involve
a journal of mathematics

An observation on generating functions with an application to a sum of secant powers

Jeffrey Mudrock

mathematical sciences publishers

2011 vol. 4, no. 2

INVOLVE 4:2(2011)

An observation on generating functions with an application to a sum of secant powers

Jeffrey Mudrock

(Communicated by Nigel Boston)

Suppose that $P(x), Q(x) \in \mathbb{Z}[x]$ are two relatively prime polynomials, and that $P(x)/Q(x) = \sum_{n=0}^{\infty} a_n x^n$ has the property that $a_n \in \mathbb{Z}$ for all n. We show that if $Q(1/\alpha) = 0$, then α is an algebraic integer. Then, we show that this result can be used to provide a solution to Problem 11213(b) of the *American Mathematical Monthly* (2006).

1. Introduction and statement of results

This paper has two goals. One is to prove this general observation:

Theorem 1. *Suppose $P(x), Q(x) \in \mathbb{Z}[x]$ are relatively prime polynomials with integer coefficients and their quotient is the generating function of an integer series*:

$$\frac{P(x)}{Q(x)} = \sum_{n=0}^{\infty} a_n x^n, \quad \textit{with } a_n \in \mathbb{Z} \textit{ for all } n.$$

Then the inverse of any root of Q is an algebraic integer.

The second goal is to apply this result to solve a problem from the *American Mathematical Monthly*:

Problem 11213 [AMM 2006]. *Proposed by Stanley Rabinowitz, Chelmsford, MA.* For positive integers n and m with n odd and greater than 1, let

$$S(n,m) = \sum_{k=1}^{(n-1)/2} \sec^{2m}\left(\frac{k\pi}{n+1}\right).$$

(a) Show that if n is one less than a power of 2, then $S(n,m)$ is a positive integer.

(b*) Show that if n does not have the form of Part (a), then there exists a positive integer m such that $S(n,m)$ is not an integer.

MSC2000: primary 11R04; secondary 11R18.

Keywords: algebraic number theory, generating functions, secant function.

The * indicates that no solution was known to the *Monthly* editors. (A solution to (a) was provided in [AMM 2008].) We solve part (b) of Problem 11213 by proving the contrapositive:

Theorem 2. *Let $n > 1$ be an odd integer. If, for every positive integer m, the sum*

$$S(n,m) = \sum_{k=1}^{(n-1)/2} \sec^{2m} \frac{k\pi}{n+1}$$

has an integer value, then $n+1$ is a power of 2.

A similar result to Theorem 1 (but less general) had appeared before in the *Monthly*, as a problem proposed and solved by Michael Larsen:

Problem E 2993 [AMM 1983; 1986]. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ a complex numbers such that $\sum_1^n \alpha_i^m$ is an integer for every positive m; then the polynomial $\prod_1^n (x - \alpha_i)$ has integer coefficients.

Here is an outline of the paper. After recalling the necessary concepts from algebraic number theory in Section 2, we prove in Section 3 two intermediate results: $S(n,m)$ is always rational, and the generating function of the sequence $\{S(n,m)\}_{m>0}$ (for fixed odd $n > 0$) has integer coefficients. In Section 4 we prove Theorem 1, from which Theorem 2 follows easily given the intermediate results.

2. Background

We review some basic algebraic number theory, which is carefully laid out in [Stewart and Tall 2002], for example. (This citation will be abbreviated as [ST].)

An *algebraic number* is any zero of a polynomial with integer coefficients. An *algebraic integer* is any zero of a monic polynomial with integer coefficients. The set of algebraic numbers is a field, and the set of algebraic integers forms a ring [ST, Theorems 2.1 and 2.9].

For example, if p is prime, $\zeta_p = e^{2\pi i/p}$ is an algebraic integer since it is a zero of the polynomial $x^p - 1$.

The *minimal polynomial* of an algebraic number α is the monic polynomial $p(x)$ with rational coefficients and the smallest possible degree such that $p(\alpha) = 0$. All polynomials of which α is a root are divisible by p. For example, $r(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x^p - 1)/(x-1)$ is the minimal polynomial of ζ_p.

Definition. If K is a field contained in L, we say that L is a field extension of K, and we denote this by $L : K$.

If K is a field and α is an algebraic number let $K(\alpha)$ denote the smallest field containing all the elements of K and α. One way to think about field extensions is that if $L : K$ is a field extension, then L has a natural structure as a vector space over

K. The dimension of this vector space, which is called the *degree*, is represented with $[L:K]$. If $[L:K]$ is a number the field extension is called finite. If H, K, and L are fields such that K is a subset of L and H is a subset of K, then

$$[L:H]=[L:K][K:H] \tag{1}$$

[ST, Theorem 1.10].

In algebraic number theory field extensions of the form $\mathbb{Q}(\alpha)$ are of interest. If α is an algebraic number, then $[\mathbb{Q}(\alpha):\mathbb{Q}]$ equals the degree of the minimal polynomial of α [ST, Theorem 1.1]. A field K is called an *algebraic number field* if $[K:\mathbb{Q}]$ is finite. If $K=\mathbb{Q}(\alpha)$ and α is an algebraic number, then the ring of algebraic integers in K is finitely generated as an abelian group [ST, Theorem 2.16].

Definition. If $K=\mathbb{Q}(\alpha)$ is an algebraic number field of degree n, then there are n distinct monomorphisms $\sigma_1,\ldots,\sigma_n$ from K to $\mathbb{C}$. The *conjugates* of an element $\beta\in K$ are the numbers $\sigma_i(\beta)$ for all i between 1 and n.

The conjugates of an algebraic number α are the zeros of the minimal polynomial of α. For example, if $\alpha=\zeta_n=e^{2\pi i/n}$, where $n>0$ is an integer, then α has $\phi(n)$ conjugates in $\mathbb{Q}(\alpha)$, where ϕ is the Möbius function. The conjugates of ζ_n are all the elements in the set

$$\{e^{2\pi ik/n}:(k,n)=1\}.$$

This information can be found in [Milne 2009, page 93].

Definition. Let $K=\mathbb{Q}(\alpha)$ be an algebraic number field, and consider $\beta\in K$. The *trace* of β in K, denoted by $\mathrm{Tr}_K\beta$, is the sum of all the conjugates of β. The *norm* of β in K, denoted by $N_K(\beta)$, is the product of all of the conjugates of β.

Thus $\mathrm{Tr}_K\zeta_p=-1$ and $N_K(\zeta_p)=(-1)^{p-1}$ for p prime, where $K=\mathbb{Q}(\zeta_p)$. If one notes that

$$\frac{\zeta_n+\zeta_n^{-1}}{2}=\cos\frac{2\pi}{n}$$

and applies (1) one can see that the conjugates of $\alpha=\cos\dfrac{2\pi}{n}$ in $\mathbb{Q}(\alpha)$ are all the elements in the set

$$\left\{\cos\frac{2\pi k}{n}:(k,n)=1,\ 0<k<n/2\right\}. \tag{2}$$

A formal proof of this can be found in [Milne 2009, pages 95–96]. Also, as a consequence of Theorem 2.6(a), Lemma 2.13, and Lemma 1.7 of [ST], if α is an algebraic number its trace is rational; and as a consequence of Lemma 2.14 of the same reference, if α is an algebraic integer its norm is an integer.

3. Intermediate results

Lemma 3. *If $n>1$ is odd and $m\geq 1$, the sum $S(n,m)$ of Theorem 2 is a rational number.*

Proof. We make use of the trigonometric identity $\sec^2 x = \dfrac{2}{\cos(2x)+1}$ to write $\sec^{2m} x = f(\cos 2x)$, where

$$f(x) := \Big(\frac{2}{x+1}\Big)^m.$$

Then, dropping m from the notation and introducing $N=n+1$ for convenience, we can rewrite our sum as

$$\sum_{0<k<N/2} s(k), \quad \text{where } s(k) := f\Big(\cos\frac{2\pi k}{N}\Big). \tag{3}$$

We assume at first that $N/2$ is an odd prime. All the $s(k)$ then lie in the extension $K=\mathbb{Q}(\cos 2\pi/N)$, as follows from the characterization (2) (with n in that formula equal to N here). More precisely, if k is odd, $\cos 2\pi k/N$ is a conjugate of $\cos 2\pi/N$ in K. If k is even, $\cos 2\pi k/N$ equals $-\cos 2\pi k'/N$, for $k'=N/2-k$ odd; therefore it is a conjugate of $-\cos 2\pi/N$. Either way, $\cos 2\pi k/N$ lies in K, and therefore so does $s(k)$, since f is a rational function.

The operation of taking conjugates commutes with applying f (monomorphisms preserve sums, products and inverses, and fix the numbers 1 and 2). Putting this together with the previous paragraph, we conclude that half of the $s(k)$ (those where k is odd) make up the conjugates in K of $s(1)$, while the other half make up the conjugates of $s(2)$ (taking $k=2$ as a representative of the even k's). It follows that

$$\sum_{k=1}^{N/2-1} s(k) = \operatorname{Tr}_K s(1) + \operatorname{Tr}_K s(2) = \operatorname{Tr}_K f\Big(\cos\frac{2\pi k}{N}\Big) + \operatorname{Tr}_K f\Big(\cos\frac{2\times 2\pi k}{N}\Big).$$

Thus $S(n,m)$ is the sum of two traces of algebraic numbers, and so rational.

Now let $N/2$ be arbitrary. Our strategy is the same: we partition the values of k according to their gcd with N. Let $d_1,\dots,d_l$ be all the divisors of N apart from N and $N/2$, and define

$$D_i := \{k : \gcd(k,N)=d_i,\ 0<k<N/2\} = \{d_i j : \gcd(j,N/d_i)=1,\ 0<j<N/(2d_i)\}.$$

The D_i are disjoint, and together they account for all the k in the sum (3). Moreover,

$$\sum_{k\in D_i} s(k) = \sum_{\substack{j:\gcd(j,N/d_i)=1\\ 0<j<N/(2d_i)}} f\Big(\cos\frac{2\pi j}{N/d_i}\Big) = \operatorname{Tr}_{\mathbb{Q}(\cos\frac{2\pi}{N/d_i})} f\Big(\cos\frac{2\pi}{N/d_i}\Big),$$

where the last equality follows from the same reasoning used earlier for k odd (with N replaced by N/d_i). We have expressed $S(n,m)$ as a sum of traces of algebraic numbers, which means it is rational. □

This result allows us to prove that the generating function for the sequence $\{S(n,m)\}_{m>0}$ (for fixed odd $n > 0$) is a rational function.

Lemma 4. *If $n > 1$ is odd, $m \geq 1$, and*

$$F_n(x) = \sum_{m=0}^{\infty} S(n,m)x^m,$$

then there exist $P(x), Q(x) \in \mathbb{Z}[x]$ such that $F_n(x) = P(x)/Q(x)$.

Proof. Using the formula for the sum of a geometric series, we write

$$F_n(x) = \sum_{m=0}^{\infty}\left(\sum_{k=1}^{(n-1)/2} \sec^{2m}\frac{k\pi}{n+1}\right)x^m = \sum_{k=1}^{(n-1)/2} \frac{1}{1 - x\sec^2\frac{k\pi}{n+1}},$$

so that

$$Q(x) = \prod_{k=1}^{(n-1)/2}\left(1 - x\sec^2\frac{k\pi}{n+1}\right).$$

We will show that $Q(x)$ is a polynomial with rational coefficients. Set

$$b_k := \sec^2\frac{k\pi}{n+1},$$

where $1 \leq k \leq (n-1)/2$. Let s_i be the sum of the products of each i-element subset of the set $\{b_1, b_2, \ldots, b_{(n-1)/2}\}$ (in other words, s_i is the i-th elementary symmetric polynomial applied to the b_i). The coefficient of x^i in $Q(x)$ is $(-1)^i s_i$. Also, let

$$p_r := \sum_{k=1}^{n} b_k^r.$$

The Newton–Girard formulas tell us that

$$p_i - s_1 p_{i-1} + s_2 p_{i-2} + \cdots + (-1)^{i-1} s_{i-1} p_1 + (-1)^i i s_i = 0,$$

for all $1 \leq i \leq (n-1)/2$. It is clear that p_i is rational for all i by Lemma 4. An easy induction argument implies that s_i is rational for all i. Since the coefficients of $Q(x)$ can be expressed in terms of the s_i, we see that $Q(x)$ has rational coefficients. Thus $P(x) = F_n(x)Q(x)$ has rational coefficients. The desired result follows. □

Lemma 5. *Suppose that a and b are algebraic numbers, and*

$$F(x) = \frac{a}{1-bx} = \sum_{n=0}^{\infty} a_n x^n.$$

If a_n is an algebraic integer for all n, then b is an algebraic integer.

Proof. The assumption implies that $a_n = ab^n$. We know that ab^n is an algebraic integer for all n, and so lies in the ring of algebraic integers of the field $K = \mathbb{Q}(b)$. This ring is finitely generated as an abelian group. Suppose that it is generated by $\{v_1, v_2, \dots, v_l\}$. Then b^n must be in the finitely generated abelian group generated by $\{v_1/a, \dots, v_l/a\}$ for all n. Lemma 2.8 of [ST] states that a complex number θ is an algebraic integer if and only if the additive group generated by all powers $1, \theta, \theta^2, \dots$ is finitely generated. Thus, b is an algebraic integer. □

Now, we wish to expand upon the ideas presented in Lemma 5.

Definition. A sequence $\{a_n\}$ of algebraic numbers has a *bounded denominator* if there exists a positive integer m such that ma_n is an algebraic integer for all n.

Lemma 6. *Let*

$$F(x) = \sum_{n=0}^{\infty} a_n x^n,$$

where $\{a_n\}$ is a sequence with bounded denominator. Suppose $p(x)$ is a polynomial whose coefficients are algebraic numbers and let

$$F(x)p(x) = \sum_{n=0}^{\infty} b_n x^n.$$

Then, the sequence $\{b_n\}$ has bounded denominator.

Proof. This follows from the fact that the algebraic numbers form a subfield of the complex numbers and the fact that given an algebraic number a there exists a positive integer n such that na is an algebraic integer. □

Lemma 7. *Let $\zeta_{4p} = e^{2\pi i/4p}$, where p is an odd prime. Then*

$$N_{\mathbb{Q}(\zeta_{4p})}(\zeta_{4p} + \zeta_{4p}^{-1}) = p^2.$$

Proof. First note that

$$\zeta_{4p} + \zeta_{4p}^{-1} = 2\cos\frac{\pi}{2p},$$

and recall the characterization of the conjugates of $\cos 2\pi/n$ given in (2). We have

$$N_{\mathbb{Q}(\zeta_{4p})}(\zeta_{4p} + \zeta_{4p}^{-1}) = \prod_{\substack{(k,4p)=1 \\ 1\le k\le 4p}} \left(e^{\frac{2\pi ik}{4p}} + e^{\frac{-2\pi ik}{4p}}\right) = \zeta_{4p}^{-\phi(4p)2p} \prod_{\substack{(k,4p)=1 \\ 1\le k\le 4p}} \left(e^{\frac{4\pi ik}{4p}} + 1\right).$$

Now, we know that

$$N_{\mathbb{Q}(\zeta_{2p})}(\zeta_{2p} + 1) = \prod_{\substack{(k,2p)=1 \\ 1\le k\le 2p}} (e^{\frac{2\pi ik}{2p}} + 1).$$

This implies

$$\zeta_{4p}^{-\phi(4p)2p} \prod_{\substack{(k,4p)=1 \\ 1\le k\le 4p}} \left(e^{\frac{4\pi ik}{4p}}+1\right) = N_{\mathbb{Q}(\zeta_{2p})}(\zeta_{2p}+1)^2(e^{-2\pi i}).$$

Now, the minimal polynomial of ζ_{2p} is the same as that of $-\zeta_p$. Furthermore,

$$r(x) = x^{p-1}+x^{p-2}+\cdots+x+1 = \prod_{k=1}^{p-1}(x-\zeta_p^k).$$

So, $N_{\mathbb{Q}(\zeta_p)}(1-\zeta_p) = r(1) = p$ since the minimal polynomial of ζ_p is $r(x)$. Thus,

$$N_{\mathbb{Q}(\zeta_{2p})}(\zeta_{2p}+1)^2(e^{-2\pi i}) = N_{\mathbb{Q}(\zeta_p)}(1-\zeta_p)^2 = p^2,$$

as desired. □

Lemma 8. *If, for all k satisfying $1 \le k \le (n-1)/2$, the value of $\sec^2 \frac{k\pi}{n+1}$ is an algebraic integer, then $n+1$ is a power of two.*

Proof. Assume that $n+1$ is not a power of two. Let p be an odd prime factor of $2(n+1)$. Since n is odd, $2(n+1)$ is a multiple of 4 and so $4p$ divides $2(n+1)$. Let $k = 2(n+1)/(4p)$, so $2(n+1)/k = 4p$. Then

$$\sec^2\frac{k\pi}{n+1} = \left(\frac{2}{\zeta_{2(n+1)}^k+\zeta_{2(n+1)}^{-k}}\right)^2 = \left(\frac{2}{\zeta_{4p}+\zeta_{4p}^{-1}}\right)^2.$$

Now, from the previous lemma, $N_{\mathbb{Q}(\zeta_{4p})}(\zeta_{4p}+\zeta_{4p}^{-1}) = p^2$. This implies

$$N_{\mathbb{Q}(\zeta_{4p})}\left(\frac{2}{\zeta_{4p}+\zeta_{4p}^{-1}}\right)^2 = \frac{2^{2\phi(4p)}}{p^4}.$$

Then, since p is an odd prime we know that $2^{2\phi(4p)}/p^4$ is not an integer. This means that with the chosen k, $\sec^2 k\pi/(n+1)$ is not an algebraic integer. This proves the desired result. □

4. Proof of the theorems

Proof of Theorem 2. This is a more general version of Lemma 5. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be all the numbers whose reciprocals are zeros of $Q(x)$. Then $F(x)$ has a partial fraction expansion whose terms are of the form

$$\frac{A_{i,l}}{(1-\alpha_i x)^l},$$

plus a polynomial part. Write

$$Q(x)=\prod_{i=1}^{n}(1-\alpha_i x)^{k_i}.$$

Let j be the largest positive integer such that in the partial fraction decomposition of $F(x)$ the term $A_{i,j}/(1-\alpha_i x)^j$ is nonzero. Clearly $j>0$, since $P(x)$ and $Q(x)$ are relatively prime. Now, let

$$Q_i(x)=\frac{Q(x)}{(1-\alpha_i x)^{k_i-j+1}}.$$

The highest power of $(1-\alpha_i x)$ that divides $Q_i(x)$ is clearly $j-1$.

We have

$$F(x)Q_i(x)=\sum_{n=0}^{\infty}b_n x^n.$$

Then, by Lemma 6, $\{b_n\}$ has a bounded denominator. Now, we will consider the effect of multiplying $F(x)$ and $Q_i(x)$ by considering what happens to each term in the partial fraction expansion of $F(x)$. With the exception of the term

$$\frac{A_{i,j}}{(1-\alpha_i x)^j},$$

$Q_i(x)$ times a term in the partial fraction expansion of $F(x)$ is a polynomial of finite degree. Now, one can see that

$$Q_i(x)\frac{A_{i,j}}{(1-\alpha_i x)^j}=\frac{Q_i(x)}{(1-\alpha_i x)^{j-1}}\frac{A_{i,j}}{(1-\alpha_i x)}.$$

It is clear that $Q_i(x)/(1-\alpha_i x)^{j-1}$ is a polynomial. Thus,

$$F(x)Q_i(x)=q(x)+\frac{D_i}{1-\alpha_i x},$$

where $q(x)$ is a polynomial and D_i is some algebraic number. So, we can say that for sufficiently large n, $b_n=D_i\alpha_i^n$ where D_i and b_n are algebraic numbers. Then, by Lemma 5, α_i is an algebraic integer. □

Proof of Theorem 1. Suppose $S(n,m)$ is an integer for all $m>0$. By Lemma 4,

$$F_n(x)=\sum_{m=0}^{\infty}\left(\sum_{k=1}^{(n-1)/2}\sec^{2m}\frac{k\pi}{n+1}\right)x^m=\sum_{k=1}^{(n-1)/2}\left(\frac{1}{1-x\sec(\frac{k\pi}{n+1})}\right)$$

is a rational function. Hence, $F_n(x)=P(x)/Q(x)$ where $P(x),\ Q(x)\in\mathbb{Q}[x]$. Theorem 1 now implies that $\sec^2(k\pi/(n+1))$ is an algebraic integer for all k with $1\le k\le(n-1)/2$. According to Lemma 8, this means $n+1$ is a power of two. □

Acknowledgements

The author thanks his advisor, Jeremy Rouse, for introducing him to this problem and keeping him motivated throughout the project. The author also thanks the anonymous referee for helpful comments.

References

[AMM 1983] M. Larsen, "Problems and solutions: E 2993", *Amer. Math. Monthly* **90**:4 (1983), 287.

[AMM 1986] M. Larsen, "Solution to problem E 2993: An application of Newton's formulae", *Amer. Math. Monthly* **93**:6 (1986), 483.

[AMM 2006] AMM, "Problems and solutions", *Amer. Math. Monthly* **113** (2006), 268.

[AMM 2008] S. Rabinowitz and NSA Problems Group, "Problems and solutions. Solutions: sometimes an integer: 11213(a)", *Amer. Math. Monthly* **115**:4 (2008), 366–367.

[Milne 2009] J. S. Milne, *Algebraic number theory* (version 3.00), 2009.

[Stewart and Tall 2002] I. Stewart and D. Tall, *Algebraic number theory and Fermat's last theorem*, 3rd ed., A K Peters, Natick, MA, 2002. MR 2002k:11001 Zbl 0994.11001

Received: 2010-07-19 Revised: 2011-02-01 Accepted: 2011-02-02

mudrock2@illinois.edu

Mathematics Department,
University of Illinois at Urbana-Champaign,
1409 West Green Street, Urbana, IL 61801, United States

involve

pjm.math.berkeley.edu/involve

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

The subscription price for 2011 is US $100/year for the electronic version, and $130/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2011 vol. 4 no. 2