Uniform Distribution Theory **2** (2007), no.2, 19–34

uniform distribution theory

COMMON PRIME FACTORS OF $a^n - b$ AND $c^n - d$

Christian Ballot — Florian Luca

ABSTRACT. In this note, we study the set of primes such that the two congruences $a^n \equiv b \pmod{p}$ and $c^n \equiv d \pmod{p}$ have a simultaneous solution n under some assumptions on the rationals $a,\ b,\ c,\ d$.

Communicated by Sergei Konyagin

1. Introduction

Motivated by a question of Schinzel, Skałba [9] investigated the set $\mathcal{S}$ of primes p dividing $\gcd(2^n-3, 3^n-2)$ for some positive integer n. Writing $\mathcal{S}(x) = \mathcal{S} \cap [1, x]$, Skalba showed that

$$\#\mathcal{S}(x) \ll x/(\log x)^{\nu+o(1)}, \qquad \text{as } x \to \infty, \tag{1}$$

where $\nu = 8/9 + 2\beta \log \beta$, and β is the only solution in the interval $(0,1)$ of the transcendental equation $\beta \log \beta - (1 + 6\log(10/9))\beta + 4/3 = 0$. Numerically, $\beta = 0.642903968956\ldots$ and $\nu = 1.024362276264\ldots.$ He also noted that his approach combined with results concerning divisors of shifted primes in short intervals from [4] leads to the better exponent $\nu = 2 - (1 + \log\log 2)/\log 2 = 1.08607133206\ldots.$

In this paper, $a,\ b,\ c$ and d being non-zero rational numbers, we investigate the set of primes for which the system of simultaneous exponential congruences

$$a^n \equiv b \pmod{p} \qquad \text{and} \qquad c^n \equiv d \pmod{p}, \tag{2}$$

is solvable for some natural number n. We say that the prime p divides the rational number r if p divides the numerator of r and $a^n \equiv b \pmod{p}$ if p divides $a^n - b$. We use again the same notation $\mathcal{S} = \mathcal{S}(a,b,c,d)$ for the set of primes for which (2) is solvable.

The set of primes for which only one, instead of two, such congruences is solvable has been the subject of many studies. The set of primes arising as

2000 Mathematics Subject Classification: 11N37, 11A07.
Keywords: Greatest common divisor, prime numbers, congruences.

a factor of some term of an integral binary linear recurrence may yield such a congruence. As explained in Section 3 of [1], our motivation came from the study of the set of primes that are a factor of two consecutive terms of some integral ternary linear recurrence, a set which can be expressed as the set of primes for which a system like (2) is solvable.

Here we restrict our attention to the case when the rank of the multiplicative group generated by the four numbers a, b, c and d inside $\mathbb{Q}^*$ is 2 at most.

Two main cases are distinguished. Let

$$M(a,b,c,d) = \begin{bmatrix} \log|a| & \log|c| \\ \log|b| & \log|d| \end{bmatrix}, \tag{3}$$

where log stands for the natural logarithm. We say that (a,b,c,d) is in the *singular case* if the rational rank of M is 1. By this we mean that *either* the rows of M *or* the columns of M are linearly dependent and the linear dependence relation has rational coefficients. This case is thus divided into the *row-singular* case and the *column-singular* case. The case of the rational rank of M being 2 is referred to as the *regular* case. Note that we end our paper with an appendix containing a proof that the rational rank of M is 1 at most if and only if $\det M = 0$.

Our main result is the following theorem.

Theorem 1. *Assume that a, b, c, d are non-zero rational numbers, $a \neq 1$, $c \neq 1$, and $\operatorname{rank}\langle a,b,c,d\rangle_{\mathbb{Q}^*}$ is 1 or 2. If (a,b,c,d) is in the regular case, then for every $\varepsilon > 0$ the inequality*

$$\#\mathcal{S}(x) \leq \frac{x}{\log x(\log\log\log x)^{1/2-\varepsilon}}$$

holds for all $x > x(\varepsilon)$. Thus $\mathcal{S}$ has 0 natural density within the set of primes.

On the other hand, if (a,b,c,d) is in the singular case and b and d are positive, then $\mathcal{S}$ has positive lower relative asymptotic density. In the row-singular case our proof of the existence of a positive lower density is unconditional, whereas, in the column-singular case, the result is unconditional in the rank 1 case, but depends on the generalized Riemann hypothesis in the rank 2 case.

Note that (a,b,c,d) is in the regular case if and only if (a^2,b^2,c^2,d^2) is. Moreover, by squaring the congruences in (2), we see that $\mathcal{S}(a,b,c,d) \subset \mathcal{S}(a^2,b^2,c^2,d^2)$, so that to prove the result of our theorem in the regular case, we may replace a, b, c, d by their squares and assume that they are all positive. In fact, we do assume throughout Sections 3.2 and 3.3 that a, b, c, d are positive. But, in the singular case, we determine a set of primes of positive lower density solving (2) and see that it solves (2) irrespective of the signs of a and c, which explains the statement we have in this case. We also assume that $a \neq 1$ and $c \neq 1$ (for if not, either the corresponding b or d is 1, in which case the resulting congruence is trivial and gives no information, or it is not in which case $\mathcal{S}$ is finite). Our results are always stated up to finitely many exceptional primes. In particular primes dividing the numerators or the denominators of either a, b, c or d are excluded from consideration.

Skałba's method does not only apply to the case $(a, b, c, d) = (2, 3, 3, 2)$, but to a more general situation, where a, b, c and d satisfy some technical condition (see [9]). This technical condition is satisfied, for instance, when a and b are multiplicatively independent and the ordered pairs (a, b) and (d, c) are identical. It does not cover all the cases we cover, nor do we cover all instances of rationals satisfying his technical condition. In fact, under Skałba's hypothesis, the multiplicative group generated by the four rationals a, b, c and d may have rank equal to 3.

For instance, consider the following systems of congruences

$$2^n \equiv 25 \pmod{p} \qquad \text{and} \qquad 15^n \equiv 36 \pmod{p}, \tag{4}$$

$$\left(\frac{s}{t}\right)^n \equiv \frac{1}{t} \pmod{p} \qquad \text{and} \qquad s^n \equiv -\frac{1}{ts^2} \pmod{p}, \tag{5}$$

where t is an integer satisfying $|t| \geq 2$ and $s = t^2 - t + 1$, and

$$3^n \equiv 2 \pmod{p} \qquad \text{and} \qquad 5^n \equiv 3 \pmod{p}. \tag{6}$$

The sets $\mathcal{S}$ associated to system (4) or to the systems in (5) all have a 0 natural density of primes. System (4) falls under Skałba's condition. Note that $\langle 2, 25, 15, 36 \rangle = \langle 2, 3^2, 3 \cdot 5 \rangle$ and our theorem does not apply here. However Skalba's conditions are not satisfied by any system in (5), but by squaring the two congruences of such a system, we get a regular rank 2 system since $\langle s^2/t^2, 1/t^2, s^2, 1/t^2 s^4 \rangle = \langle s^2, t^2 \rangle$. Thus our result applies. But system (6) is a simple rank 3 system to which neither our work nor Skałba's result apply.

Throughout this paper, we use the Vinogradov symbols $\gg$ and $\ll$ and the Landau symbols O and o with their regular meanings. The constants implied by them might depend on some other parameters such as a, b, c, d, K, ε, etc. For coprime integers $1 \leq k \leq \ell$, we write $\pi(x; k, \ell)$ for the number of primes $p \leq x$ in the arithmetic progression $\ell \pmod{k}$. For a matrix A we use A^T to denote its transpose.

Acknowledgements. This paper was initiated during a very enjoyable visit by the second author to the Laboratoire Nicolas Oresme of the University of Caen; he wishes to express his thanks to that institution for its hospitality and support. During the preparation of this paper, F. L. was also partly supported by grants

SEP-CONACYT 46755, PAPIIT IN104505 and a Guggenheim Fellowship. The authors are thankful to the referee for a fast appreciation.

2. Preliminary Results

The first preliminary result is essentially an argument due to Hooley from [3]. Let a and b be any fixed non-zero rational numbers. Let $\mathcal{T}_{a,b}$ be the set of all primes dividing some non-zero expression of the form $a^t - b$ for some positive integer t. Note that, by Fermat's Little Theorem, if $p \in \mathcal{T}_{a,b}$ is sufficiently large (i.e., it does not divide either the numerator or the denominator of either a or b), then p divides some non-zero expression of the form $a^t - b$ for some positive $t \le p-1$. For any real numbers $1 \le y \le x$ we put

$$\mathcal{T}_{a,b}(x,y) = \{p \le x \ : \ p \mid a^t - b \text{ for some } t \le y \text{ and } a^t - b \ne 0\}.$$

The result we will use is the following:

Proposition 2. *Uniformly for $1 \le y \le x$, we have*

$$\#\mathcal{T}_{a,b}(x,y) \ll \frac{y^2 + x^{1/2}}{\log x}.$$

Proof. We may assume $|a| > 1$, for if $|a| < 1$, then we may replace a by $1/a$ and b by $1/b$. Writing $a = a_1/a_2$, $b = b_1/b_2$, with a_1, a_2, b_1, b_2 integers and $a_1 > 0$ and putting $\mathcal{T}_1 = \{p \le \sqrt{x}\}$, we get by the Prime Number Theorem that $\#\mathcal{T}_1 \ll x^{1/2}/\log x$. Put $\mathcal{T}_2 = \mathcal{T}_{a,b}(x,y) \backslash \mathcal{T}_1$. Then

$$\begin{aligned} x^{\#\mathcal{T}_2/2} &\le \prod_{\substack{p \in \mathcal{T}_{a,b}(x,y) \\ p \ge x^{1/2}}} p \le \prod_{\substack{1 \le t \le y \\ a^t - b \ne 0}} |b_2 a_1^t - b_1 a_2^t| \le O\big((|b_1| + |b_2|)^y\big) |a_1|^{\sum_{1 \le t \le y} t} \\ &= \exp(O(y^2)), \end{aligned}$$

which gives $\#\mathcal{T}_2 \ll y^2/\log x$ and completes the proof of the proposition. □

The next result appears in [4].

Proposition 3. *Let K be any positive constant. The set of primes $p \le x$ such that $p-1$ has a divisor in the interval $[x^{1/2}/(\log x)^K, x^{1/2}(\log x)^K]$ has cardinality $O(x \log\log x/(\log x)^{1+\nu})$, where $\nu = 2 - (1 + \log\log 2)/\log 2 = 0.08607133\ldots$.*

Let $f(X)$ be any integer valued irreducible polynomial with rational coefficients of degree > 1. For a positive real number x and a rational number $a \neq 0, \pm 1$, we write

$$\mathcal{U}_{a,f}(x) = \{p \leq x : p \mid a^{f(n)} - 1 \text{ for some positive integer } n\}.$$

Proposition 4. *Let $f(X) \in \mathbb{Q}[X]$ be integer valued, irreducible and of degree $d \geq 2$. For every $\varepsilon > 0$ there exists $x_\varepsilon > 0$ such that the inequality*

$$\#\mathcal{U}_{a,f}(x) < \frac{x}{\log x (\log\log\log x)^{(d-1)/d! - \varepsilon}} \qquad \text{holds for } x > x_\varepsilon.$$

Proof. This result appears in [1], but only for an integer a not 0 or ± 1. Here, we merely indicate to the reader how to adjust the proof in [1] to the case of $a \in \mathbb{Q}$. To prove the result in [1], we needed an estimate for $\#\mathcal{A}(x, m)$, the number of prime numbers $p \leq x$ such that m divides the order of a modulo p, with an error term *uniform* in the natural number m. To be precise, we had for every $\varepsilon > 0$

$$\#\mathcal{A}(x, m) = \kappa_m \left(1 + O\left(\frac{m^{1-2\varepsilon}}{(\log x)^{1/8-\varepsilon}}\right)\right) \pi(x),$$

for some explicit positive constant κ_m, uniformly in m and x.

Now by Theorem 2 of [6], for m odd and squarefree, and g a rational, the natural density $\delta_g(m)$ of the set of primes p for which m divides the order of g modulo p exists and is again equal to

$$\delta_g(m) = \kappa_m = \prod_{\ell \mid m} \frac{\ell^2}{\ell^2 - 1}, \qquad (\ell \text{ prime}),$$

where κ_m is the real number that appeared above in the expression of $\#\mathcal{A}(x, m)$, as long as g is not a k-th power of a rational for any $k \geq 2$. This last condition may be achieved by replacing $f(X)$ by the integer valued polynomial $h(X) = kf(X)$.

Now Lemma 1 of [6], gives an estimate for the number of primes $p \leq x$ for which m divides the order of g modulo p with an error term E given as

$$E = \pi(x)\, O_m\left(\frac{(\log\log x)^{\omega(m)}}{(\log x)^{1/8}}\right).$$

However, by working out the dependency of E on m in Lemma 2 and in the proof of Lemma 1 in [6], and in particular using the estimate $\omega(m)/\varphi(m) \ll (\log m)/m$, we got

$$E = \pi(x)\, O\left(\frac{\log m\ (\log\log x)^{\omega(m)}}{(\log x)^{1/8}}\right). \tag{7}$$

With the above remarks, we can reiterate the proof of Theorem 1 in [1]. For x large and $y = \frac{1}{20}\log\log x$, we considered all odd primes $q_1, \dots, q_s \le y$ not dividing the polynomial sequence $(f(n))_{n\ge 0}$ so as to get an asymptotic formula with a main term and an error term bounding above $\#\mathcal{U}_{a,f}(x)$. This argument carries over to the case of a rational. Indeed, the expression of the main term remains identical if we set $y = \alpha \log\log x$, for any positive real number α. Also, in this proof, m being any factor of the integer $q_1 \dots q_s$, we have for x large enough $\omega(m) \le s \le \pi(y) = \big(1 + o(1)\big)y/\log y \le 2\alpha(\log\log x)/\log\log\log x$, implying $(\log\log x)^{\omega(m)} \le (\log x)^{2\alpha}$. Noting that $\log m \le m$, we end up with the exact same error term we got in [1], i.e. $E = \pi(x)\ O\big((\log x)^{-1/20}\big)$, if we choose $\alpha = 1/40$. □

3. The Proof

3.1. A basic lemma

In this subsection we prove a lemma valid in both the regular and the singular cases. The signs of the non-zero rationals a, b, c and d are also irrelevant.

Lemma 5. *If $a^n \equiv b \pmod p$ and $c^n \equiv d \pmod p$ and the rank of $\langle a,\ b,\ c,\ d\rangle_{\mathbb{Q}^*}$ is at most 2, then there are three rational integers A, B and C such that the congruence*

$$x^{An^2+Bn+C} \equiv 1 \pmod p, \tag{8}$$

holds for $x = a, b, c$ or d.

Proof. Since the rank of $\langle a,\ b,\ c,\ d\rangle_{\mathbb{Q}^*}$ is 2 at most, it follows that there exist at least two linearly independent vectors $(\alpha_i, \beta_i, \gamma_i, \delta_i) \in \mathbb{Z}^4$ for $i = 1,\ 2$, such that

$$a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} = 1, \qquad \text{for } i = 1,\ 2. \tag{9}$$

Raising the two congruences

$$a^n \equiv b \pmod p, \qquad \text{and} \qquad c^n \equiv d \pmod p, \tag{10}$$

to the powers α_i and γ_i, respectively, and multiplying the resulting relations, we get

$$a^{\alpha_i n} c^{\gamma_i n} \equiv b^{\alpha_i} d^{\gamma_i} \pmod p, \qquad \text{for } i = 1,\ 2.$$

Using relations (9) to replace $a^{\alpha_i} c^{\gamma_i}$ by $b^{-\beta_i} d^{-\delta_i}$, we get

$$b^{-\beta_i n} d^{-\delta_i n} \equiv b^{\alpha_i} d^{\gamma_i} \pmod p, \qquad \text{for } i = 1,\ 2,$$

which we rewrite as

$$b^{\beta_i n + \alpha_i} d^{\delta_i n + \gamma_i} \equiv 1 \pmod p, \qquad \text{for } i = 1,\ 2. \tag{11}$$

Raising congruence (11) above to the power $\beta_2 n + \alpha_2$, for $i = 1$, and to the power $\beta_1 n + \alpha_1$, for $i = 2$, and dividing the two resulting relations, we get

$$d^{(\beta_2 n+\alpha_2)(\delta_1 n+\gamma_1)-(\beta_1 n+\alpha_1)(\delta_2 n+\gamma_2)} \equiv 1 \pmod{p}. \tag{12}$$

If instead we would have raised congruence (11) for $i = 1$ to $\delta_2 n + \gamma_2$ and the one for $i = 2$ to $\delta_1 n + \gamma_1$ and divided the resulting congruences we would have gotten the same congruence as (12) with d replaced by b.

Thus, if we write

$$\begin{aligned} A &= \beta_2\delta_1 - \beta_1\delta_2, \\ B &= (\beta_2\gamma_1 - \beta_1\gamma_2) + (\alpha_2\delta_1 - \alpha_1\delta_2), \\ C &= \alpha_2\gamma_1 - \alpha_1\gamma_2, \end{aligned}$$

we get that

$$b^{An^2+Bn+C} \equiv 1 \pmod{p}, \tag{13}$$

and that the same congruence holds true with b replaced by d.

If instead we had raised the two congruences (10) to the powers β_i and δ_i, respectively, and multiplied them out we would have gotten, using (9)

$$a^{\beta_i n} c^{\delta_i n} \equiv b^{\beta_i} d^{\delta_i} \equiv a^{-\alpha_i} c^{-\gamma_i} \pmod{p}, \qquad \text{for } i = 1,\ 2,$$

giving

$$a^{\beta_i n+\alpha_i} c^{\delta_i n+\gamma_i} \equiv 1 \pmod{p} \qquad \text{for } i = 1,\ 2. \tag{14}$$

Now raising congruences (14) above to the power $\beta_2 n + \alpha_2$, for $i = 1$, and to the power $\beta_1 n + \alpha_1$, for $i = 2$, we get

$$c^{(\beta_2 n+\alpha_2)(\delta_1 n+\gamma_1)-(\beta_1 n+\alpha_1)(\delta_2 n+\gamma_2)} \equiv 1 \pmod{p},$$

which shows that congruence (13) holds with b replaced by c. Finally, a similar argument also shows that congruence (13) holds when b is replaced by a. □

3.2. The regular case

We proceed in several steps. Recall that, for convenience, we assume the rationals $a,\ b,\ c$ and d positive so that

$$M(a,b,c,d) = \begin{bmatrix} \log a & \log c \\ \log b & \log d \end{bmatrix}.$$

Step 1. *One of the two vectors (β_i, δ_i) is zero for $i = 1$ or 2.*

Assume, say that $(\beta_1, \delta_1) = (0, 0)$ and p to be a prime in $\mathcal{S}$. Then the first relation (9) is $a^{\alpha_1} c^{\gamma_1} = 1$. This leads, upon exponentiation by n, and using $a^{\alpha_1 n} \equiv b^{\alpha_1} \pmod{p}$ and $c^{\gamma_1 n} \equiv d^{\gamma_1} \pmod{p}$, to the relation $b^{\alpha_1} d^{\gamma_1} \equiv 1 \pmod{p}$. So, $\mathcal{S}$ is finite unless $b^{\alpha_1} d^{\gamma_1} = 1$. But if $b^{\alpha_1} d^{\gamma_1} = 1 = a^{\alpha_1} c^{\gamma_1}$, we get that $(\alpha_1, \gamma_1)^T$ is a non-trivial rational zero of the matrix $M(a, b, c, d)$, which is a contradiction. □

From now on, we assume that $(\beta_i, \delta_i) \neq 0$ for $i = 1,\ 2$. We analyze the expression

$$f(n) = An^2 + Bn + C.$$

Step 2. *The case $A = B = C = 0$.*

We are about to show that this case cannot occur under our hypotheses. Since $A = 0$, there is a $\lambda \in \mathbb{Q}$ such that

$$(\beta_2, \delta_2) = (\lambda\beta_1, \lambda\delta_1).$$

Also $C = 0$ implies the existence of a rational μ with

$$(\alpha_2, \gamma_2) = (\mu\alpha_1, \mu\gamma_1).$$

Therefore, $B = (\lambda\beta_1\gamma_1 - \beta_1\mu\gamma_1) + (\delta_1\mu\alpha_1 - \alpha_1\lambda\delta_1) = (\lambda - \mu)(\beta_1\gamma_1 - \alpha_1\delta_1)$. Since $B = 0$, one has $\lambda = \mu$ or $\beta_1\gamma_1 - \alpha_1\delta_1 = 0$. But $\lambda = \mu$ cannot be for it would mean that the two vectors $v_i = (\alpha_i, \beta_i, \gamma_i, \delta_i),\ i = 1,\ 2$, are linearly dependent. Hence $\lambda - \mu$ is a non-zero rational number.

Now $\beta_1\gamma_1 - \alpha_1\delta_1 = 0$ implies the existence of a $\nu \in \mathbb{Q}$ with

$$\begin{aligned} \beta_1 &= \nu\alpha_1, \\ \delta_1 &= \nu\gamma_1. \end{aligned}$$

Note that since (β_1, δ_1) is not the zero vector, ν is non-zero and the vector (α_1, γ_1) is not the zero vector.

Let us rewrite relations (9)

$$\begin{aligned} 1 &= a^{\alpha_1} b^{\nu\alpha_1} c^{\gamma_1} d^{\nu\gamma_1}, \\ 1 &= a^{\mu\alpha_1} b^{\lambda\nu\alpha_1} c^{\mu\gamma_1} d^{\lambda\nu\gamma_1}. \end{aligned}$$

Raising the first relation to the λ^{th} power (resp. μ^{th} power) and dividing through by the second yields respectively

$$a^{\alpha_1(\lambda-\mu)} c^{\gamma_1(\lambda-\mu)} = 1 \quad \text{and} \quad b^{\nu\alpha_1(\lambda-\mu)} d^{\nu\gamma_1(\lambda-\mu)} = 1,$$

implying $a^{\alpha_1} c^{\gamma_1} = 1$ and $b^{\alpha_1} d^{\gamma_1} = 1$. But these two identities mean that the non-zero vector $(\alpha_1, \gamma_1)^T$ is in the kernel of $M(a, b, c, d)$, which contradicts our hypothesis. □

So, from now on, we may and will assume that $f(X)$ is not zero.

Step 3. *$f(X)$ is of degree 0 or 1.*

Then $f(n) = Bn + C$. Thus,

$$a^{Bn+C} \equiv 1 \pmod{p}, \qquad \text{which yields} \qquad b^B a^C \equiv 1 \pmod{p},$$

and

$$c^{Bn+C} \equiv 1 \pmod p \qquad \text{yielding} \qquad d^B c^C \equiv 1 \pmod p,$$

so either $\mathcal{S}$ is finite, or $a^C b^B = c^C d^B$, giving that $(C, B)^T$ is a non-zero rational vector in the kernel of $M(a, b, c, d)^T$, which is again not the case we are considering. □

Therefore in the last three steps, we assume $f(X)$ to be of degree 2.

Step 4. *$f(X) \in \mathbb{Q}[X]$ is irreducible.*

In this case, by Proposition 4, we get that

$$\#\mathcal{S}(x) = O\left(\frac{x}{\log x (\log\log\log x)^{1/2-\varepsilon}}\right).$$

□

Step 5. *$f(X)$ has two distinct rational roots.*

The crux of our proof is, in this case, embedded in the lemma below.

Lemma 6. *Let $a,\ b \in \mathbb{Q}^*\backslash\{\pm 1\}$, α, β, γ and δ be rational integers such that*

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0.$$

Then the set $\mathcal{R}$ of primes p for which the system

$$\begin{aligned} a^{\alpha n+\beta} &\equiv 1 \pmod p, \\ b^{\gamma n+\delta} &\equiv 1 \pmod p, \end{aligned}$$

is solvable (for some n in $\mathbb{N}$), satisfies

$$\#\mathcal{R}(x) \ll \frac{x \log\log x}{(\log x)^{1+\nu}},$$

where $\nu = 2 - (1 + \log\log 2)/\log 2 > 0$.

Proof. Assume x is large and p is in $\mathcal{R}(x)$. Putting $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_p(b)$, we have, for some n in $\mathbb{N}$, $e \mid \alpha n + \beta$, $f \mid \gamma n + \delta$, and therefore $\gcd(e, f) \mid \gamma(\alpha n + \beta) - \alpha(\gamma n + \delta) = \gamma\beta - \alpha\delta$, a non-zero integer by our hypothesis. Thus, $\gcd(e, f) = O(1)$. Since $\mathrm{lcm}[e, f]$ divides $p - 1$, we get that $ef = \mathrm{lcm}[e, f] \gcd(e, f) = O(p - 1) = O(x)$ if $p \in \mathcal{R}(x)$. Hence, writing $y = x^{1/2}/\log x$, at least one of the three statements below holds true : $e < y$, or $f < y$, or $e \in [y, x^{1/2} \log^2 x]$. Indeed, for x large enough, if f were larger than y and e larger than $x^{1/2} \log^2 x$, then we would have $ef > x \log x$ contradicting $ef = O(x)$.

Writing $\mathcal{R}_1(x) = \{p \in \mathcal{R}(x) : e < y\}$, $\mathcal{R}_2(x) = \{p \in \mathcal{R}(x) : f < y\}$, and $\mathcal{R}_3(x) = \mathcal{R}(x) \backslash (\mathcal{R}_1(x) \cup \mathcal{R}_2(x))$, we get, by Proposition 2, that

$$\#\mathcal{R}_1(x) \le \#\mathcal{T}_{a,1}(x,y) \ll \frac{y^2}{\log x} = \frac{x}{(\log x)^3},$$

$$\#\mathcal{R}_2(x) \le \#\mathcal{T}_{b,1}(x,y) \ll \frac{y^2}{\log x} = \frac{x}{(\log x)^3},$$

and by Proposition 3, that

$$\#\mathcal{R}_3(x) \ll \frac{x \log\log x}{(\log x)^{1+\nu}}.$$

Hence,

$$\#\mathcal{R}(x) \le \#\mathcal{R}_1(x) + \#\mathcal{R}_2(x) + \#\mathcal{R}_3(x) \ll \frac{x \log\log x}{(\log x)^{1+\nu}}.$$

□

Now since $f(X)$ has two distinct roots, we may write $Af(n)$ as $(r_1n+s_1)(r_2n+s_2)/\ell$ for some integers r_1, r_2, s_1, s_2, ℓ with $r_1r_2\ell \neq 0$ and $-s_1/r_1 \neq -s_2/r_2$. Replacing $f(X)$ by $\ell A f(X)$, congruences (8) imply that

$$a^{(r_1n+s_1)(r_2n+s_2)} \equiv 1 \pmod{p},$$

and that the same congruence holds true with a replaced by b, c or d. The congruences $a^n \equiv b \pmod{p}$ and $c^n \equiv d \pmod{p}$ lead to $a^{r_in+s_i} \equiv b_i \pmod{p}$ and $c^{r_in+s_i} \equiv d_i \pmod{p}$, where $b_i = b^{r_i}a^{s_i}$ and $d_i = d^{r_i}c^{s_i}$ for $i = 1, 2$. Assume first that neither b_1 nor d_2 is 1. Then

$$b_1^{r_2n+s_2} \equiv a^{(r_1n+s_1)(r_2n+s_2)} \equiv 1 \pmod{p},$$

and

$$d_2^{r_1n+s_1} \equiv c^{(r_2n+s_2)(r_1n+s_1)} \equiv 1 \pmod{p}.$$

Now the result follows by applying Lemma 6.

A similar argument applies when neither one of b_2 or d_1 is 1. Now if both b_1 and d_2 are 1, then $a^{r_1n+s_1} \equiv 1 \pmod{p}$, and $c^{r_2n+s_2} \equiv 1 \pmod{p}$, so Lemma 6 can again be applied. Thus, we may assume that one and only one of b_1 and d_2 is 1. Similarly, if both b_2 and d_1 are 1, we get that $a^{r_2n+s_2} \equiv 1 \pmod{p}$, and $c^{r_1n+s_1} \equiv 1 \pmod{p}$ and Lemma 6 applies. So, we may assume that one and only one of b_2 and d_1 is 1. To fix ideas, assume that $b_1 = 1$. Then $d_2 \neq 1$. If $d_1 = 1$, then $b^{r_1}a^{s_1} = b_1 = 1$ and $c^{r_1}d^{s_1} = d_1 = 1$, therefore $(s_1, r_1)^T$ is a non-zero zero of $M(a,b,c,d)^T$, which is impossible. So $d_1 \neq 1$, which forces $b_2 = 1$. Hence, $a^{r_1n+s_1} \equiv b_1 = 1 \pmod{p}$ and $a^{r_2n+s_2} \equiv b_2 = 1 \pmod{p}$. Thus, $e = \operatorname{ord}_p(a)$ divides both r_1n+s_1 and r_2n+s_2; hence, $e = O(1)$, which shows that $\mathcal{S}$ is finite. This completes the proof of this case. □

Step 6. *$f(X)$ has a double root.*

We can then write $Af(n)$ as $(rn+s)^2/\ell^2$ for some integers $r,\ s,\ \ell$, with $r > 0$ and $\ell > 0$. By replacing $f(n)$ by $A\ell^2 f(n)$ in congruences (8), we get

$$a^{(rn+s)^2} \equiv 1 \pmod p,$$

and the same is true if we replace a by either one of b, c or d. From $a^n \equiv b \pmod p$, we get $a^{rn+s} \equiv b_1 \pmod p$, where $b_1 = b^r a^s$. Similarly, $c^n \equiv d \pmod p$ leads to $c^{rn+s} \equiv d_1 \pmod p$, where $d_1 = d^r c^s$. Again, not both b_1 and d_1 can be 1, since this would lead to the fact that $(s, r)^T$ is a non-zero rational zero of $M(a, b, c, d)^T$.

Let $\mathcal{Q}(x)$ be the set of primes $p \le x$ such that $p - 1$ contains a square factor $e > z = \log x$. We will first show that the cardinality of $\mathcal{Q}(x)$ is $o(\pi(x))$.

Fix any square number $e \le x$. Then the number of primes $p < x$ such that $e \mid p - 1$ is $\pi(x; e, 1)$. If $e \le x^{1/2}$, then, by the Brun-Titchmarsh Theorem,

$$\pi(x; e, 1) \ll \frac{e}{\phi(e)} \frac{1}{e} \frac{x}{\log(x/e)} \ll \frac{x \log\log x}{e \log x},$$

where we used the minimal order $\phi(e)/e \gg (\log\log x)^{-1}$ when e is in the interval $[1, x]$. If $e > x^{1/2}$, we use the trivial bound $\pi(x; e, 1) \le x/e$. Thus,

$$\begin{aligned} \#\mathcal{Q}(x) &\ll \frac{x \log\log x}{\log x} \sum_{\substack{e > \log x \\ e \text{ square}}} \frac{1}{e} + x \sum_{\substack{e > x^{1/2} \\ e \text{ square}}} \frac{1}{e} \\ &\ll \frac{x \log\log x}{(\log x)^{3/2}} + x^{3/4} \ll \frac{x \log\log x}{(\log x)^{3/2}}, \end{aligned}$$

where in the above estimates we used the fact that the estimate

$$\sum_{\substack{e > t \\ e \text{ square}}} \frac{1}{e} \ll \frac{1}{t^{1/2}}$$

holds uniformly in $t > 1$.

Now let $\mathcal{S}_1(x) = \mathcal{S}(x) \backslash \mathcal{Q}(x)$. Recall that not both b_1 and d_1 can be 1 so assume for instance that $b_1 \ne 1$. Since $a^{(rn+s)^2} \equiv 1 \pmod p$, it follows that $\mathrm{ord}_p(a) \mid (rn+s)^2$. Since also $\mathrm{ord}_p(a) \mid p - 1$ and $p \notin \mathcal{Q}(x)$, it follows that there exists a number $u < \log x$, such that $\mathrm{ord}_p(a) \mid u(rn+s)$. But then $a^{u(rn+s)} \equiv 1 \pmod p$, giving $b_1^u \equiv 1 \pmod p$. This shows using Proposition 2 that

$$\#\mathcal{S}_1(x) \le \mathcal{T}_{b_1,1}(z, x) \ll \frac{\log^2 x + x^{1/2}}{\log x} \ll \frac{x^{1/2}}{\log x}.$$

Hence, we showed that

$$\#\mathcal{S}(x) \le \#\mathcal{Q}(x) + \#\mathcal{S}_1(x) \ll \frac{x \log\log x}{(\log x)^{3/2}}.$$

This completes the proof of the regular case. □

3.3. The singular case

We recall that, in opposition to the regular case, we are to show that there is a positive lower asymptotic density of primes p for which the system of simultaneous exponential congruences (2) is solvable for some natural number n. Here $a,\ b,\ c,\ d$ are assumed positive.

3.3.1. The row-singular case

Saying that (a, b, c, d) is in the row-singular case comes down to asserting the existence of two coprime integers r and s, s not zero (since $a \neq 1$), such that the vector equality

$$r \cdot (\log a, \log c) = s \cdot (\log b, \log d) \quad \text{holds.} \tag{15}$$

But (15) says that $a^r = b^s$ and $c^r = d^s$. Assume first that the rank of the group generated by a, b, c and d in $\mathbb{Q}_+^*$ is 2. Let g_1 and g_2 be two generators of this group. Then there are integers m_1, m_2, n_1 and n_2 with

$$a = g_1^{m_1} g_2^{m_2} \qquad \text{and} \qquad b = g_1^{n_1} g_2^{n_2}. \tag{16}$$

Therefore $g_1^{rm_1} g_2^{rm_2} = g_1^{sn_1} g_2^{sn_2}$, implying $rm_1 = sn_1$ and $rm_2 = sn_2$. Thus there exist integers λ_1 and λ_2 with $n_1 = \lambda_1 r$, $m_1 = \lambda_1 s$ and $n_2 = \lambda_2 r$, $m_2 = \lambda_2 s$. Putting $\rho_1 = g_1^{\lambda_1} g_2^{\lambda_2}$, we thus obtain $a = \rho_1^s$ and $b = \rho_1^r$.

Following a similar argument one would get $c = \rho_2^s$ and $d = \rho_2^r$ where $\rho_2 = g_1^{\mu_1} g_2^{\mu_2}$ for some integers μ_1 and μ_2. Now (2) is equivalent to

$$\rho_1^{sn-r} \equiv 1 \pmod p \qquad \text{and} \qquad \rho_2^{sn-r} \equiv 1 \pmod p. \tag{17}$$

The above system (17) is clearly solvable if $sn \equiv r \pmod{p-1}$. For s odd, this last congruence is solvable in n for any odd prime $p \equiv -1$ or $2 \pmod s$. These primes have positive density by the Dirichlet Density Theorem.

For generic s, say $|s| = 2^\alpha s'$, s' odd ≥ 1, we claim that there also is a set of primes p of positive density such that (17) is solvable.

In fact any prime $p \equiv -1 \pmod{s'}$ splitting in $\mathbb{Q}(\sqrt{\rho_1}\ ,\ \sqrt{\rho_2}\ )$ and inert in $\mathbb{Q}(i)$, say, will do. Indeed, such primes satisfy $p \equiv 3 \pmod 4$, $\rho_1^{(p-1)/2} \equiv \rho_2^{(p-1)/2} \equiv 1 \pmod p$. Moreover s is prime to $\frac{p-1}{2}$. Hence the congruence $sn \equiv r\ (mod\ e)$, where e is the least common multiple of the orders of ρ_1 and $\rho_2 \pmod p$, is solvable. Therefore (17) is solvable for such primes.

Now by the Chebotarev Density Theorem such primes have positive density provided the congruence $p \equiv -1 \pmod{s'}$ and the congruences resulting from the condition that p splits completely in $\mathbb{Q}(\sqrt{\rho_1}\,, \sqrt{\rho_2}\,)$ be non exclusive of each other. This is the case if none of the two real quadratic fields $\mathbb{Q}(\sqrt{\rho_j}\,)$, $j = 1$ or 2, is included in the cyclotomic field $\mathbb{Q}(\, e^{2i\pi/s'}\,)$. Otherwise, say if $\mathbb{Q}(\sqrt{\rho_j}\,) \subset \mathbb{Q}(\, e^{2i\pi/s'}\,)$, then we must check that the congruence $p \equiv -1 \pmod{s'}$ implies that p splits in $\mathbb{Q}(\sqrt{\rho_j}\,)$. But $p \equiv -1 \pmod{s'}$ implies that p splits completely in $\mathbb{Q}(\, e^{2i\pi/s'} + e^{-2i\pi/s'}\,)$, since the Frobenius automorphism of p for the extension $\mathbb{Q}(\, e^{2i\pi/s'}\,)$ over $\mathbb{Q}$ is, for $p \equiv -1 \pmod{s'}$, of order 2 and corresponds to complex conjugation. Now $\mathbb{Q}(\, e^{2i\pi/s'} + e^{-2i\pi/s'}\,)$ contains any real subfield of $\mathbb{Q}(\, e^{2i\pi/s'}\,)$ and therefore $\mathbb{Q}(\sqrt{\rho_j}\,)$. Hence, in this case, p splits completely in $\mathbb{Q}(\sqrt{\rho_j}\,)$ follows from the fact that $p \equiv -1 \pmod{s'}$.

Therefore we have shown that (17) is solvable for a set of primes of positive lower density.

Note that our result is valid whether a and c are negative or positive rationals. Indeed, in the set of primes we constructed for generic s, the modulus e of the congruence $sn \equiv r \pmod{e}$ is odd, so that, by the Chinese Remainder Theorem, we may impose the additional condition that n be even. And for n even, congruences (2) also hold when we replace one (or both) rationals a or c by respectively $-a$ and $-c$.

Finally if the rank of the group generated by a, b, c and d in $\mathbb{Q}_+^*$ is 1 and g is a generator of this group, then (2) is equivalent to

$$g^{\lambda(sn-r)} \equiv 1 \equiv g^{\lambda'(sn-r)} \pmod{p},$$

for some integers λ and λ' that depend on a, b, c and d. This actually comes down to a single congruence

$$\rho^{sn-r} \equiv 1 \pmod{p}, \qquad \text{where } \rho = g^{\gcd(\lambda,\lambda')},$$

for which we can show in the same manner as above the existence of a positive lower density of primes solving it. □

3.3.2. The column-singular case

Here we have coprime non-zero integers r and s with $a^r = c^s$ and $b^r = d^s$. Following the argument of the row-singular case, we end up with $a = \rho_1^s$, $c = \rho_1^r$, $b = \rho_2^s$ and $d = \rho_2^r$, where ρ_1 and ρ_2 are two positive rationals. Thus (2) is equivalent to

$$\rho_1^{sn} \equiv \rho_2^s \quad \text{and} \quad \rho_1^{rn} \equiv \rho_2^r \pmod{p},$$

which will certainly hold if $\rho_1^n \equiv \rho_2 \pmod{p}$. When ρ_1 and ρ_2 are multiplicatively independent in $\mathbb{Q}^*$, then Theorem 2 of [7], for instance, yields the existence, conditional to the generalized Riemann hypothesis, of a positive density of primes for which $\rho_1^n \equiv \rho_2 \pmod{p}$ holds. Note that since ρ_1^2 and ρ_2 are also multiplicatively independent in $\mathbb{Q}^*$ we may further impose that n be even in $\rho_1^n \equiv \rho_2 \pmod{p}$. Thus again the result holds irrespective of the signs of a and c.

When ρ_1 and ρ_2 are multiplicatively dependent, which in particular is the case when $\operatorname{rank}\langle a, b, c, d\rangle_{\mathbb{Q}^*}$ is 1, then

$$\rho_1^n \equiv \rho_2 \pmod{p} \iff g^{\lambda n-\mu} \equiv 1 \pmod{p},$$

for some rational g and integers λ and μ. The fact that $a \neq 1$ implies that $\lambda \neq 0$. We have shown in the proof of the row-singular case the existence of a set of primes of positive density solving a congruence such as $g^{\lambda n-\mu} \equiv 1 \pmod{p}$. □

4. Appendix

Here, we show that if a, b, c, d are non-zero rationals generating a multiplicative subgroup of $\mathbb{Q}^*$ of rank at most 2, then $M(a, b, c, d)$ has rational rank at most 1 if and only if its determinant is zero.

Proposition 7. *Assume that a, b, c and d are positive rational numbers such that* $\operatorname{rank}\langle a, b, c, d\rangle_{\mathbb{Q}^*} \leq 2$. *Then the rational rank of $M(a, b, c, d)$ is at most* 1 *if and only if* $\det M(a, b, c, d) = 0$.

Proof. If $\langle a, b, c, d\rangle_{\mathbb{Q}^*} = \{1\}$, then $M(a, b, c, d)$ is the zero matrix and there is nothing to prove. If $\langle a, b, c, d\rangle_{\mathbb{Q}^*} = \langle \rho \rangle$ for some positive rational number $\rho \neq 1$, then $M(a, b, c, d)$ is a non-zero scalar multiple of a matrix with rational entries (the scalar being exactly $\log \rho$), and the equivalence to be shown clearly holds. Assume now that $\langle a, b, c, d\rangle_{\mathbb{Q}^*} = \langle \rho, \delta \rangle$, where ρ and δ are some positive rational numbers which are multiplicatively independent. Then $\det M = F(\log \rho, \log \delta)$, where $F(X, Y) \in \mathbb{Q}[X, Y]$ is either zero, or is a homogeneous polynomial with rational coefficients of degree two. Thus, if $F(X, Y)$ is not identically zero, then $\det M = 0$ implies that $\log \rho / \log \delta$ is either quadratic or rational. However, $\log \rho / \log \delta$ cannot be quadratic by the well-known Gelfond-Schneider Theorem (see [2] and [8]), and the case when $\log \rho / \log \delta$ is rational is also impossible because it implies that ρ and δ are multiplicatively dependent. Thus, it remains to look at the case when $F(X, Y)$ is identically zero and to show that the rational rank of M is ≤ 1. Writing

$$a = \rho^{x_1}\delta^{x_2}, \quad b = \rho^{x_3}\delta^{x_4}, \quad c = \rho^{y_1}\delta^{y_2}, \quad \text{and} \quad d = \rho^{y_3}\delta^{y_4},$$

we get that

$$\begin{aligned} \det M(a,b,c,d) &= F(\log\rho, \log\delta) = (x_1y_3 - y_1x_3)(\log\rho)^2 \\ &+ (x_1y_4 + x_2y_3 - x_4y_1 - x_3y_2)\log\rho\log\delta \\ &+ (x_2y_4 - x_4y_2)(\log\delta)^2. \end{aligned}$$

Thus, $F(X, Y)$ is the zero polynomial if and only if

$$x_1y_3 = y_1x_3, \quad x_2y_4 = x_4y_2, \quad \text{and} \quad x_1y_4 + x_2y_3 = x_4y_1 + x_3y_2. \tag{18}$$

If $y_1 = y_3 = 0$, then $x_2y_4 = x_4y_2$ and $x_1y_4 = x_3y_2$. Thus, if both y_2 and y_4 are also zero, then the second row of $M(a,b,c,d)$ is zero (hence, the rational rank of M is ≤ 1), while if not both y_2 and y_4 are zero, we see that

$$y_4 \begin{bmatrix} \log a \\ \log c \end{bmatrix} - y_2 \begin{bmatrix} \log b \\ \log d \end{bmatrix} = 0,$$

which again shows that the rational rank of $M(a,b,c,d)$ is ≤ 1. A similar argument applies if both y_2 and y_4 are zero (just interchange ρ and δ). Finally, assume that not both y_1 and y_3 are zero, and that not both y_2 and y_4 are zero. The first and second relations of (18) show that

$$(x_1, x_3) = \lambda(y_1, y_3) \quad \text{and} \quad (x_2, x_4) = \mu(y_2, y_4),$$

with some rational numbers λ and μ, and now the last relation in (18) shows that

$$(\lambda - \mu)(y_1y_4 - y_2y_3) = 0.$$

If $y_1y_4 = y_2y_3$, we get that $(y_2, y_4) = \gamma(y_1, y_3)$, and now one checks easily that

$$y_1 \begin{bmatrix} \log a \\ \log c \end{bmatrix} - y_3 \begin{bmatrix} \log b \\ \log d \end{bmatrix} = 0,$$

which again shows that the rational rank of $M(a,b,c,d)$ is ≤ 1. Finally, if $\lambda - \mu = 0$, we then get that the first row of $M(a,b,c,d)$ equals λ times the second row of $M(a,b,c,d)$, so that again the rational rank of $M(a,b,c,d)$ is ≤ 1. □

REFERENCES

[1] BALLOT, C. – LUCA, F.: *Prime factors of $a^{f(n)} - 1$ with an irreducible polynomial f,* New York J. Math. **12** (2006), 39–45.

[2] GELFOND, A.O.: *Sur le septième problème de Hilbert,* Izvestia Akad. Nauk SSSR **7** (1934), 623–630; Doklady Akad. Nauk SSSR **2** (1934), 1–6.

[3] HOOLEY, C.: *On Artin's conjecture,* J. reine angew. Math. **225** (1967), 209–220.

[4] INDLEKOFER, H.-K. – TIMOFEEV, N.M.: *Divisors of shifted primes,* Publ. Math. Debrecen **60** (2002), 307–345.

[5] IVIĆ, A.: *The Riemann Zeta-Function. Theory and Applications,* Dover, Mineola, New York, 2003.

[6] MOREE, P.: *On primes p for which d divides* $\mathrm{ord}_p(g)$*,* Funct. Approx. Comment. Math. **33** (2005), 85–95.

[7] MOREE, P. – STEVENHAGEN, P.: *A two-variable Artin conjecture,* J. Number Theory **85** (2000), 291–304.

[8] SCHNEIDER, Th.: *Transzendenzuntersuchungen periodischer Funktionen: I Transzendenz von Potenzen; II Transzendenzeigenschaften elliptischer Funktionen,* J. reine angew. Math. **172** (1934), 65–74.

[9] SKAŁBA, M.: *Primes dividing both* $2^n - 3$ *and* $3^n - 2$ *are rare*, Arch. Math. (Basel) **84** (2005), 485–495.

Received July 7, 2007
Accepted September 9, 2007

Christian Ballot
Laboratoire Nicolas Oresme
Université de Caen
F14032 Caen Cedex
FRANCE
E-mail: Christian.Ballot@math.unicaen.fr

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán
MÉXICO
E-mail: fluca@matmor.unam.mx