For $n = 2$, $k \geq 3$, all pairs of nilpotent matrices satisfy (1), but not all nilpotent matrices of size 2 commute, e.g.,

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \text{and} \quad B = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}.$$

ACKNOWLEDGMENTS. We thank the referees for their useful remarks. This work has been supported in part by the Microsoft Research – INRIA Joint Centre and by Université Paris Diderot – Paris 7.

REFERENCES

1. S. H. Weintraub, *A Guide to Advanced Linear Algebra*, The Dolciani Mathematical Expositions, Vol. 44, MAA Guides, 6, Mathematical Association of America, Washington, DC, 2011.
2. M. Balaj, Romanian National Mathematical Olympiad, Problems and Solutions—11th grade, April 2011, available at http://www.onm2011.isjbihor.ro/subiecte/finala11_sol.pdf (in Romanian).

Algorithms Project, Inria Paris-Rocquencourt, 78153 Le Chesnay, France
Alin.Bostan@inria.fr

Observatoire de Paris, 77 Avenue Denfert-Rochereau, 75014 Paris, France
Combot@imcce.fr

Generalizing Gauss's Gem

Ezra Brown and Marc Chamberland

Abstract. Gauss's Cyclotomic Formula is extended to a formula with p variables, where p is an odd prime. This new formula involves the determinant of a circulant matrix. An application involving the Wendt determinant is given.

Gauss's Cyclotomic Formula [**3**, pp. 425–428, p. 467] is a neglected mathematical wonder.

Theorem 1 (Gauss). *Let p be an odd prime and set $p' = (-1)^{(p-1)/2}p$. Then there exist integer polynomials $R(x, y)$ and $S(x, y)$ such that*

$$\frac{4(x^p + y^p)}{x + y} = R(x, y)^2 - p'S(x, y)^2.$$

The goal of this note is to generalize this theorem. Denote a circulant matrix as

$$\operatorname{circ}(x_1, x_2, \ldots, x_p) = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_p \\ x_p & x_1 & x_2 & \cdots & x_{p-1} \\ x_{p-1} & x_p & x_1 & \cdots & x_{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{bmatrix}.$$

http://dx.doi.org/10.4169/amer.math.monthly.119.07.597
MSC: Primary 11C08

Let $\left(\frac{j}{p}\right)$ be the Legendre symbol, that is, for $j \not\equiv 0 \pmod p$, $\left(\frac{j}{p}\right) = 1$ or -1 according as j is or is not a quadratic residue mod p. A multivariable generalization of Theorem 1 follows. Theorem 1 is a special case of Theorem 2 with $x_3 = \cdots = x_p = 0$.

Theorem 2. *Let p be an odd prime and $p' = (-1)^{(p-1)/2}p$. Then there exist integer polynomials $R(x_1, x_2, \ldots, x_p)$ and $S(x_1, x_2, \ldots, x_p)$ such that*

$$\frac{4 \cdot \det(\operatorname{circ}(x_1, x_2, \ldots, x_p))}{x_1 + x_2 + \cdots + x_p} = R(x_1, x_2, \ldots, x_p)^2 - p' S(x_1, x_2, \ldots, x_p)^2.$$

Specifically, one can take $R(x_1, x_2, \ldots, x_p) = A + B$ and $S(x_1, x_2, \ldots, x_p) = (A - B)/\sqrt{p'}$ where

$$A = \prod_{\left(\frac{j}{p}\right)=1} (x_1 + \zeta^j x_2 + \zeta^{2j} x_3 + \cdots + \zeta^{(p-1)j} x_p),$$

$$B = \prod_{\left(\frac{j}{p}\right)=-1} (x_1 + \zeta^j x_2 + \zeta^{2j} x_3 + \cdots + \zeta^{(p-1)j} x_p),$$

and ζ is a primitive pth *root of unity.*

Proof. It is well-known [**4**] that

$$\frac{\det(\operatorname{circ}(x_1, x_2, \ldots, x_p))}{x_1 + x_2 + \cdots + x_p} = \prod_{j=1}^{p-1} (x_1 + \zeta^j x_2 + \zeta^{2j} x_3 + \cdots + \zeta^{(p-1)j} x_p). \qquad (1)$$

The choice of R and S given above then easily satisfy the desired equation,

$$\begin{aligned} R^2 - p'S^2 &= (A + B)^2 - p' \left(\frac{A - B}{\sqrt{p'}}\right)^2 \\ &= 4AB \\ &= 4 \prod_{j=1}^{p-1} \sum_{i=1}^{p} x_i \zeta^{j(i-1)} \\ &= \frac{4 \cdot \det(\operatorname{circ}(x_1, x_2, \ldots, x_p))}{x_1 + x_2 + \cdots + x_p}. \end{aligned}$$

The challenge now is to show that both R and S are polynomials with integer coefficients.

Let p be a prime > 3, let $p' = (-1)^{(p-1)/2}p$, let ζ be a primitive pth root of unity, and let $K = \mathbb{Q}(\zeta)$ be the cyclotomic field of pth roots of unity. For any integer k such that $1 \le k \le p - 1$, define the mapping σ_k on K by setting $\sigma_k(\zeta) = \zeta^k$ and extending the map linearly. Then K is a Galois extension of degree $p - 1$ over the rational field $\mathbb{Q}$ with cyclic Galois group $G = \{\sigma_k | 1 \le k \le p - 1\}$. G also acts on $\mathbb{Q}(\zeta)[x_1, \ldots, x_p]$ by setting $\sigma_k(x_i) = x_i$ and extending the action linearly; see [**2**, p. 596ff] for details and further information.

Let $\alpha = \sum_{(r/p)=1} \zeta^r$ and $\beta = \sum_{(n/p)=-1} \zeta^n$. A bit of algebra shows that $\beta = -\alpha - 1$ and $\alpha\beta = (1-p')/4$; thus, $\alpha = (-1 \pm \sqrt{p'})/2$ and $\beta = (-1 \mp \sqrt{p'})/2$, for some choice of signs. The set of mappings $H = \{\sigma_k | (k/p) = 1\}$ is a subgroup of G of index 2, whose fixed field is the quadratic field $\mathbb{Q}(\alpha)$. Note that both A and B are in $\mathbb{Z}(\zeta)[x_1, \ldots, x_p]$. We now show that $A + B \in \mathbb{Z}[x_1, \ldots, x_p]$ and that $A - B \in \mathbb{Z}(\alpha)[x_1, \ldots, x_p]$.

The product rule for the Legendre symbol states that if j and k are relatively prime to p then

$$\left(\frac{jk}{p}\right) = \left(\frac{j}{p}\right)\left(\frac{k}{p}\right).$$

Thus, if $\left(\frac{k}{p}\right) = 1$, then replacing ζ by ζ^k in A and B permutes the factors of A and the factors of B. Similarly, if $\left(\frac{k}{p}\right) = -1$, then replacing ζ by ζ^k in A and B exchanges the factors of A with the factors of B. It follows that if $\left(\frac{k}{p}\right) = 1$, then the action of σ_k on $\mathbb{Q}(\zeta)[x_1, \ldots, x_p]$ fixes both A and B, while if $\left(\frac{k}{p}\right) = -1$, then the action of σ_k on $\mathbb{Q}(\zeta)[x_1, \ldots, x_p]$ interchanges A and B. We conclude that $\sigma_k(A + B) = A + B$ for all k, so that $A + B$ is invariant under the action of every element of the Galois group G. Thus, the coefficients of $A + B$ lie in the fixed field of G, namely the rational field $\mathbb{Q}$, and so $A + B \in \mathbb{Q}[x_1, \ldots, x_p]$. But $A + B \in \mathbb{Z}(\zeta)[x_1, \ldots, x_p]$, so it follows that $R = A + B$ is a polynomial with integer coefficients.

We now turn to $S = (A - B)/\sqrt{p'}$. By previous results, the coefficients of A and B are in the field fixed by the index-2 subgroup H of the Galois group G, namely $\mathbb{Q}(\alpha)$. Since $A, B \in \mathbb{Z}(\zeta)[x_1, \ldots, x_p]$, it follows that both A and B are in $\mathbb{Z}(\alpha)[x_1, \ldots, x_p]$. Hence, there exist polynomials $f = f(x_1, \ldots, x_p)$ and $g = g(x_1, \ldots, x_p)$ with integer coefficients such that $A = f + g\alpha$.

Let n be a fixed quadratic nonresidue mod p. The nontrivial automorphism of $\mathbb{Q}(\alpha)$ sends α to β. As A is not fixed by σ_n, we see that $\sigma_n(\alpha) = \beta$. Hence,

$$B = \sigma_n(A) = \sigma_n(f + g\alpha) = f + g\beta.$$

It follows that $A - B = g(\alpha - \beta)$, where g has integer coefficients. Then, by previous work and a little more algebra, we see that $\alpha - \beta = \pm\sqrt{p'}$. It follows that

$$S = \frac{A - B}{\sqrt{p'}} = \frac{\pm g\sqrt{p'}}{\sqrt{p'}} = \pm g,$$

a polynomial with integer coefficients. ■

In the case when $p \equiv 1 \bmod 4$, the functions R and S given in Theorem 2 are not unique. The Pell equation

$$x^2 - py^2 = 1 \tag{2}$$

has infinitely many integer solutions for any prime p (see [**1**]). Since

$$(x_1^2 - py_1^2)(x_2^2 - py_2^2) = (x_1x_2 + py_1y_2)^2 - p(x_1y_2 + x_2y_1)^2,$$

any solution (x, y) to equation (2) may be used in conjunction with the solution (R, S) in Theorem 2 to produce another pair of polynomials

$$R' = xR + pyS, \quad S' = xS + yR.$$

which make Theorem 2 work. Indeed, infinitely many such R and S exist.

The polynomials R and S rapidly grow in size. For $p = 5$, one has

$$R = 2{x_1}^2 - x_2x_5 - x_5x_3 - x_2x_1 + 2{x_2}^2 - x_1x_3 - x_5x_4 - x_3x_2 - x_1x_4 \\ - x_2x_4 + 2{x_3}^2 + 2{x_5}^2 - x_1x_5 - x_4x_3 + 2{x_4}^2$$

and

$$S = -x_2x_4 - x_1x_4 + x_4x_3 + x_5x_4 - x_5x_3 + x_3x_2 + x_1x_5 - x_1x_3 + x_2x_1 - x_2x_5.$$

For $p = 7$, R has 84 terms and S has 56 terms.

A simple application of Theorem 2 involves a determinant considered by Wendt in conjunction with Fermat's Last Theorem. The so-called Wendt determinant is defined by

$$W_n = \det\left(\operatorname{circ}\left(\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}\right)\right).$$

E. Lehmer claimed (later proved by J.S. Frame [**5**, p.128]) that

$$W_n = (-1)^{n-1}(2^n - 1)u^2$$

for some $u \in \mathbb{N}$. Since

$$\sum_{k=0}^{n-1} \binom{n}{k} = 2^n - 1,$$

if n is an odd prime p, Theorem 2 implies

$$(2u)^2 = R^2 - p'S^2$$

for some integers u, R, and S. This equation clearly has a trivial solution if $S = 0$. This situation occurs when $p \equiv -1 \pmod 4$ since

$$\begin{aligned} B &= \prod_{\left(\frac{j}{p}\right)=-1} \left((1+\zeta^j)^p - 1\right) \\ &= \prod_{\left(\frac{j}{p}\right)=1} \left((1+\zeta^{-j})^p - 1\right) \\ &= \prod_{\left(\frac{j}{p}\right)=1} \left((1+\zeta^j)^p - 1\right) \\ &= A. \end{aligned}$$

The first few cases where $S \neq 0$ are

$$22^2 = 147^2 - 5 \cdot 65^2,$$
$$15431414598^2 = 20522387091091^2 - 13 \cdot 5691884464123^2,$$

$$1062723692434942886^2 = 895443706750215357146071 4^2 - 17 \cdot 217176999101512803520332 0^2$$

and

$$\begin{aligned} &871893957249629312559181905534122486670670255064527530 2^2 \\ &\quad = 880186691565639771602151953225868736277240996217998079037404740678842 7^2 \\ &\qquad -29 \cdot 163446565349221920232421758360000678245992119030883644603837566845152 5^2. \end{aligned}$$

REFERENCES

1. E. Barbeau, *Pell's Equation*. Springer, New York, 2003.
2. D. S. Dummit, R. M. Foote, *Abstract Algebra*, third edition. John Wiley, Hoboken, NJ, 2004.
3. C. F. Gauss, *Untersuchungen über höhere Arithmetik*. Translated from German by H. Maser. Chelsea, New York, 1965.
4. G. Golub, C. Van Loan, *Matrix Computations*, third edition, John Hopkins University Press, Baltimore, 1996.
5. P. Ribenboim, *Fermat's Last Theorem For Amateurs*. Springer, New York, 1999.

Department of Mathematics, Virginia Tech, Blacksburg, VA 24061,
ezbrown@math.vt.edu

Department of Mathematics and Statistics, Grinnell College, Grinnell, IA 50112,
chamberl@math.grinnell.edu

Norms as a Function of p Are Linearly Independent in Finite Dimensions

Greg Kuperberg

Abstract. We show that there are no non-trivial linear dependencies among p-norms of vectors in finite dimensions that hold for all p. The proof is by complex analytic continuation.

Theorem 1. *Let $v_1, v_2, \ldots, v_n$ be non-zero vectors with $v_k \in \mathbb{R}^{d_k}$. Suppose that*

$$\alpha_1 ||v_1||_p + \alpha_2 ||v_2||_p + \cdots + \alpha_n ||v_n||_p = 0 \tag{1}$$

for all $p \in [a, b]$ with $1 \leq a < b \leq \infty$. Then the equation is trivial in the following sense. Call two of the vectors equivalent if they differ by adding zeros, permuting or negating coordinates, and rescaling. Then the terms of (1) in each equivalence class, with the given coefficients, already sum to zero.

The result was stated as a question by Steve Flammia on MathOverflow.

http://dx.doi.org/10.4169/amer.math.monthly.119.07.601
MSC: Primary 46B07