Canad. J. Math. Vol. **XX** (Y), ZZZZ pp. 1–29

Finding and Excluding b-ary Machin-Type Individual Digit Formulae

Jonathan M. Borwein, David Borwein and William F. Galway

Abstract. Constants with formulae of the form treated by D. Bailey, P. Borwein, and S. Plouffe (*BBP formulae* to a given base b) have interesting computational properties, such as allowing single digits in their base b expansion to be independently computed, and there are hints that they should be *normal* numbers, *i.e.,* that their base b digits are randomly distributed. We study a formally limited subset of BBP formulae, which we call *Machin-type BBP formulae*, for which it is relatively easy to determine whether or not a given constant κ has a Machin-type BBP formula. In particular, given $b \in \mathbb{N}$, $b > 2$, b not a proper power, a b-ary Machin-type BBP arctangent formula for κ is a formula of the form $\kappa = \sum_m a_m \arctan(-b^{-m})$, $a_m \in \mathbb{Q}$, while when $b = 2$, we also allow terms of the form $a_m \arctan(1/(1 - 2^m))$. Of particular interest, we show that π has no Machin-type BBP arctangent formula when $b \neq 2$. To the best of our knowledge, when there is no Machin-type BBP formula for a constant then no BBP formula of any form is known for that constant.

1 Introduction

1.1 Preliminaries

Given $b \in \mathbb{N}$, $b > 1$, we say that a constant $\kappa \in \mathbb{R}$ has a *BBP formula* to the base b, or a b-ary BBP formula, if

$$\kappa = \sum_{k \geq 0} \frac{p(k)}{q(k)} b^{-k}, \tag{1}$$

where $p \in \mathbb{Z}[k]$, $q \in \mathbb{Z}[k]$.

BBP formulae are of interest because, for fixed b, the nth b-ary digit of a number with a BBP formula can be found without computing prior digits—using only $O(n \ln n)$ operations on numbers with $O(\ln n)$ bits [BBP97]. For example, a BBP formula has been used to compute the quadrillionth bit (10^{15}th bit) in the binary expansion of π [Per00].

There are also recent results that relate BBP formulae to the behavior of a dynamical system, and which suggest a "road-map" towards a proof that irrational numbers

Received by the editors January 8, 2003; revised January 30, 2004.

The first author's research was supported by NSERC and the Canada Research Chair Programme, while the second author's research was supported by NSERC, and the third author's research was performed at the Centre for Experimental and Constructive Mathematics at Simon Fraser University, partially supported as a Post Doctoral Fellow of the Pacific Institute for the Mathematical Sciences

AMS subject classification: Primary: 11Y99; Secondary: 11A51, 11Y50, 11K36, 33B1.

Keywords: BBP formulae, Machin-type formulae, arctangents, logarithms, normality, Mersenne primes, Bang's theorem, Zsigmondy's theorem, primitive prime factors, p-adic analysis.

with BBP formulae must be *normal* in base b, *i.e.,* their base b digits are randomly distributed [BC01]. For example, setting $z = 1/2$ in the Taylor series expansion of $-\ln(1-z)$ yields the particularly simple binary BBP formula:

$$\ln(2) = \sum_{k\geq 0} \frac{1}{2k+2} 2^{-k}.$$

In consequence the system with $x_0 := 0$, and

$$x_n := (2x_{n-1} + 1/n) \mod 1$$

for $n > 0$ has the property that *if the sequence of x_n is equidistributed in* $[0,1)$ *then* $\ln 2$ *is a normal number base 2.*

While BBP formulae are interesting for these reasons, they are somewhat mysterious because there are few methods known for finding a formula for a given constant, and even after a formula has been found experimentally it may be difficult to rigorously prove its validity. A recent summary of work in the field is to be found in Chapter Four of [BB03]. Consider for example, *Catalan's constant* $G := \sum_{k=0}^{\infty}(-1)^k(2k+1)^{-2}$ which is not proven irrational. In a series of inspired computations using *polylogarithmic ladders* David Broadhurst has found—and proved—BBP formulae for constants such as G, $\zeta(3)$, and $\zeta(5)$ [Bro98]. Broadhurst's hexadecimal BBP formula for G is:

$$\begin{aligned} G = 3\sum_{k=0}^{\infty} \frac{1}{2\cdot 16^k}\Bigg(&\frac{1}{(8k+1)^2} - \frac{1}{(8k+2)^2} + \frac{1}{2(8k+3)^2} \\ &- \frac{1}{2^2(8k+5)^2} + \frac{1}{2^2(8k+6)^2} - \frac{1}{2^3(8k+7)^2}\Bigg) \\ - 2\sum_{k=0}^{\infty} \frac{1}{8\cdot 16^{3k}}\Bigg(&\frac{1}{(8k+1)^2} + \frac{1}{2(8k+2)^2} + \frac{1}{2^3(8k+3)^2} \\ &- \frac{1}{2^6(8k+5)^2} - \frac{1}{2^7(8k+6)^2} - \frac{1}{2^9(8k+7)^2}\Bigg). \end{aligned}$$

Given $m \in \mathbb{N}$, a BBP formula to the base b can be rewritten as a BBP formula to the base b^m, since

$$\sum_{k\geq 0} \frac{p(k)}{q(k)} b^{-k} = \sum_{k\geq 0} \left(\sum_{j=0}^{m-1} \frac{p(mk+j)}{b^j\, q(mk+j)} \right) b^{-mk}, \tag{2}$$

and the inner sum can be recast as a rational function in k. Although it is a minor abuse of language, we shall also refer to formulae to the base b^m as base b, or b-ary, BBP formulae. Under this convention the sum $\sum_k (-1)^k \big(p(k)/q(k)\big)\, b^{-k}$ may also be considered to be a b-ary BBP formula—a convention that lets one write some "base b" formulae in a shorter form, although we shall avoid doing so in this paper.

Unless we mention otherwise, we shall now assume b is not a proper power, *i.e.,* that b does not have the form a^n, for any $a \in \mathbb{N}$, $n \in \mathbb{N}$, $n > 1$.

For fixed b, the set of numbers with b-ary BBP formulae is a vector space over $\mathbb{Q}$. To the best of our knowledge, nearly all research has focused on subspaces generated by elements of the form

$$L(s, b, n, j) := \sum_{k \geq 0} \frac{1}{(nk + j)^s} b^{-k}, \tag{3}$$

with $s, n, j \in \mathbb{N}$, $1 \leq j \leq n$. Numbers within these spaces have been called *polylogarithmic*. We will show in Appendix B that it suffices to restrict the analysis of such formulae to $\mathbb{Q}$-linear combinations of $L(s, b, n, j)$ in which only j is allowed to vary.

In his *Compendium* [Bai00], Bailey catalogues many polylogarithmic constants. Bailey uses the notation

$$P(s, b, n, A) := \sum_{k \geq 0} b^{-k} \sum_{j=1}^{n} \frac{a_j}{(nk + j)^s}, \tag{4}$$

where $A = [a_1, \ldots, a_n] \in \mathbb{Z}^n$. In terms of our $L(s, b, n, j)$ we have

$$P(s, b, n, A) = \sum_{j=1}^{n} a_j \, L(s, b, n, j). \tag{5}$$

Let $\operatorname{span}\{\alpha_k\}$ denote the vector space over $\mathbb{Q}$ spanned by the set $\{\alpha_k\}$. The spaces of polylogarithmic constants explored by Bailey have the form

$$\operatorname{span}\{P(s, b, n, A) : \ A \in \mathbb{Z}^n\} = \operatorname{span}\{L(s, b, n, j) : \ 1 \leq j \leq n\}$$

with s, b, n fixed, and with b allowed to be a power, such as 2^4. Bailey has found many "interesting" constants κ in these spaces by computing κ and a table of $L(s, b, n, j)$, $1 \leq j \leq n$, to high precision; and then using the PSLQ integer relation algorithm [FBA99] to find $a \in \mathbb{Z}$, $A \in \mathbb{Z}^n$ such that $a\kappa = P(s, b, n, A)$.

1.2 Our goals

In this paper we focus our attention on *degree one*, or "logarithmic", BBP formulae, *i.e.,* those where $s = 1$ in (4). We further restrict ourselves to formulae of a special form which we call *Machin-type*. Roughly speaking, we write κ has a Machin-type BBP formula to the base b (or κ has a b-ary Machin-type BBP formula) if κ can be written either as a $\mathbb{Q}$-linear combination of real parts of logarithms, or of imaginary parts of logarithms, where the logarithms are chosen so as to yield a BBP formula to the base b.

The numbers whose logarithms we consider all lie in the multiplicative group $\mathbb{Q}[i]^\times$. Knowledge of how numbers factor into primes over $\mathbb{Z}[i]$ (the Gaussian integers) or over $\mathbb{Z}$ serves as a tool both for finding Machin-type BBP formulae and for showing no such formula exists. Despite the restricted nature of Machin-type BBP formulae, to the best of our knowledge when we can show that there is no b-ary Machin-type formula for a constant then no b-ary BBP formula of any form is known for that constant.

2 Machin-Type BBP Formulae for Arctangents

2.1 A Brief Survey of Machin-Type Formulae

The original Machin formula is the identity

$$\pi/4 = 4\arctan(1/5) - \arctan(1/239) \qquad \text{(Machin, 1706)}. \tag{6}$$

Machin used this formula to compute 100 digits of π. Similar *Machin-type formulae* for π, *i.e.,* formulae which express π as a $\mathbb{Z}$-linear combination of arctangents, have been used in most other extended computations of π until around 1980 and a few million digits. In recent years it has generally been believed that quite different formulae for π, such as the "AGM formula", are better suited for the computation of π. These AGM methods have been used beyond 200 billion digits and are surely of lower operational complexity, but involve full precision intermediate calculation.

However, in December 2002, Yasumasa Kanada announced the record computation of 1.24 trillion decimal digits of π, using the identities

$$\begin{aligned} \pi &= 48\arctan(1/49) + 128\arctan(1/57) - 20\arctan(1/239) \\ &\qquad + 48\arctan(1/110443), \end{aligned} \tag{7}$$

$$\begin{aligned} \pi &= 176\arctan(1/57) + 28\arctan(1/239) - 48\arctan(1/682) \\ &\qquad + 96\arctan(1/12943). \end{aligned} \tag{8}$$

Indeed, for the size of computation being undertaken, full precision floating point operations again seem impracticable. (See [BB98, §11.1] and [BB03, Chapter 3] for additional history on π computations.)

One way to "discover" Machin's formula (6) is to observe that

$$\arctan(y/x) \equiv \Im \ln(x + iy) \pmod{\pi}. \tag{9}$$

(We shall give our choice of branch-cut for $\arctan(\rho)$ and $\ln(z)$ below.) Equation (9), and the fact that $(5+i)^4(239+i)^{-1} = 2 + 2i$ imply

$$\pi/4 = \arctan(1) \equiv 4\arctan(1/5) - \arctan(1/239) \pmod{\pi}. \tag{10}$$

True equality of the congruence is easily verified numerically, by computing both sides to sufficient precision to ensure that they differ by less than π. Similarly, the process of verifying Equations (7) and (8) can be reduced to verifying that the products

$$(49+i)^{48}(57+i)^{128}(239+i)^{-20}(110443+i)^{48}$$

and

$$(57+i)^{176}(239+i)^{28}(682+i)^{-48}(12943+i)^{96}$$

both yield negative rational numbers.

This technique of formulating a question about arctangents in terms of $\mathbb{Z}[i]$ was used by Størmer in 1897 to solve a problem of Gravé. Gravé's problem asks if there are only four non-trivial integral solutions to

$$m \arctan(1/u) + n \arctan(1/v) = k\pi/4,$$

namely Machin's formula (6), and

$$\pi/4 = \arctan(1/2) + \arctan(1/3) \quad \text{(Euler, 1738)}, \tag{11}$$

$$\pi/4 = 2\arctan(1/2) - \arctan(1/7) \quad \text{(Hermann, 1706)}, \tag{12}$$

$$\pi/4 = 2\arctan(1/3) + \arctan(1/7) \quad \text{(Hutton, 1776)}. \tag{13}$$

Further information on Størmer's solution can be found in [BB98, §11.1, Exercise 6], or, more completely, in [Rib94, §A.12].

2.2 Notational Conventions

Throughout, $\arctan(\rho)$ denotes the principal branch of the arctangent function, defined so $-\pi/2 < \arctan(\rho) < \pi/2$ for $\rho \in \mathbb{R}$. We also allow $\rho = \infty$, and define $\arctan(\infty) := \pi/2$ and $\tan(\pm\pi/2) := \infty$. Given $\rho \neq 0$ we define $\rho/0 := \infty$, regardless of the sign of ρ. Similarly, $\ln(z)$ denotes the principal branch of the logarithm, defined so $\ln(z) = \ln(|z|) + i\theta$ satisfies $-\pi < \theta \leq \pi$. In other words $\theta = \Im \ln(z)$ satisfies $e^{i\theta} = z/|z|$, $-\pi < \theta \leq \pi$. Given $x, y \in \mathbb{R}$, our definitions of $\ln(z)$ and $\arctan(\rho)$ ensure that

$$\arctan(y/x) = \Im \ln(x + iy) = \frac{1}{2i} \ln\left(\frac{x + iy}{x - iy}\right),$$

provided $x > 0$. More generally, under our conventions we always have

$$\arctan(y/x) \equiv \Im \ln(x + iy) \pmod{\pi},$$

even for $x = 0$, $y \neq 0$.

2.3 Using Group Homomorphisms

As with Machin's formula in Section 2.1, we shall use some basic group theory to guide our search for BBP formulae. We start with a set $\{\kappa_1, \kappa_2, \dots\}$ of constants with known BBP formulae, and a constant κ for which we wish to determine a BBP formula. Provided $\kappa \in \operatorname{span}\{\kappa_1, \kappa_2, \dots\}$, finding a BBP formula for κ in terms of formulae for κ_j is equivalent to finding a $\mathbb{Q}$-linear relationship of the form

$$\kappa = \sum_j a_j \kappa_j,$$

or, rearranging and multiplying through by a common denominator, to finding a $\mathbb{Z}$-linear relationship of the form

$$n\kappa + \sum_j n_j \kappa_j = 0. \tag{14}$$

In other words, we ask if there is an $n \in \mathbb{Z}$ for which $n\kappa$ lies in the additive Abelian group G generated by $\{\kappa_1, \kappa_2, \dots\}$. Despite little knowledge of G, we can choose a group homomorphism $f\colon G \to H$ where the *target group* H is *well understood*. (Note f need not be surjective—in our applications we shall typically have img $f \subsetneqq H$.)

Given the homomorphism f, we seek a relationship

$$nf(\kappa) + \sum_j n_j f(\kappa_j) = 0 \quad \text{or} \quad f(\kappa)^n \prod_j f(\kappa_j)^{n_j} = 1, \tag{15}$$

according to whether H is an additive group or an Abelian multiplicative group. If there is no solution to (15) then there is no solution to (14), and κ cannot be represented in terms of $\{\kappa_1, \kappa_2, \dots\}$. Yet, a solution to (15) does not ensure a solution to (14), but only ensures that

$$n\kappa + \sum_j n_j \kappa_j = \kappa_0 \tag{16}$$

for some $\kappa_0 \in \ker f$. Thus, to verify that κ can be represented in terms of $\{\kappa_1, \kappa_2, \dots\}$, it suffices to solve (15) and to verify either that $\ker f = \{0\}$ or to further examine the left side of (16) (*e.g.*, numerically) to verify $\kappa_0 = 0$.

In our search for arctangent formulae there are two, nearly equivalent, choices of target group that seem convenient, and we will use both. In some cases we shall identify an angle $\theta \in \mathbb{R}$ with the line of slope $\tan(\theta)$. Writing members of group quotients as explicit cosets, the corresponding homomorphism is essentially $f\colon \mathbb{R} \to \mathbb{C}^\times/\mathbb{R}^\times$, $f(\theta) = e^{i\theta}\mathbb{R}^\times$. We shall call $\mathbb{C}^\times/\mathbb{R}^\times$ the *group of slopes*. More precisely, with $f(\theta)$ as above, we shall be using the homomorphism $f\,|\,G$, the restriction of f to G. Since we are working with $G < \mathbb{R}$ generated by elements of the form $\arctan(\rho)$, $\rho \in \mathbb{Q}$ we may take $H = \mathbb{Q}[i]^\times\mathbb{R}^\times/\mathbb{R}^\times \cong \mathbb{Q}[i]^\times/\mathbb{Q}^\times$, a group with a rich number-theoretical structure which will guide us in our search.

In other cases we shall identify an angle θ with the directed ray $e^{i\theta}\mathbb{R}_+^\times$, via the homomorphism $f\colon \mathbb{R} \to \mathbb{C}/\mathbb{R}_+^\times$, $f(\theta) = e^{i\theta}\mathbb{R}_+^\times$, where $\mathbb{R}_+^\times$ is the multiplicative group of positive real numbers. By identifying the ray $e^{i\theta}\mathbb{R}_+^\times$ with the point $e^{i\theta}$ we see that $\mathbb{C}/\mathbb{R}_+^\times$ is isomorphic to the *unit circle* group $\mathbb{S} := \{z \in \mathbb{C} : |z| = 1\}$. As before, in this case we may take the target group to be $H = \mathbb{Q}[i]^\times\mathbb{R}_+^\times/\mathbb{R}_+^\times \cong \mathbb{Q}[i]^\times/\mathbb{Q}_+^\times$.

Remark Our group of slopes, $\mathbb{C}^\times/\mathbb{R}^\times$, can be considered as the real projective line $\mathbb{P}_\mathbb{R}$, endowed with a group structure. In more detail,

$$\mathbb{P}_\mathbb{R} := \{(y, x) \in \mathbb{R} \times \mathbb{R} : (y, x) \neq (0, 0)\},$$

under the equivalence relation $(y, x) \sim (\lambda y, \lambda x)$ for all $\lambda \neq 0$, $\lambda \in \mathbb{R}$. Writing y/x to denote the equivalence class of (y, x), we can embed $\mathbb{R} \subset \mathbb{P}_{\mathbb{R}}$ under the map $y \mapsto y/1$. Of course $1/0$ denotes ∞: the *point at infinity*. In some earlier research notes we have written $(y_1/x_1) \otimes (y_2/x_2)$ for multiplication in this group, where

$$\frac{y_1}{x_1} \otimes \frac{y_2}{x_2} \sim \frac{y_1x_2 + y_2x_1}{x_1x_2 - y_1y_2}.$$

With this notation, $\mathbb{P}_{\mathbb{R}}$ has identity $0/1$, and the (multiplicative) inverse of y/x is $-y/x$.

2.4 Generators for Machin-Type BBP Arctangent Formulae

We now describe our *Machin-type BBP generators* and the resulting formulae. Given b not a proper power, $b > 2$, these are generators of the form

$$\begin{aligned} \arctan(-b^{-m}) = \Im \ln(1 - ib^{-m}) &= -b^{-m} \sum_{k \geq 0} \frac{(-1)^k}{2k+1} b^{-2mk} \\ &= b^{-3m} P(1, b^{4m}, 4, [-b^{2m}, 0, 1, 0]). \end{aligned}$$

Setting $x = \pm 2^{-m}$ in the series expansion for $\arctan(x/(1 + x))$ yields a binary BBP formula which is distinct from the generators above.

Thus, when $b = 2$ we use additional generators of the form

$$\arctan\left(1/(1 - 2^m)\right) = \Im \ln(1 - (1 + i)2^{-m}).$$

We call these generators *Aurifeuillian* because of their similarity to the Aurifeuillian logarithmic generators defined in Section 3, where we also discuss Aurifeuille's work. The BBP formulae for these Aurifeuillian generators are given in Appendix A.

Definition 1 Given $\kappa \in \mathbb{R}$, $2 \leq b \in \mathbb{N}$, b not a proper power, we say that κ has a $\mathbb{Z}$-linear or $\mathbb{Q}$-linear *Machin-type BBP arctangent formula* to the base b if and only if κ can be written as a $\mathbb{Z}$-linear or $\mathbb{Q}$-linear combination (respectively) of generators of the form described above. A non-Aurifeuillian formula is one which does not use Aurifeuillian generators. (Note all formulae are non-Aurifeuillian when $b > 2$.) More briefly, when κ has a $\mathbb{Q}$-linear formula we say that κ has a b-ary Machin-type BBP arctangent formula.

Remarks Although our Machin-type BBP formulae are in one sense more restricted than the formulae considered by Bailey, they also appear to be more general, in that we allow linear combinations of $P(1, b^m, n, \dots)$ where both m and n may vary. However, in Appendix B we show that any Machin-type BBP formula may be reduced to Bailey's form.

We call the generators of Definition 1 the *minimal set* of arctangent generators, although for fixed b this set is not necessarily linearly independent. When $b = 2$ it is sometimes convenient when doing hand computations to use all elements of the form $\Im \ln(1 \pm (1+i)2^{-m}) = \arctan(1/(1 \pm 2^m))$ as generators. Note however that both our minimal set of generators and the *full set* described above span the same space, as can easily be shown using

$$\Im \ln(1 + (1+i)2^{-m}) = \Im \ln(1 - i2^{1-2m}) - \Im \ln(1 - (1+i)2^{-m}).$$

Note that $(1 - ib^{-m})\mathbb{R}^\times = (b^m - i)\mathbb{R}^\times$. Hence, both sides of the equality represent the same element in our group of slopes. Along the same lines we have $\Im \ln(1 - ib^{-m}) = \Im \ln(b^m - i)$. Since it is generally easier to work with elements of $\mathbb{Z}[i]^\times$ instead of $\mathbb{Q}[i]^\times$, we will often write $(b^m - i)\mathbb{R}^\times$ instead of $(1 - ib^{-m})\mathbb{R}^\times$. Similarly, we will often prefer $(2^m - 1 - i)\mathbb{R}^\times$ to $(1 - (1+i)2^{-m})\mathbb{R}^\times$ and prefer to write the inverse of $(x+iy)\mathbb{R}^\times$ as $(x-iy)\mathbb{R}^\times$. (We follow the corresponding practice when working with elements of $\mathbb{C}^\times/\mathbb{R}_+^\times$, with $\mathbb{R}_+^\times$ replacing the role of $\mathbb{R}^\times$.)

2.5 Finding Machin-Type BBP Arctangent Formulae

With these preliminary remarks out of the way, we almost immediately find a binary Machin-type BBP formulae for $\pi/4$ by noting that

$$\begin{aligned}\pi/4 &= -\Im \ln(1-i) = -\arctan(-1) \\ &= 2^{-4}P(1, 2^4, 8, [8, 8, 4, 0, -2, -2, -1, 0]).\end{aligned} \tag{17}$$

(This formula seems to have first been observed by Helaman Ferguson. See [Bai00, Equation (13)] and also [FBA99, p. 352].)

Further binary formulae for $\pi/4$ can be found in much the same way as in our development of Formula (10), and as in Størmer's solution to Gravé's problem, by looking for products of the form

$$z := \prod_j (2^{m_j} - i)^{n_j} \prod_j (2^{m_j} - 1 - i)^{n_j} \tag{18}$$

which yield $z \in (1+i)\mathbb{R}_+^\times$, and thus $\Im \ln(z) \equiv \pi/4 \pmod{2\pi}$. More generally, when looking for $\mathbb{Z}$-linear formulae for some multiple of π, we would consider products of the form (18) yielding $z \in (1+i)^n\mathbb{R}_+^\times$, and thus $\Im \ln(z) \equiv n\pi/4 \pmod{2\pi}$. Note that when $n \equiv 0 \pmod 8$ it is possible that $\Im \ln(z) = 0$.

A hand search for additional formulae soon reveals that

$$(2-i)(3-i) = 5 - 5i, \tag{19}$$

$$(2-i)^2(7+i) = 25 - 25i, \tag{20}$$

$$(3-i)^2(7-i) = 50 - 50i, \tag{21}$$

corresponding to the solutions (11)–(13) of Gravé's problem. Since each factor on the left-hand sides has one of the desired forms $2^m - i$ or $2^m - 1 - i$ for some m we see that (11), (12), and (13) all yield binary Machin-type BBP arctangent formulae for $\pi/4$.

Similarly, a hand search gives binary Machin-type BBP arctangent formulae for $\arctan(1/6)$, $\arctan(5/6)$, and $\arctan(1/11)$ via the factorizations

$$6+i = (5+i)(31-i)/26,$$
$$6+5i = (1+i)(5-i)(9+i)(255-i)/2132,$$
$$11+i = (1+i)(6-5i), \text{ and then factor } (6-5i) \text{ as } \overline{6+5i}.$$

These factorizations give formulae in terms of our full set of generators:

$$\arctan(1/6) = \arctan(1/5) - \arctan(1/31)$$

and

$$\arctan(5/6) = \arctan(1) - \arctan(1/5) + \arctan(1/9) - \arctan(1/255)$$

while

$$\arctan(1/11) = \arctan(1) - \arctan(5/6).$$

No formulae for these three arctangents are listed in Bailey's *Compendium* of November 2000 [Bai00, §3]. However, the above results show that $\arctan(1/6)$, $\arctan(5/6)$ and $\arctan(1/11)$ do indeed admit binary Machin-type BBP formulae. (The process of converting such formulae to Bailey's form is detailed in Appendix B.) Among the values missing in Bailey's list, the first arctangent for which we have been unable to find a binary Machin-type BBP formula is $\arctan(2/7)$.

We can make the search for arctangent formulae more systematic by examining how $2^m - i$ and $2^m - 1 - i$ factor into primes over $\mathbb{Z}[i]$. Since primes in $\mathbb{Z}[i]$ are only defined up to a factor of i^n, we shall always take a "canonical" factorization of $z \in \mathbb{Z}[i]$, of the form

$$z = i^n \prod_j \mathfrak{p}_j^{n_j}, \tag{22}$$

where $\mathfrak{p}_j$ runs through a subset of the primes of $\mathbb{Z}[i]$, and for each prime $\mathfrak{p}$ we require $\Re\mathfrak{p} > 0$ and $-\Re\mathfrak{p} < \Im\mathfrak{p} \le \Re\mathfrak{p}$, so that $-\pi/4 < \Im\ln\mathfrak{p} \le \pi/4$. These conditions uniquely define $n \pmod 4$, where n is the exponent appearing in i^n. To make n unique, we further require that $-1 \le n \le 2$.

The factorization of $z \in \mathbb{Z}[i]$ can easily be found in the computer algebra system Maple using the GaussInt package, or in the system Mathematica using FactorInteger[z, GaussianIntegers→True]. (However, in both cases additional work is needed to get a canonical factorization in our sense.) Since, given $z, w \in \mathbb{C}$, $\Im\ln(zw) \equiv \Im\ln(z) + \Im\ln(w) \pmod{2\pi}$, the factorization (22) gives

$$\Im\ln(z) \equiv n\pi/2 + \sum_j n_j \Im\ln\mathfrak{p}_j \pmod{2\pi}.$$

In many cases, this equivalence modulo 2π corresponds to true equality, but the example $z = (2+i)^{12} = 11753 - 10296i$, $\Im\ln(z) \approx -0.7194$ while $12\Im\ln(2+i) \approx 5.5638$, demonstrates that this is not always true.

More detailed discussion of such experimental and symbolic computational matters is to be found in [BB03] and on the associated website www.expmath.info.

To illustrate, we use this technique to more systematically find formulae for π. Let $\beta_m := \Im\ln(2^m - i)$ and $\alpha_m := \Im\ln(2^m - i - 1)$ denote our binary Machin-type BBP arctangent generators. For the first few generators, factoring the arguments $2^m - i$ of $\Im\ln(\ldots)$ into primes over $\mathbb{Z}[i]$ gives

$$2^1 - i = 2 - i \tag{23}$$

$$2^2 - i = 4 - i \tag{24}$$

$$2^3 - i = (2+i)(3-2i), \tag{25}$$

while for the Aurifeuillian arguments $2^m - 1 - i$ we find

$$2^1 - 1 - i = 1 - i \tag{26}$$

$$2^2 - 1 - i = i^{-1}(1+i)(2+i) \tag{27}$$

$$2^3 - 1 - i = (1+i)(2-i)^2. \tag{28}$$

Using $\Im\ln(i) = \pi/2$, $\Im\ln(1+i) = \pi/4$, $\Im\ln(\overline{\mathfrak{p}}) = -\Im\ln(\mathfrak{p})$; and checking that we have the correct congruence class modulo 2π, the factorizations (23) through (25) give

$$\beta_1 = -\Im\ln(2+i) \tag{29}$$

$$\beta_2 = -\Im\ln(4+i) \tag{30}$$

$$\beta_3 = \Im\ln(2+i) - \Im\ln(3+2i), \tag{31}$$

while, by (26) through (28), our Aurifeuillian generators decompose as

$$\alpha_1 = -\pi/4 \tag{32}$$

$$\alpha_2 = -\pi/4 + \Im\ln(2+i) \tag{33}$$

$$\alpha_3 = \pi/4 - 2\Im\ln(2+i). \tag{34}$$

(The presence of $\pi/4$ in our Aurifeuillian generators could have been predicted from the fact that $1 + i \mid x + iy$ when $x^2 + y^2$ is even.)

With these decompositions—essentially a change of basis in our vector space over $\mathbb{Q}$—we can easily spot $\mathbb{Z}$-linear dependencies between β_1, α_1, α_2, and α_3. From these dependencies we once again get formulae for $\pi/4$ corresponding to Equations (19)–(21). Equivalently, we get two linearly independent zero relations such as

$$\alpha_1 + \alpha_3 - 2\beta_1 = 0 \tag{35}$$

$$\alpha_1 - 2\alpha_2 - \alpha_3 = 0. \tag{36}$$

2.6 Exclusion Criteria for Machin-Type BBP Arctangent Formulae

The type of reasoning above can also be used to exclude the possibility of a Machin-type BBP formula, as illustrated in Theorems 1 and 2 below.

In the following discussion, $\nu_b(p)$ denotes the order of b in the multiplicative group modulo a prime p. Given $z \in \mathbb{Q}$, $\mathrm{ord}_p(z)$ denotes the usual *p-adic order of z*, which can be defined by stating that $\mathrm{ord}_p(p) = 1$, $\mathrm{ord}_p(q) = 0$ for any prime $q \neq p$, and $\mathrm{ord}_p(zw) = \mathrm{ord}_p(z)+\mathrm{ord}_p(w)$. We remark that we cannot have $\mathrm{ord}_p(x^2+y^2)$ odd when $p \equiv 3 \pmod 4$. Note also that $\mathrm{ord}_p \colon \mathbb{Q}^\times \to \mathbb{Z}$ is a group homomorphism. For more information on p-adic orders, see, for example, the book by Koblitz [Kob84].

Theorem 1 *Given $2 \le b \in \mathbb{N}$, b not a proper power, and given $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, suppose there is a prime $p \equiv 1 \pmod 4$ with $\mathrm{ord}_p(x^2 + y^2)$ odd, such that either $p \mid b$; or $p \nmid b$, $4 \nmid \nu_b(p)$. Then* $\arctan(y/x)$ *does not have a $\mathbb{Z}$-linear Machin-type BBP arctangent formula to the base b.*

Proof (a) We first consider the simpler case where $b > 2$, so that there are no Aurifeuillian generators to consider. In this case, if there were a formula for $\arctan(y/x)$, we would have

$$(x + iy)\mathbb{R}^\times = \prod_j (b^{m_j} - i)^{n_j}\mathbb{R}^\times, \tag{37}$$

$m_j \in \mathbb{N}$, $n_j \in \mathbb{Z}$. Since a real-valued product of elements of $\mathbb{Q}[i]^\times$ must lie in $\mathbb{Q}^\times$, we conclude from Equation (37) that

$$(x + iy)\prod_j (b^{m_j} - i)^{-n_j} = M/N \in \mathbb{Q}^\times. \tag{38}$$

Taking norms (multiplying each expression by its complex conjugate) in (38) yields

$$(x^2 + y^2)\prod_j (b^{2m_j} + 1)^{-n_j} = M^2/N^2.$$

Since $\mathrm{ord}_p(x^2 + y^2)$ is assumed odd but $\mathrm{ord}_p(M^2/N^2)$ must be even, we must have $p \mid b^{2m_j} + 1$ for at least one j. Clearly this cannot happen if $p \mid b$. Now assuming that $p \nmid b$, $4 \nmid \nu_b(p)$, and letting $m = m_j$ we find

$$b^{2m} \equiv -1 \pmod p, \tag{39}$$

and so $b^{4m} \equiv 1 \pmod p$. Thus we conclude that $\nu_b(p) \mid 4m$. But $4 \nmid \nu_b(p)$, so $\nu_b(p) \mid 2m$, giving $b^{2m} \equiv 1 \pmod p$, contradicting (39).

(b) The argument when $b = 2$ is similar. Note that we cannot have $p \mid b$ in this case. Now, if there were a formula for $\arctan(y/x)$, we would have an identity of the form

$$(x + iy)\mathbb{R}^\times = \prod_j (2^{m_j} - i)^{n_j} \prod_j (2^{m_j} - (1 + i))^{n_j}\mathbb{R}^\times. \tag{40}$$

Arguing as before, and taking norms, we conclude that

$$(x^2+y^2)\prod_j(2^{2m_j}+1)^{-n_j}\prod_j(2^{m_j}-(1+i))^{-n_j}(2^{m_j}-(1-i))^{-n_j}=M^2/N^2.$$

Since $p\equiv 1 \pmod 4$, there is an $I\in\mathbb{Z}$ satisfying $I^2\equiv -1 \pmod p$. As before, since $\mathrm{ord}_p(x^2+y^2)$ is assumed odd but $\mathrm{ord}_p(M^2/N^2)$ must be even, at least one of $p \mid 2^{2m_j}+1$; $p\mid 2^{m_j}-(1+I)$; or $p\mid 2^{m_j}-(1-I)$ must hold.

The first case immediately leads to a contradiction, as when $b>2$. The latter two cases give $2^{m_j}\equiv 1\pm I \pmod p$. Raising both sides to the fourth power gives $2^{4m_j}\equiv -4 \pmod p$, so, letting $m=2m_j-1$, we have $2^{2m}\equiv -1 \pmod p$, which again leads to a contradiction, as when $b>2$. ■

Example 1 Using $p=5$ and $\mathrm{ord}_5(2^2+1^2)=1$ in Theorem 1, we conclude that there is no b-ary $\mathbb{Z}$-linear Machin-type BBP formulae for $\arctan(1/2)$ when $5\,|\,b$. Similarly, using $p=13$ and $\mathrm{ord}_{13}(5^2+1^2)=1$, we conclude that there is no b-ary $\mathbb{Z}$-linear Machin-type BBP formulae for $\arctan(1/5)$ when $13\,|\,b$.

Example 2 Using the second exclusion criterion of Theorem 1, with $p=13$ and noting $3^2+2^2=13$ and $\nu_3(13)=3$, we conclude that $\arctan(2/3)$ has no 3-ary $\mathbb{Z}$-linear Machin-type BBP arctangent formula. More generally, no odd multiple of $\arctan(2/3)$ has a 3-ary $\mathbb{Z}$-linear Machin-type BBP arctangent formula.

Similarly, with $b=2$ and $p=73$, noting that $8^2+3^2=73$, we conclude that $\arctan(3/8)$ has no binary $\mathbb{Z}$-linear Machin-type BBP arctangent formula, as $\nu_2(73)=9$.

Correspondingly, with $b=2$ and $p=89$, noting that $8^2+5^2=89$, we conclude that $\arctan(5/8)$ has no binary $\mathbb{Z}$-linear Machin-type BBP formula. Similarly, $\arctan(5/11)$ has no binary formula, since $146=2\cdot 73$. Also $9/16$ yields the prime 337 with $\nu_2(337)=21$, and $11/18$ yields 445 which is divisible by the prime 89 with $\nu_2(89)=11$. (See also Appendix C on density of arctans with or without Machin-type formulae.)

The arguments above rule out formulae for $3/8$ and $5/8$. Binary $\mathbb{Q}$-linear Machin-type formulae are known for all other fractions with denominator less than 10, with the exceptions of $2/7$, $4/9$, $5/9$, which are presently in limbo. In these three cases the exclusion criterion of Theorem 1 fails. We return to these orphans in Example 3.

We shall derive a stronger exclusion criterion for Machin-type BBP arctangent formulae by looking at how $(x+iy)$ factors in $\mathbb{Z}[i]$:

Definition 2 Given $z\in\mathbb{Q}[i]$, and a rational prime $p\equiv 1 \pmod 4$, let $\vartheta_p(z)$ denote $\mathrm{ord}_{\mathfrak{p}}(z)-\mathrm{ord}_{\overline{\mathfrak{p}}}(z)$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the two conjugate Gaussian primes dividing p, and where we require $0<\Im\mathfrak{p}<\Re\mathfrak{p}$ to make the definition of ϑ_p unambiguous.

Note that ϑ_p is a group homomorphism, since

$$\vartheta_p(zw)=\vartheta_p(z)+\vartheta_p(w). \tag{41}$$

Theorem 2 *Given* $2 \le b \in \mathbb{N}$, *b not a proper power, and given* $x \in \mathbb{N}$, $y \in \mathbb{N}$, *suppose there is a prime* p *not dividing* b, *with* $p \equiv 1 \mod 4$ *and* $\vartheta_p(x+iy) \neq 0$. *Suppose either* (a) $4 \nmid \nu_b(p)$, *or* (b) *the prime* $p \equiv 1 \pmod 4$, *such that* $4 \mid \nu_b(p)$, *is unique, and there is a prime* $q \equiv 1 \pmod 4$ *with* $\vartheta_q(x+iy) = 0$ *and* $\nu_b(p) = \nu_b(q)$.

Then in case (a) $\arctan(y/x)$ *does not have a* $\mathbb{Q}$*-linear Machin-type BBP arctangent formula to the base b; and in case* (b) $\arctan(y/x)$ *has no non-Aurifeuillian* $\mathbb{Q}$*-linear Machin-type BBP arctangent formula to the base b.*

Proof Our proof of (a) is similar to the proof of Theorem 1. Again, we first consider the case $b > 2$, where there are no Aurifeuillian generators to consider. In this case, if there were a $\mathbb{Q}$-linear Machin-type BBP formula for $\arctan(y/x)$ then for some $n \in \mathbb{Z}$, $n \neq 0$ we would have

$$(x+iy)^n \prod_j (b^{m_j} - i)^{-n_j} = M/N \in \mathbb{Q}^\times.$$

Our assumption that $\vartheta_p(x+iy) \neq 0$ implies $\vartheta_p\big((x+iy)^n\big) \neq 0$, which together with $\vartheta_p(M/N) = 0$ implies $\vartheta_p(b^{m_j} - i) \neq 0$ for at least one j. So, at least one of $\mathfrak{p}$, $\overline{\mathfrak{p}}$ divides $b^{m_j} - i$. Thus, letting $m = m_j$, assume that $\mathfrak{p} \mid b^m - i$. (The argument when $\overline{\mathfrak{p}} \mid b^m - i$ is nearly identical.) Since $\mathfrak{p} \mid b^m - i$ we have $\overline{\mathfrak{p}} \mid b^m + i$, and thus $\mathfrak{p}\overline{\mathfrak{p}} \mid b^{2m} + 1$. In other words, $b^{2m} \equiv -1 \pmod p$, which gives a contradiction, as in the proof of Theorem 1.

We now consider the case when $b = 2$. In this case a formula for $\arctan(y/x)$ would imply that we had an identity of the form

$$(x+iy)\mathbb{R}^\times = \prod_j (2^{m_j} - i)^{n_j} \prod_j (2^{m_j} - (1+i))^{n_j} \mathbb{R}^\times.$$

Our assumption that $\vartheta_p(x+iy) \neq 0$ leads us to conclude that at least one of $\mathfrak{p}$, $\overline{\mathfrak{p}}$ divides at least one of $2^{m_j} - i$ or $2^{m_j} - (1+i)$ for some j. Again, without loss of generality, assume that $\mathfrak{p}$ is the divisor. If $\mathfrak{p} \mid 2^{m_j} - i$ we get a contradiction, as when $b > 2$. If $\mathfrak{p} \mid 2^{m_j} - (1+i)$ then, letting $m = 2m_j - 1$, it follows that $b^{2m} \equiv -1 \pmod p$, which again gives a contradiction.

We defer the proof of part (b) until Section 3.4. ∎

Example 3 Continuing Example 2, looking for a ternary arctangent formula for $\arctan(2/3)$, we use $p = 13$ in Theorem 2 (a), still noting that $\nu_3(13) = 3$, and using $\vartheta_{13}(3+2i) = 1$, to conclude that $\arctan(2/3)$ has no 3-ary $\mathbb{Q}$-linear Machin-type BBP arctangent formula. This can be applied to various of the other fractions in Example 2 such as $3/8, 5/8, 5/11, 9/16$, and $11/18$.

We illustrate Theorem 2 (b), as follows. First it shows us that $\arctan(1/4)$ has no 3-ary $\mathbb{Q}$-linear Machin-type BBP arctangent, since $\nu_3(17) = \nu_3(193) = 16$. Correspondingly, we may rule out non-Aurifeuillian binary formulae for arctangents of the fractions $2/7, 4/9$ and $5/9$. Indeed $2^2 + 7^2 = 53$, $5^2 + 9^2 = 53 \cdot 2$ and $\nu_2(53) = \nu_2(157) = 52$. Similarly, $4^2 + 9^2 = 97$ and $\nu_2(97) = \nu_2(673) = 48$.

We can clarify the meaning of ϑ_p by extending its definition to cover every prime p. We define $\vartheta_p(z) := 0$ when $p \equiv 3 \pmod 4$, since these primes do not factor further over $\mathbb{Z}[i]$ and thus contribute nothing to $\Im \ln(z)$. To deal with the case $p = 2$ we note that $z \in \mathbb{Q}[i]^\times$ can be rewritten as $z\mathbb{R}^\times = z_0\mathbb{R}^\times$ with $z_0 \in \mathbb{Z}[i]$, and so that z_0 factors over $\mathbb{Z}[i]$ as

$$z_0 = (1+i)^k \prod_{\substack{p \equiv 1 \ (\mathrm{mod}\ 4) \\ p = \mathfrak{p}\overline{\mathfrak{p}}}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(z)}\, \overline{\mathfrak{p}}^{\,\mathrm{ord}_{\overline{\mathfrak{p}}}(z)}, \tag{42}$$

with $0 \le k < 8$ and with $0 < \Im\mathfrak{p} < \Re\mathfrak{p}$. (When $z \in \mathbb{Z}[i]$ we have $k \equiv 2n + \mathrm{ord}_{1+i}(z) \pmod 8$, where n is defined by the canonical factorization of z defined following Equation (22). Similarly, when $z \in \mathbb{Q}[i]$, we can compute $k \pmod 8$ from the canonical factorizations of the numerator and denominator of z.) Now, let $\vartheta_2(z) := k$, where k is given by Equation (42). (Note that $\vartheta_2(zw) \equiv \vartheta_2(z) + \vartheta_2(w) \pmod 8$.)

With this extended definition of ϑ_p, we have

$$\Im \ln(z) \equiv \vartheta_2(z)\Im\ln(1+i) + \sum_{p \equiv 1 \ (\mathrm{mod}\ 4)} \vartheta_p(z)\Im\ln(\mathfrak{p}) \pmod{2\pi}.$$

Thus, $\vartheta_p(z)$ measures the contribution to $\Im\ln(z)$ which can be attributed to $1+i$ (the single Gaussian prime dividing 2) and to the Gaussian primes $\mathfrak{p} \mid p$, $\overline{\mathfrak{p}} \mid p$, $p \equiv 1 \pmod 4$.

Given a finite set of generators of the form $\Im\ln(z)$, $z \in \mathbb{Q}[i]$, we could, in principle, use values of ϑ_p to automate the process which we informally used to spot the zero relations (35) and (36) given earlier. For each generator of the form $\Im\ln(z)$ we would compute a vector of $\vartheta_p(z)$, indexed by p, where p runs through a finite subset of $\{2\} \cup \{p \text{ prime} : p \equiv 1 \pmod 4\}$. (The ϑ_2 component of the vectors should be treated as an element of $\mathbb{Z}/(8\mathbb{Z})$.)

Given these vectors, the process of finding possible linear dependencies could be automated by using the algorithms described in [Coh93, §2.4] for analyzing $\mathbb{Z}$-modules, (*i.e.,* Abelian groups). The dependencies found this way are only "potential" dependencies, both because knowledge of $\vartheta_p(z)$ for all p only determines $\Im\ln z \pmod{2\pi}$, and because we may choose to restrict ourselves to a small subset of primes, and thus will get less than complete information about how the various z factor in $\mathbb{Z}[i]$. (Consider the problem of completely factoring $2^{1001} - i$ over $\mathbb{Z}[i]$.) we shall return to this idea of using vectors when we discuss *valuation vectors* in Section 3, below.

At the conclusion of Section 3, we shall introduce another exclusion criterion for Machin-type BBP arctangent formulae to show that any Machin-type BBP arctangent formula for π must be a binary formula. In particular, there is no decimal Machin-type BBP arctangent formula for π. This result is based on a technique which is also useful for excluding Machin-type BBP "logarithm formulae"—the topic to which we now turn.

3 Machin-Type BBP Formulae for Logarithms

3.1 Machin-Type Logarithmic Generators and Formulae

Our definition of a Machin-type BBP logarithm formula is analogous to our definition of a Machin-type BBP arctangent formula, with $\Re \ln(z) = \ln|z|$ replacing the role of $\Im \ln(z)$. Although group theory plays a less important role here, we note that we are working with the multiplicative group $\mathbb{C}^\times/\mathbb{S}$. The group $\mathbb{C}^\times/\mathbb{S}$ is isomorphic to the additive group $\mathbb{R}$, under the isomorphism that sends $t \in \mathbb{R}$ to the coset $e^t\mathbb{S}$. The inverse map is $z\mathbb{S} \mapsto \Re \ln(z) = \ln|z|$. However, since $\mathbb{C}^\times/\mathbb{S}$ is so readily identified with the isomorphic multiplicative group $\mathbb{R}_+^\times$, we usually prefer to treat the latter group and its obvious isomorphism to the additive group $\mathbb{R}$, $\ln(z)\colon \mathbb{R}_+^\times \to \mathbb{R}$.

We begin by describing our *logarithmic generators*. (We give BBP formulae for these generators in Appendix A.) Given b not a proper power, $b > 2$, these are generators of the form $\ln(1 - b^{-m})$. In the case $b = 2$ we include additional *Aurifeuillian* generators, of the form $\ln|1 - (1 + i)2^{-m}|$. We call these additional generators Aurifeuillian because some terms which appear in the equation

$$\ln\left|1 \pm (1+i)2^{-m}\right| = \frac{1}{2}\ln\left(2^{1-2m}(2^{2m-1} \pm 2^m + 1)\right) = \left(\frac{1}{2} - m\right)\ln(2) + \frac{1}{2}\ln(2^{2m-1} \pm 2^m + 1). \tag{43}$$

correspond to factors in the equation

$$2^{4m-2} + 1 = (2^{2m-1} + 2^m + 1)(2^{2m-1} - 2^m + 1). \tag{44}$$

Such factorizations were discovered by Aurifeuille and Le Lasseurre but first described in print in 1878 by Lucas (see [Wil98, p. 126]).

Definition 3 Given $\kappa \in \mathbb{R}$, $2 \le b \in \mathbb{N}$, b not a proper power, we say that κ has a $\mathbb{Z}$-linear or $\mathbb{Q}$-linear *Machin-type BBP logarithm formula* to the base b if and only if κ can be written as a $\mathbb{Z}$-linear or $\mathbb{Q}$-linear combination (respectively) of generators of the form described in the previous paragraph.

A non-Aurifeuillian formula is one which does not use Aurifeuillian generators. More briefly, when κ has a $\mathbb{Q}$-linear formula we shall say that κ has a b-ary Machin-type BBP logarithm formula.

Remark We call the generators of Definition 3 the *minimal set* of logarithm generators. From the identities $\ln(1+b^{-m}) = \ln(1-b^{-2m}) - \ln(1-b^{m})$ and $\ln|1 \pm ib^{-m}| = \ln(1 + b^{-2m})/2$ we find that our minimal set generates

$$\operatorname{span}\left\{\ln(1 \pm b^{-m}), \ln\left|1 \pm ib^{-m}\right| : m \in \mathbb{N}\right\}.$$

The Aurifeuillian identity (44) implies that when $b = 2$ our minimal set generates

$$\operatorname{span}\left\{\ln(1 \pm 2^{-m}), \ln\left|1 \pm i2^{-m}\right|, \ln\left|1 \pm (1 \pm i)2^{-m}\right| : m \in \mathbb{N}\right\}.$$

As in the arctangent case, for hand computations it is often convenient to use the "full set" of generators implied by these relations.

3.2 Using Valuation Vectors and Factorizations

When searching for Machin-type BBP logarithm formulae, we take much the same approach that we described for finding Machin-type BBP arctangent formulae for π.

Given a finite set of generators of the form $\{\ln|z| : |z| \in \mathcal{G} \subset \mathbb{Q}[i]\}$, we begin by computing a *valuation vector* for each $|z|$, $|z| \in \mathcal{G}$. Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$. (We allow $z \in \overline{\mathbb{Q}}$ so as to give a more general result, although we shall only consider examples with $z \in \mathbb{Q}[i]$.) Given $z \in \overline{\mathbb{Q}}$, a valuation vector for z is a vector with entries indexed by a fixed set of primes $\mathcal{P}$, where the entry indexed by $p \in \mathcal{P}$ gives $\operatorname{ord}_p(z)$. Note that $\operatorname{ord}_p(z)$ can be extended so as to be defined for $z \in \overline{\mathbb{Q}}$; see, for example, [Kob84, Chapter III]. For our purposes, it suffices to recall that $\operatorname{ord}_p(zw) = \operatorname{ord}_p(z) + \operatorname{ord}_p(w)$, and thus $\operatorname{ord}_p(1 - b^{-m}) = \operatorname{ord}_p(b^m - 1) - m \operatorname{ord}_p(b)$ while, as in the derivation of Equation (43), we find

$$\begin{aligned}(45)\qquad \operatorname{ord}_p\left(\left|1-(1+i)2^{-m}\right|\right) &= \operatorname{ord}_p\left(2^{1/2-m}\sqrt{2^{2m-1}-2^m+1}\right)\\ &= \left(\frac{1}{2}-m\right)\operatorname{ord}_p(2)+\frac{1}{2}\operatorname{ord}_p(2^{2m-1}-2^m+1).\end{aligned}$$

For example, indexing by the primes $\{2,3,5\}$ (in that order) the valuation vector for $1 - 2^{-4} = 15/16$ is $[-4, 1, 1]$, while the valuation vector for $\left|1-(1+i)2^{-4}\right| = \sqrt{2}\sqrt{113}/16$ is $[-3.5, 0, 0]$. In contrast, if we use $\mathcal{P} = \{2, 3, 5, 113\}$, the valuation vector for $\left|1-(1+i)2^{-4}\right|$ is $[-3.5, 0, 0, 1]$.

An important property of ord_p is that $|z| = \prod_p p^{\operatorname{ord}_p(|z|)}$, where the product runs through all primes p for which $\operatorname{ord}_p(|z|) \neq 0$. This implies that if we choose

$$\mathcal{P} = \bigcup_{|z|\in\mathcal{G}} \left\{p : \operatorname{ord}_p(|z|) \neq 0\right\}.$$

then the vector space over $\mathbb{Q}$ generated by $\{\ln|z| : |z| \in \mathcal{G}\}$ is isomorphic to the space of valuation vectors indexed by $\mathcal{P}$.

Thus, in principle, it should be possible to reduce the task of searching for Machin-type BBP logarithm formulae (arising from a fixed set of generators) to doing $\mathbb{Z}$-linear algebra with valuation vectors, again using algorithms described in [Coh93, §2.4].

In practice, this might require finding the prime factorization of inordinately large numbers, in which case we can use a smaller set $\mathcal{P}$ at the cost of losing some information. Because of the nature of our generators, the task of finding Machin-type BBP formulae for logarithms is closely related to the *Cunningham Project* [BLS88]: an ongoing project to find factorizations of numbers of the form $b^m \pm 1$, for $b \in \{2, 3, 5, 6, 7, 10, 11, 12\}$.

As indicated above, one way to find the valuation vector for $1 - b^{-m}$ is to factor b and $b^m - 1$. Similarly, by Equation (45), we can find the valuation vector for $|1-(1+i)2^{-m}|$ by factoring b and $2^{2m-1} - 2^m + 1$. By the Aurifeuillian identity (44), the task of factoring $2^{2m-1} - 2^m + 1$ is closely related to the task of factoring $2^{4m-2} + 1$. One technique used in the Cunningham Project has been to break $b^m - 1$ into smaller factors by algebraically factoring $b^m - 1$ into cyclotomic polynomials $\psi_d(b)$, using the relationship

$$b^m - 1 = \prod_{d|m} \psi_d(b). \tag{46}$$

The cyclotomic polynomials can be defined by the inversion formula corresponding to (46), namely

$$\psi_d(b) = \prod_{m|d} (b^m - 1)^{\mu(d/m)}. \tag{47}$$

where $\mu(d)$ denotes the Möbius function. (Cyclotomic polynomials are discussed in many references, for example [NZM91].)

In the case $b = 2$, the Aurifeuillian identity (44) is also useful as an algebraic factorization for $2^m - 1$. Further information about Aurifeuillian factorizations can be found in [Rie94, Appendix 6] and [Bre93]. A paper by Chamberland gives further discussion of the use of cyclotomic polynomials and Aurifeuillian factorizations to find BBP formulae [Cha].

3.3 Using Bang's Theorem as an Exclusion Criterion

Since formulae for $\ln(z)$, $z \in \mathbb{Q}$, can be generated as $\mathbb{Z}$-linear combinations of formulae for $\ln(p)$, p prime, most of the search for BBP formulae has focused on the latter case. However, as we shall show below, Machin-type BBP formulae for $\ln(p)$ often fail to exist. Our main tool for excluding Machin-type BBP formulae for logarithms is a theorem due to Bang.

We begin with a definition used in the statement of the theorem.

Definition 4 Given fixed $b > 1$, we shall say a prime p is a *primitive prime factor* of $b^m - 1$ if m is the least integer such that p divides $b^m - 1$. In other words, p is a primitive prime factor of $b^m - 1$ provided $\nu_b(p) = m$.

Theorem 3 (Bang, 1886) *The only cases where $b^m - 1$ has no primitive prime factor(s) are when $b = 2$, $m = 6$, $b^m - 1 = 3^2 \cdot 7$; and when $b = 2^N - 1$, $N \in \mathbb{N}$, $m = 2$, $b^m - 1 = 2^{N+1}(2^{N-1} - 1)$.*

Bang's Theorem is often called "Zsigmondy's Theorem", since Zsigmondy generalized Bang's result to expressions of the form $b^m - a^m$. A survey of Zsigmondy's Theorem and related results can be found in [Rib91], while a proof of Bang's Theorem can be found in [Roi97].

We shall call the cases where there is no primitive prime factor the "exceptional cases" of Bang's Theorem, and will let M_b denote the value of m, depending on b, for which an exceptional case occurs, or $M_b := 0$ when there is no exceptional case. Thus

$$M_b := \begin{cases} 6 & \text{when } b = 2, \\ 2 & \text{when } b = 2^N - 1, N \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases} \tag{48}$$

Bang's Theorem can often be used to exclude the possibility of a constant having a Machin-type logarithm formula. We illustrate this with an example due to Carl Pomerance, first mentioned briefly in [BBP97, §5]:

Theorem 4 *There is no non-Aurifeuillian binary Machin-type BBP logarithm formula for* $\ln(23)$ *nor for* $\ln(89)$.

Proof Suppose instead that $\ln(23)$ has a non-Aurifeuillian binary Machin-type formula. This is equivalent to being able to write

$$23^n = 2^t \prod_{m=1}^{M} (2^m - 1)^{n_m} \tag{49}$$

with $n_m \in \mathbb{Z}$, $n_M \neq 0$, $n \in \mathbb{N}$, and $t = -\sum_{m=1}^{M} m n_m$. Since $\nu_2(23) = 11$ we must have $M \geq 11$, so $2^M - 1$ has a primitive prime factor, say p. Since p cannot occur as a factor of $2^m - 1$, $m < M$, we must have $p = 23$, for otherwise we would not be able to cancel it out in (49). Since 23 is a primitive prime factor of $2^{11} - 1 = 23 \cdot 89$ we must have $M = 11$. But 89 is also a primitive prime factor $2^{11} - 1$, and cannot be cancelled out of (49).

The above argument also shows that $\ln(89)$ can not be obtained. ■

The same argument applies to many other pairs of primes having the property that the first prime has a prime "friend" which is also a primitive prime factor of the same $2^M - 1$. For example, two primes with logarithms having no non-Aurifeuillian binary formula are 47 and 53, since $2^{23} - 1 = 47 \cdot 178481$, and $\nu_2(47) = \nu_2(178481) = 23$. Another such pair is 29 and 113, since $2^{28} - 1 = 3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$, and $\nu_2(29) = \nu_2(113) = 28$.

If we exclude Aurifeuillian generators, then to say $\ln(z)$ has a b-ary Machin-type BBP formula means $\ln(z) \in \operatorname{span}\{\ln(1 - b^{-m}) : 1 \leq m \leq M\}$ for some $M < \infty$. A consequence of Bang's Theorem is that, for fixed z, elements of the form $\ln(1 - b^{-m})$ and $\ln(z)$ are likely to be linearly independent, which excludes the possibility of a Machin-type BBP formula.

We now develop somewhat more technical tools for demonstrating linear independence of logarithms. Lemma 5 below gives a general criterion for linear independence for elements of the form $\ln(z)$, $z \in \overline{\mathbb{Q}}$. The idea behind Lemma 5 is to find a sequence of valuation vectors, which, when arranged in a matrix, give a triangular matrix with nonzero entries along the diagonal.

Lemma 5 *Given* $z_0, z_1, \ldots, z_K$*, all elements of* $\overline{\mathbb{Q}}$*, then a sufficient condition that* $\ln(z_0), \ldots, \ln(z_K)$ *be* $\mathbb{Q}$*-linearly independent is that there be distinct primes* $p_0, \ldots, p_K$ *with* $\operatorname{ord}_{p_k}(z_k) \neq 0$ *and* $\operatorname{ord}_{p_j}(z_k) = 0$ *when* $j > k$.

Proof If there were a $\mathbb{Q}$-linear dependence among the $\ln(z_k)$ then for some $n_k \in \mathbb{Z}$, not all zero, we would have

$$\sum_{k=0}^{m} n_k \ln(z_k) = 0, \quad \text{and so} \quad \prod_{k=0}^{m} z_k^{n_k} = 1, \tag{50}$$

where m denotes the largest k for which $n_k \neq 0$. Writing $n := n_m$ and $p := p_m$, our conditions give $\operatorname{ord}_p(z_k) \neq 0$ if and only if $k = m$, while Equation (50) gives the contradiction

$$\operatorname{ord}_p\left(\prod_{k=0}^{m} z_k^{n_k}\right) = n \operatorname{ord}_p(z_m) = 0.$$

■

Theorem 6, below, gives a fairly general exclusion criterion for Machin-type BBP logarithm formulae. We shall make use of the facts that if $\operatorname{ord}_p(b^m - 1) \neq 0$ then $\operatorname{ord}_p(b) = 0$, and that $\operatorname{ord}_p(1 - b^{-k}) = \operatorname{ord}_p(b^k - 1)$, for any $k \in \mathbb{Z}$.

Theorem 6 *Given $z_0 \in \overline{\mathbb{Q}}$ and $2 \leq b \in \mathbb{N}$, b not a proper power, assume that there is at least one prime p such that $\operatorname{ord}_p(z_0) \neq 0$ (equivalently, assume that z_0 is not a root of unity) and let p_0 be the largest such prime. Let*

$$M_0 := \max(M_b, p_0 - 1), \tag{51}$$

where M_b is defined by Equation (48), and let

$$U := \operatorname{span}\{\ln(1 - b^{-m}) : 1 \leq m \leq M_0\}$$

so that U has a basis of the form $\ln(z_k)$, $1 \leq k \leq \dim(U)$. Suppose there are distinct primes $p_1, \ldots, p_{\dim(U)}$ such that for $0 \leq j, k \leq \dim(U)$ we have $\operatorname{ord}_{p_k}(z_k) \neq 0$ and $\operatorname{ord}_{p_j}(z_k) = 0$ when $j > k$.

Then there is no non-Aurifeuillian $\mathbb{Q}$-linear Machin-type BBP logarithm formula for $\ln(z_0)$.

Proof Suppose, to the contrary, that there is a Machin-type BBP formula for $\ln(z_0)$, *i.e.*, $\ln(z_0) \in V := \operatorname{span}\{\ln(1 - b^{-m}) : 1 \leq m \leq M\}$ for some $M < \infty$. Without loss of generality, we may assume $M \geq M_0$, *i.e.*, $U \subseteq V$. For $k > \dim(U)$ let $m_k := M_0 + k - \dim(U)$, so m_k ranges over $M_0 + 1 \leq m_k \leq M$ as k ranges over $\dim(U) + 1 \leq k \leq \dim(U) + M - M_0$. Let $z_k := 1 - b^{-m_k}$, and let p_k denote a primitive prime factor of $b^{m_k} - 1$. (Note that p_k exists since $m_k > M_0 \geq M_b$.) Clearly, $V = \operatorname{span}\{\ln(z_k) : 0 \leq k \leq \dim(U) + M - M_0\}$. We shall show that z_k, p_k, $0 \leq k \leq \dim(U) + M - M_0$ satisfy the conditions of Lemma 5. This will establish our result since the linear independence of $\ln(z_k)$ contradicts our assumption that $\ln(z_0) \in V$.

To show our z_k, p_k satisfy the conditions of Lemma 5 we note that $\operatorname{ord}_{p_k}(z_k) \neq 0$ by our assumptions and that, for $k > \dim(U)$, we have $\operatorname{ord}_{p_k}(1 - b^{-m_k}) = \operatorname{ord}_{p_k}(b^{m_k} - 1) \neq 0$. It remains to show that $\operatorname{ord}_{p_j}(z_k) = 0$ when $j > k$.

We first treat the case $k = 0$. By assumption, $\operatorname{ord}_{p_j}(z_0) = 0$ for $1 \leq j \leq \dim(U)$. For $j > \dim(U)$, p_j is a primitive prime factor of $b^{m_j} - 1$, and $m_j > M_0$. By Fermat's "Little Theorem", we know that if p is a primitive prime factor of $b^m - 1$ then $m \mid p - 1$ and thus $p \geq m + 1$. Thus $p_j \geq m_j + 1 > M_0 + 1 \geq p_0$, and it follows that $\operatorname{ord}_{p_j}(z_0) = 0$ since, by definition, p_0 is the largest prime such that $\operatorname{ord}_{p_0}(z_0) \neq 0$.

We next treat the case $1 \le k \le \dim(U)$. Again, by assumption, $\mathrm{ord}_{p_j}(z_k) = 0$ for $1 \le k < j \le \dim(U)$. Since $\ln(z_k) \in U$, we know that $\ln(z_k)$ is a $\mathbb{Q}$-linear combination of elements of the form $\ln(1 - b^{-m})$, $1 \le m \le M_0$. Thus, there are $n_m \in \mathbb{Z}$, not all zero, and some $n \ne 0$, such that

$$z_k^n = \prod_{m=1}^{M_0} (1 - b^{-m})^{n_m}. \tag{52}$$

Now, when $j > \dim(U)$ we have $\mathrm{ord}_{p_j}(1 - b^{-m}) = 0$ for $1 \le m \le M_0$, since p_j is a primitive prime factor of $b^{m_j} - 1$ and $m_j > M_0$. From this and Equation (52) it follows that

$$\mathrm{ord}_{p_j}(z_k) = \frac{1}{n} \sum_{m=1}^{M_0} n_m \, \mathrm{ord}_{p_j}(1 - b^{-m}) = 0.$$

Finally, when $\dim(U) < k < j$, $\mathrm{ord}_{p_j}(z_k) = 0$ follows from the fact that p_j is a primitive prime factor of $b^{m_j} - 1$. ■

Remark Theorem 6 implies that when searching for a non-Aurifeuillian Machin-type BBP logarithm formula for $\ln(z_0)$, one only need consider generators $\ln(1 - b^{-m})$, $1 \le m \le M_0$, with M_0 as in Equation (51).

Example 4 When $M_b = 0$ it follows that there is no Machin-type BBP logarithm formula for $\ln(b)$ to the base b. In particular, there is no decimal Machin-type BBP logarithm formula for $\ln(10)$. Here we use $z_0 = b$, p_0 the largest prime divisor of b. For $k > 0$ we use $z_k := 1 - b^{-k}$ and choose p_k to be any primitive prime factor of $b^k - 1$, noting that p_k exists since $M_b = 0$. Our result then follows immediately from Theorem 6. Since, when $M_b = 0$, there is no b-ary formula for $\ln(b)$, it seems unlikely in this case that there is a b-ary formula for any $\ln(n)$, $n \in \mathbb{N}$, but we have failed to prove this.

Example 5 When $b = 7 = 2^3 - 1$ we have $M_b = 2$, and the argument of the previous example does not apply. However, again we find that there is no 7-ary Machin-type BBP logarithm formula for $\ln(7)$. Here we have $z_0 = 7$, $p_0 = 7$. Since $M_0 = \max(M_b, p_0 - 1) = 6$, we need to find suitable z_k, p_k for $1 \le k \le 6$. We begin with $z_1 = 8/7$, $p_1 = 2$; $z_2 = 48/49 = 1 - 7^{-2}$, $p_2 = 3$. For $k > M_b = 2$ we can simply use $z_k = 1 - 7^{-k}$, p_k some primitive prime factor of $7^k - 1$. We can easily see that the conditions for Theorem 6 are satisfied, and the result follows.

Remark In Example 5, when $k = 1$ we had to modify the "obvious" choice of basis element, namely $z_k = 1 - 7^{-k}$, in order to make our p_k satisfy the conditions of Theorem 6. In particular, we require $\mathrm{ord}_3(z_1) = 0$. We accomplished this task by using valuation vectors. Here, indexing by the primes $\{7, 2, 3\}$ (in that order), the valuation vector for 7 is $v_0 := [1, 0, 0]$, while the vectors for $1 - 7^{-1} = 6/7$ and $1 - 7^{-2} = 48/49$ are $v_1 := [-1, 1, 1]$ and $v_2 := [-2, 4, 1]$ respectively. Searching for z_1 such that $\mathrm{ord}_3(z_1) = 0$ leads us to find the valuation vector $[-1, 3, 0] = v_2 - v_1$, and thus $z_1 = 7^{-1} \cdot 2^3 = 8/7$.

Example 6 To demonstrate the result of Theorem 4 in the language of Theorem 6, we begin with $z_0 = 23$, $p_0 = 23$, $z_1 = 1 - 1/2$, $p_1 = 2$. Our rule of thumb starting with $k = 2$ will be to use $z_k = 1 - 2^{-m_k}$ for an increasing sequence m_k, and to choose p_k to be a primitive prime factor of $2^{m_k} - 1$. Thus, $z_2 = 1 - 2^{-2} = 3/4$, $p_2 = 3$, $z_3 = 1 - 2^{-3} = 7/8$, $p_2 = 7, \ldots$. We let $m_6 = 7$ rather than 6, since $\ln(1-2^{-6})$ is linearly dependent on earlier $\ln(z_k)$. Continuing in this manner, letting $m_{k+1} = m_k+1$, we come to $z_{10} = 1-2^{-11}$. We have $2^{11}-1 = 23{\cdot}89$, both factors being primitive prime factors. Since $23 = p_0$, we choose $p_{10} = 89$. For $k > 10$ we may continue using our rule of thumb, with no complications, through $m_k = M_0 = 22$, at which point we have established the necessary conditions for Theorem 6.

We again note that it is not always necessary to present p_k explicitly. More specifically, when $m_k > M_b$ we are assured that $b^{m_k} - 1$ has a primitive prime factor p_k, and to guarantee that p_k has not occurred earlier in our sequence we only need check that $\gcd(z_0, b^{m_k} - 1) = 1$.

Remarks (i) We have been unable to exclude the possibility that there might be a binary Machin-type BBP logarithm formula for ln(23) that uses some Aurifeuillian generators, although it seems unlikely. Using Equation (45), and some simple number theory, one can also show for odd primes p that

$$\operatorname{ord}_p\big(\,\big|1-(1+i)2^{-m}\big|\,\big) \neq 0$$

implies $\nu_2(p) \equiv 0 \pmod 4$. This restricts the possibilities for any Aurifeuillian binary Machin-type BBP logarithm formula for ln(23) and suggests that any such representation must have truly “massive” generators, if it exists at all.

(ii) It is interesting to contrast ln(23) with ln(113), since the cases are similar, but ln(113) *does* have an Aurifeuillian binary Machin-type BBP logarithm formula. Here we have $\nu_2(113) = 28$, and $2^{28} - 1 = 3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$.

Since we also have $\nu_2(29) = 28$ then, as illustrated immediately after the proof of Theorem 4, we can conclude that ln(113) has no non-Aurifeuillian binary Machin-type BBP logarithm formula. However, using Equation (44), we find that

$$2^{28} - 1 = (2^{14} - 1)(2^7 + 2^4 + 1)(2^7 - 2^4 + 1),$$

where $2^7 - 2^4 + 1 = 113$. Using Equation (43), it follows that

$$\ln(113) = 2\ln\big|1-(1+i)2^{-4}\big| - 7\ln(1-2^{-1}),$$

which is a linear combination of binary Machin-type logarithmic generators, the first term being an Aurifeuillian generator.

3.4 Applications to Arctangent Formulae

We now apply Theorem 3 (Bang's Theorem) to demonstrate that there are no b-ary Machin-type *arctangent formulae* for π unless $b = 2$.

Theorem 7 *Given $b > 2$ and not a proper power, there is no $\mathbb{Q}$-linear b-ary Machin-type BBP arctangent formula for π.*

Proof It follows immediately from the definition of a $\mathbb{Q}$-linear Machin-type BBP arctangent formula (Definition 1) that any such formula has the form

$$\pi = \frac{1}{n}\sum_{m=1}^{M} n_m \Im \ln(b^m - i), \tag{53}$$

where $n \in \mathbb{N}$, $n_m \in \mathbb{Z}$, and $M \geq 1$, $n_M \neq 0$. This implies that

$$\prod_{m=1}^{M}(b^m - i)^{n_m} \in e^{ni\pi}\mathbb{Q}^{\times} = \mathbb{Q}^{\times}. \tag{54}$$

For any $b > 2$ and not a proper power we have $M_b \leq 2$, so it follows from Bang's Theorem that $b^{4M} - 1$ has a primitive prime factor, say p. Furthermore, p must be odd, since $p = 2$ can only be a *primitive* prime factor of $b^m - 1$ when b is odd and $m = 1$. Since p is a primitive prime factor, it does not divide $b^{2M} - 1$, and so p must divide $b^{2M} + 1 = (b^M + i)(b^M - i)$. We cannot have both $p \mid b^M + i$ and $p \mid b^M - i$, since this would give the contradiction that $p \mid (b^M + i) - (b^M - i) = 2i$.

It follows that $p \equiv 1 \pmod 4$, and that p factors as $p = \mathfrak{p}\overline{\mathfrak{p}}$ over $\mathbb{Z}[i]$, with exactly one of $\mathfrak{p}$, $\overline{\mathfrak{p}}$ dividing $b^M - i$. Referring to Definition 2, we see that we must have $\vartheta_p(b^M - i) \neq 0$. Furthermore, for any $m < M$ neither $\mathfrak{p}$ nor $\overline{\mathfrak{p}}$ can divide $b^m - i$ since this would imply $p \mid b^{4m} - 1$, $4m < 4M$, contradicting the fact that p is a primitive prime factor of $b^{4M} - 1$. So for $m < M$ we have $\vartheta_p(b^m - i) = 0$. Referring to Equation (54), using Equation (41) and $n_M \neq 0$, we get the contradiction that

$$0 \neq n_M \vartheta_p(b^M - i) = \sum_{m=1}^{M} n_m \vartheta_p(b^m - i) = \vartheta_p(\mathbb{Q}^{\times}) = 0.$$

Thus, our assumption that there was a b-ary Machin-type BBP formula for π must be false. ∎

We finish the section with our deferred proof.

Proof of Theorem 2b It again follows from the definition of a $\mathbb{Q}$-linear Machin-type BBP arctangent formula (Definition 1) that any such formula may be written as

$$n \arctan(y/x) + t\pi = \sum_{m=1}^{M} n_m \Im \ln(b^m - i), \tag{55}$$

where $n \in \mathbb{N}$, $n_m, t \in \mathbb{Z}$, and $M \geq 1$, $n_M \neq 0$. This implies that

$$\prod_{m=1}^{M}(b^m - i)^{n_m} \in (x + iy)^n(1 + i)^{4t}\mathbb{Q}^{\times} = (x + iy)^n\mathbb{Q}^{\times}. \tag{56}$$

It follows from Bang's Theorem that $b^{4M} - 1$ has a primitive prime factor, say p'. Furthermore, p' must be odd, since $p' = 2$ can only be a *primitive* prime factor of $b^m - 1$ when b is odd and $m = 1$. Since p' is a primitive prime factor, it does not divide $b^{2M} - 1$, and so p' must divide $b^{2M} + 1 = (b^M + i)(b^M - i)$. Again, we cannot have both $p' \mid b^M + i$ and $p' \mid b^M - i$, since this would give the contradiction that $p' \mid (b^M + i) - (b^M - i) = 2i$. It follows that $p' \equiv 1 (\bmod 4)$, and that p' factors as $p' = \mathfrak{p}'\overline{\mathfrak{p}'}$ over $\mathbb{Z}[i]$, with exactly one of $\mathfrak{p}'$, $\overline{\mathfrak{p}'}$ dividing $b^M - i$.

Referring to Equation (56), using Equation (41) and $n_M \neq 0$, we have

$$0 \neq n_M \vartheta_{p'}(b^M - i) = \sum_{m=1}^{M} n_m \vartheta_{p'}(b^m - i) = \vartheta_{p'}(x + iy)^n.$$

In consequence $p' = p$, since p is the unique prime divisor of $x^2 + y^2$ congruent to 1 modulo 4. It follows that $4M = \nu_b(p) = \nu_b(q)$ and hence, much as above, that

$$0 \neq n_M \vartheta_q(b^M - i) = \sum_{m=1}^{M} n_m \vartheta_q(b^m - i) = \vartheta_q(x + iy)^n = 0,$$

where the final equality is by hypothesis. Thus, our assumption that there was a non-Aurifeuillian b-ary Machin-type BBP formula for $\arctan(x/y)$ must be false. ■

A BBP Formulae for Machin-Type BBP Generators

For b not a proper power, $b > 2$ our arctangent generators are

$$\arctan(-b^{-m}) = \Im \ln(1 - ib^{-m}) = b^{-3m} P(1, b^{4m}, 4, [-b^{2m}, 0, 1, 0]).$$

When $b = 2$, we also use the "Aurifeuillian" generators

$$\begin{aligned}\arctan(1/(1 - 2^m)) &= \Im \ln(1 - (1 + i)2^{-m}) \\ &= 2^{-7m+3} P(1, 2^{8m-4}, 8, [-2^{6m-3}, -2^{5m-2}, -2^{4m-2}, 0, 2^{2m-1}, 2^m, 1, 0]).\end{aligned}$$

For b not a proper power, $b > 2$ our logarithmic generators are

$$\ln(1 - b^{-m}) = -b^{-m} \sum_{k \geq 0} \frac{1}{k+1} b^{-mk}.$$

In terms of Bailey's $P(s, b, n, A)$, these generators are

$$\ln(1 - b^{-m}) = -b^{-m} P(1, b^m, 1, [1]).$$

When $b = 2$, we also use the "Aurifeuillian" generators

$$\begin{aligned}&\ln \left|1 - (1 + i)2^{-m}\right| \\ &\quad = 2^{-8m+4} P(1, 2^{8m-4}, 8, [-2^{7m-4}, 0, 2^{5m-3}, 2^{4m-2}, 2^{3m-2}, 0, -2^{m-1}, -1]).\end{aligned}$$

Note that the BBP formulae for both the arctangent and logarithmic Aurifeuillian generators may be derived by extracting imaginary and real parts (for arctangent and logarithmic generators, respectively) from the formula

$$\begin{aligned}\ln(1-(1+i)2^{-m}) &= -\sum_{r=1}^{8} 2^{-mr}(1+i)^r \sum_{k\geq 0} \frac{(1+i)^{8k}}{8k+r} 2^{-8mk} \\ &= -\sum_{r=1}^{8} 2^{-mr}(1+i)^r \sum_{k\geq 0} \frac{1}{8k+r} 2^{(4-8m)k}.\end{aligned}$$

B Conversion to Polylogarithmic Formulae

In this Appendix we shall analyze vector spaces of constants with *polylogarithmic* BBP formulae, *i.e.*, constants κ which have the form

$$\kappa = \sum_{k\geq 0}\sum_{j=1}^{n} \frac{a_j}{(nk+j)^s} b^{-mk} = P(s, b^m, n, [a_1, \ldots, a_n]), \tag{57}$$

with $a_j \in \mathbb{Q}$, $s, b, m, n \in \mathbb{N}$, $b > 1$. Our main purpose is to demonstrate that any constant with a Machin-type BBP formula also has a polylogarithmic BBP formula. (Although our interest will be focused on the case where b is not a proper power we allow any $b \in \mathbb{N}$, $b > 1$.)

Definition 5 Recall that $\operatorname{span}\{\alpha_k\}$ denotes the vector space over $\mathbb{Q}$ spanned by the set $\{\alpha_k\}$. Given $s, b, m, n \in \mathbb{N}$, $b > 1$, let

$$V_{s,b,m,n} := \operatorname{span}\left\{ \sum_{k\geq 0} \frac{1}{(nk+j)^s} b^{-mk} : 1 \leq j \leq n \right\},$$

$$V_{s,b,m} := \operatorname{span}\left\{ \bigcup_{n\geq 1} V_{s,b,m,n} \right\}, \qquad V_{s,b} := \operatorname{span}\left\{ \bigcup_{m\geq 1} V_{s,b,m} \right\}.$$

Referring to Appendix A, we see that our non-Aurifeuillian arctangent generators, $\arctan(-b^{-m})$, lie in $V_{1,b,4m,4}$. The Aurifeuillian arctangent generators, $\arctan(1/(1-2^m))$, lie in $V_{1,2,8m-4,8}$. In the case of our logarithmic generators we have $\ln(1-b^{-m}) \in V_{1,b,m,1}$ (non-Aurifeuillian generators), while

$$\ln\left|1-(1+i)2^{-m}\right| \in V_{1,2,8m-4,8}$$

(Aurifeuillian generators).

Lemma 8 *Given $d \in \mathbb{N}$ we have*

$$V_{s,b,m,n} \subseteq V_{s,b,m,dn}, \tag{58}$$

and

$$V_{s,b,m} \subseteq V_{s,b,dm,dn}. \tag{59}$$

Proof To establish (58) we note that $\kappa \in V_{s,b,m,n}$ is equivalent to

$$\kappa = \sum_{j=1}^{n} \sum_{k\geq 0} \frac{a_j}{(nk+j)^s} b^{-mk} \tag{60}$$

$$= \sum_{j=1}^{n} \sum_{k\geq 0} \frac{d^s a_j}{(dnk+dj)^s} b^{-mk}$$

$$= \sum_{j=1}^{dn} \sum_{k\geq 0} \frac{a'_j}{(dnk+j)^s} b^{-mk} \in V_{s,b,m,dn};$$

where we let

$$a'_j := \begin{cases} d^s a_{j/d} & \text{when } d \mid j, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, to establish (59) we proceed from Equation (60) to find

$$\kappa = \sum_{j=1}^{n} \sum_{k\geq 0} \sum_{r=0}^{d-1} \frac{a_j b^{-mr}}{(dnk+nr+j)^s} b^{-dmk}$$

$$= \sum_{j'=1}^{dn} \sum_{k\geq 0} \frac{a'_{j'}}{(dnk+j')^s} b^{-dmk} \in V_{s,b,dm,dn};$$

where we let $j' := nr + j$, so that $r = \lfloor j'/n \rfloor$, $j \equiv j' \pmod{n}$, $1 \leq j \leq n$, and where $a'_{j'} := a_j b^{-mr}$. ∎

Theorem 9 *Given $\kappa \in V_{s,b,m}$ then $\kappa \in V_{s,b,m,n}$, where n depends on κ.*

Proof Let $\kappa = \kappa_1 + \kappa_2$ where $\kappa_1 \in V_{s,b,m,n_1}$, $\kappa_2 \in V_{s,b,m,n_2}$. From (58), it follows that both κ_1 and κ_2 are elements of $V_{s,b,m,\mathrm{lcm}(n_1,n_2)}$, and thus $\kappa \in V_{s,b,m,\mathrm{lcm}(n_1,n_2)}$.

By definition, $\kappa \in V_{s,b,m}$ means that

$$\kappa = \sum_q \alpha_q \kappa_q, \tag{61}$$

where $\alpha_q \in \mathbb{Q}$, $\kappa_q \in V_{s,b,m,n_q}$, and where the sum is finite. By using induction on the number of terms on the right side of (61), applying the result of the previous paragraph when summing two terms, the conclusion follows. ∎

Theorem 10 *Given $\kappa \in V_{s,b}$ then $\kappa \in V_{s,b,m,n}$, where m, n depend on κ.*

Proof Let $\kappa = \kappa_1 + \kappa_2$ where $\kappa_1 \in V_{s,b,m_1}$, $\kappa_2 \in V_{s,b,m_2}$. By Theorem 9 we may assume that $\kappa_1 \in V_{s,b,m_1,n_1}$, $\kappa_2 \in V_{s,b,m_2,n_2}$. Applying (59) and then (58), it follows that both κ_1 and κ_2 are elements of $V_{s,b,\mathrm{lcm}(m_1,m_2),\mathrm{lcm}(N_1,N_2)}$, where $N_1 := n_1m_2/\gcd(m_1,m_2)$, $N_2 := n_2m_1/\gcd(m_1,m_2)$.

By definition, $\kappa \in V_{s,b}$ means that

$$\kappa = \sum_q \alpha_q \kappa_q, \tag{62}$$

where $\alpha_q \in \mathbb{Q}$, $\kappa_q \in V_{s,b,m_q}$, and where the sum is finite. By using induction on the number of terms on the right side of (62), applying the result of the previous paragraph when summing two terms, the conclusion follows. ∎

The above proofs implicitly give a constructive method for finding a polylogarithmic BBP formula for any element of $V_{s,b}$. In particular we may find a polylogarithmic BBP formula for any constant with a b-ary Machin-type BBP formulae, since such constants lie within $V_{1,b}$. For example, in Section 2.5 we found that $\arctan(1/6) = \arctan(1/5) - \arctan(1/31)$.

Referring to Appendix A, and using Bailey's $P(s,b,n,A)$, we have

$$\arctan(1/5) = 2^{-11}P(1,2^{12},8,[2^9,-2^8,2^6,0,-2^3,2^2,-1,0]) \in V_{1,2,12,8},$$

$$\arctan(1/31) = 2^{-32}P(1,2^{36},8,[2^{27},2^{23},2^{18},0,-2^9,-2^5,-1,0]) \in V_{1,2,36,8}.$$

Note that Appendix A covers $\arctan(1/5)$ as it equals $\arctan(1/3) - \arctan(1/8)$, by the note at the end of Section 2.4. Applying (59) from Lemma 8, we can re-express $\arctan(1/5)$ as an element of $V_{1,2,36,24}$, giving

$$\begin{aligned}\arctan(1/5) = 2^{-11}P(1,2^{36},24,[\ & 2^9,-2^8,2^6,0,-2^3,2^2,-1,0,\\ & 2^{-3},-2^{-4},2^{-6},0,-2^{-9},2^{-10},-2^{-12},0,\\ & 2^{-15},-2^{-16},2^{-18},0,-2^{-21},2^{-22},-2^{-24},0\ ]).\end{aligned}$$

We then apply (58) in order to re-express $\arctan(1/31)$ as an element of $V_{1,2,36,24}$, giving

$$\begin{aligned}\arctan(1/31) = 2^{-32}&P(1,2^{36},24,\\ &[\ 0,0,3\cdot 2^{27},\ 0,0,3\cdot 2^{23},\ 0,0,3\cdot 2^{18},\ 0,0,0,\\ &\ 0,0,-3\cdot 2^9,\ 0,0,-3\cdot 2^5,\ 0,0,-3,\ 0,0,0\ ]).\end{aligned}$$

Finally, taking the difference of these two results and factoring out the denominator from the vector of coefficients, we get

$$\begin{aligned}\arctan(1/6) &= \arctan(1/5) - \arctan(1/31)\\ &= 2^{-35}P(1,2^{36},24,[\ 2^{33},-2^{32},-2^{31},0,-2^{27},-2^{27},-2^{24},0,\\ &\qquad -2^{22},-2^{20},2^{18},0,-2^{15},2^{14},2^{13},0,\\ &\qquad 2^9,2^9,2^6,0,2^4,2^2,-1,0\ ]).\end{aligned}$$

C Density Results

We discuss the density of arctangents with Machin-type BBP arctangent formulae. We begin by noting that if $\theta = \arctan(\rho)$ has a Machin-type BBP formula then any element of $\theta\mathbb{Q}$ has a $\mathbb{Q}$-linear arctangent formula. For a fixed base b, we have Machin-type BBP arctangent formulae for $\Im \ln(1 - ib^{-m})$, so any one of these will generate a dense set of $\theta \in \mathbb{R}$ with base b $\mathbb{Q}$-linear Machin-type BBP arctangent formula. If, in order to be considered an "arctangent", we prefer the convention that θ satisfies $-\pi/2 < \theta < \pi/2$, it remains clear that the set of $\theta \in (-\pi/2, \pi/2)$ with a $\mathbb{Q}$-linear Machin-type BBP arctangent formula is dense.

If we prefer to restrict ourselves to θ with $\mathbb{Z}$-linear arctangent formulae, then the set $n\theta$, $n \in \mathbb{Z}$, is not dense in $\mathbb{R}$. On the other hand, if we write $\theta = \Im \ln(x + iy)$ and define x_n, y_n to satisfy $x_n + iy_n := (x + iy)^n$, $n \in \mathbb{Z}$, then $n\theta \equiv \Im \ln(x_n + iy_n) \equiv \arctan(y_n/x_n) \pmod{\pi}$. In other words $\tan(n\theta) = y_n/x_n$ for all $n \in \mathbb{Z}$. By [NZM91, Theorem 6.16], θ cannot be a rational multiple of π unless $\tan(\theta) \in \{0, \pm 1, \infty\}$. In particular, for fixed $b \geq 2$, $\theta = \Im \ln(1 - ib^{-m}) = \arctan(-b^{-m})$ is not a rational multiple of π for any $m \in \mathbb{N}$, since $-b^{-m} \notin \{0, \pm 1, \infty\}$.

It follows by Weyl's theorem [HW79, Theorem 445] that for such θ the sequence $n\theta$ is uniformly distributed modulo π. Thus, if there is a b-ary $\mathbb{Z}$-linear Machin-type BBP formula for π then the set $n_1\theta + n_2\pi$, n_1, $n_2 \in \mathbb{Z}$, is dense in the interval $(-\pi/2, \pi/2)$, and clearly $n_1\theta + n_2\pi$ has a b-ary $\mathbb{Z}$-linear Machin-type BBP arctangent formula. If there is no b-ary $\mathbb{Z}$-linear Machin-type BBP formula for π we may still conclude $\{\tan(n\theta) : n \in \mathbb{Z}\}$ is dense in $\mathbb{R}$.

Finally, suppose b and $x + iy$ satisfy Theorem 2. That is, suppose there is a prime $p \nmid b$, $p \equiv 1 \pmod 4$, $4 \nmid \nu_b(p)$, and $\vartheta_p(x + iy) \neq 0$. By Theorem 2, there is no $\mathbb{Q}$-linear Machin-type BBP formula for $\arctan(y/x)$. Furthermore, since $\vartheta_p((x+iy)^n) = n\vartheta_p(x+iy)$, there is no $\mathbb{Q}$-linear Machin-type BBP formula for $\arctan(y_n/x_n)$ for any $n \neq 0$, $n \in \mathbb{Z}$. Thus, provided $x/y \notin \{0, \pm 1, \infty\}$, the set $\{\arctan(y_n/x_n)\}$ is dense in $\mathbb{R}$, and no member has a b-ary $\mathbb{Q}$-linear arctangent formula.

D Comments and Research Problems

We've tried to arrange these comments in increasing order of difficulty.

(1) Note that $3 + i = 2 + (1 + i) = 4 - (1 - i)$, gives two distinct binary Machin-type BBP formulae for $\arctan(1/3)$. Should this count as a trivial zero relation, or is it "interesting"?

(2) How many $\mathbb{Q}$-linearly-independent binary Machin-type BBP arctangent zero relations exist? Are there good upper bounds?

(3) The first BBP formula found for π in [BBP97] was

$$\pi = \sum_{k \geq 0} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right) 2^{-4k}. \tag{63}$$

This does not appear to be a $\mathbb{Q}$-linear combination of Machin-type BBP generators. (Equation (64), below, is an aid in seeing this.) Is there a simple way to derive (63) from a Machin-type formula?

(4) If infinitely many primes $p \equiv 1 \pmod 4$ with $4 \nmid \nu_b(p)$ exist, then Theorem 2

gives infinitely many examples base b with no b-ary Machin-type BBP arctangent formula. Does their existence follow from Chebotarëv's density theorem, or another well-known result?

(5) Our main tool has been group homomorphisms like $z \mapsto \operatorname{ord}_p(z)$ and $z \mapsto \vartheta_p(z)$. When $\operatorname{ord}_p(z) = 0$ can one similarly use the homomorphism $z \mapsto (z/p)$ arising from the Jacobi symbol (z/p)? As $(z/p) \in \{-1, 1\}$ when $\operatorname{ord}_p(z) = 0$, each such homomorphism only gives a "bit" of information. It should be possible to get more information by choosing many such p.

(6) Our use of ord_p and ϑ_p works best when we can factor numbers rapidly. Since factorization is difficult in general, can we combine our approach with the use of an integer relation algorithm such as PSLQ [FBA99]? The idea would be to find the "easy" factors, and use the resulting information to help guide PSLQ.

(7) Zsigmondy's theorem has been generalized to number fields [Sch74, BHV01], in what Carl Pomerance calls a grand generalization of Bang's theorem, with effective bounds on the exceptional cases. These should give an effective version of Zsigmondy's theorem for $\mathbb{Q}[i]$, providing an exclusion criterion for Machin-type BBP arctangent formulae analogous to Theorem 6.

(8) For the binary case, can we find exclusion criteria that deal with Aurifeuillian generators in logarithm formulae?

(9) We could generalize the definition of a BBP-formula to allow sums of the form $\sum_{k\geq 0} b^{-k} p(k)/q(k)$, $b \in \mathbb{Z}[i]$, $p, q \in \mathbb{Z}[i, k]$. Doing so should avoid the need to treat arctangents and logarithms as separate cases. Could we get cleaner or more general results this way?

(10) Let ζ_n denote a primitive nth root of unity, and recall that $L(s, b, n, A)$ is defined by Equation (3). It is clear that for $1 \leq j \leq n$ we have

$$L(1, b, n, j) = -\frac{1}{n} b^{j/n} \sum_{r=0}^{n-1} \zeta_n^{-rj} \ln(1 - \zeta_n^r b^{-1/n}). \tag{64}$$

(In his answer to [Knu98, Exercise 4.3.1.39], Knuth gives a different version of an explicit formula for $L(1, b, n, j)$.) Can our techniques be applied to determine whether κ is a linear combination of $L(1, b^m, n, j)$, with b, and perhaps n, fixed? This would probably require a good understanding of $\mathbb{Q}[\zeta_n, b^{1/n}]$, among other things.

(11) How can we justify the idea that our limited set of "Machin-type" BBP generators gives all (or most) "interesting" arctans and logs?

Acknowledgements Carl Pomerance was the first to observe the importance of Bang's theorem as a tool for excluding the possibility of non-Aurifeuillian logarithm formulae. Pomerance also provided references for some of the papers, cited above, that generalize Zsigmondy's Theorem. Imin Chen and Nils Bruin gave advice on various aspects of ord_p and algebraic number theory. The material in Appendix B is adapted from notes provided by David Bailey.

References

[Bai00] David H. Bailey, *A compendium of BBP-type formulas for mathematical constants.* Manuscript available at http://www.nersc.gov/~dhbailey/dhbpapers, March 2004.

[BB98] Jonathan M. Borwein and Peter B. Borwein, *Pi and the AGM, a study in analytic number theory and computational complexity.* John Wiley & Sons, New York, 1998,

[BB03] Jonathan M. Borwein and David H. Bailey, *Mathematics by Experiment: Plausible Reasoning in the 21st Century.* A K Peters, Nattick, MA, 2003,

[BBP97] David Bailey, Peter Borwein, and Simon Plouffe, *On the rapid computation of various polylogarithmic constants.* Math. Comp. **66**(1997), 903–913.

[BC01] David H. Bailey and Richard E. Crandall, *On the random character of fundamental constant expansions.* Experiment. Math. **10**(2001), 175–190,

[BHV01] Yu. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte.* J. Reine Angew. Math. **539**(2001), 75–122.

[BLS88] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers.* second ed., American Mathematical Society, Providence, RI, 1988, (Third ed. available at http://www.ams.org/online_bks/conm22).

[Bre93] Richard P. Brent, *On computing factors of cyclotomic polynomials.* Math. Comp. **61**(1993), 131–149.

[Bro98] D. J. Broadhurst, *Polylogarithmic ladders, hypergeometric series and the ten millionth digits of* $\zeta(3)$ *and* $\zeta(5)$. Available at http://xxx.lanl.gov/abs/math/9803067, March 1998.

[Cha] Marc Chamberland, *Binary BBP-forumulas for logarithms, cyclotomic polynomials and Aurifeuillian identities.* Draft of circa December, 2001, to appear.

[Coh93] Henri Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

[FBA99] Helaman R. P. Ferguson, David H. Bailey, and Steve Arno, *Analysis of PSLQ, an integer relation finding algorithm.* Math. Comp. **68**(1999), 351–369.

[HW79] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers.* Fifth ed., Oxford University Press, Oxford, 1979.

[Knu98] Donald E. Knuth, *The art of computer programming.* vol. 2: Seminumerical algorithms, third ed., Addison-Wesley, Reading, Mass., 1998,

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions.* Second ed., Graduate Texts in Mathematics, 58, Springer-Verlag, New York, 1984.

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers.* Fifth ed., John Wiley & Sons, New York, 1991.

[Per00] Colin Percival, *The quadrillionth bit of pi is '0'.* See http://www.cecm.sfu.ca/projects/pihex/announce1q.html, September 2000.

[Rib91] Paulo Ribenboim, *The little book of big primes.* Springer-Verlag, New York, 1991.

[Rib94] ———, *Catalan's conjecture: Are* 8 *and* 9 *the only consecutive powers?* Academic Press, Boston, MA, 1994.

[Rie94] Hans Riesel, *Prime numbers and computer methods for factorization.* Second ed., Birkhäuser, Boston, MA, 1994.

[Roi97] Moshe Roitman, *On Zsigmondy primes.* Proc. Amer. Math. Soc. **125**(1997), 1913–1919.

[Sch74] A. Schinzel, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields.* J. Reine Angew. Math. **268/269** (1974), 27–33,

[Wil98] Hugh C. Williams, *Édouard Lucas and primality testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, 22, John Wiley & Sons., New York, 1998.

Computer Science
Dalhousie University
Halifax, NS
B3H 1W5
e-mail: jborwein@cs.dal.ca

Mathematics
University of Western Ontario
London, ON
N6A 5B7
e-mail: dborwein@uwo.ca

Mathematics
Simon Fraser University
Burnaby, BC
V5A 1S6
e-mail: wfgalway@cecm.sfu.ca