AURIFEUILLIAN FACTORIZATION

Andrew Granville and Peter Pleasants

Abstract. The Cunningham project seeks to factor numbers of the form $b^n \pm 1$ with $b = 2, 3, \ldots$ small. One of the most useful techniques is *Aurifeuillian Factorization* whereby such a number is partially factored by replacing b^n by a polynomial in such a way that polynomial factorization is possible. For example, by substituting $y = 2^k$ into the polynomial factorization $(2y^2)^2 + 1 = (2y^2 - 2y + 1)(2y^2 + 2y + 1)$ we can partially factor $2^{4k+2} + 1$. Schinzel [Sc] gave a list of such identities that have proved useful in the Cunningham project; we believe that Schinzel identified *all* numbers that can be factored by such identities and we prove this if one accepts our definition of what "such an identity" is. We then develop our theme to similarly factor $f(b^n)$ for any given polynomial f, using deep results of Faltings from algebraic geometry and Fried from the classification of finite simple groups.

1. Introduction

In 1925 Cunningham and Woodall published a book of factorizations of numbers of the form $2^n \pm 1$, $3^n \pm 1$, etc. Evidently such information provides useful examples for several topics in elementary number theory. As the theory of factoring has developed, such numbers have proved to be fertile ground for the initial development of factoring techniques, which may subsequently be generalizable to factoring arbitrary integers. The book [BL] contains a good historical account up to the time it was written; and for up-to-date data see the website `http://www.cerias.purdue.edu/homes/ssw/cun/index.html`. Indeed even the number field sieve, the latest general factoring technique, was first suggested by Pollard to attack numbers in the "Cunningham Project". The end of these developments is not yet in sight:

The invention of new [factorization] methods may push off the limits of the unknown a little further, just as the invention of a new astronomical instrument may push off a little the boundaries of the physical universe; but the unknown regions are infinite, and if we could come back a thousand years from now we should no doubt find workers in the theory of numbers announcing in the journals new schemes and new processes for the resolution of a given number into its factors. D.N. Lehmer, *Scientific Monthly*, Sept 1918.

Le premier auteur est partiellement soutenu par une bourse du Conseil de recherches en sciences naturelles et en génie du Canada; and was supported, in part, by the National Science Foundation when this project began.

The number $b^n - 1$ can be partially factored by substituting $x = b$ into the "algebraic factorization" $x^n - 1 = \prod_{d|n} \varphi_d(x)$, where $\varphi_d(x)$ is the dth *cyclotomic polynomial*, the monic, irreducible polynomial whose roots are the primitive dth roots of unity. The factors $\varphi_d(b)$ may factor further, of course, and they can be considerably smaller than $b^n - 1$ so may come within the range of other factorization techniques. Similarly $b^n + 1$ can be partially factored as $\prod_d \varphi_d(b)$ where the product is over integers d dividing $2n$ but not n. This is a proper factorization when n is not a power of 2. We call these "*cyclotomic factorizations*".

One can generalize this technique by seeking polynomials $g(x) \in \mathbb{Q}[x]$ such that $g(x) \pm 1$ factors over $\mathbb{Q}$, then substituting values for x to get partial factorizations of numbers in the Cunningham project. This is a cyclotomic factorization when $g(x) = \pm x^n$, but a non-cyclotomic example is given by $g(y) = (2y^2)^2$:

$$(2y^2)^2 + 1 = (2y^2 + 1)^2 - (2y)^2 = (2y^2 - 2y + 1)(2y^2 + 2y + 1),$$

allowing us to factor numbers $2^{2(2k+1)} + 1$. This is an *Aurifeuillian factorization*, which we define to be a factorization given by taking $g(y) = \pm(ay^2)^n$, with $a \neq \pm 1$, that refines the cyclotomic factorization given by $g(x) = \pm x^n$. Here are some other examples,

$$\begin{aligned}
\frac{(3y^2)^3 + 1}{3y^2 + 1} &= (3y^2 + 1)^2 - (3y)^2 \quad (\text{with } g(y) = (3y^2)^3),\\
\frac{(5y^2)^5 - 1}{5y^2 - 1} &= (25y^4 + 15y^2 + 1)^2 - (5y)^2(5y^2 + 1)^2 \quad (\text{with } g(y) = (5y^2)^5),\\
\frac{(7y^2)^7 + 1}{7y^2 + 1} &= (7y^2 + 1)^6 - (7y)^2(49y^4 + 7y^2 + 1)^2 \quad (\text{with } g(y) = (7y^2)^7),
\end{aligned}$$

where we have written the factorizations as differences of squares, Notice that in each case we can take $y = p^k$ to get a partial factorization of $p^{p(2k+1)} \pm 1$. Aurifeuillian factorizations split certain cyclotomic factors into two factors of about the same size, which is a most useful step in finding a complete factorization.

In an 1878 paper [Lu], Lucas explained how Aurifeuille proved that there are identities like those above for every prime exponent n, and in 1962 Schinzel [Sc] found similar identities for every composite exponent n not divisible by 8. He showed that if $n = N, 2N$ or $4N$, with N odd, and d is any squarefree divisor of N (where d is allowed to be negative when $n = 4N$) then there exist polynomials $U_{n,d}(x), V_{n,d}(x) \in \mathbb{Z}[x]$ such that

$$\begin{aligned}
\varphi_N(x) &= U_{N,d}(x)^2 - \varepsilon_d dx V_{N,d}(x)^2,\\
\varphi_{2N}(x) &= U_{2N,d}(x)^2 + \varepsilon_d dx V_{2N,d}(x)^2,\\
\varphi_{4N}(x) &= U_{4N,d}(x)^2 - 2dx V_{4N,d}(x)^2,
\end{aligned} \tag{1}$$

where

$$\varepsilon_d = \left(\frac{-1}{d}\right) = (-1)^{(d-1)/2}.$$

On substituting in ay^2 for x, where $a = \varepsilon_d d, -\varepsilon_d d$ or $2d$, respectively, the above expressions become differences of two squares, and we obtain a polynomial factorization of $\varphi_n(ay^2)$. (Later, Stevenhagen [St] and Brent [Br] gave new proofs of these identities, as well as algorithms for computing the polynomials U and V.) We shall give a motivated description of these factorizations at the end of Section 4.

Since they have proved so useful to the Cunningham project, it has long been desired to find more such "Aurifeuillian factorizations", or some analogous construction. However, what is desired does not seem to have been precisely defined in the literature. Here we put forward a definition but prove that it does not encompass any more factorizations than the cyclotomic and Aurifeuillian ones already known.

We can restrict our attention to classifying factorizations of $b^n - 1$ given by factoring $g(x) - 1$, since the factorizations of $b^n + 1$ given by factoring $g(x) + 1$ are accounted for within the factorizations of $b^{2n} - 1$ given by factoring $g(x)^2 - 1$.

Definition. *A* Cunningham factoring polynomial *is a polynomial $g(x) \in \mathbb{Q}[x]$ such that $g(x)-1$ is reducible in $\mathbb{Q}[x]$, and there exist infinitely many pairs of integers m, n for which $g(m) = b^n$, for some integer $b \neq -1, 0$ or 1.*

One note of caution: If in a Cunningham factoring polynomial $g(x)$ we replace x by a polynomial $h(y) \in \mathbb{Q}[y]$ such that none of the irreducible factors of $g(x) - 1$ factors further in $\mathbb{Q}[y]$ yet $g(h(y))$ still represents infinitely many powers of b, then $g(h(y))$ is also a Cunningham factoring polynomial. We say $g(h(y))$ *derives* from $g(x)$. Evidently such derivations provide no additional factorizations and so are of no interest for us.

Our main result (proved in Section 6) is to identify all Cunningham factoring polynomials and show that they give precisely the cyclotomic factorizations and Schinzel's Aurifeuillian factorizations and no others. Before stating it we define a^*, for a non-zero rational a, as the squarefree integer with the sign of a whose absolute value is the product of the primes that occur to an odd power in the prime-power decomposition of a. So a^* is a canonical representative of a in the multiplicative group of $\mathbb{Q}^\times$ modulo squares.

Theorem. *Every Cunningham factoring polynomial $g(y) \in \mathbb{Q}[y]$ has the form $g(y) = (a(y + c)^q)^n$ with $a, c \in \mathbb{Q}$ and $a^{1/p}$ irrational for every prime divisor p of q.*

When q is even and $a^* \mid n$ and either

(i) *n is odd and $a^* \equiv 1 \pmod 4$, or*
(ii) *n is even and $a^* \neq -1$ is odd, or*
(iii) *$4 \mid n$ and a^* is even*

then $g(y)$ derives from $(a^*x^2)^n$ (by substituting $x = \sqrt{a/a^*}(y + c)^{q/2}$) and leads to one of Schinzel's Aurifeuillian factorizations of some of the cyclotomic factors of

$$(a^*x^2)^n - 1 = \prod_{d \mid n} \varphi_d(a^*x^2). \tag{2}$$

Those terms of the product that factor in this way have two irreducible factors of equal degree.

When q is even and $a^* = -1$ then $g(y)$ derives from $(-x^2)^n$ (by substituting $x = \sqrt{|a|}(y+c)^{q/2}$) and gives only cyclotomic factorizations.

In all other cases $n > 1$ and $g(y)$ derives from x^n (by substituting $x = a(y+c)^q$) and also gives only cyclotomic factorizations.

A drawback of discarding the plus sign in the definition of Cunningham factoring polynomials is that the Theorem does not tell us, when we want to factor $b^n + 1$, whether the Aurifeuillian factorization is relevant or is just a factorization of some of the cyclotomic factors of $b^n - 1$. More specifically, we might like to know precisely which of the cyclotomic factors on the right of (2) factorizes further in $\mathbb{Q}[x]$. To remedy this we add a

Supplement. *If a is an integer with $|a| > 1$ then $\varphi_d(ax^2)$ is reducible in $\mathbb{Q}[x]$ precisely in the following cases:*

(i) $a^* \equiv 1 \pmod 4$ *and d is an odd multiple of a^*, or*
(ii) $a^* \equiv -1 \pmod 4$ *and d is 2 times an odd multiple of a^*, or*
(iii) *a^* is even and d is 4 times an odd multiple of a^*.*

This reiterates the information given by the identities (1) and shows that there are no similar identities for other values of N and d.

Among the data in [BL] there are examples which suggest that there may be some other way, not captured by our definition, to extend Aurifeuillian factorizations. For instance, Wagstaff points out the following interesting example from the Cunningham project:

$$\frac{6^{106}+1}{6^2+1} = 26713 \times 175436926004647658810244613736479118917 \times 175787157418305877173455355755546870641,$$

where the last two factors differ by about one-fifth of a percent. Is this just a coincidence?

2. Generalizations

The ideas used above can be developed for a far more general problem: For a given irreducible polynomial $f(x) \in \mathbb{Q}[x]$ we wish to factor $f(m)$ for all integers m, or perhaps for m in some special subset (such as the powers of some fixed integer). First we will want to determine $g(y) \in \mathbb{Q}[y]$ for which $f(g(y))$ is reducible.

Lemma 1. *Let $f(x) \in \mathbb{Q}[x]$ be monic and irreducible with splitting field K, and α any root of f. Then, for any $g(y) \in \mathbb{Q}[y]$, if the irreducible factorization of $g(y) - \alpha$ in $K[y]$ is*

$$g(y) - \alpha = a_1^{r_1}(y)a_2^{r_2}(y)\cdots a_k^{r_k}(y) \tag{3}$$

then the irreducible factorization of $f(g(y))$ in $\mathbb{Q}[y]$ is

$$f(g(y)) = A_1^{r_1}(y)A_2^{r_2}(y)\cdots A_k^{r_k}(y), \tag{4}$$

with $A_j(y) = \mathrm{Norm}_{K/\mathbb{Q}}\, a_j(y)$ for $j = 1, \dots, k$.

Proof. Since the factorization (4) results from taking norms of both sides of (3), it is enough to show that each $A_i(y)$ is irreducible in $\mathbb{Q}[y]$. Let $A(y)$ be any factor of $f(g(y))$

in $\mathbb{Q}[y]$ and put $a(y) = \gcd(A(y), g(y) - \alpha) \in K[y]$. Since $f(g(y))$ is the product of the conjugates over $\mathbb{Q}$ of $g(y) - \alpha$ and these conjugates are coprime, $A(y) = \operatorname{Norm} a(y)$. So every factor of $f(g(y))$ in $\mathbb{Q}[y]$ is the norm of some factor of $(g(y) - \alpha)$ over K, and hence the $A_i(y)$'s are irreducible over $\mathbb{Q}$.

Corollary 1. *With f, K, α and g as in Lemma 1, $f(g(y))$ is reducible in $\mathbb{Q}[y]$ if and only if $g(y) - \alpha$ is reducible in $K[y]$.*

Note that $f(y) \mid f(y + f(y))$, so that there is no difficulty in finding $g(y)$ with $\deg g \geq \deg f$ for which $f(g(y))$ is reducible. (More generally, if $k(y), l(y) \in \mathbb{Q}[y]$ and $h(y)$ is any factor of $f(k(y))$ then $h(y) \mid f(g(y))$ for $g(y) = k(y) + l(y)h(y)$.) This leads us to the

Question. *Suppose that $f(x) \in \mathbb{Q}[x]$ is irreducible. Can one find infinitely many $g(y) \in \mathbb{Q}[y]$ with $\deg g < \deg f$ for which $f(g(y))$ is reducible in $\mathbb{Q}[y]$, where the $g(y)$ are distinct under transformations replacing y by a polynomial in y?*

It seems difficult to apply the criterion of Corollary 1 in general, though it may work in special cases. On the other hand, researchers have studied the problem of determining, for a given $g(y)$, the set of rational integers a for which $g(y) - a$ is reducible: Trivially $y - m$ divides $g(y) - g(m)$, so $g(y) - a$ is reducible if $a = g(m)$ for some integer m. Also if $g(y)$ is a composition, such as $p(q(y))$, then $q(y) - m$ divides $g(y) - p(m)$. In 1986, Fried [Fr] showed that if g is not a composition of polynomials and is not a member of a certain family of degree five polynomials, then there are at most finitely many a, not equal to $g(m)$ for some m, for which $g(y) - a$ is reducible. The deep proof involves Faltings' Theorem as well as an application of the classification of finite simple groups. Similar results can be proved with a restricted to any given field. (The exceptional monic quintics are parametrized by $x^5 + tb^2x^3 - (t+5)b^3x^2 + (t^2 - 2t - 15)b^4x/4 + c$, where $t = (u^2 - 5v^2 - 10)/2$ and $b, c, u, v \in \mathbb{Q}$. Fascinating but beside the point.)

Returning now to Aurifeuillian factorization, we proceed a little differently (as in the examples at the beginning of the article), investigating whether we can find infinitely many non-constant $g(x) \in \mathbb{Z}[x]$ without repeated roots such that $g(m)$ is a square for infinitely many integers m and there exist $u(x), v(x), w(x) \in \mathbb{Z}[x]$ satisfying

$$w(x)f(x) = u(x)^2 - g(x)v(x)^2. \tag{5}$$

Note that if $g(m) = l^2$ then $w(m)f(m) = (u(m) - lv(m))(u(m) + lv(m))$ and it is likely that $\gcd(f(m), u(m) \pm lv(m))$ will be non-trivial factors of $f(m)$. Note also that there is no loss of generality in our assumption that the polynomials in (5) are in $\mathbb{Z}[x]$ rather than $\mathbb{Q}[x]$, since we may multiply through by an appropriate constant (though leaving f fixed).

Equation (5) is equivalent to the assertion that $g(x)$ corresponds to a square in the quotient field $\mathbb{Q}[x]/(f(x))$. If there are infinitely many integers m for which $g(m)$ is a square then, by Siegel's Theorem on integer solutions of $y^2 = g(x)$ [Si], g must be of degree ≤ 2. Thus we will know that there are only finitely many such g if the following conjecture holds true for $d = 1$ and $d = 2$:

Conjecture 1. *Fix an integer $d \geq 1$. There exists an integer $D \geq 1$ (depending on d) such that if f is an irreducible polynomial of degree $\geq D$ then there are only finitely*

many squarefree polynomials $g(x) \in \mathbb{Z}[x]$ of degree d that correspond to squares in the field $\mathbb{Q}[x]/(f(x))$.

Equation (5) is also equivalent to the assertion that $g(\alpha) \in \mathbb{Q}(\alpha)^2$ for any, or all, of the roots α of $f(x)$. Therefore $\prod_\alpha g(\alpha) \in \mathbb{Q}^2$, and this is $|\text{Resultant}(f,g)|$ when f is monic. Thus Conjecture 1 is implied by the following:

Conjecture 2. *Fix an integer $d \geq 1$. There exists an integer $D \geq 1$ (depending on d) such that if f is an irreducible polynomial of degree $\geq D$ in $\mathbb{Q}[x]$ then there are only finitely many squarefree polynomials $g(x) \in \mathbb{Z}[x]$ of degree d for which $|\text{Resultant}(f,g)| \in |f_0|^d\mathbb{Q}^2$, where f_0 is the leading coefficient of f.*

Let $f(x,y) = y^{\deg f} f(x/y)$ be the homogenization of f. We now consider the case $d = 1$ above. Writing $g(x) = ax - b$, we have $\text{Resultant}(f,g) = \pm f(b,a)$. However $f(b,a) \in \pm\mathbb{Q}^2$ for only finitely many pairs of coprime integers a, b if $\deg f \geq 5$, by Theorem 2 of [DG] (which is a consequence of Faltings' Theorem [F1]). Thus both conjectures are true with $D_1 = 5$ when $d = 1$.

When $d = 2$ we have been unable to prove these conjectures, though it is possible to deduce such a result from Faltings [F2] if we assume that $w(x) = 1$ in (5), since then $f(\beta) \in \mathbb{Q}(\beta)^2$ for every root β of $g(\beta) = 0$.

Finally, we mention special values of binary homogeneous forms $f(x,y) \in \mathbb{Z}[x,y]$; that is, we wish to factor $f(l,m)$, where $(l,m) = 1$. As before, we investigate whether we can find infinitely many homogeneous $g_1(x,y), g_2(x,y) \in \mathbb{Z}[x,y]$, non-constant and without repeated factors, with

$$w(x,y)f(x,y) = g_1(x,y)u(x,y)^2 - g_2(x,y)v(x,y)^2$$

and with $g_1(l,m)/g_2(l,m) \in \mathbb{Q}^2$ for infinitely many pairs of coprime integers l, m; in other words $g(l,m) \in \mathbb{Q}^2$, where $g = g_1g_2$. By Theorem 2 of [DG] this implies that $\deg g \leq 4$. Dehomogenizing our equation, we find that we are again requiring $g(x)$ to correspond to a square in $\mathbb{Q}[x]/(f(x))$, so our problem will be resolved if Conjectures 1 or 2 are true for each $d \leq 4$.

3. Bounds for degrees

We shall need the following technical result:

Lemma 2. *If $K = k(\alpha)$ is a simple field extension of degree D and r, s are non-negative integers with $r + s = D - 1$, then every $\beta \in K$ can be written as $\beta = u(\alpha)/v(\alpha)$ with $\deg u \leq r$ and $\deg v \leq s$.*

Proof. If $\beta = 0$ we can take $u(\alpha) = 0$ and $v(\alpha) = 1$. Otherwise, regarding K as a vector space over k, the sets $\{1, \alpha, \dots, \alpha^r\}$ and $\{\beta, \beta\alpha, \dots, \beta\alpha^s\}$ are individually linearly independent, but their union is linearly dependent, and hence there is a vector that is a non-zero linear combination of both sets. This vector simultaneously has the forms $u(\alpha)$, with $\deg u \leq r$, and $\beta v(\alpha)$, with $\deg v \leq s$, where $u(\alpha), v(\alpha)$ are both non-zero.

Corollary 2. *Suppose that $f(x), g(x) \in \mathbb{Z}[x] \setminus \{0\}$ are of degrees $D > d$, respectively, where $f(x)$ is irreducible and $g(x)$ is a square in $\mathbb{Q}[x]/(f(x))$. Then there is a non-trivial solution $u(x), v(x), w(x) \in \mathbb{Q}[x] \setminus \{0\}$ to (5) with $\deg(w) \le d/2$.*

Proof. Let $\beta(x)^2 = g(x) \in \mathbb{Q}[x]/(f(x))$ and apply the lemma with $r = \lfloor D/2 + d/4 \rfloor$. We obtain $u(x)$ and $v(x)$ satisfying (5) with $\deg u \le D/2 + d/4$ and $\deg v \le D/2 - d/4$. Then $\deg w \le D + d/2 - \deg f = d/2$.

4. Gauss and Aurifeuille: History and Motivation

In Article 356 of [Ga], Gauss had shown that $\tau_p^2 = (-1)^{(p-1)/2} p = \varepsilon_p p$, where the Gauss sum τ_p is defined by

$$\tau_p := \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \xi_p^a \quad \text{with } \xi_p = e^{2i\pi/p}.$$

He used this in Article 357 to establish that for all odd primes p one has

$$4\left(\frac{x^p - 1}{x - 1}\right) = Y(x)^2 - \varepsilon_p p Z(x)^2$$

for some $Y(x), Z(x) \in \mathbb{Z}[x]$. For example,

$$4\left(\frac{x^3 - 1}{x - 1}\right) = (2x + 1)^2 + 3 \cdot 1^2 \quad \text{and} \quad 4\left(\frac{x^5 - 1}{x - 1}\right) = (2x^2 + x + 2)^2 - 5x^2.$$

For the proof he expands

$$\begin{aligned} z := \prod_{\left(\frac{r}{p}\right)=1} \left(x - \xi_p^r\right) &= R + S \sum_{\left(\frac{r}{p}\right)=1} \xi_p^r + T \sum_{\left(\frac{n}{p}\right)=-1} \xi_p^n \\ &= R - \frac{(S+T)}{2} + \frac{(S-T)}{2} \tau_p \end{aligned}$$

for some $R = R(x)$, $S = S(x)$, $T = T(x)$ in $\mathbb{Z}[x]$. Multiplying this by a conjugate over $\mathbb{Q}$ that takes τ_p to $-\tau_p$, and taking $Y = 2R - S - T$, $Z = T - S$, he obtains the result.

Gauss wrote[1]:

It is easy to see that the two terms of highest degree in the function Y will always be $2x^m + x^{m-1}$ and the highest in the function Z, x^{m-1}. The remaining coefficients, all of which will be integers, will vary according to the nature of the number n and cannot be given a general analytic formula.

However in 1993 Brent [Br] gave the delightful formulae

$$Y(x) = 2\sqrt{\frac{x^p - 1}{x - 1}} \cos\left(\frac{\sqrt{p}}{2} f_p(x)\right) \quad \text{and} \quad Z(x) = \frac{2}{\sqrt{p}} \sqrt{\frac{x^p - 1}{x - 1}} \sin\left(\frac{\sqrt{p}}{2} f_p(x)\right)$$

[1]Here Gauss's n is our prime p and his m is $(p-1)/2$

whenever $p \equiv 3 \pmod 4$, where $f_p(x) = \sum_{m\ge 1}(\frac{m}{p})\frac{x^m}{m}$. He also gave an analogous expression, involving cosh and sinh, for $4\varphi_n(x)$ when n is any odd squarefree number > 3.

Aurifeuille [Lu] gave a result similar to, but a little different from, Gauss's: For all odd primes p one has

$$\frac{x^p-1}{x-1} = U(x)^2 - \varepsilon_p p x V(x)^2$$

for some $U(x), V(x) \in \mathbb{Z}[x]$. This extra "$x$" is rather useful to the Cunningham project, for by taking $x = \varepsilon_p p y^2$ we get

$$\frac{(py^2)^p \mp 1}{py^2 \mp 1} = U(\pm py^2)^2 - (py)^2 V(\pm py^2)^2, \tag{6}$$

a difference of two squares and so factorable. The examples of Aurifeuillian factorization in the introduction are so deduced from the identities

$$x^2+1 = (x+1)^2 - 2x\cdot 1^2, \qquad \frac{x^3+1}{x+1} = (x+1)^2 - 3x\cdot 1^2,$$
$$\frac{x^5-1}{x-1} = (x^2+3x+1)^2 - 5x(x+1)^2 \quad\text{and}\quad \frac{x^7+1}{x+1} = (x+1)^6 - 7x(x^2+x+1)^2.$$

Brent [Br] also gave direct expressions for $U(x)$ and $V(x)$, similar to those for $Y(x)$ and $Z(x)$ in Gauss's identity, as follows:

$$U(x) = \sqrt{\frac{x^p+1}{x+1}}\cosh(\sqrt{p}g_p(\sqrt{x})) \quad\text{and}\quad V(x) = \frac{1}{\sqrt{px}}\sqrt{\frac{x^p+1}{x+1}}\sinh(\sqrt{p}g_p(\sqrt{x}))$$

whenever $p \equiv 3 \pmod 4$, where $g_p(x) = \sum_{m \text{ odd } \ge 1}\left(\frac{p}{m}\right)\frac{x^m}{m}$, (and similar expressions when p is replaced by any squarefree number).

In 1992 Hendrik Lenstra showed the first-named author a delightful direct proof of (6): Write $\alpha = \xi_p^{(p+1)/2}$, so that $\alpha^2 = \xi_p$ and thus

$$\varepsilon_p p y^2 - \xi_p = (\tau_p y)^2 - \alpha^2 = (\tau_p y + \alpha)(\tau_p y - \alpha),$$

where $\tau_p y \pm \alpha \in \mathbb{Z}[\xi_p][y]$. Taking $\mathrm{Norm}_{\mathbb{Q}(\xi_p)/\mathbb{Q}}$ of both sides we obtain

$$\frac{(py^2)^p - \varepsilon_p}{py^2 - \varepsilon_p} = A(y)B(y) \tag{7}$$

where $A(y) = \mathrm{Norm}(\tau_p y + \alpha)$ and $B(y) = \mathrm{Norm}(\tau_p y - \alpha)$. Now, by definition, both $A(y)+B(y)$ and $(A(y)-B(y))/y$ are fixed by the map $y \mapsto -y$, so both are functions in $\mathbb{Z}[y^2]$. Moreover A and B are products of terms of the form $(\pm\tau_p y \pm \alpha^\sigma)$, and so $A(y)+B(y)$ and $(A(y)-B(y))/py$ are in $\mathbb{Z}[(\tau_p y)^2] = \mathbb{Z}[py^2]$. Also $A(y) \equiv B(y) \pmod 2$. These observations give (6) with

$$U(\pm py^2) = \frac{A(y)+B(y)}{2} \quad\text{and}\quad V(\pm py^2) = \frac{A(y)-B(y)}{2py}.$$

Lenstra's proof depends on noting that ξ_p and $\varepsilon_p p$ are both squares in $\mathbb{Q}(\xi_p)$ though, modifying it slightly, it suffices to note that their product is a square. This then generalizes easily: Suppose that a is an integer, $\xi_n = e^{2i\pi/n}$ and a/ξ_n is a square in $\mathbb{Q}(\xi_n)$, say $a/\xi_n = \tau^2$. Then $(ay^2 - \xi_n)/\xi_n = (\tau y)^2 - 1 = (\tau y + 1)(\tau y - 1)$, and so $\varphi_n(ay^2)$, which is the norm from $\mathbb{Q}(\xi_n)$ to $\mathbb{Q}$ of $(ay^2 - \xi_n)/\xi_n$, factors as $\mathrm{Norm}(\tau y + 1)\,\mathrm{Norm}(\tau y - 1)$. This leads to equations of the type (1) with

$$U(ay^2) = \frac{1}{2}\big(\mathrm{Norm}(1 + \tau y) + \mathrm{Norm}(1 - \tau y)\big)$$

and

$$V(ay^2) = \frac{1}{2ay}\big(\mathrm{Norm}(1 + \tau y) - \mathrm{Norm}(1 - \tau y)\big),$$

where an argument similar to before shows that $U(x)$ and $V(x)$ are in $\mathbb{Z}[x]$. To see that this includes all instances of Schinzel's equations we need to know when $a\xi_n$ is a square in $\mathbb{Q}(\xi_n)$. This is determined by Lemma 3 in Section 6.

In the light of the above, Lemma 1 can be seen as a further generalization of Lenstra's idea.

5. Developing Lenstra's perspective

We re-interpret Lenstra's proof by noting that

$$\tau_p^2 = \gamma_p(\xi_p)^2 \equiv \gamma_p(x)^2 \mod (x - \xi_p)$$

where we define the *Fekete polynomial*

$$\gamma_p(x) := \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) x^a.$$

This congruence holds for any primitive pth root of unity in place of ξ_p, so

$$\gamma_p(x)^2 \equiv \tau_p^2 \mod \varphi_p(x) = \prod_{a=1}^{p-1}(x - \xi_p^a);$$

in other words, $\gamma_p(x)^2 = \tau_p^2$ in $\mathbb{Q}[x]/(\varphi_p(x))$. Applying Corollary 2 with $g(x) = \tau_p^2 = \varepsilon_p p$ we recover Gauss's identity, up to a constant. The same proof but with $g(x) = \varepsilon_p p x$ gives Aurifeuille's identity up to a constant, since

$$x \equiv (x^{(p+1)/2})^2 \pmod{\varphi_p(x)}$$

so x is a square in $\mathbb{Q}[x]/(\varphi_p(x))$.

In 1994 Hahn [Ha] showed how similar ideas could be used to simplify the process of determining a factor of $P := (p^p - \varepsilon_p)/(p - \varepsilon_p)$, a sequence of numbers that have long

been of interest. (For example, $(p^p-1)/(p-1)$ is conjectured to be the period mod p of the sequence of Bell numbers; see [LD] and [Wa].) Taking $x=\tau_p^2=\varepsilon_p p$ above, we obtain $\gamma_p(\tau_p^2)^2\equiv\tau_p^2\equiv((\tau_p^2)^{(p+1)/2})^2 \pmod P$. Note also that because $\tau_p^2=\varepsilon_p p$ is divisible by p so are $\gamma_p(\tau_p^2)\pm(\tau_p^2)^{(p+1)/2}$ $(=p\rho_+,\ p\rho_-$, say). When $p>3$, $\rho_\pm$ are integers less than P, so $(\rho_\pm,P)$ are non-trivial factors of P. In fact they are the Aurifeuillian factors of P: taking norms of the congruences

$$\gamma_p(\tau_p^2)\pm(\tau_p^2)^{(p+1)/2}\equiv\gamma_p(\xi_p)\pm\xi_p^{(p+1)/2} \pmod{\tau_p^2-\xi_p}$$

gives $(p\rho_+)^{p-1}\equiv A(1)$ and $(p\rho_-)^{p-1}\equiv B(1) \pmod P$ (with A and B as in (7)) which together with $\rho_+\rho_-\equiv 0 \pmod P$ imply that $(\rho_+,P)=A(1)$ and $(\rho_-,P)=B(1)$. Sun et al. [SH, SR] extended Hahn's method to find the Aurifeuillian factors in the top line of (1) (Case (i) of our Supplement).

Dirichlet found a fast way to calculate Y and Z in Gauss's identity (generalized to U and V in Aurifeuille's identity by Brent [Br]): From Gauss we have

$$Y(x)-\sqrt{\varepsilon_p p}Z(x)=\prod_{(\frac{a}{p})=1}(x-\xi_p^a)=\sum_{j=0}^{\frac{p-1}{2}}(-1)^j a_j x^{\frac{p-1}{2}-j}.$$

Dirichlet (1863) used Newton's recurrence (1707), $ka_k=-\sum_{0\le j<k}s_{k-j}a_j$, where

$$s_i=\sum_{(\frac{a}{p})=1}\xi_p^{ai}=\begin{cases}\frac12\left(\left(\frac{i}{p}\right)\sqrt{\varepsilon_p p}-1\right), & \text{if } p\not| i,\\ \frac12(p-1), & \text{if } p\mid i,\end{cases}$$

to determine the elementary symmetric functions a_k by induction.

6. Finding all Aurifeuillian factorizations: Proof of the theorem

Before embarking on the proof of the Theorem and Supplement we need two lemmas.

Lemma 3. *Let a be rational and $\xi_d=e^{2i\pi/d}$. Then $a\xi_d$ is a square in $\mathbb{Q}(\xi_d)$ if and only if $a^*\mid d$ and one of the following holds:*

(i) d is odd and $a^*\equiv 1 \pmod 4$,
(ii) $2\parallel d$ and $a^*\equiv -1 \pmod 4$ or
(iii) $4\parallel d$ and a^* is even.

Proof. During this proof a "square" will mean the square of a number in $\mathbb{Q}(\xi_d)$.

If $a\xi_d$ is a square then all of the prime divisors of a^* ramify in $\mathbb{Q}(\xi_d)/\mathbb{Q}$, so divide d, and hence $a^*\mid d$.

As we have seen, for any odd prime p the Gauss sum τ_p is in $\mathbb{Q}(\xi_p)$, and its square is $(-1/p)p$. Therefore, for an odd positive squarefree divisor l of d, $(-1/l)l$ is the square of $\prod_{p\mid l}\tau_p$, so is a square in $\mathbb{Q}(\xi_d)$, since this field contains each $\mathbb{Q}(\xi_p)$.

We can write a^* as $a^* = rs$, where $r = \pm 1$ or ± 2 and $s = (-1/|s|)|s| \equiv 1 \pmod 4$. Then s is a square, so $a\xi_d$ is a square if and only if $r\xi_d$ is. Note that -1 is a square if and only if $4 \mid d$ and ± 2 is a square if and only if $8 \mid d$, in which case ± 2 are both squares.

If d is odd then $\xi_d = (\xi_d^{(d+1)/2})^2$ is a square but $-\xi_d$ and $\pm 2\xi_d$ are not. So $a\xi_d$ is a square if and only if $a^* = s$, corresponding to (i).

If $2 \parallel d$ then $-\xi_d = (\xi_d^{(d+2)/4})^2$ is a square but ξ_d and $\pm 2\xi_d$ are not. So $a\xi_d$ is a square if and only if $a^* = -s$, corresponding to (ii).

If $4 \parallel d$ then $\pm 2\xi_d = ((1 \mp i)\xi_d^{(d+4)/8})^2$ are squares but $\pm\xi_d$ are not. So $a\xi_d$ is a square if and only if $a^* = \pm 2s$, corresponding to (iii).

If $8|d$ then ξ_d is not a square, so neither are $-\xi_d$ or $\pm 2\xi_d$. Hence $a\xi_d$ is not a square.

Proof of the Supplement. This follows from Lemma 3 and Corollary 1 with $f = \varphi_d$ and $g(y) = ay^2$.

Lemma 4. *If $b \in \mathbb{Q}$ with $b \neq -1, 0$ or 1, and m is a positive integer for which $b^{1/m}$ lies in a cyclotomic field then $b^{2/m}$ is rational.*

Proof. If the smallest positive integer d with $b^{d/m}$ rational were > 2 then the Galois group of the Galois closure of $\mathbb{Q}(b^{1/m})$ would contain the non-abelian dihedral group D_d of order $2d$ (generated by $b^{1/m} \mapsto \xi_d b^{1/m}$ and complex conjugation) which is incompatible with $b^{1/m}$ belonging to a cyclotomic field, whose Galois group would be abelian.

Proof of the Theorem. Schinzel and Tijdeman [ST], applying results of Siegel and Baker, showed that if $h(y) \in \mathbb{Q}[y]$ has more than one complex root then there are no solutions to $h(m) = b^N$ in integers $b, m > 1$ once N is sufficiently large. Hence if $g(y)$ is a Cunningham factoring polynomial then it is of the form

$$A(y + c)^Q = (a(y + c)^q)^n,$$

where $A, c \in \mathbb{Q}$ with $A \neq 0$, n is the largest divisor of Q with $A^{1/n}$ rational, $q = Q/n$ and $a = A^{1/n}$. Note that if $A = -1$ or 1 then we may take $a = A$ and the theorem is easily established directly. So we may assume that $a \neq -1, 0$ or 1. Putting $t = y + c$, we have

$$(at^q)^n - 1 = \prod_{d|n} \varphi_d(at^q). \tag{8}$$

If none of the terms on the right factors further in $\mathbb{Q}[t]$ then this is a cyclotomic factorization and derives from $g(x) = x^n$ (with $x = a(y + c)^q$).

A typical term on the right of (8) is $\varphi_d(at^q)$, and by Lemma 1 its factorization mirrors the factorization of $at^q - \xi_d$ over $\mathbb{Q}(\xi_d)$. Any monic factor $f(t)$ of $at^q - \xi_d$ has the form

$$f(t) = \prod_{j \in J} (t - \xi_{dq}\xi_q^j a^{-1/q}) = \sum_{i=0}^{|J|} c_i a^{-i/q} t^{|J|-i},$$

where $J \subseteq \{0, 1, \ldots, q - 1\}$ and each $c_i \in \mathbb{Q}(\xi_{dq})$. If $c_i a^{-i/q}$ is in $\mathbb{Q}(\xi_d) \setminus \{0\}$ then, by Lemma 4 (since $a \neq -1, 0$ or 1), $a^{2i/q}$ is rational so, by the definition of q, $q \mid 2i$ and either

$i = 0$, $i = q$ or q is even and $i = q/2$, as $|J| \le q$. Hence $at^q - \xi_d$ is either irreducible over $\mathbb{Q}(\xi_d)$ or q is even and $at^q - \xi_d$ is the product of two binomial factors of degree $q/2$, irreducible over $\mathbb{Q}(\xi_d)$. The latter occurs if and only if $a\xi_d$ is a square in $\mathbb{Q}(\xi_d)$, in which case $\varphi_d(at^q)$ splits into precisely two irreducible factors over $\mathbb{Q}$ of equal degrees. In this case too $a^*x^2 - \xi_d$ factors over $\mathbb{Q}(\xi_d)$ so, by Lemma 1 again, $\varphi_d(a^*x^2)$ factors over $\mathbb{Q}$ and the substitution $h(y) = (a(y+c)^q)^n$ derives from $g(x) = (a^*x^2)^n$, with $x = \sqrt{a/a^*}(y+c)^{q/2}$.

Finally, Lemma 3 enables us to identify when $a\xi_d$ is a square in $\mathbb{Q}(\xi_d)$ for some $d \mid n$. Case (i) of Lemma 3 holds for some divisor d of n, if and only if $a^* \equiv 1 \pmod 4$ and $a^* \mid n$. This corresponds to Case (i) of the first alternative of the Theorem and Case (ii) with $a^* \equiv 1 \pmod 4$. Similarly, Case (ii) of Lemma 3 corresponds to Case (ii) of the first alternative of the Theorem with $a^* \equiv -1 \pmod 4$ (when $a^* \ne -1$) and to the second alternative (when $a^* = -1$). Finally, Case (iii) of Lemma 3 corresponds to Case (iii) of the Theorem.

7. Linear $g(x)$

We consider the following question, which arises from Section 2 when we restrict attention to solutions of (5) with $\deg g = 1$: *For what irreducible $f(x) \in \mathbb{Q}[x]$ are there infinitely many monic linear $g(x)$ with non-trivial solutions to* (5)*?* Since $\mathbb{Q}[x]/(f(x))$ is a field when f is irreducible, $v(x)$ has an inverse mod f, so this is equivalent to asking whether there are infinitely many monic polynomials $u(x) \in \mathbb{Q}[x]$ of degree $\le \deg f - 1$, such that $u(x)^2$ is linear mod f. We saw in Section 2 that $\deg f \le 4$. After a linear substitution we can write any f of degree D as $x^D - ax^{D-2} - bx^{D-3} - \cdots - c$.

If $\deg f = 2$ then every polynomial is congruent to a linear polynomial mod f, so there are infinitely many such u and hence infinitely many g.

If $\deg f = 3$ then write $f(x) = x^3 - ax - b$ and $u(x) = x^2 + rx + s$. The coefficient of x^2 in $u(x)^2 \pmod f$ is $r^2 + 2s + a$, which can be made 0, for any r, by taking $s = -(r^2+a)/2$. So again there are infinitely many g.

If $\deg f = 4$ write $f(x) = x^4 - ax^2 - bx - c$. It is easily checked that $u(x) = x^2 - a/2$ is the only monic polynomial of degree ≤ 2 to give a linear g, so we can take $u(x) = x^3 + rx^2 + sx + t$. Then the coefficients of $u(x)^2 \pmod f$ are polynomials in r, s and t. We find that the coefficient of x^2 is 0 if $t = -(c + a^2 + 2sa + 2rb + r^2a + s^2)/2r$ when $r \ne 0$. The coefficient of x^3 is then $1/r$ times a polynomial in r and s which is quadratic in s. This has a rational root if and only if its discriminant as a quadratic polynomial in s is a square, and computationally we found that this discriminant is exactly $4f(r)$. Thus there are infinitely many such g if and only if there are infinitely many rational points on the genus one curve $y^2 = f(x)$.

Acknowledgements. Thanks are due to Hendrik Lenstra for his proof of Aurifeuille's identity discussed in Section 4 which inspired this paper, to Mike Fried for his helpful email correspondence, to Sam Wagstaff for his example mentioned above, to others in the computational number theory community who encouraged us to publish these notes, and to Dan Abramovic, Mitch Rothstein and Tom Tucker for conversations about applying Faltings' Theorem to the quadratic g case, even though we never succeeded! This paper is an

expanded version of the first-named author's lecture at the ANTS III conference at Reed College, Oregon in 1998. The second-named author is indebted to the University of the South Pacific for providing employment and study leave during its preparation.

References

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

[BL] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. 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*, Amer. Math. Soc., Providence, RI, 1988.

[DG] H. Darmon and A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bull. London Math. Soc. **27** (1995), 513–543.

[F1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[F2] ———, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), 549–576.

[Fr] M. Fried, *Applications of the classification of simple groups to monodromy, Part II: Davenport and Hilbert-Siegel problems* (to appear).

[Ga] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801; English transl. Yale U. Press, New Haven, Connecticut, 1966.

[Ha] S. Hahn, *A remark on Aurifeuillian factorizations*, Math. Japon. **39** (1994), 501–502.

[LD] J. Levine and R. E. Dalton, *Minimum periods, modulo p, of first order Bell exponential integers*, Math. Comp. **16** (1962), 416–423.

[Lu] E. Lucas, *Théorèmes d'arithmétique*, Atti. Roy. Acad. Sci. Torino **13** (1878), 271–284.

[Sc] A. Schinzel, *On primitive prime factors of $a^n - b^n$*, Proc. Cambridge Philos. Soc. **58** (1962), 555–562.

[ST] A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. **31** (1976), 199–204.

[Si] C. L. Siegel (under the pseudonym 'X'), *The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$*, J. London Math. Soc. **1** (1926), 66–68; *Gesammelte Abhandlungen*, vol. I, Springer, Berlin, 1966, pp. 207–208.

[St] P. Stevenhagen, *On Aurifeuillian factorizations*, Indag. Math. **49** (1987), 451–468.

[SH] Q. Sun, S.F. Hong,, *Aurifeuillian factorizations of $q^q \pm 1$ ($q = p^n$)*, Gaoxiao Yingyong Shuxue Ser. A **13** (1998), 342–348.

[SR] Q. Sun, D. Ren, S. Hong, P. Yuan and Q. Han, *A new class of Aurifeuillian factorization of $M^n \pm 1$*, Sci. Math. **2** (1999), 353–360.

[Wa] S. S. Wagstaff Jr, *Aurifeuillian factorizations and the period of the Bell numbers modulo a prime*, Math. Comp. **65** (1996), 383–391.

Département de mathématiques et de statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal, QC H3C 3J7, Canada

E-mail address: andrew@DMS.UMontreal.CA

Department of Mathematics, University of Queensland, QLD 4072, Australia

E-mail address: peterpleasants@iprimus.com.au