Bull. Aust. Math. Soc. **99** (2019), 42–50
doi:10.1017/S0004972718000965

LINEAR INDEPENDENCE OF POWERS OF SINGULAR MODULI OF DEGREE THREE

FLORIAN LUCA and ANTONIN RIFFAUT✉

(Received 8 May 2018; accepted 24 July 2018; first published online 12 September 2018)

Abstract

We show that two distinct singular moduli $j(\tau), j(\tau')$, such that for some positive integers m and n the numbers $1, j(\tau)^m$ and $j(\tau')^n$ are linearly dependent over $\mathbb{Q}$, generate the same number field of degree at most two. This completes a result of Riffaut ['Equations with powers of singular moduli', *Int. J. Number Theory*, to appear], who proved the above theorem except for two explicit pairs of exceptions consisting of numbers of degree three. The purpose of this article is to treat these two remaining cases.

2010 *Mathematics subject classification*: primary 11J20; secondary 11F03, 11J61, 11J86.

Keywords and phrases: linear independence, singular moduli, linear forms in two logarithms.

1. Introduction

Let j be the classical j-function on the Poincaré plane $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. A *singular modulus* is a number of the form $j(\tau)$, where $\tau \in \mathbb{H}$ is a complex algebraic number of degree two. It is known that $j(\tau)$ is an algebraic integer and, by class field theory,

$$[\mathbb{Q}(j(\tau)) : \mathbb{Q}] = [\mathbb{Q}(\tau, j(\tau)) : \mathbb{Q}(\tau)] = h_\Delta$$

is the class number of the order $\mathcal{O}_\Delta = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2]$, where Δ is the discriminant of the minimal polynomial of τ over $\mathbb{Z}$. Moreover, $\mathbb{Q}(\tau, j(\tau))/\mathbb{Q}(\tau)$ is an abelian Galois extension with Galois group (canonically) isomorphic to the class group of the order $\mathcal{O}_\Delta$. One can also interpret $\mathcal{O}_\Delta$ as the automorphism ring of the lattice $\langle 1, \tau\rangle$ or of the corresponding elliptic curve. For details, see, for instance, [7, Sections 7 and 11].

Starting from the ground-breaking article of André [2], equations involving singular moduli were studied by many authors (see [1, 4, 10] for a historical account and further references). In particular, Kühne [8] proved that the equation $x + y = 1$ has no solutions in singular moduli x, y and Bilu *et al.* [5] proved that the same conclusion holds for the equation $xy = 1$. These results were generalised in [1] and [4]. In [1], solutions of all linear equations $Ax + By = C$, with $A, B, C \in \mathbb{Q}$, were determined. The main result of [1] is the following theorem.

Theorem 1.1 (Allombert *et al.* [1]). *Let x, y be two singular moduli and A, B, C rational numbers with $AB \neq 0$. Assume that $Ax + By = C$. Then we have one of the following options:*

(trivial case) $A + B = C = 0$ *and* $x = y$*;*
(rational case) $x, y \in \mathbb{Q}$*;*
(quadratic case) $x \neq y$ *and* x, y *generate the same number field over* $\mathbb{Q}$ *of degree two.*

This result is best possible, since in both the rational case and the quadratic case of Theorem 1.1 one easily finds $A, B, C \in \mathbb{Q}$ such that $AB \neq 0$ and $Ax + By = C$. Moreover, the lists of singular moduli of degrees one and two over $\mathbb{Q}$ are widely available or can be easily generated using a suitable computer package, such as PARI [11]. In particular, there are 13 rational singular moduli and 29 pairs of $\mathbb{Q}$-conjugate singular moduli of degree two (see [4, Section 1] for more details). This means that Theorem 1.1 gives a completely explicit characterisation of all solutions.

In [10], Riffaut generalised Theorem 1.1 by introducing exponents; that is, instead of $Ax + By = C$, he considered the more general equation $Ax^m + By^n = C$, where the positive integer exponents m, n are unknown as well. He proved that, if $x \neq y$, then x, y generate the same number field of degree $h \leq 3$ and $h = 3$ is possible only if either $\{\Delta, \Delta'\} = \{-4 \times 23, -23\}$ or $\{\Delta, \Delta'\} = \{-4 \times 31, -31\}$, where Δ, Δ' denote the respective discriminants of x and y. In this article, we eliminate these two remaining cases. Here is the statement of our result.

Theorem 1.2. *Let $x = j(\tau), y = j(\tau')$ be two singular moduli of respective discriminants Δ and Δ' and m, n two positive integers. If $\{\Delta, \Delta'\} = \{-4 \times 23, -23\}$ or $\{\Delta, \Delta'\} = \{-4 \times 31, -31\}$, then the numbers $1, x^m, y^n$ are linearly independent over $\mathbb{Q}$.*

Consequently, Theorem 1.2 together with [10, Theorem 1.5] completely solves the above equation for distinct singular moduli and we deduce the following theorem.

Theorem 1.3. *Let $x = j(\tau), y = j(\tau')$ be two distinct singular moduli of respective discriminants Δ and Δ' and m, n two positive integers. Assume that $Ax^m + By^n = C$ for some $A, B, C \in \mathbb{Q}^\times$. Then x and y generate the same number field over $\mathbb{Q}$ of degree at most two.*

As previously, this result is now best possible for distinct singular moduli, since, if $h \leq 2$, then for all exponents m, n one easily finds $A, B, C \in \mathbb{Q}^\times$ with $Ax^m + By^n = C$. However, our current methods are still not able to handle the case $x = y$, which is equivalent to the following question: can a singular modulus of degree three or higher be a root of a trinomial with rational coefficients? Much about trinomials is known, but this knowledge is still insufficient to rule out such a possibility. Otherwise, the assumption $C \neq 0$ is seemingly restrictive, but, in fact, the case $C = 0$ is contained in [10, Theorem 1.6].

Our calculations were performed using the PARI/GP package [11]. The sources are available from the second author.

2. Preliminaries

Below we briefly recall some basic facts about the conjugates of a singular modulus and the height of an algebraic number.

2.1. Fields generated by a power of a singular modulus. Let $j(\tau)$ be a singular modulus of discriminant Δ. It is well known that the conjugates of $j(\tau)$ over $\mathbb{Q}$ can be described explicitly (see, for instance, [10, Subsection 2.2]). In particular, $j(\tau)$ admits one real conjugate which has the property that it is much larger in absolute value than all its other conjugates, called the *dominant j-value* of discriminant Δ. As a useful consequence, a singular modulus and any of its powers generate the same field over $\mathbb{Q}$ (see [10, Lemma 2.6]). We reproduce this statement as Lemma 2.1.

LEMMA 2.1. *Let x be a singular modulus of discriminant Δ, with $|\Delta| \geq 11$, and n a nonzero integer. Then $\mathbb{Q}(x) = \mathbb{Q}(x^n)$.*

2.2. The height of a nonzero algebraic number. Let α be a nonzero algebraic number of degree d over $\mathbb{Q}$ and $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ all its conjugates in $\overline{\mathbb{Q}}$. The logarithmic height of α, denoted by $\mathrm{h}(\alpha)$, is defined to be

$$\mathrm{h}(\alpha) = \frac{1}{d}\Big(\log|a| + \sum_{k=1}^{d} \log\max\{1, |\alpha_k|\}\Big),$$

where a is the leading coefficient of the minimal polynomial of α in $\mathbb{Z}$. In particular, $\log|a| = 0$ when α is an algebraic integer.

Here are some useful properties of the logarithmic height.

- For any nonzero algebraic number α and $\lambda \in \mathbb{Q}^*$, we have $\mathrm{h}(\alpha^\lambda) = |\lambda|\mathrm{h}(\alpha)$. In particular, $\mathrm{h}(1/\alpha) = \mathrm{h}(\alpha)$ (see [6, Lemma 1.5.18]).
- For any two nonzero algebraic numbers α and β, we have $\mathrm{h}(\alpha\beta) \leq \mathrm{h}(\alpha) + \mathrm{h}(\beta)$.

3. Linear forms in two logarithms

Let α be an algebraic number with $|\alpha| = 1$, but not a root of unity, and n a positive integer. We are interested in estimating the quantity $\lambda = 1 - \alpha^n$, which is closely related to a linear form in two logarithms.

Laurent *et al.* describe in [9] a lower bound on the absolute value of a general linear form in two logarithms (see [9, Théorème 3]). In our particular case, Mignotte *et al.* give in [3] a slight sharpening of this bound. The following theorem is a corollary of [3, Theorems A.1.2 and A.1.3].

THEOREM 3.1. *Let α be a complex algebraic number with $|\alpha| = 1$, but not a root of unity, and $m > 1$ an integer. There exists an effectively computable constant $c_1(\alpha) > 0$, depending only on the degree d of α over $\mathbb{Q}$ and its logarithmic height* $\mathrm{h}(\alpha)$, *such that*

$$|1 - \alpha^m| > 0.99e^{-c_1(\alpha)(\log m)^2}.$$

https://doi.org/10.1017/S0004972718000965 Published online by Cambridge University Press

Proof. We briefly detail the proof, especially to explain how to compute $c_1(\alpha)$ in terms of d and $\mathrm{h}(\alpha)$.

We apply [3, Theorems A.1.2 and A.1.3] to the linear form

$$\Lambda = 2i\pi - m\log\alpha,$$

where we choose the principal complex logarithm (defined on $\mathbb{C}\setminus\mathbb{R}^-$) for $\log\alpha$. We have

$$\log|\Lambda| > -(9.03\mathcal{H}^2 + 0.23)(D\mathrm{h}(\alpha) + 25.84) - 2\mathcal{H} - 2\log\mathcal{H} - 0.7D + 2.07,$$

where $D = d/2$ and $\mathcal{H} = D(\log m - 0.96) + 4.49 \le c_1'(d)\log m$ for $m \ge 13$, with

$$c_1'(d) = D + \max\left\{0, \frac{4.49 - 0.96D}{\log 13}\right\} > 0.$$

Hence,

$$\begin{aligned}\log|\Lambda| &> -(\log m)^2\Big(9.03c_1'(d)^2(D\mathrm{h}(\alpha) + 25.84) + \frac{2c_1'(d)}{\log m} + \frac{2\log\log m}{(\log m)^2}\\ &\qquad + \frac{0.23(D\mathrm{h}(\alpha) + 25.84) + 2\log c_1'(d) + 0.7D - 2.07}{(\log m)^2}\Big)\\ &> -c_1(\alpha)(\log m)^2,\end{aligned}$$

with

$$\begin{aligned}c_1(\alpha) = 9.03c_1'(d)^2(D\mathrm{h}(\alpha) + 25.84) + \frac{2c_1'(d)}{\log 13} + \frac{2\log\log 13}{(\log 13)^2}\\ + \frac{0.23(D\mathrm{h}(\alpha) + 25.84) + 2\log c_1'(d) + 0.7D - 2.07}{(\log 13)^2}.\end{aligned}$$

By the mean value theorem,

$$|1 - \alpha^m| > \frac{e^{-c_1(\alpha)(\log m)^2}}{1 + e^{-c_1(\alpha)(\log m)^2}} > 0.99e^{-c_1(\alpha)(\log m)^2}. \qquad \square$$

In practice, if α is explicitly known (as an algebraic number in a number field L), it is possible to compute $c_1(\alpha)$ for $m \ge 13$. For $m < 13$, one just has to estimate directly $|1 - \alpha^m|$.

Another way of estimating $1 - \alpha^m$ is to reduce it modulo a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$. More precisely, we want to evaluate its valuation $v_\mathfrak{p}(1 - \alpha^m)$ at $\mathfrak{p}$; for simplicity, for an element $z \in L$, we write $v_\mathfrak{p}(z)$ instead of $v_\mathfrak{p}(z\mathcal{O}_L)$. This can be obtained as follows.

Proposition 3.2. *Let α be an algebraic integer that is not a root of unity in a number field L of degree d and m a positive integer. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$ over a prime number p. Assume that $\mathfrak{p} \nmid \alpha$. Denote by m_0 the order of α in $\mathcal{O}_L/\mathfrak{p}$, that is, the least positive integer such that $1 - \alpha^{m_0} = 0 \bmod \mathfrak{p}$, and $v_0 = v_\mathfrak{p}(1 - \alpha^{m_0})$. Then, assuming that $p > d + 1$,*

$$v_\mathfrak{p}(1 - \alpha^m) = \begin{cases} 0 & \text{if } m_0 \nmid m,\\ s v_\mathfrak{p}(p) + v_0 & \text{if } m = m_0 p^s r,\ \gcd(p, r) = 1.\end{cases}$$

https://doi.org/10.1017/S0004972718000965 Published online by Cambridge University Press

PROOF. If $m_0 \nmid m$, it is clear that $1 - \alpha^m \not\equiv 0 \bmod \mathfrak{p}$; hence, $v_\mathfrak{p}(1-\alpha^m) = 0$. Otherwise, write $m = m_0 p^s r$ with $\gcd(p, r) = 1$. We proceed by induction on $s \geq 0$. For $s = 0$, factoring $1 - \alpha^m$ gives

$$1 - \alpha^m = (1 - \alpha^{m_0})\biggl(\sum_{l=0}^{r-1} \alpha^{m_0 l}\biggr).$$

Since $\alpha^{m_0 l} \equiv 1 \bmod \mathfrak{p}$ for all $l \in \{0, \ldots, r-1\}$, we deduce that

$$v_\mathfrak{p}(1-\alpha^m) = v_\mathfrak{p}(1-\alpha^{m_0}) + v_\mathfrak{p}(r) = v_0.$$

We now let $\beta = \alpha^{r m_0}$ and treat the case $s = 1$. Writing $\beta = 1 + \lambda$, where $\lambda \in \mathfrak{p}$,

$$\frac{\beta^p - 1}{\beta - 1} = \frac{(1+\lambda)^p - 1}{\lambda} = \sum_{k=1}^{p-1} \binom{p}{k} \lambda^{k-1} + \lambda^{p-1}.$$

On the right-hand side, $v_\mathfrak{p}(\lambda) \geq 1$ and $v_\mathfrak{p}(\lambda^{p-1}) \geq (p-1) > d \geq v_\mathfrak{p}(p)$, so

$$v_\mathfrak{p}\biggl(\sum_{k=1}^{p-1} \binom{p}{k} \lambda^{k-1} + \lambda^{p-1}\biggr) = v_\mathfrak{p}(p).$$

Hence, for $s = 1$,

$$v_\mathfrak{p}(1-\alpha^m) = v_\mathfrak{p}(1-\alpha^{m_0 r}) + v_\mathfrak{p}\Bigl(\frac{\beta^p - 1}{\beta - 1}\Bigr) = v_0 + v_\mathfrak{p}(p).$$

The statement now follows by induction on s, where the induction step from s to $s+1$ is done as above (by replacing α by α^{p^s}). □

4. Proof of Theorem 1.2

Let $x = j(\tau), y = j(\tau')$ be two singular moduli of respective discriminants Δ and Δ', with $\{\Delta, \Delta'\} = \{-4 \times 23, -23\}$ or $\{\Delta, \Delta'\} = \{-4 \times 31, -31\}$, such that

$$Ax^m + By^n = C \tag{4.1}$$

for some $A, B, C \in \mathbb{Q}^\times$ and m, n positive integers.

Both x and y are of degree three over $\mathbb{Q}$ and admit one real conjugate corresponding to the dominant j-value and two complex conjugates. If x is real, then y is also real. Indeed, if not, then, together with (4.1),

$$Ax^m + B\bar{y}^n = C.$$

This gives $y^n = \bar{y}^n$, which contradicts Lemma 2.1.

The equation (4.1) implies that $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$; hence, $\mathbb{Q}(x) = \mathbb{Q}(y)$ by Lemma 2.1. In particular, the Galois orbit of (x, y) over $\mathbb{Q}$ has exactly three elements and each conjugate of x occurs exactly once as the first coordinate of a point in the orbit, just as each conjugate of y occurs exactly once as the second coordinate.

https://doi.org/10.1017/S0004972718000965 Published online by Cambridge University Press

We denote by $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ the conjugates of (x, y), with x_1, y_1 real, and x_2, x_3 and y_2, y_3 complex conjugates. By (4.1) again, the points (x_i^m, y_i^n), $i \in \{1, 2, 3\}$, are collinear. We can write the relation of collinearity of these points in one of the following two ways:

$$\begin{vmatrix} 1 & x_1^m & y_1^n \\ 1 & x_2^m & y_2^n \\ 1 & x_3^m & y_3^n \end{vmatrix} = 0; \tag{4.2}$$

$$\left(\frac{x_1}{x_2}\right)^{-m}\left(\frac{y_1}{y_2}\right)^{n} = \frac{1 - (\frac{y_3}{y_2})^n - (\frac{x_3}{x_1})^m}{1 - (\frac{y_3}{y_1})^n - (\frac{x_3}{x_2})^m}. \tag{4.3}$$

We focus first on the case $\{\Delta, \Delta'\} = \{-4 \times 23, -23\}$ and we detail afterwards the slight differences in the treatment of the case $\{\Delta, \Delta'\} = \{-4 \times 31, -31\}$. We denote by L the Galois closure of $\mathbb{Q}(x) = \mathbb{Q}(y)$, which, by definition, contains all the x_i and y_i.

As announced above, we consider the case $\Delta = 4\Delta' = -4 \times 23$. Using PARI, one can find a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ over $p = 23$ such that $\mathfrak{p} | x_2\mathcal{O}_L$, $\mathfrak{p} | x_3\mathcal{O}_L$, but $\mathfrak{p} \nmid x_1y_2y_3\mathcal{O}_L$. Hence, modulo $\mathfrak{p}^m$, (4.2) becomes

$$1 - \alpha^n = 0 \bmod \mathfrak{p}^m,$$

with $\alpha = y_3/y_2$. On the one hand, we deduce that $m \leq v_{\mathfrak{p}}(1 - \alpha^n)$. On the other hand, we apply Proposition 3.2, checking first that $1 - \alpha = 0 \bmod \mathfrak{p}$, $v_{\mathfrak{p}}(1 - \alpha) = 1$, $v_{\mathfrak{p}}(p) = 2 < 6 < 22 = p - 1$; writing $n = p^s r$ with $\gcd(p, r) = 1$,

$$v_{\mathfrak{p}}(1 - \alpha^n) = s v_{\mathfrak{p}}(p) + 1 = 2s + 1.$$

Consequently,

$$m \leq 2\frac{\log n}{\log 23} + 1. \tag{4.4}$$

Next, we want to estimate the expression on the right-hand side of (4.3) in terms of m and n (in fact, only in terms of n thanks to (4.4)), in order to obtain a bound on n. The principal difficulty is to find a lower bound of the absolute value of its denominator. Since y_3/y_1 is close to 0, it depends essentially on the quantity $1 - \beta^m$ with $\beta = x_3/x_2$. Since $|\beta| = 1$ and β is not a root of unity, then, according to Theorem 3.1, there exists a constant $c_1(\beta) > 0$ such that

$$|1 - \beta^m| > 0.99e^{-c_1(\beta)(\log m)^2}.$$

Explicitly, for $m \geq 13$, we can choose $c_1(\beta) = 4973.14$. It follows that

$$\begin{aligned}\left|1 - \left(\frac{y_3}{y_1}\right)^n - \left(\frac{x_3}{x_2}\right)^m\right| &> 0.99\exp\left(-4973.15(\log m)^2\right) - \left|\frac{y_3}{y_1}\right|^n \\ &> 0.99\exp\left(-4973.14\left(\log\left(2\frac{\log n}{\log 23} + 1\right)\right)^2\right) - \left|\frac{y_3}{y_1}\right|^n\end{aligned}$$

https://doi.org/10.1017/S0004972718000965 Published online by Cambridge University Press

TABLE 1. Constants $c_2(m)$ and bounds on n for each $m < 13$, in the case $\Delta = 4\Delta' = -4 \times 23$.

m	$c_2(m)$	Upper bound of n
1	1.15	2
2	1.21	5
3	11.97	8
4	1.10	10
5	1.28	13
6	6.00	16
7	1.07	18
8	1.38	21
9	4.02	24
10	1.04	26
11	1.50	29
12	3.04	32

(recall the inequality (4.4)). By a quick calculation, we observe that the last term of the previous inequality is positive provided that $n > 2074$. More specifically, if $n > 2075$, then

$$\left|1 - \left(\frac{y_3}{y_1}\right)^n - \left(\frac{x_3}{x_2}\right)^m\right| > 0.98 \exp\left(-4973.14\left(\log\left(2\frac{\log n}{\log 23} + 1\right)\right)^2\right).$$

Finally, for $m \geq 13$ and $n > 2075$,

$$\left|\frac{x_1}{x_2}\right|^{-m}\left|\frac{y_1}{y_2}\right|^n \leq 2.05 \exp\left(4973.14\left(\log\left(2\frac{\log n}{\log 23} + 1\right)\right)^2\right)$$

and

$$-\left(2\frac{\log n}{\log 23} + 1\right)\log\left|\frac{x_1}{x_2}\right| + n\log\left|\frac{y_1}{y_2}\right| \leq \log 2.05 + 4973.14\left(\log\left(2\frac{\log n}{\log 23} + 1\right)\right)^2.$$

This last inequality yields $n \leq 2092$ and then (4.4) gives $m \leq 5$. This is in contradiction with the previous assumptions $m \geq 13$ and $n > 2075$. Therefore, either $m < 13$ or $n \leq 2075$. In both cases, $m < 13$ and, for each possible m, we can explicitly compute a constant $c_2(m)$ such that

$$\left|\frac{x_1}{x_2}\right|^{-m}\left|\frac{y_1}{y_2}\right|^n \leq c_2(m).$$

This allows us to bound n. Table 1 summarises all constants $c_2(m)$ and all bounds we obtain. Again, inequality (4.4) eliminates all entries of Table 1 with $m \geq 3$. Consequently, either $m = 1$ and $n \leq 2$, or $m = 2$ and $n \leq 5$. For each of these remaining pairs (m, n), a direct calculation shows that the determinant in (4.2) does not vanish.

To finish, we repeat this process for the case $\Delta = 4\Delta' = -4 \times 31$. In this case, one can find a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ over $p = 11$ such that $\mathfrak{p}|x_2\mathcal{O}_L$, $\mathfrak{p}|x_3\mathcal{O}_L$, but $\mathfrak{p} \nmid x_1y_2y_3\mathcal{O}_L$ as before and

$$m \leq \frac{\log n}{\log 11} + 2. \tag{4.5}$$

https://doi.org/10.1017/S0004972718000965 Published online by Cambridge University Press

TABLE 2. Constants $c_2(m)$ and bounds on n for each $m < 13$, in the case $\Delta = 4\Delta' = -4 \times 31$.

m	$c_2(m)$	Upper bound of n
1	1.13	3
2	1.25	6
3	6.17	10
4	1.06	13
5	1.44	16
6	3.13	19
7	1.02	22
8	1.76	26
9	2.13	29
10	1.01	32
11	2.33	36
12	1.65	39

We obtain as well, for $m \geq 13$ and $n > 1440$,

$$\left|\frac{x_1}{x_2}\right|^{-m}\left|\frac{y_1}{y_2}\right|^{n} \leq 2.05\exp\left(4820.16\left(\log\left(\frac{\log n}{\log 11}+2\right)\right)^2\right);$$

then

$$-\left(\frac{\log n}{\log 11}+2\right)\log\left|\frac{x_1}{x_2}\right| + n\log\left|\frac{y_1}{y_2}\right| \leq \log 2.05 + 4820.16\left(\log\left(\frac{\log n}{\log 11}+2\right)\right)^2,$$

which yields $n \leq 1720$ and $m \leq 5$; again a contradiction. For each possible $m < 13$, we compute a constant $c_2(m)$ as defined above and we deduce a bound on n. This gives Table 2. Inequality (4.5) eliminates all entries of Table 2 with $m \geq 3$. Consequently, either $m = 1$ and $n \leq 3$, or $m = 2$ and $n \leq 6$. Each of these remaining possibilities can be excluded by a direct calculation showing that the respective determinant does not vanish.

References

[1] B. Allombert, Yu. Bilu and A. Pizarro-Madariaga, ‘CM-points on straight lines’, in: *Analytic Number Theory in Honor of Helmut Maier’s 60th Birthday* (eds. C. Pomerance and M. T. Rassias) (Springer, Cham, Switzerland, 2015), 1–18.

[2] Y. André, ‘Finitudes des couples d’invariants modulaires singuliers sur une courbe algébrique plane non modulaire’, *J. reine angew. Math.* **505** (1998), 203–208.

[3] Yu. Bilu, G. Hanrot, P. M. Voutier and M. Mignotte, ‘Existence of primitive divisors of Lucas and Lehmer numbers’, *J. reine angew. Math.* **539** (2001), 75–122.

[4] Yu. Bilu, F. Luca and A. Pizarro-Madariaga, ‘Rational products of singular moduli’, *J. Number Theory* **158** (2016), 397–410.

[5] Yu. Bilu, D. Masser and U. Zannier, ‘An effective “Theorem of André” for CM-points on a plane curve’, *Math. Proc. Cambridge Philos. Soc.* **154** (2013), 145–152.

[6] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry* (Cambridge University Press, Cambridge, 2006).

https://doi.org/10.1017/S0004972718000965 Published online by Cambridge University Press

[7] D. A. Cox, *Primes of the Form* $x^2 + ny^2$ (Wiley, New York, 1989).
[8] L. Kühne, 'An effective result of André–Oort type II', *Acta Arith.* **161** (2013), 1–19.
[9] M. Laurent, M. Mignotte and Y. Nesterenko, 'Formes linéaires en deux logarithmes et déterminants d'interpolation', *J. Number Theory* **55** (1995), 285–321.
[10] A. Riffaut, 'Equations with powers of singular moduli', *Int. J. Number Theory* (to appear), arXiv:1710.03547.
[11] The PARI Group, PARI/GP, version 2.7.1 (2014), Bordeaux; available from http://pari.math.u-bordeaux.fr/.

FLORIAN LUCA, School of Mathematics, University of the Witwatersrand,
Private Bag X3, Wits 2050, Johannesburg, South Africa;
Max Planck Institute for Mathematics, Vivatsgasse 7,
53111 Bonn, Germany
and
Department of Mathematics, Faculty of Sciences, University of Ostrava,
30 dubna 22, 701 03 Ostrava 1, Czech Republic
e-mail: Florian.Luca@wits.ac.za

ANTONIN RIFFAUT, Institut de Mathématiques de Bordeaux,
Université de Bordeaux, A33, 351 Cours de la Libération,
33400 Talence, France
e-mail: antonin.riffaut@math.u-bordeaux.fr