, so indeed $a \in (1, n)$. Now

$$a^n = (p^{k-1}m + 1)^n = \sum_{t=0}^{n} \binom{n}{t} (p^{k-1}m)^t,$$

and since $n \mid (p^{k-1}m)^t$ for $t \geq 2$, it is clear that $a^n \equiv n \cdot p^{k-1}m + 1 \equiv 1 \pmod{n}$. Similarly,

$$a^{a-1} = (p^{k-1}m + 1)^{p^{k-1}m} \equiv p^{k-1}m \cdot p^{k-1}m + 1 \equiv 1 \pmod{n}.$$

We remark that, by exactly the same argument, we can also show that $a = \varphi(p^k)m + 1$ is also a solution in this case. This will be used later.

Next, assume that n is square-free, whose prime factors are $p_1, \ldots, p_t$, with $p_2 \mid p_1 - 1$. By the last assumption, there are elements (mod p_1) such that the order of each of them modulo p_1 is p_2. Let b be such an element, and let a be the least positive solution of the following Chinese Remainder equations

$$\begin{cases} a \equiv b \pmod{p_1}, \\ a \equiv 1 \pmod{p_i} \text{ for all } i \neq 1. \end{cases}$$

Clearly $a > 1$ since $b \not\equiv 1 \pmod{p_1}$. It follows by our choice of a that $a^{a-1} \equiv 1 \pmod{p_i}$ and $a^n \equiv 1 \pmod{p_i}$ are both trivial for $i \neq 1$. Also, since $a \equiv 1 \pmod{p_2}$ and $p_2 \mid n$, it is also clear that $a^{a-1} \equiv 1 \pmod{p_1}$ and $a^n \equiv 1 \pmod{p_1}$ by the choice of b. □

Since the existence of a nontrivial solution of congruence (1.2) is essentially implied by that of congruence (2.1), it make sense to examine the second equation of congruence (1.2) independently. Our next section does exactly that.

3 Conditions for Primality

In this section we shall give some primality conditions obtained by studying the solutions of the congruence

$$a^{a-1} \equiv 1 \pmod{n}. \tag{3.1}$$

Again we consider only those a such that $a \in [1, n)$, and $a = 1$ is considered as the trivial solution. The outcome is summarized in the next theorem:

Theorem 2. *Let n be a positive integer.*

(i) *If congruence* (3.1) *has no non-trivial solution, then n is a prime number, and either $n = 2$ or $n \equiv \pm 3 \pmod{8}$;*

(ii) *If n is odd and $a = (n + 1)/2$ is the only non-trivial solution to congruence* (3.1)*, then n is a prime number and $n \equiv \pm 1 \pmod{8}$;*

(iii) *If $a = n-1$ is the only non-trivial solution to congruence* (3.1)*, then n is twice a prime number.*

Proof: (i) Suppose that n is composite, and we will show that congruence (3.1) has a non-trivial solution. The construction will break into the following four cases.

1. If $n > 2$ is even, then $a = n-1$ is a non-trivial solution.

2. If n is odd and not square-free, then the proof of Theorem 1 actually gives a non-trivial solution $a = \varphi(p^k)m + 1$ that satisfies even more.

3. Suppose that $n = pm$, where p is an odd prime and $m > 2$ odd, square-free and not divisible by p, and also $p \nmid m-1$. Then $a = (p-1)m+1$ will be a non-trivial solution, since
$$a^{a-1} \equiv \left((1-m)^{p-1}\right)^m \equiv 1 \pmod{p},$$
and $a \equiv 1 \pmod{q}$ for any prime factor q of m.

4. Finally, if n does not fit into any of the previous cases, then we must be able to write $n = pql$, where p, q are distinct odd primes that do not divide l, which is odd and square-free, and also we have $p \mid ql-1$ and $q \mid pl-1$. Then $a = (p-1)(q-1)l+1$ is a non-trivial solution: we have $a^{a-1} \equiv 1 \pmod{l}$, and
$$a \equiv 1 - ql + l \equiv l \pmod{p},$$
so $a^{a-1} \equiv (l^{p-1})^{(q-1)l} \equiv 1 \pmod{p}$, and similarly $a^{a-1} \equiv 1 \pmod{q}$.

For the last statement, one observes that, if n is a prime number, then $a = (n+1)/2$ is a non-trivial solution if and only if $n \equiv \pm 1 \pmod{8}$, since by Euler's criterion we have
$$a^{a-1} \equiv \left(\frac{n+1}{2}\right)^{\frac{n-1}{2}} = \left\langle \frac{2^{-1}}{n} \right\rangle = \left\langle \frac{2}{n} \right\rangle \pmod{n},$$
where the angle brackets are Legendre symbols.

(ii) It now suffices to show that none of the solutions constructed in part (i) is equal to $(n+1)/2$. Certainly that is true if n is even, and in case (2), if $\varphi(p^k)m + 1 = (n+1)/2$ then $n = 2p^{k-1}m - 1$, an obvious contradiction. In case (3), if $(p-1)m + 1 = (n+1)/2$ then $1 = (2-p)m < 0$, also a contradiction. Finally in case (4), if $a = (n+1)/2$ then $1 = l(2p + 2q - 2 - pq)$, and it follows that $l = 1$ and $p = q = 3$, but that contradicts the hypothesis that n is square-free.

(iii) Obviously, here n must be even. We will first prove that either $n = 4$, or $n = 2m$ with m an odd square-free number. To see this, first suppose that $n = 2^k m$ where $k \geq 2$ and m is odd. Then as we have seen, $a = 2^{k-1}m + 1$ is a non-trivial solution, but according to condition (iii) this must be equal to $n-1$, so we get $n = 4$. Next assume that $n = 2p^k m$ where p is an odd prime, $k \geq 2$, and m is odd and not divisible by p. Again $a = 2p^{k-1}m + 1$ is a non-trivial solution, and since this is equal to $n-1$, we have $n(p-1) = 2$, which is clearly not possible.

It then suffices to show that, if $n = 2pm$ with p being a odd prime and m an odd square-free number not divisible by p, then in fact $m = 1$. First, if $p \mid m-1$, then $a = (p-1)m + 1$

is again a non-trivial solution as in the proof of case (3) above (clearly $a \equiv 1 \pmod 2$), and $a = n - 1$ leads to $n = 2p$, so indeed $m = 1$. Next, if $n = 2pql$ where p, q, l are the same as in case (4) above, then again $a = (p-1)(q-1)l + 1$ is a non-trivial solution, and $a = n - 1$ leads to $pql + ql + pl = l + 2$, a contradiction. □

We remark that each converse of the parts of Theorem 2 is not true. Counterexamples are $(n, a) = (13, 5), (17, 13), (26, 5 \text{ or } 21)$, respectively. It seems to be very difficult to give a complete characterization for those numbers n such that congruence (3.1) has only trivial solution.

We are obviously interested in shortening the range in which the absence of solutions for congruence (3.1) will still force n to be a prime number. In this respect we notice that the non-trivial solutions constructed for congruence (3.1) in Part (i) are all greater than $\varphi(n)$. Although the absence of solutions for congruence (3.1) in the range $\varphi(n) < x < n$ do characterize the prime numbers, this is obviously an ineffective method, since in this case the value of $\varphi(n)$ itself would be the best certificate for the primality of n. However, one may easily replace $\varphi(n)$ by a simpler function of n, as seen in the following result.

Corollary 1. *Let n be an odd positive integer. If there exists no integer a with $8n/15 < a < n$ satisfying $a^{a-1} \equiv 1 \pmod n$, then n is a prime number.*

Proof: We check that all the solutions obtained in cases (1)–(4) in the proof of Theorem 2 above are bigger than $8n/15$. Case (1) is trivial, and for both cases (2) and (3) we have

$$\frac{a}{n} > \frac{\varphi(p^k)m}{n} > 1 - \frac{1}{p} \geq \frac{2}{3} > \frac{8}{15},$$

while in the conditions of (4) we have

$$\frac{a}{n} > \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \geq \frac{2}{3} \cdot \frac{4}{5} = \frac{8}{15}.$$

□

Remark 1. *For each c, $8/15 < c < 1$, one may find a finite set of small primes $\mathbb{P}_c$ such that an odd number is prime provided that no $p \in \mathbb{P}_c$ divides n and there exists no solution for the congruence (7) in the range $cn < a < n$. For instance, $\mathbb{P}_c = \{3\}$ for any c between $8/15$ and $24/35$, and $\mathbb{P}_c = \{3, 5\}$ for $24/35 < c < 60/77$.*

In order to prove that an integer n is a prime number we may prove on one hand that n is a prime power, and on the other hand that n is square-free, as in the following result.

Proposition 2. *We have the following:*

(i) *An odd integer $n > 2$ is a prime power if and only if there exists no integer a with $2\sqrt{2n} < a < n$ satisfying $a^{a-1} \equiv 1 \pmod n$ and $a^{a+1} \equiv 1 \pmod n$;*

(ii) *An integer $n > 1$ is square-free if and only if a^2 is not divisible by n, for all integers a with $\sqrt{n} \leq a < n$.*

Proof: (i) Since for $a > 1$ we have

$$\gcd\left(a^{a-1} - 1, a^{a+1} - 1\right) = a^{\gcd(a-1,a+1)} - 1,$$

an integer $a > 1$ will satisfy both congruences in the statement of our result if and only if a is odd and $a^2 \equiv 1 \pmod{n}$.

Let $n = p^k$, with $k \geq 1$ and p an odd prime number, and let us assume there exists a with $2\sqrt{2n} < a < n$ satisfying both our congruences. Then a must be odd, say $a = 2u + 1$, and p^k divides $u(u + 1)$. This implies that either u or $u + 1$ is divisible by p^k, and in both cases we have $a \geq 2n - 1 > n$, a contradiction.

Conversely, let us assume that $n = uv$, with u, v odd relatively prime integers. There exist integers s and t with $1 \leq s < v$, $1 \leq t < u$ and such that $su - tv = 1$. Since u and v are both odd integers, it follows that the products st and $(v - s)(u - t)$ are both even. Let $a = 2su - 1 = 2tv + 1$. Then $a \leq 2u(v - 1) - 1 < 2n - 6$ and $a^2 = (2su - 1)(2tv + 1) = 4stn + 1$, so $a^2 \equiv 1 \pmod{n}$. In case $a > n$, we may consider $a_1 = 2n - a$, which satisfies $a_1 < n$ and $a_1^2 \equiv 1 \pmod{n}$. We prove now that $a > 2\sqrt{2n}$ and $a_1 > 2\sqrt{2n}$.

Using the fact that $a = 2su - 1 = 2tv + 1$ we obtain $a = su + tv$, which implies

$$a \geq 2\sqrt{stuv} \geq 2\sqrt{2n},$$

since st is even. Similarly we obtain

$$a_1 = 2n - su - tv = u(v - s) + v(u - t) \geq 2\sqrt{uv(v - s)(u - t)} \geq 2\sqrt{2n},$$

since $(v - s)(u - t)$ is even too.

(ii) Let us assume that n is square-free, say $n = p_1 \cdots p_k$ with $p_1, \ldots, p_k$ distinct prime numbers. If there exists $a \geq \sqrt{n}$ such that n divides a^2, then a will be divisible by each of the primes $p_1, \ldots, p_k$, which implies that n divides a, and hence $a \geq n$. Conversely, assume there exists a prime p such that p^2 divides n. We consider then $a = \frac{n}{p}$ and we obviously have $\sqrt{n} \leq a < n$, while n divides a^2, and this completes the proof. □

We note here that a more general square-free criterion may be stated as follows.

Proposition 3. *Let $m \geq 2$ be a fixed, arbitrarily chosen integer. An integer $n > 1$ is square-free if and only if $n \nmid a^m$ for each integer a with $\sqrt{n} \leq a < n$.*

This result was proved in [1] and was adapted to obtain square-free criteria for polynomials that use no derivatives or discriminants.

4 Cyclic groups matched by automorphisms

Now we go back and consider the system of congruences (1.1). In this section, we will prove the following:

Theorem 3. *Congruence* (1.1) *has a non-trivial solution if and only if either of the following condition holds:*

(1) $\gcd(n, m, \varphi(n), \varphi(m)) > 1$.

(2) *We can write* $n = n_1 n_2$ *and* $m = m_1 m_2$, *such that* $\gcd(n_1, n_2) = 1$, $\gcd(m_1, m_2) = 1$, $\gcd(n_1, \varphi(m_2)) > 1$ *and* $\gcd(m_1, \varphi(n_2)) > 1$.

We note that these two conditions are not exclusive. To demonstrate the claim, consider $n = 4, m = 6$. One can verify that $\gcd(n, m, \varphi(n), \varphi(m)) = 2$, and congruence (1.1) has a non-trivial solution $(a, b) = (3, 5)$. Or, if $n = 14, m = 15$, then we can choose $(n_1, n_2, m_1, m_2) = (2, 7, 3, 5)$, and condition (2) holds, so congruence (1.1) has non-trivial solutions $(a, b) = (9, 4)$ and $(11, 4)$. On the other hand, if $\gcd(n, \varphi(m)) = 1$ or $\gcd(m, \varphi(n)) = 1$, then clearly not even the first line of congruence (1.1) has a non-trivial solution. For a not-so-trivial example where both conditions in theorem fail, consider $n = 3, m = 14$. Then condition (1) fails, and there is no way to come up with the decomposition in condition (2), so in this case congruence (1.1) has only trivial solutions.

In the following, we are going to introduce the parameters p_n, p_m, q_n and q_m. We should clarify that the subscripts of these are all symbolic, that is, p_n and p_m are considered as different parameters even if $n = m$. The subscript simply indicates that, for example, p_n is a prime factor of n, and so on. In the rest of the paper, the notation $\mathrm{ord}_p(a)$ means the order of a modulo p.

Proof: [Proof of Theorem 3] First we observe that the stated condition is equivalent to the following: there are four primes (not necessarily distinct) p_n, p_m, q_n, q_m such that

$$\begin{cases} p_n \mid \gcd(n, \varphi(q_m^M)), & q_m^M \parallel m, \\ p_m \mid \gcd(m, \varphi(q_n^N)), & q_n^N \parallel n, \end{cases} \tag{4.1}$$

and satisfy either of the following conditions:

(i) $p_n \neq q_n$ and $p_m \neq q_m$.

(ii) $p_n = p_m$.

It is easy to see that condition (i) is equivalent to condition (2), while condition (ii) is equivalent to condition (1). We will prove the theorem under the formulations above.

(Sufficiency) First suppose that condition (i) holds. Let a be the least positive integer such that

$$\begin{cases} a \equiv 1 \pmod{q^\nu} \text{ for all } q^\nu \parallel n \text{ such that } q \neq q_n, \\ \mathrm{ord}_{q_n^N}(a) = p_m. \end{cases} \tag{4.2}$$

The existence of such a is guaranteed by the Chinese Remainder Theorem and the fact that $p_m \mid \varphi(q_n^N)$, as in the proof of Theorem 1, and we have $a \in (1, n)$. Construct b in the symmetric way.

Now, since $p_n \neq q_n$, by the first line of equation (4.2) we clearly have

$$a \equiv 1 \pmod{p_n}, \tag{4.3}$$

so since $\mathrm{ord}_{q_m^M}(b) = p_n$, we have $b^{a-1} \equiv 1 \pmod{q_m^M}$, and since $p_n \mid n$, we also have $b^n \equiv 1 \pmod{q_m^M}$. It is clear that by construction we have $b^{a-1} \equiv b^n \equiv 1 \pmod{q^\nu}$ for all $q^\nu \parallel m$ such that $q \neq q_m$, so the left half of congruence (1.1) holds. By the same reasoning the right half also holds.

Next, suppose that condition (ii) holds, and, without loss of generality, suppose that condition (i) does not hold, say for example $p_m = p_n = q_n$ (and let us simply denote all these by just p). Then since $p \mid \varphi(p^N)$, we must have $N \geq 2$. Write $n = p^N n'$, and let $a = p^{N-1}n' + 1$. Then equation (4.3) is still true, and since $a^p = (p^{N-1}n' + 1)^p \equiv 1 \pmod{n}$ and $a \not\equiv 1 \pmod{p^N}$, equation (4.2) is also true.

Now, if we also have $p_m = q_m$, then we construct b in the symmetric way by writing $m = p^M m'$ and let $b = p^{M-1}m' + 1$, and if $p_m \neq q_m$, then b is constructed the same way as in the case where condition (i) holds. It follows that in either case b also satisfies the analogue of equation (4.2) and equation (4.3). So by the same argument, congruence (1.1) holds.

(Necessity) Suppose that (a, b) is a non-trivial solution. Since $b \not\equiv 1 \pmod{m}$, there must be some $q_m^M \parallel m$ such that $b \not\equiv 1 \pmod{q_m^M}$. Then we must have $\mathrm{ord}_{q_m^M}(n)$ dividing all $n, a-1$ and $\varphi(q_m^M)$ (the first two follow from congruence (1.1), and the last one is just the property of the order), so $\mathrm{ord}_{q_m^M}(b)$ has a prime factor p_n that divides $\gcd(n, a-1, \varphi(q_m^M))$. By the same method, we can choose q_n^N and p_m. Certainly, this procedure does not necessarily give a unique choice of (p_n, p_m, q_n, q_m), but we claim that, as long as we choose these four primes by the said procedure, our choice will always satisfy either condition (i) or (ii). To prove the claim, it suffices to show that, if our choice leads to $p_n = q_n$, then we must have $p_n = p_m$.

So, suppose that $p_n = q_n$. Then since $a \equiv 1 \pmod{p_n}$ (by construction) and $a \not\equiv 1 \pmod{p_n^N}$ (by $p_n = q_n$), we must have $N \geq 2$, and also a is of the form $kp_n + 1$, where $1 \leq k \leq p_n^{N-1} - 1$. But then observe that

$$a^{p_n^{N-1}} = (kp_n + 1)^{p_n^{N-1}} = \sum_{t=0}^{p_n^{N-1}} \binom{p_n^{N-1}}{t} (kp_n)^t,$$

where all the summands (besides the one corresponding to $t = 0$) contain p_n to the power of

$$t + (N-1) - \left\lfloor \frac{t}{p_n} \right\rfloor - \left\lfloor \frac{t}{p_n^2} \right\rfloor - \cdots > t + (N-1) - \frac{t}{p_n - 1} \geq N - 1,$$

that is, they all contain p_n^N. Therefore, $a^{p_n^{N-1}} \equiv 1 \pmod{p_n^N}$, which implies that $\mathrm{ord}_{p_n^N}(a)$ must be a power of p_n, so by construction, we must have $p_m = p_n$. □

A useful special case of the theorem is the following.

Corollary 2. *If* $\gcd(n, m)$ *is not a cyclic number, then congruence* (1.1) *has a non-trivial solution.*

Proof: If $\gcd(n, m)$ is not square-free, say $p^2 \mid \gcd(n, m)$ for some prime p, then we may simply choose $p_n = p_m = q_n = q_m = p$ and condition (ii) is satisfied. If $\gcd(n, m)$ is square-free but has prime factors p, q such that $p \mid q - 1$, then set $p_n = p_m = p$ and $q_n = q_m = q$, and condition (ii) is again satisfied. □

5 A special set of pairs of prime numbers

It follows from Theorem 3 that, in the case when both n and m are prime numbers, congruence (1.1) has no non-trivial solutions. But what if we consider only the second line of congruence (1.1)?

If the following, let us denote by $\mathcal{A}$ the set of pairs (p, q) of distinct prime numbers for which the pair of congruences

$$a^{b-1} \equiv 1 \pmod{p} \quad \text{and} \quad b^{a-1} \equiv 1 \pmod{q} \tag{5.1}$$

does not have any solutions in integer numbers satisfying $a \in (1, p)$ and $b \in (1, q)$. A few questions naturally arise from this definition. Is the set $\mathcal{A}$ infinite? Are there infinitely many pairs of distinct prime numbers not in $\mathcal{A}$? If we fix one of the two primes, q say, are there infinitely many prime numbers p for which the pair (p, q) is in $\mathcal{A}$? Are there infinitely many prime numbers p for which the pair (p, q) is not in $\mathcal{A}$?

Our goal in this section is to prove the following two results.

Theorem 4. *For any odd prime number $q \equiv 2 \pmod{3}$, a positive proportion of prime numbers p are such that the pair (p, q) is in $\mathcal{A}$. More precisely,*

$$\liminf_{x\to\infty} \frac{(\log x)\#\{p \text{ prime} : p \le x, (p, q) \in \mathcal{A}\}}{x} \ge c_q, \tag{5.2}$$

where

$$c_q = \frac{1}{2} \prod_{\substack{p' \text{ prime} \\ q \equiv 1 \pmod{p'}}} \frac{p'-3}{p'-1} \prod_{\substack{p' \text{ odd prime} \\ q \not\equiv 1 \pmod{p'} \\ p' \le q-2}} \frac{p'-2}{p'-1}.$$

Theorem 5. *Suppose that q is an odd prime such that $q - 1 = km$ with $k = 2^l$ and m odd, and $m = q^\delta$ for some $\delta > 0$. If $q \gg_\delta 1$, then there is a positive proportion of prime numbers p such that the pair (p, q) is not in $\mathcal{A}$.*

As a side remark, let us note that, as $q \to \infty$,

$$c_q \gg \frac{1}{\log\log q}.$$

We start with the following lemma.

Lemma 1. *Let q be an odd prime number. If p is a prime number satisfying the following conditions:*

(i) $p \equiv 3 \pmod{4}$,

(ii) $p \not\equiv 1 \pmod{p'}$ *for any odd prime p' such that $p' \le q - 2$, and*

(iii) $p \not\equiv 2 \pmod{p'}$ *for any odd prime divisor p' of $q - 1$,*

then the pair $(p, q) \in \mathcal{A}$.

Proof: Indeed, if there exist integers $a \in (1,p)$ and $b \in (1,q)$ such that congruence (5.1) holds, then $\mathrm{ord}_p(a) \mid \gcd(b-1, p-1)$. For any odd prime divisor p' of $b-1$ (if there is one), since $p' \leq b-1 \leq q-2$, by (ii) we know that $p \not\equiv 1 \pmod{p'}$, and thus we deduce that $\gcd(p-1, b-1)$ is a power of 2, and by (i), it follows that $\gcd(p-1, b-1) = 1$ or 2. Consequently, $\mathrm{ord}_p(a)$ is either 1 or 2. The first case is impossible since $a \neq 1$. The second case forces $a = p-1$. Then the congruence $b^{a-1} \equiv 1 \pmod{q}$ reduces to $b^{p-2} \equiv 1 \pmod{q}$. Hence $\mathrm{ord}_q(b) \mid \gcd(p-2, q-1)$. Note that $p-2$ is odd, so $\gcd(p-2, q-1)$ is odd. Also, for any prime divisor p' of $q-1$ we know by (iii) that p' is not a divisor of $p-2$. We conclude that $\mathrm{ord}_q(b) = \gcd(p-2, q-1) = 1$, which is a contradiction since $b \neq 1$. □

Proof: [Proof of Theorem 4] Let us fix an odd prime number q, with $q \equiv 2 \pmod 3$, and let m_q be defined by

$$m_q = 4 \prod_{\substack{p' \text{ odd prime} \\ p' < q}} p'.$$

There are $\varphi(m_q)$ residue classes modulo m_q relatively prime to m_q. For each such residue class, b say, by the Prime Number Theorem for Arithmetic Progressions (see [4, Chapter 22]), we know that

$$\#\{p \text{ prime} : p \leq x, p \equiv b \pmod{m_q}\} \sim \frac{1}{\varphi(m_q)} \frac{x}{\log x}.$$

Here

$$\varphi(m_q) = 2 \prod_{\substack{p' \text{ odd prime} \\ p' < q}} (p'-1).$$

The estimate (5.2) follows by counting the residue classes b modulo m_q which satisfy Lemma 1. There is exactly one residue class modulo 4 as in Lemma 1, namely $3 \pmod 4$. Next, for each odd prime divisor p' of $q-1$, there are $p'-3$ admissible residue classes modulo p', namely those which are not congruent to 0, 1, or 2 modulo p'. Lastly, for any odd prime number p' with $p' \leq q-2$ for which p' does not divide $q-1$, there are $p'-2$ admissible classes modulo p', namely those which are not congruent to 0 or 1 modulo p'. By combining all the above with the Chinese Remainder Theorem we see that the number of residue classes b modulo m_q which are relatively prime to m_q and satisfy the conditions from Lemma 1, call it M_q, is given by

$$M_q = \prod_{\substack{p' \text{ odd prime} \\ q \equiv 1 \pmod{p'}}} (p'-3) \prod_{\substack{p' \text{ odd prime} \\ q \not\equiv 1 \pmod{p'} \\ p' \leq q-2}} (p'-2).$$

Since each prime number p in any of these M_q arithmetic progressions modulo m_q is such that the pair (p,q) is good, it follows that

$$\liminf_{x \to \infty} \frac{(\log x)\#\{p \text{ prime} : p \leq x, (p,q) \in \mathcal{A}\}}{x} \geq \frac{M_q}{\varphi(m_q)} = c_q.$$

□

To prove Theorem 5, first we make the following deduction.

Lemma 2. *Suppose that q is an odd prime. If there exists an odd number $b \in (1, q)$ such that $\mathrm{ord}_q(b)$ is odd, then there is a positive proportion of prime numbers p such that the pair (p, q) is not in $\mathcal{A}$.*

Proof: We observe that, under the hypothesis, any prime number p with $p \equiv 2 \pmod{\mathrm{ord}_q(b)}$ will guarantee that $(p, q) \notin \mathcal{A}$, and by the Prime Number Theorem for Arithmetic Progressions, there is a positive portion of such primes since $\mathrm{ord}_q(b)$ is odd. Indeed, for those p, we can simply choose $a = p - 1$. Since b is odd, we have $a^{b-1} \equiv 1 \pmod{p}$, and since $p \equiv 2 \pmod{\mathrm{ord}_q(b)}$, we have $b^{a-1} = b^{p-2} \equiv 1 \pmod{q}$. □

To complete the proof of Theorem 5, we would need a result by Bourgain [3] which states the following.

Theorem 6 ([3, Corollary of Theorem B])**.** *Let H be a subgroup of $\mathbb{F}_q^*$ where q is a prime, and $|H| = q^\delta$. Then*

$$\max_{(t,q)=1} \left| \sum_{x \in H} e_q(tx) \right| < q^{-\delta'} |H|,$$

where $e_q(x) = \exp(2\pi i x/q)$, and $\delta' > exp(-C/\delta)$ for some absolute constant $C > 1$.

We are now ready to prove Theorem 5.

Proof: [Proof of Theorem 5] By Lemma 2, we need to find an odd number $b \in (1, q)$ such that $\mathrm{ord}_q(b)$ is odd. Consider the set $H = \{x^k : x \in \mathbb{F}_q^*\}$, then the order of each element in H divides m, and thus all the elements in H have odd order. It then suffices to show that there is at least one element in H other than 1 such that its minimal positive representative is odd. Now H is a subgroup of $\mathbb{F}_q^*$ of order m, so by Theorem 6, for any t relatively prime to q we have

$$\left| \sum_{x \in H} e_q(tx) \right| < q^{-\delta'} |H| = o(|H|), \tag{5.3}$$

and we will use this to show that if $q \gg_\delta 1$ then the desired element must exist.

In the following we will identify the elements in H with their minimal positive representatives. Suppose that the only odd element in H is 1, say $H = \{1, 2h_1, 2h_2, \ldots, 2h_{|H|-1}\}$ with $h_i \in [1, q/2)$. Let $A = \{i : h_i \in (\frac{1}{12}q, \frac{5}{12}q)\}$ and $B = \{i : h_i \notin A\}$. Denote by $\Re(z)$ and $\Im(z)$ the

real and imaginary parts of z, respectively. Then take $t = (q+1)/2$, and then we have

$$\begin{aligned}\Im\left(\sum_{x\in H} e_q(tx)\right) &= \Im\left(\sum_i e_q(h_i) + e_q\left(\frac{q+1}{2}\right)\right)\\ &= \sum_i \sin\left(\frac{2\pi h_i}{q}\right) + \sin\left(\frac{\pi(q+1)}{q}\right)\\ &> \sum_{i\in A} \sin\left(\frac{2\pi h_i}{q}\right) + \sin\left(\frac{\pi(q+1)}{q}\right)\\ &\geq \frac{1}{2}|A| + \sin\left(\frac{\pi(q+1)}{q}\right),\end{aligned}$$

so by inequality (5.3) we must have $|A| = o(|H|)$ as $q \to \infty$. On the other hand, as we take $t = 1$, we have

$$\begin{aligned}\Re\left(\sum_{x\in H} e_q(tx)\right) &= \Re\left(\sum_i e_q(2h_i) + e_q(2)\right)\\ &= \sum_i \cos\left(\frac{2\pi h_i}{q}\right) + \cos\left(\frac{4\pi}{q}\right)\\ &= \sum_{i\in B} \cos\left(\frac{2\pi h_i}{q}\right) + \sum_{i\in A} \cos\left(\frac{2\pi h_i}{q}\right) + \cos\left(\frac{4\pi}{q}\right)\\ &\geq \frac{1}{2}|B| - |A| + \cos\left(\frac{4\pi}{q}\right) \gg |H| \quad \text{for } |H| \text{ large},\end{aligned}$$

but this is not possible for large q by inequality (5.3). This completes the proof. □

Acknowledgement. Research of the fourth author was supported in part by the National Science Foundation Grant DMS-0901621.

References

[1] E. Alkan, A.I. Bonciocat, N.C. Bonciocat and A. Zaharescu, Square-free criteria for polynomials using no derivatives, *Proc. Amer. Math. Soc.* **135** (2007), 677–687.

[2] N. C. Bonciocat, Groups bicrossed product by automorphisms, *Mathematical Reports* **3**(53)(2001), 145–151.

[3] J. Bourgain, Multilinear exponential sums in prime fields under optimal entropy condition on the sources, *Geom. Funct. Anal.* **18** (2009), no. 5, 1477–1502.

[4] H. Davenport, *Multiplicative number theory*, Third edition, Revised and with a preface by Hugh L. Montgomery, Graduate Texts in Mathematics, **74**. Springer-Verlag, New York, 2000; MR1790423.

[5] P. Erdős, Some asymptotic formulas in number theory, *J. Indian Math. Soc. (N.S.)* **12** (1948), 75–78.

[6] T. Szele, Über die endichen Ordnungszahlen, zu denen nur eine Gruppe gehört (German), *Comment. Math. Helv.* **20** (1947), 265–267.

[7] M. Takeuchi, Matched pairs of groups and bismash products of Hopf algebras, *Comm. Algebra* **9**(8) (1981), 841–882.

Received: 5.01.2013,

Accepted: 23.02.2013.

Simion Stoilow Institute of Mathematics of the Romanian Academy,
Research Unit nr. 5, P.O. Box 1-764, RO-014700 Bucharest, Romania
E-mail: Nicolae.Bonciocat@imar.ro, Mihai.Cipu@imar.ro

Department of Mathematics, University of Illinois at Urbana-Champaign,
Altgeld Hall, 1409 W. Green Street, Urbana, IL, 61801, USA
E-mail: tsai39@illinois.edu, zaharesc@math.uiuc.edu