Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Simultaneous insolvability of exponential congruences

Olli Järviniemi

Department of Mathematics and Statistics, University of Turku, 20014 Turku, Finland

ARTICLE INFO

Article history:
Received 20 September 2021
Accepted 28 December 2021
Available online xxxx
Communicated by F. Pellarin

Keywords:
Artin's primitive root conjecture
Multiplicative order
Chebotarev density theorem
Kummer extensions

ABSTRACT

We determine a necessary and sufficient condition for the infinitude of primes p such that none of the equations $a_i^x \equiv b_i \pmod p, 1 \leq i \leq n$, are solvable. We control the insolvability of $a^x \equiv b \pmod p$ by power residues for multiplicatively independent a and b, and by divisibilities and, most importantly, parities of orders in multiplicatively dependent cases. We also consider a more general problem concerning divisibilities of orders. The problems are motivated by Artin's primitive root conjecture and its variants.

1. Introduction

The famous Artin primitive root conjecture asserts that any integer a, not equal to a square or -1, is a primitive root modulo p for infinitely many primes p.

It is still an open problem to prove the statement for any such a. However, considerable progress has been made. Hooley [2] famously proved that, under a suitable generalization of the Riemann hypothesis (GRH), the set of primes p for which a is a primitive root modulo p has a density, positive for a not equal to -1 or a square. Unconditionally,

E-mail address: olli.a.jarviniemi@utu.fi.

https://doi.org/10.1016/j.jnt.2021.12.007

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

Heath-Brown [1] has shown that the statement is true for "many" values, for example for all prime values of a with at most two exceptions. For a comprehensive survey on Artin's conjecture, see [6].

The so-called two-variable Artin conjecture concerns the set of primes p for which the equation $a^x \equiv b \pmod p$ is solvable for fixed integers a and b. In the multiplicatively dependent case one can show (unconditionally) that the density of such p exists and is a rational number, positive except for cases where this set is trivially finite. The density question has been solved for the multiplicatively independent case assuming GRH. We refer to [7] for these results.

Let $f(a,b,x)$ denote the number of primes $p \leq x$ such that $a^x \equiv b \pmod p$ is solvable. While it has been proven that $f(a,b,x)$ is of magnitude $c\pi(x)$ under GRH, where $\pi(x)$ is the number of primes $p \leq x$ and $c = c(a,b)$ is a constant, the best unconditional results in this direction are $f(a,b,x) \geq c' \log(x)$ for multiplicatively independent a, b, proven recently in [8].

One generalization for the Artin conjecture is considering the set of primes p for which all of the integers $a_1, \dots, a_n$ are primitive roots modulo p. This problem has been treated by Matthews in [5], where it is determined when this set is infinite under GRH.

It is thus natural to consider the simultaneous solvability of congruences of the form $a^x \equiv b \pmod p$. In [3] it was proven that, under GRH, for any integers $a_1, \dots, a_n, b_1, \dots, b_n > 1$ the set of primes p such that each of $a_i^x \equiv b_i \pmod p, 1 \leq i \leq n$ is solvable has positive density. Some remarks on the case of negative integers are also given in [3].

Here we consider the complementary problem: when do there exist infinitely many primes p such that none of the congruences $a_i^x \equiv b_i \pmod p$ are solvable?

Schinzel [11] has considered systems of exponential congruences, though he has studied systems of the form $\prod_{1 \leq i \leq k} a_{j,i}^{x_i} \equiv b_j \pmod p, j = 1, 2, \dots, n$, so the results do not immediately apply to our problem. However, his results suffice to settle the case of one equation (which he has also considered in [10]). Similarly, Somer [12] has studied the maximal divisors of kth order linear recurrences, and while the results solve our problem for one equation, they do not apply to the general case in our problem.

We will see that multiplicatively independent pairs (a_i, b_i) do not affect the infinitude of primes p such that all exponential congruences are simultaneously insolvable (Corollary 3.2). In the dependent cases one has to guarantee divisibility of orders by odd primes and parity conditions on orders. The former do not cause any obstructions either, but the parities do. As an easy example, 2 and 3 having odd orders modulo a prime implies that 6 has odd order too.

Motivated by this, we consider the general problem on satisfiability of (in)divisibility conditions on multiplicative orders. We prove that such conditions may be reduced to considering (in)divisibility by prime powers.

This article is structured as follows. First, using only elementary considerations, we bring the problem into a more tractable form. We then state the results, our main

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

results being Theorems 3.1 and 3.4, which we prove after introducing some notation and preliminaries.

The author thanks Joni Teräväinen for helpful discussions and comments on earlier versions of the manuscript, and the referees for thorough reading of the article, corrections and suggestions.

2. Solvability of exponential congruences

We first characterize the solvability of an equation $a^x \equiv b \pmod p$, $a, b \in \mathbb{Z}$. We use the following terminology.

Definition 2.1. We say that a pair of integers (a, b) is...

- ...*trivial*, if $|a| \leq 1$, $b \in \{0, 1\}$, or $b = a^k$ for some $k \geq 1$.
- ...*irrational*, if a and b are multiplicatively independent over $\mathbb{Q}$.
- ...*odd*, if $b = -a^k$ for some $k \geq 0$.
- ...*divisible*, if $b^s = \pm a^r$ for some positive r, s with $\gcd(r, s) = 1$ and $s \geq 2$ not a power of two.
- ...*even*, if $b^s = a^r$ for some positive r, s with $\gcd(r, s) = 1$ and $s \geq 2$ a power of two.
- ...*strongly even*, if $b^s = -a^r$ for some positive r, s with $\gcd(r, s) = 1$ and $s \geq 2$ a power of two.

For a trivial pair (a, b) it is trivial to determine whether the equation $a^x \equiv b \pmod p$ is solvable or not: if b is a power of a, the equation is always solvable, and otherwise it is insolvable for all but finitely many p.

If the pair (a, b) is divisible, even or strongly even, then $b^s = \pm a^r$ for some $\gcd(r, s) = 1$. If $b^s = a^r$, there exists an integer c such that $b = c^r$ and $a = c^s$. If $b^s = -a^r$, there exists an integer c for which $b = c^r$ and $a = -c^s$. The number c is called the *core* of the pair (a, b).

In the following lemmas we give sufficient conditions for the insolvability of exponential congruences in different cases. Here and in what follows p is a prime and $\mathrm{ord}_p(a)$ denotes the order of a modulo p. We always assume $p \nmid a$ when using this notation.

Lemma 2.2. *Let (a, b) be a pair of integers, and let p be a prime not dividing ab. The equation $a^x \equiv b \pmod p$ is solvable if and only if $\mathrm{ord}_p(b) | \mathrm{ord}_p(a)$.*

Proof. Let g be a primitive root modulo p, and let $g^A \equiv a \pmod p$ and $g^B \equiv b \pmod p$. The equation $a^x \equiv b \pmod p$ is equivalent with

$$Ax - B \equiv 0 \pmod{p-1}.$$

This equation is solvable if and only if $(A, p-1) | B$, which is equivalent to the condition, as $\mathrm{ord}_p(a) = (p-1)/(A, p-1)$ and $\mathrm{ord}_p(b) = (p-1)/(B, p-1)$. □

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

Lemma 2.3. *Let (a, b) be an odd pair, and let $p \nmid 2ab$ be a prime. The equation $a^x \equiv b \pmod p$ has no solution if and only if $\mathrm{ord}_p(a)$ is odd.*

Proof. Let $b = -a^k$ with integer k. The equation $a^x \equiv b \pmod p$ is equivalent to $a^{x-k} \equiv -1 \pmod p$. By Lemma 2.2 this is insolvable if and only if $2 = \mathrm{ord}_p(-1) \nmid \mathrm{ord}_p(a)$. □

Lemma 2.4. *Let (a, b) be an even pair, let c be its core, and let $p \nmid 2ab$ be a prime. The equation $a^x \equiv b \pmod p$ is insolvable if and only if $2 \mid \mathrm{ord}_p(c)$.*

Proof. Write $a = c^s$ and $b = c^r$ for integers $(r, s) = 1$, and write $a^x \equiv b \pmod p$ as $c^{sx-r} \equiv 1 \pmod p$. This is insolvable if and only if $sx - r \equiv 0 \pmod{\mathrm{ord}_p(c)}$ is insolvable, which is equivalent to $(s, \mathrm{ord}_p(c)) \nmid r$. By assumption, s is a power of two, so we must have $2 \mid \mathrm{ord}_p(c)$. This is also sufficient for insolvability. □

Lemma 2.5. *Let (a, b) be a strongly even pair, let c be its core, and let $p \nmid 2ab$ be a prime. The equation $a^x \equiv b \pmod p$ is insolvable if and only if $2 \mid \mathrm{ord}_p(c^2)$.*

Proof. Write $a = -c^s$ and $b = c^r$, so $a^x \equiv b \pmod p$ is equivalent with $(-c^s)^x \equiv c^r \pmod p$. If x is even, this is equivalent with the insolvability of $c^{sx-r} \equiv 1 \pmod p$, which, as in the previous lemma, is equivalent to $2 \mid \mathrm{ord}_p(c)$. If x is odd, this is equivalent with $c^{sx-r} \equiv -1 \pmod p$, that is,

$$sx - r \equiv \frac{\mathrm{ord}_p(c)}{2} \pmod{\mathrm{ord}_p(c)}.$$

Using the fact that $s \geq 2$ is a power of two, the insolvability of this is equivalent to $4 \mid \mathrm{ord}_p(c)$, which in turn is equivalent with $2 \mid \mathrm{ord}_p(c^2)$. □

Finally, for divisible pairs we have the following lemma. The proof is so similar to the proofs above that we omit it.

Lemma 2.6. *Let (a, b) be a divisible pair, and let c be its core. Pick some $p \nmid 2ab$. Write $b = c^r$ and $a = \pm c^s$ with $(r, s) = 1$. The equation $a^x \equiv b \pmod p$ is insolvable if $q | \mathrm{ord}_p(c)$ for some odd prime $q | s$.*

(If s is even, one could also obtain insolvability by the condition $2 \mid \mathrm{ord}_p(c)$, but for our purposes it is best to impose a divisibility condition by an odd prime in the case of divisible pairs.)

Thus, to ensure the simultaneous insolubility of given exponential congruences, we have to:

(i) Guarantee the insolvability of $a^x \equiv b \pmod p$ for irrational pairs (a, b).
(ii) For divisible pairs (a, b), guarantee the divisibility of $\mathrm{ord}_p(c)$ by an odd prime q, where c is the core of (a, b).

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

(iii) For odd pairs (a, b), guarantee the oddness of $\mathrm{ord}_p(c)$, where c is the core of (a, b).
(iv) For even and strongly even pairs (a, b), guarantee the evenness of $\mathrm{ord}_p(c)$, where c is the core or the square of the core of (a, b).

We will see that (i) and (ii) cause no obstructions at all, so we are mainly concerned with (iii) and (iv). We now let $o_1, \dots, o_O$ denote the integers whose order are required to be odd in (iii) and $e_1, \dots, e_E$ denote the integers whose orders are required to be even in (iv).

We note right away that if the product $o_1^{x_1} \cdots o_O^{x_O}$ equals -1 for some $x_1, \dots, x_O \in \mathbb{Z}$, then there are only finitely many desired primes. Indeed, as the product of integers having odd order modulo a prime has odd order, all of $\mathrm{ord}_p(o_i)$ being odd would imply $\mathrm{ord}_p(-1)$ being odd, which is not possible for $p > 2$. Thus, we may without loss of generality assume that no product of o_i equals -1.

To describe the obstructions in the general case, we need the following lemma [3, Lemma 5.1].

Lemma 2.7. *Let $o_1, \dots, o_O$ be non-zero integers, no subproduct of which equals -1. There exists a subset S of $\{o_1, \dots, o_O\}$ with the following properties.*

- *The elements of S are multiplicatively independent (i.e. there is no product of elements of S equal to 1 except for the empty product).*
- *For any $1 \le i \le O$ there exists an odd integer x and a function $f : S \to \mathbb{Z}$ with*

$$o_i^x = \prod_{s \in S} s^{f(s)}.$$

This allows us to reduce to the case when $o_1, \dots, o_O$ are multiplicatively independent:

Lemma 2.8. *Let $o_1, \dots, o_O$ be non-zero integers, no subproduct of which equals -1. Let S be a set as in Lemma 2.7 and let p be a prime (not dividing any of $o_1, \dots, o_O$). The orders $\mathrm{ord}_p(o_i)$ are all odd if and only if $\mathrm{ord}_p(s)$ is odd for all $s \in S$.*

Proof. "Only if" is clear. "If": Let $1 \le i \le O$ and write

$$o_i^x = \prod_{s \in S} s^{f(s)}$$

with x odd. The order of the right hand side modulo p is odd, so $\mathrm{ord}_p(o_i^x)$ is odd and thus $\mathrm{ord}_p(o_i)$ is odd. □

From now on we assume that the numbers o_i are multiplicatively independent.

Let $Q = \{q_1, \dots, q_{|Q|}\}$ be the set of primes q which divide at least one of the numbers $|o_i|$. For each $n \in \mathbb{Z}$ for which the prime factorization of $|n|$ consists only of primes in Q, let $\mathbf{v}(n) = (v_{q_1}(|n|), \dots, v_{q_{|Q|}}(n))$. Define $\epsilon(n) = 0$ if $n > 0$ and $\epsilon(n) = \frac{1}{2}$ if $n < 0$.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

Let A be the subset of elements $a \in \{e_1, \dots, e_E\}$ such that $\mathbf{v}(a)$ lies in the $\mathbb{Q}$-span of $\mathbf{v}(o_i), 1 \le i \le O$. Let $c_i \in \mathbb{Q}$ be such that

$$\mathbf{v}(a) = \sum_{i=1}^{O} c_i \mathbf{v}(o_i).$$

To each $a \in A$, associate the $O+1$-dimensional vector

$$\mathbf{c}(a) = \left(\epsilon(a) + \sum_{i=1}^{O} c_i \epsilon(o_i), c_1, \dots, c_O \right). \tag{2.1}$$

Let B be the rest of $\{e_1, \dots, e_E\}$.

3. Results

The main result gives a complete characterization for the simultaneous insolvability of exponential congruences.

Theorem 3.1. *Let $a_i^x \equiv b_i \pmod p, 1 \le i \le n$, be a set of exponential congruences. Assume no pair (a_i, b_i) is trivial. As in Section 2, let $o_1, \dots, o_O$ be the integers whose orders are required to be odd, which may be taken to be multiplicatively independent, and let $e_1, \dots, e_E$ be the integers whose orders are required to be even. Partition the set $\{e_1, \dots, e_E\}$ into A and B as in Section 2, and let $\mathbf{c}(a)$ be defined as in (2.1). Let $M \in \mathbb{Z}_+$ be such that the denominator of $2^M \mathbf{c}(a)_i$ is odd (when written in its lowest terms) for all $a \in A, 1 \le i \le O$.*

There are infinitely many primes p such that none of $a_i^x \equiv b_i \pmod p$ are solvable if and only if the system

$$2^{M+1}\mathbf{c}(a)_0 + \sum_{i=1}^{O} 2^{M+1}\mathbf{c}(a)_i x_i \not\equiv 0 \pmod{2^{M+1}}, a \in A \tag{3.1}$$

of incongruences has an integer solution $(x_1, \dots, x_O)$.

Furthermore, if there are infinitely many such primes, then their lower density is positive.

We therefore see that the simultaneous insolvability of exponential congruences translates to the solvability of simultaneous linear incongruences.

Note that irrational and divisible pairs do not affect the infinitude of the primes under consideration.

Corollary 3.2. *Let n be a positive integer, and let $a_1, \dots, a_n, b_1, \dots, b_n$ be integers. Assume that there are infinitely many primes p such that none of $a_i^x \equiv b_i \pmod p, 1 \le i \le n$*

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

are solvable. Let (a_{n+1}, b_{n+1}) be a pair of integers which is either irrational or divisible. Then there are infinitely many primes p such that none of $a_i^x \equiv b_i \pmod p, 1 \le i \le n+1$ are solvable. Furthermore, the lower density of such primes is positive.

Another corollary is that for positive a_i, b_i, the only cases when there are only finitely many desired primes are the trivial ones.

Corollary 3.3. *Let $a_1, \dots, a_n, b_1, \dots, b_n$ be integers greater than 1. Assume that b_i is not a power of a_i for any i. There are infinitely many primes p such that none of the equations $a_i^{x_i} \equiv b_i \pmod p$ are solvable. Furthermore, the lower density of such primes is positive.*

Proof. Note that none of the pairs (a_i, b_i) are odd, so the conditions of Theorem 3.1 are trivially satisfied as long as no pair (a_i, b_i) is trivial. □

We then make a couple of comments on the system in Theorem 3.1. The numbers $\mathbf{c}(a)_i 2^{M+1}$ are rational numbers whose denominators are odd, so they may be viewed as integers modulo 2^{M+1}. However, they are not necessarily zero modulo 2^{M+1} due to cancellations, e.g. if $\mathbf{c}(a)_i = 1/2^{M+1}$.

As an example, if $\mathrm{ord}_p(4)$ and $\mathrm{ord}_p(9)$ are required to be odd, and $\mathrm{ord}_p(2), \mathrm{ord}_p(3)$ and $\mathrm{ord}_p(6)$ are required to be even, we obtain the system

$$2x_1 \not\equiv 0 \pmod 4, 2x_2 \not\equiv 0 \pmod 4, 2x_1 + 2x_2 \not\equiv 0 \pmod 4.$$

This system has no solutions, and hence there are only finitely many desired primes. The idea is that if p is a prime with $v_2(p-1) = k$, then $\mathrm{ord}_p(4)$ and $\mathrm{ord}_p(9)$ being odd implies that 2 and 3 are perfect 2^{k-1}th powers modulo p. One sees (cf. multiplicativity of Legendre's symbol) that this implies that at least one of $2, 3$ and 6 is a perfect 2^kth power modulo p, implying that at least one of $\mathrm{ord}_p(2), \mathrm{ord}_p(3), \mathrm{ord}_p(6)$ is odd.

We have been careful in addressing the signs of o_i and $a \in A$. The underlying reason is that there is no canonical way to define square roots of elements of $\mathbb{F}_p^\times$, but nevertheless we would like to perform such operations to infer information on both $\mathrm{ord}_p(2)$ and $\mathrm{ord}_p(-2)$ from $\mathrm{ord}_p(4)$, for example. Indeed, if one requires $\mathrm{ord}_p(4)$ to be odd and $\mathrm{ord}_p(2)$ and $\mathrm{ord}_p(-2)$ to be even, one obtains the system

$$2x_1 \not\equiv 0 \pmod 4, 2 + 2x_1 \not\equiv 0 \pmod 4$$

which has no solutions.

We note that while the solvability of a system of linear equations modulo 2 is well understood, in the general case of arbitrary M there does not seem to be a simple criterion for the existence of a solution to (3.1). Already considering the solvability of a system of linear equations is more difficult over rings than over fields, and the solvability of (3.1) corresponds to the solvability of at least one of $(2^{M+1} - 1)^{|A|}$ systems of linear congruences.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

Motivated by the above discussion, we prove a general result on (in)divisibility conditions imposed on orders.

Theorem 3.4. *Let $a_i, g_i, m_i, 1 \leq i \leq n$ be non-zero integers with $1 \leq g_i \mid m_i$ for all i. The following are equivalent.*

(i) *There are infinitely many primes p such that $\gcd(\mathrm{ord}_p(a_i), m_i) = g_i$ for all i.*
(ii) *For any prime q the following holds: There are infinitely many primes p such that $\gcd(\mathrm{ord}_p(a_i), q^{v_q(m_i)}) = q^{v_q(g_i)}$ for all i.*

Furthermore, if there are infinitely many such primes, their density exists and is positive.

Note that the condition in (ii) is interesting for only finitely many q. One can give a characterization for the satisfiability of these conditions similarly as in Theorem 3.1 in terms of systems of linear incongruences, but we do not state this result explicitly here.

In the case when one only imposes divisibility conditions (the case $g_i = m_i$ in Theorem 3.4) there are no obstructions for the infinitude of the set of primes:

Theorem 3.5. *Let $a_i, m_i, 1 \leq i \leq n$ be non-zero integers with $|a_i| > 1$ for all i. There are infinitely many primes p such that $m_i \mid \mathrm{ord}_p(a_i)$ for all i. Furthermore, the density of such primes exists and is positive.*

Similarly, given a prime $q > 2$ and indivisibility conditions $q \nmid \mathrm{ord}_p(a_i)$, there are infinitely many primes p that fit, but this is trivial: just choose $p \not\equiv 1 \pmod{q}$. The case $q = 2$ is non-trivial, though it follows directly from Theorem 3.1.

Corollary 3.6. *Let $a_i, 1 \leq i \leq n$ be integers with $|a_i| > 1$ for all i. There are infinitely many primes p such that $2 \nmid \mathrm{ord}_p(a_i)$ for all i if and only if the equation $\prod a_i^{x_i} = -1$ has no integer solution $x_1, \ldots, x_n$. Furthermore, the density of such primes exists and is positive.*

We note that questions on the divisibility of orders of integers modulo primes have attracted some attention (see [6, Section 8.2] for a list of references), but in contrast to our results, previous considerations have focused on univariate cases, in particular on giving explicit formulas for the density of primes defined by a condition of form $m \mid \mathrm{ord}_p(a)$. Our focus here is determining the necessary conditions for the infinitude of the set of primes under consideration, not on explicit formulas. However, one can easily express the density as an infinite sum. For example, the density in Corollary 3.6 is easily seen (using the Chebotarev density theorem) to be equal to

$$\sum_{k=1}^{\infty} \left(\frac{1}{[\mathbb{Q}(\zeta_{2^k}, a_1^{1/2^k}, \ldots, a_n^{1/2^k}) : \mathbb{Q}]} - \frac{1}{[\mathbb{Q}(\zeta_{2^{k+1}}, a_1^{1/2^k}, \ldots, a_n^{1/2^k}) : \mathbb{Q}]} \right),$$

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

from which one can calculate the density in some concrete example cases. While such expressions for the density in the general case of Theorem 3.4 become much more cumbersome, one can show that the density is a rational number.

Note that the density indeed exists, even though this is unknown in the case of Theorem 3.1 (due to the presence of irrational pairs). The idea is the same as the one used for giving the above formula for the density: one can express the relevant set of primes as a countable disjoint union of sets of primes with suitable Artin symbols (by controlling divisors of $p-1$ and how perfect powers a_i are modulo p). The density of such sets tends to zero, so one can apply the Chebotarev density theorem to a finite number of them to obtain arbitrarily good approximations for the density. We omit the details – the reader may wish to consult [4].

4. Notation and conventions

The letter p denotes a (rational) prime. For an integer x not divisible by p the order $\mathrm{ord}_p(x)$ of x modulo p is the smallest positive integer e such that $x^e \equiv 1 \pmod{p}$. For $x \neq 0$ we denote by $v_p(x)$ the largest e such that $p^e | x$.

By ζ_k we denote a primitive kth root of unity.

For a Galois extension K of $\mathbb{Q}$ we denote by $\mathrm{Gal}(K/\mathbb{Q})$ its Galois group. For an unramified prime p the Artin symbol of p with respect to K is denoted by

$$\left(\frac{K/\mathbb{Q}}{p}\right).$$

We use the fact that an unramified p splits completely in K if and only if $\left(\frac{K/\mathbb{Q}}{p}\right)$ is the identity element of $\mathrm{Gal}(K/\mathbb{Q})$. If $K \subset L$, then the restriction of $\left(\frac{L/\mathbb{Q}}{p}\right)$ to $\mathrm{Gal}(K/\mathbb{Q})$ is $\left(\frac{K/\mathbb{Q}}{p}\right)$.

In particular, the Artin symbol of a prime p with respect to a extension such as $\mathbb{Q}(\zeta_n, a^{1/n})$ controls the remainder of p modulo n (via the image of the root of unity ζ_n) and whether a is a dth power modulo p or not for all $d \mid n$ (via the image of the element $a^{1/n}$).

We use the following version of the Chebotarev density theorem.

Theorem 4.1 *(Chebotarev density theorem). Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G, and let C be a conjugacy class of G. Then, the set*

$$S = \{p | p \text{ is unramified in } K \text{ and } \left(\frac{K/\mathbb{Q}}{p}\right) = C\}$$

has natural relative density $\frac{|C|}{|G|}$ in the primes.

As our proofs of infinitude of sets of primes are based on the Chebotarev density theorem, this will automatically lead to a positive lower density for the set at hand.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

5. Background on Kummer-type extensions

We state the following standard Kummer-theoretic results (see e.g. [3, Section 3]). More general results may be found for example in [9].

Proposition 5.1. *Let $a_1, \dots, a_k$ be multiplicatively independent rationals, and let K be a finite Galois extension of $\mathbb{Q}$. There exists a positive integer N with the following property:*

For any integers $n, m_1, \dots, m_k$, where $m_i \mid n$ for all i, and $x, x_1, \dots, x_k$ with $(x, Nn) = 1, N \mid x - 1, x_1, \dots, x_k$ there exists an element of the Galois group of

$$K(\zeta_{Nn}, a_1^{1/Nm_1}, \dots, a_k^{1/Nm_k})/K$$

sending

$$\zeta_{Nn} \to \zeta_{Nn}^x, a_i^{1/Nm_i} \to \zeta_{Nm_i}^{x_i} a_i^{1/Nm_i}.$$

Proposition 5.2. *Let $a_1, \dots, a_k$ be multiplicatively independent rationals, and let K be a finite Galois extension of $\mathbb{Q}$. There exists an integer N such that for any $n, n', m_1, \dots m_k$, where $(n, Nn') = 1$ and $m_i \mid n$ for all i, the fields*

$$\mathbb{Q}(\zeta_n, a_1^{1/m_1}, \dots, a_k^{1/m_k})$$

and

$$K(\zeta_{Nn'}, a_1^{1/Nn'}, \dots, a_k^{1/Nn'}),$$

are linearly disjoint and the former extension has degree $\phi(n) m_1 \cdots m_k$.

Recall that finite Galois extensions K_1 and K_2 are linearly disjoint (over $\mathbb{Q}$) if and only if one has the isomorphism $\mathrm{Gal}(K_1K_2/\mathbb{Q}) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$.

6. Necessity of the conditions of Theorem 3.1

Assume that there are infinitely many primes p satisfying the conditions of Theorem 3.1. Let $p > 2$ be such a prime which is larger than all of $|o_i|$ and $|e_i|$, and let $k = v_2(p-1)$. Now o_i is a perfect 2^kth power modulo p for all i, while the numbers e_i are not.

Let g be a primitive root modulo p. For all primes $q \in Q$, define $\ell(q)$ as some integer such that $g^{\ell(q)} \equiv q \pmod{p}$. Further define

$$\ell((-1)^{f_0} q_1^{f_1} \cdots q_{|Q|}^{f_{|Q|}}) = f_0 \frac{p-1}{2} + f_1 \ell(q_1) + \ldots + f_{|Q|} \ell(q_{|Q|}),$$

for any $f_0 \in \{0, 1\}$ and (not necessarily positive) integers f_i.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

Hence ℓ is defined in particular for all o_i and $a \in A$, with $g^{\ell(x)} \equiv x \pmod p$ for any x in the domain. Thus $2^k \mid \ell(o_i)$ and $2^k \nmid \ell(a)$ for $a \in A$. Note that any positive x, y in the domain satisfy $\ell(xy) = \ell(x) + \ell(y)$.

For $n < 0$ in the domain of ℓ we have

$$\ell(n) = \ell(|n|) + \frac{p-1}{2}.$$

Hence, $2^k \mid \ell(o_i)$ is equivalent with

$$\ell(|o_i|) \equiv 2^k \epsilon(o_i) \pmod{2^k}$$

and similarly $2^k \nmid \ell(a)$ is equivalent with

$$\ell(|a|) \not\equiv 2^k \epsilon(a) \pmod{2^k}.$$

Let $\mathbf{L} = (\ell(q_1), \dots, \ell(q_{|Q|}))$. Denoting by $\langle \mathbf{v}, \mathbf{w} \rangle = \sum v_i w_i$ the dot product, we have $\ell(|n|) = \langle \mathbf{L}, \mathbf{v}(n) \rangle$ for any n in the domain of ℓ. Thus, for any i there exists an integer x_i such that

$$\langle \mathbf{L}, \mathbf{v}(o_i) \rangle = \ell(|o_i|) = 2^k (x_i + \epsilon(o_i)),$$

and hence

$$\langle \mathbf{L}, \mathbf{v}(a) \rangle = \ell(|a|) = 2^k \left(\sum_{i=1}^{O} c_i \left(x_i + \epsilon(o_i) \right) \right).$$

By $\ell(|a|) \not\equiv 2^k \epsilon(a) \pmod{2^k}$, this implies

$$\sum_{i=1}^{O} 2^k c_i (x_i + \epsilon(o_i)) \not\equiv 2^k \epsilon(a) \pmod{2^k}.$$

Rearranging and multiplying by suitable powers of two yields that $(x_1, \dots, x_O)$ is a solution to (3.1).

7. Sufficiency of the conditions of Theorem 3.1

Here is the idea of the proof. The parity conditions are handled by using a solution to the system in Theorem 3.1 to decide on values of certain discrete logarithms (cf. Section 6, where values of discrete logarithms were used to obtain a solution to the system). The divisibility of orders is based on requiring $p \equiv 1 \pmod{q^k}$ for various primes q, where k is large. This leads to $q \mid \operatorname{ord}_p(c)$ with "high probability". Similarly, irrational pairs (a, b) are controlled by taking a large prime q and requiring a to be a perfect qth power modulo $p \equiv 1 \pmod q$, and now b is not a perfect qth power with high probability. The

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

imposed conditions can all be satisfied simultaneously by the tools in Section 5 and the Chebotarev density theorem.

The set $\{|o_1|, \dots, |o_O|\}$ is such that no element of A is multiplicatively independent with o_i (equivalently, $\mathbf{v}(a)$ lies in the $\mathbb{Q}$-span of $\mathbf{v}(o_i)$ for any $a \in A$). Construct a set S_1 by adjoining absolute values of elements of B to $\{|o_1|, \dots, |o_O|\}$ so that the elements of S_1 are multiplicatively independent and no element of B is multiplicatively independent with the elements of S_1.

Let $(c_i, q_i), 1 \le i \le n_1$ denote the pairs of integers corresponding to divisible pair for which we require $q_i \mid \mathrm{ord}_p(c_i)$. Expand the set S_1 to a multiplicatively independent set S_2 so that no element of $E \cup \{c_1, \dots, c_{n_1}\}$ is multiplicatively independent with the elements of S_2.

Let N be as in Proposition 5.1 when applied to the elements of S_2 (with the field $K = \mathbb{Q}$). Let T denote two times the product of the distinct primes in $\{q_1, \dots, q_{n_1}\}$.

We now prove the existence of infinitely many primes p with $2 \nmid \mathrm{ord}_p(o_i), 2 \mid \mathrm{ord}_p(e_i), q_i \mid \mathrm{ord}_p(c_i)$.

Let k be an arbitrarily large positive integer and let $x_1, \dots, x_O$ be a solution to (3.1). Construct the function $x : S_2 \to \mathbb{Z}$ as follows.

- For $o_i \in S_2$, choose $x(|o_i|)$ to be a uniformly random integer from $[1, 2^{M+1}T^k]$ satisfying $x(|o_i|) \equiv 2^k(x_i + \epsilon(o_i)) \pmod{2^{M+1+k}}$.
- For the elements $u \in S_2 \setminus \{o_1, \dots, o_O\}$, choose $x(u)$ uniformly at random from $[1, 2^{M+1}T^k]$.

Also, let $X = NT^k + 1$.

Consider an automorphism σ_x of

$$K_k = \mathbb{Q}(\zeta_{2^{M+2}NT^k}, S_2^{1/2^{M+1}NT^k}),$$

where $S^{1/n} = \{s^{1/n}, s \in S\}$, sending

$$\zeta_{2^{M+1}NT^k} \to \zeta_{2^{M+1}NT^k}^X, s_2^{1/2^{M+1}NT^k} \to \zeta_{2^{M+1}NT^k}^{Nx(s_2)} s_2^{1/2^{M+1}NT^k}$$

for all $s_2 \in S_2$. Such σ_x exists by the choice of N.

By the Chebotarev density theorem, there are infinitely many primes p whose Artin symbol with respect to K_k contains σ_x. Consider these primes p. We make the following five observations.

(i) $p \equiv X \pmod{2^{M+1}NT^k}$, so $p \equiv 1 \pmod{NT^k}$ and $v_2(p-1) = v_2(N) + k$.

(ii) By the choice of $x(|o_i|)$, the element $o_i^{1/2^{v_2(N)+k}}$ is fixed under σ_x. Thus, o_i is a perfect $2^{v_2(N)+k}$th power modulo p, and hence $\mathrm{ord}_p(o_i)$ is odd.

(iii) For any $a \in A$, let $M' = M'(a)$ be an odd integer such that $2^{M+1}M'\mathbf{c}(a)_i$ is an integer for any i. We have

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

$$|a|^{M'/2^{v_2(N)+k}} = |a|^{2^{M+1}M'/2^{v_2(N)+k+M+1}} = \prod_{i=1}^{O} |o_i|^{2^{M+1}M'\mathbf{c}(a)_i/2^{v_2(N)+k+M+1}},$$

and under σ_x this maps to

$$\prod_{i=1}^{O} \zeta_{2^{v_2(N)+k+M+1}}^{2^{M+1}M'\mathbf{c}(a)_i Nx(|o_i|)} |o_i|^{2^{M+1}M'\mathbf{c}(a)_i/2^{v_2(N)+k+M+1}}.$$

Hence $a^{M'/2^{v_2(N)+k}} = \zeta_{2^{v_2(N)+k+1}}^{2M'\epsilon(a)} |a|^{M'/2^{v_2(N)+k}}$ is fixed under σ_x if and only if

$$2^{M+1}M'N2^k\epsilon(a) + \sum_{i=1}^{O} 2^{M+1}M'\mathbf{c}(a)_i Nx(|o_i|) \equiv 0 \pmod{2^{v_2(N)+k+M+1}}.$$

After simplifying this is exactly the condition a solution to (3.1) avoids. Hence $a^{M'}$ and thus a is not a perfect $2^{v_2(N)+k}$th power modulo p, and thus $\mathrm{ord}_p(a)$ is even.

(iv) We claim that for any $b \in B$, the probability of $2 \mid \mathrm{ord}_p(b)$ (with respect to the random choice of σ_x) approaches 1 as $k \to \infty$. To do so, it suffices to ensure $4 \mid \mathrm{ord}_p(|b|)$ with probability tending to 1.

We may write $|b|$ as

$$|b| = \prod_{s \in S_1} s^{f(s)},$$

where $f(s) = f_b(s) \in \mathbb{Q}$ and $f(s) \neq 0$ for at least one $s \in S_1 \setminus \{|o_1|, \dots, |o_O|\}$. Let $M' = M'(b) \in \mathbb{Z}_+$ be such that all of $M'f(s)$ are integers. Consider the element

$$|b|^{M'/2^{v_2(N)+k}} = \prod_{s \in S_1} s^{M'f(s)/2^{v_2(N)+k}}$$

of K_k and its image

$$|b|^{M'/2^{v_2(N)+k}} \prod_{s \in S_1} \zeta_{2^{k+v_2(N)}}^{M'f(s)Nx(s)}$$

under σ_x. Since $f(s) \neq 0$ for at least one $s \in S_1 \setminus \{|o_1|, \dots, |o_O|\}$ and the corresponding $x(s)$ is random modulo 2^k, as $k \to \infty$ the probability that

$$\sum_{s \in S_1} M'f(s)Nx(s) \equiv 0 \pmod{2^{k+v_2(N)-1}}$$

approaches 0. Thus, the probability of choosing σ_x such that $|b|^{M'}$ is a perfect $2^{k+v_2(N)-1}$th power modulo p approaches zero. This means that there are "many" choices of σ_x such that $\mathrm{ord}_p(|b|^{M'})$ and thus $\mathrm{ord}_p(|b|)$ is divisible by 4 for the primes p with $\sigma_x \in \left(\frac{K_k/\mathbb{Q}}{p}\right)$.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

(v) Let $(c_i, q_i), 1 \le i \le n_1$ be some pair corresponding to a divisible pair, so we want $q_i \mid \mathrm{ord}_p(c_i)$. We claim that this happens with probability approaching 1 as $k \to \infty$. The proof is similar to the one in (iv): Write

$$|c_i| = \prod_{s \in S_2} |s|^{f(s)},$$

where $f : S_2 \to \mathbb{Q}$. Let $M' = M'(c_i) \neq 0$ be such that $M'f(s)$ is an integer for all $s \in S_2$. The element $|c_i|^{M'/q_i^{v_q(N)+k}}$ is fixed under σ_x if and only if

$$\sum_{s \in S_2} M'f(s)Nx(s) \equiv 0 \pmod{q_i^{v_q(N)+k}}.$$

As the numbers $x(s)$ are random modulo q_i^k, this happens with probability approaching 0, so $\mathrm{ord}_p(|c_i|^{M'})$ and hence $\mathrm{ord}_p(c_i)$ is divisible by q_i with high probability.

Hence there exist some k and σ_x such that the primes p with $\sigma_x \in \left(\frac{K_k/\mathbb{Q}}{p}\right)$ satisfy the conditions $2 \nmid \mathrm{ord}_p(o_i), 2 \mid \mathrm{ord}_p(e_i), q_i \mid \mathrm{ord}_p(c_i)$. We are left with handling the irrational pairs.

Let $(a_1, b_1), \dots, (a_{n_2}, b_{n_2})$ be the irrational pairs. For each $1 \le i \le n_2$, pick a prime q_i such that the fields

$$L_i = \mathbb{Q}(\zeta_{q_i}, a_i^{1/q_i}, b_i^{1/q_i})$$

and the field K_k constructed above are linearly disjoint and such that the degree of L_i is the maximum possible $q_i^2(q_i - 1)$ for all i. The existence of such primes q_i is guaranteed by Proposition 5.2. (In fact, any choice of large enough distinct primes works.)

For each L_i there exists an element of $\mathrm{Gal}(L_i/\mathbb{Q})$ fixing ζ_{q_i} and a_i^{1/q_i} but which does not fix b_i^{1/q_i}. The primes p with the corresponding Artin symbol are such that $p \equiv 1 \pmod{q_i}$, a_i is a q_ith power modulo p and b_i is not. This leads to the insolvability of $a_i^x \equiv b_i \pmod{p}$.

We have already proved the existence of an element of $\mathrm{Gal}(K_k/\mathbb{Q})$ taking care of parities and divisibilities of orders. By linear disjointness,

$$\mathrm{Gal}(K_k L_1 \cdots L_{n_2}/\mathbb{Q}) \cong \mathrm{Gal}(K_k/\mathbb{Q}) \times \mathrm{Gal}(L_1/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(L_{n_2}/\mathbb{Q}).$$

We may therefore merge the constructed maps on $K_k, L_1, \dots, L_{n_2}$ to an automorphism of the compositum $K_k L_1 \cdots L_{n_2}$. The infinitely many primes p with the corresponding Artin symbol satisfy the conditions of Theorem 3.1.

8. Proof of Theorem 3.4

Clearly (i) implies (ii), so we focus on the other direction.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

The idea is roughly as follows. Let $\ell_1, \dots, \ell_m$ be the primes which divide at least one of $a_1, \dots, a_n$. For each prime $q \mid m_1 \cdots m_n$ take a large prime p, and consider which of the numbers of the form $\ell_1^{e_1} \cdots \ell_m^{e_m}, e_i \in \mathbb{Z}$ are perfect q^kth powers modulo p for $k = 1, 2, \dots$ This tells us how we should choose q^kth power residues modulo p in order to guarantee $\gcd(\mathrm{ord}_p(a_i), q^{v_q(m_i)}) = q^{v_q(g_i)}$. We then prove that one may combine these conditions.

Fix some prime $q \mid m_1 \cdots m_n$, and let $p \nmid 2qa_1 \cdots a_n$ be a prime such that $q^{v_q(g_i)} \mid \mathrm{ord}_p(a_i)$ and $q^{v_q(g_i)+1} \nmid \mathrm{ord}_p(a_i)$ when $q \mid m_i/g_i$. Denote $k = v_q(p-1)$. Now p is unramified in

$$K_{q,k} = \mathbb{Q}(\zeta_{2q^{k+1}}, \ell_1^{1/q^k}, \dots, \ell_m^{1/q^k}).$$

Let C denote the Artin symbol of p with respect to $K_{q,k}$, and let $\sigma_{q,k}$ be any of its elements. Let $\sigma_{q,k}$ map

$$\zeta_{2q^{k+1}} \to \zeta_{2q^{k+1}}^x, \ell_i^{1/q^k} \to \zeta_{q^k}^{x_i} \ell_i^{1/q^k}.$$

By the choice of p we have

$$v_q(x-1) = k, \tag{8.1}$$

and by the divisibility conditions on orders

$$v_q\left((x-1)\epsilon(a_j) + \sum_{i=1}^m v_{\ell_i}(a_j)x_i\right) \le k - v_q(g_j) \tag{8.2}$$

for all $1 \le j \le n$, equality occurring at least when $q \mid m_j/g_j$. Here $\epsilon(a_j) = 0$ if $a_j > 0$ and $\epsilon(a_j) = 1/2$ if $a_j < 0$, this term being present since for $a_j < 0$ we have

$$\begin{aligned}\sigma_{q,k}(a_j^{1/q^k}) &= \zeta_{2q^k}^x \sigma_{q,k}(|a_j|^{1/q^k}) = \zeta_{2q^k}^x \zeta_{q^k}^{\sum_{i=1}^m v_{\ell_i}(a_j)x_i} |a_j|^{1/q^k} \\ &= \zeta_{q^k}^{(x-1)/2 + \sum_{i=1}^m v_{\ell_i}(a_j)x_i} a_j^{1/q^k}.\end{aligned}$$

The transformation $x - 1 \to q(x-1)$, $x_i \to qx_i, k \to k+1$ does not affect the truth of (8.1) nor (8.2). We deduce that for any prime q and positive integer k, there exist integers $x, x_1, \dots, x_m$ satisfying $x > 1, q^k \mid x-1, x_1, \dots, x_m$ and

$$v_q\left((x-1)\epsilon_j + \sum_{i=1}^m v_{\ell_i}(a_j)x_i\right) \le v_q(x-1) - v_q(g_j), \tag{8.3}$$

again with equality when $q \mid m_j/g_j$.

Let N be as in Proposition 5.1 when applied to the numbers $\ell_1, \dots, \ell_m$. Let T be the product of all primes dividing at least one of $m_1, \dots, m_n$. By the Chinese remainder

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

theorem there exist integers $x, x_1, \dots, x_m$ satisfying $x > 1$, $N \mid x-1, x_1, \dots, x_m$, and (8.3) for all $q \mid T, 1 \le j \le n$ (again with correct equality cases). We may additionally assume $\gcd(x, 2NT) = 1$. Let

$$P = \prod_{q \mid T} q^{v_q(x-1)+1}.$$

By the choice of N, there exists an automorphism σ of

$$K = \mathbb{Q}(\zeta_{2NP}, \ell_1^{1/NP}, \dots, \ell_m^{1/NP})$$

mapping

$$\zeta_{2NP} \to \zeta_{2NP}^x, \ell_i^{1/NP} \to \zeta_{NP}^{x_i} \ell_i^{1/NP}.$$

Apply the Chebotarev density theorem. Let p be a prime whose Artin symbol with respect to K contains σ. From (8.3) one now sees that $\mathrm{ord}_p(a_j)$ is divisible by $q^{v_q(g_j)}$ for all $q \mid T, 1 \le j \le n$, and not by $q^{v_q(g_j)+1}$ for $q \mid m_j/g_j$.

Remark 8.1. The degree of

$$\mathbb{Q}(\zeta_t, \ell_1^{1/t}, \dots, \ell_m^{1/t})$$

is not in general $\phi(t)t^m$ due to square roots of integers lying in cyclotomic fields. (In fact, this is the only reason for non-maximality, and at least for t odd the degree is $\phi(t)t^m$.) Since the degree is not maximal, there are some restrictions on the images of ζ_t and $\ell_i^{1/t}$ under the elements of the Galois group. However, the degree is almost maximal by Proposition 5.1 (in this case the degree is at least $\phi(t)t^m/2^m$), so by repeatedly performing the transformation $x-1 \to q(x-1), x_i \to qx_i, k \to k+1$ in the proof we get away from these "low-level" restrictions on the elements of the Galois group.

References

[1] D.R. Heath-Brown, Artin's conjecture for primitive roots, Q. J. Math. 37 (1) (03 1986) 27–38.
[2] C. Hooley, On Artin's conjecture, J. Reine Angew. Math. 225 (1967) 209–220.
[3] O. Järviniemi, Equality of orders of a set of integers modulo a prime, Proc. Am. Math. Soc. 149 (09) (2021) 3651–3668.
[4] J.C. Lagarias, The set of primes dividing the Lucas numbers has density 2/3, Pac. J. Math. 118 (2) (1985) 449–461.
[5] K. Matthews, A generalisation of Artin's conjecture for primitive roots, Acta Arith. 29 (2) (1976) 113–146.
[6] P. Moree, Artin's primitive root conjecture – a survey, Integers 12 (2005) 01.
[7] P. Moree, P. Stevenhagen, A two-variable Artin conjecture, J. Number Theory 85 (2) (2000) 291–304.
[8] M.R. Murty, F. Séguin, C.L. Stewart, A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences, J. Number Theory 194 (2019) 8–29.
[9] A. Perucca, P. Sgobba, Kummer theory for number fields and the reductions of algebraic numbers, Int. J. Number Theory 15 (08) (2019) 1617–1633.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007

[10] A. Schinzel, On the congruence $a^x \equiv b \pmod{p}$, Bull. Acad. Pol. Sci., Sér. Sci. Math. Astron. Phys. 8 (1960) 307–309.
[11] A. Schinzel, Systems of exponential congruences, Demonstr. Math. 18 (1) (1985) 377–396.
[12] L. Somer, Linear recurrences having almost all primes as maximal divisors, in: Fibonacci Numbers and Their Applications, Patras, 1984, 1986, pp. 257–272.

Please cite this article in press as: O. Järviniemi, Simultaneous insolvability of exponential congruences, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2021.12.007