Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 20 (1974)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: CONSTRUCTION OF GAUSS
Autor: Barnes, C. W.
DOI: https://doi.org/10.5169/seals-46891

A CONSTRUCTION OF GAUSS

by C. W. Barnes

1. Introduction

Every prime of the form $4n + 1$ can be expressed uniquely as the sum of two squares. Suppose $p = x^2 + y^2$ where p is a prime of the form $4n + 1$. A construction for x and y was given by Legendre [8] in terms of the continued fraction for $\sqrt{p}$. In [1] we gave a new construction for x and y, again using the continued fraction for $\sqrt{p}$. A summary of the various constructions is given in Davenport [5], pages 120-123.

Gauss [6] remarked that if $p = 4n + 1$, and if α and β are defined by $\beta \equiv \frac{(2n)!}{2(n!)^2} \pmod{p}$, $\alpha \equiv (2n)!\,\beta \pmod{p}$, where $|\alpha| < \frac{p}{2}$, $|\beta| < \frac{p}{2}$ then $p = \alpha^2 + \beta^2$; a particularly simple construction to state. Proofs of the construction of Gauss were given by Cauchy [4], page 414, and Jacobsthal [7]; however, neither of them is simple.

In the present note we give a simple proof of the construction of Gauss based on the method in [1].

2. Continued Fractions

We continue with the notation in [1]. The results we need can be found in Perron [9]. We denote the simple continued fraction

(1)
$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{\cdot}{\cdot \; \cdot \; + \cfrac{1}{a_n}}}}$$

by $[a_0, a_1, ..., a_n]$. For $0 \leq m \leq n$ we denote the numerator and denominator of the m^{th} approximant to $[a_0, a_1, ..., a_n]$ by A_m and B_m respectively.

If p is a prime of the form $4n + 1$, then

$$\sqrt{p} = [a_0, \overline{a_1, \ldots, a_m, a_m, \ldots, a_1, 2a_0}] \tag{2}$$

in the usual notation for a periodic continued fraction. The symmetric part of the period does not have a central term. In [1] we proved that $p = x^2 + y^2$ where

$$x = pB_mB_{m-1} - A_mA_{m-1} \tag{3}$$

$$y = A_m^2 - pB_m^2 \tag{4}$$

and where $\frac{A_m}{B_m}$ is the m^{th} approximant to (2). We also showed that

$$p = \frac{A_m^2 + A_{m-1}^2}{B_m^2 + B_{m-1}^2}. \tag{5}$$

3. The Quadratic Character of $\frac{(2n)!}{2(n!)^2}$.

It is well known that if p is a prime of the form $4n + 1$ then $\{(\frac{p-1}{2})!\}^2 \equiv -1 \pmod p$; that is, $(2n)!^2 \equiv -1 \pmod p$. We make use of this in the

Lemma. If $p = 4n + 1$ is a prime then $\frac{(2n)!}{2(n!)^2}$ is a quadratic residue of p.

Proof. We use Euler's criterion. Thus if we suppose that $\frac{(2n)!}{2(n!)^2}$ is a quadratic nonresidue of p we have $\{\frac{(2n)!}{2(n!)^2}\}^{\frac{p-1}{2}} \equiv -1 \pmod p$ and thus $\{(2n)!^2\}^{\frac{p-1}{4}} \equiv -\{2(n!)^2\}^{\frac{p-1}{2}} \pmod p$. Since $(2n)!^2 \equiv -1 \pmod p$ and $n!^{p-1} \equiv 1 \pmod p$ we have $(-1)^n \equiv -2^{\frac{p-1}{2}} \pmod p$, or $(-1)^{n+1} \equiv (-1)^{\frac{p^2+1}{8}}$, using the standard result for the quadratic character of 2 with respect to an odd prime. We finally get $(-1)^{n+1} \equiv (-1)^{2n^2+n}$ or $(-1)^{n+1} \equiv (-1)^n \pmod p$ which is a contradiction since p is an odd prime. Thus $\dfrac{(2n)\,!}{2\,(n\,!)^2}$ is a quadratic residue of p.

4. The Construction of Gauss

THEOREM. Suppose $p = 4n + 1$ is a prime and $p = x^2 + y^2$ where x and y are given by (3) and (4). Let β and α denote respectively the numerically smallest residues of $\dfrac{(2n)\,!}{2\,(n\,!)^2}$ and $(2n)\,!\,\beta$ modulo p, so that $|\,\alpha\,| < \dfrac{p}{2}$, $|\,\beta\,| < \dfrac{p}{2}$. Then $p = \alpha^2 + \beta^2$.

Proof. By (5) we have, using the remark at the beginning of section 3, $A_m^2 + A_{m-1}^2 \equiv 0 \pmod p$ and hence $-A_m^2 \equiv A_{m-1}^2 \pmod p$, so that $\{(2n)\,!\}^2 A_m^2 \equiv A_{m-1}^2 \pmod p$, and since p is a prime $(2n)\,!\,A_m \equiv \pm A_{m-1} \pmod p$. Supposing the negative sign holds we have $(2n)\,!\,A_m^2 \equiv -A_m A_{m-1} \pmod p$. Therefore we obtain $(2n)\,!\,A_m^2 - (2n)\,!\,pB_m^2 \equiv (pB_m B_{m-1} - A_m A_{m-1}) \pmod p$, so that by (3) and (4) we get

$$x \equiv (2n)\,!\,y \pmod p\,. \tag{6}$$

If the positive sign holds above it follows that $x \equiv -(2n)\,!\,y \pmod p$ which is just as good for our present purposes since we are not concerned with the signs of x and y. We will comment on the signs in section 5.

By the lemma we have $\left\{\dfrac{(2n)\,!}{2\,(n\,!)^2}\right\}^{\frac{p-1}{2}} \equiv 1 \pmod p$ so $(2n)\,!^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} (n\,!)^{p-1} \pmod p$, and therefore $(2n)\,!^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \pmod p$ since $(n\,!, p) = 1$. We have $x \equiv \pm (2n)\,!\,y \pmod p$, and since each of y and -1 is a quadratic residue of p, $x^{\frac{p-1}{2}} \equiv (2n)\,!^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \pmod p$, and in terms of the Legendre symbol it follows that $\left(\dfrac{x}{p}\right) = \left(\dfrac{2}{p}\right)$; that is, the quadratic character of x with respect to p is the same as the quadratic character of 2 with respect to p.

Suppose 2 is a quadratic residue of p. Then

$2^{\frac{p-1}{2}} (n\,!)^{p-1} (A_m A_m - 1)^{\frac{p-1}{2}} \equiv (A_m A_{m-1})^{\frac{p-1}{2}} \equiv (-x)^{\frac{p-1}{2}} \equiv x^{\frac{p-1}{2}} \equiv 1$ (mod p).

Next, if 2 is a quadratic nonresidue of p we have

$2^{\frac{p-1}{2}} (n\,!)^{p-1} (A_m A_{m-1})^{\frac{p-1}{2}} \equiv -(-x)^{\frac{p-1}{2}} \equiv -(x)^{\frac{p-1}{2}} \equiv -(-1) \equiv 1$ (mod p),

and we conclude that $2\,(n\,!)^2\, A_m A_{m-1}$ is a quadratic residue of p. By (3), (4), and (6) we have

$$(2n)\,!\, y \equiv -A_m A_{m-1} \pmod{p},$$

$$2\,(n\,!)^2\,(2n)\,!\, y \equiv -2\,(n\,!)^2\, A_m A_{m-1} \pmod{p}$$

and

$$-2\,(n\,!)^2\,(2n)\,!\, y \equiv b^2 \pmod{p}$$

for some quadratic residue b^2. Therefore

$$-2\,(n\,!)^2\,(2n)\,!\, y \equiv -(2n)\,!^2\, b^2 \pmod{p},$$

$$-2\,(n\,!)^2\, y \equiv -(2n)\,!\, b^2 \pmod{p},$$

and finally

$$y \equiv \frac{(2n)\,!}{2\,(n\,!)^2}\, b^2 \pmod{p}.$$

Hence by (6)

$$x \equiv \frac{(2n)\,!^2}{2\,(n\,!)}\, b^2 \pmod{p}.$$

Let $b^2 \equiv r$ (mod p), $|\,r\,| < \frac{p}{2}$, so that $(r, p) = 1$. Then in terms of α, β, and r, $x \equiv \alpha\, r$ (mod p) and $y \equiv \beta\, r$ (mod p). There are unique integers K and L such that $x = \alpha\, r + K p$, $y = \beta\, r + L\, p$. Then

$$x^2 + y^2 = (\alpha^2 + \beta^2)\, r^2 + (K^2 + L^2)\, p^2 + 2rp\,(\alpha K + \beta L),$$

or

$$p = (\alpha^2 + \beta^2)\, r^2 + (K^2 + L^2)\, p^2 + 2rp\,(\alpha K + \beta L).$$

Suppose that $|\,r\,| > 1, K \neq 0$, and $L \neq 0$. The last equation can be written

(7) $\quad pK^2 + (2r\alpha p)\,K + \{\,L^2p^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p\,\} = 0\,.$

Since (7) is a quadratic in K and we are supposing that the integral root is not zero we have

$$K \mid \{\,L^2p^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p\,\}\,.$$

There is an integer t such that

$$L^2p^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p = Kt$$

and therefore (7) vanishes when

$$K = \frac{L^2p^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p}{t}\,.$$

That is

$$\begin{aligned}(8)\qquad &\{\,L^2p^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p\,\}\,\{\,t^2 + 2r\alpha pt \\ &\quad + p\,\{\,L^2p^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p\,\}\} = 0\end{aligned}$$

The discriminant of the quadratic function

$$t^2 + 2r\alpha pt + p\,\{\,p^2L^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p\,\}$$

is $4\,p^2\,\{\,p - (pL+\beta r)^2\,\}$ which is not zero. It follows that the second factor in (8) cannot be zero; otherwise we would have two distinct integral values for t giving rise to two distinct integers K, whereas K is unique. Hence we have

$$(9)\qquad p^2L^2 + 2r\beta pL + (\alpha^2+\beta^2)\,r^2 - p = 0$$

and since we are supposing that $L \neq 0$, we see that

$L \mid \{\,(\alpha^2+\beta^2)\,r^2 - p\,\}$ so that for an integer u we have $(\alpha^2+\beta^2)\,r^2 - p = L\,u$ and (9) vanishes when

$$L = \frac{(\alpha^2+\beta^2)\,r^2 - p}{u}\,,$$

so that

(10) $\{\,(\alpha^2+\beta^2)\,r^2 - p\,\}\,\{\,u^2 + 2r\beta pu + p^2\,\{\,(\alpha^2+\beta^2)\,r^2 - p\,\}\} = 0\,.$

As before we consider the quadratic function

$$u^2 + 2r\beta pu + p^2\,\{\,(\alpha^2+\beta^2)\,r^2 - p\,\}$$

The discriminant is $4p^2(p-\alpha^2 r^2)$ which cannot vanish, so that, as before, the first factor in (10) must be zero, and we have

$$(\alpha^2+\beta^2)\,r^2 - p = 0 \tag{11}$$

which is a contradiction since $\alpha^2 + \beta^2 > 1$ and we are supposing that $|r| > 1$.

Therefore we cannot have $|r| > 1, K \neq 0$, and $L \neq 0$. If $|r| = 1$ we see that $K = L = 0$ since $|x - \alpha r| < p$ and $|y - \beta r| < p$ in this case. If $|r| > 1$ with $K = L = 0$ we would have $x = \alpha r$, $y = \beta r$ and hence $(x, y) > 1$, whereas x and y are relatively prime. Finally it remains to consider the possibility of having $|r| > 1$ with one of K and L zero, the other nonzero. This if we suppose that $|r| > 1$, $K = 0$, $L \neq 0$, we obtain (9) which, as we have seen, leads to a contradiction. On the other hand the supposition that $|r| > 1$ with $K \neq 0$, $L = 0$ implies that (11) would hold with $r^2 > 1$.

We conclude that $|r| = 1$, $K = 0$ and $L = 0$. Hence $x = \pm\alpha$, $y = \pm\beta$ and $\alpha^2 + \beta^2 = p$.

In [1], Corollary 2, we observed that if $p = x^2 + y^2$ then, in our notation, y is a quadratic residue of p. Collecting our results we have the

Corollary. Let $p = x^2 + y^2$ where p is a prime of the form $4n + 1$ with x and y given by (3) and (4). Then $\left(\frac{x}{p}\right) = \left(\frac{2}{p}\right)$ and $\left(\frac{y}{p}\right) = 1$.

5. Conclusion

We saw that $x = \pm\alpha$, $y = \pm\beta$. When $p = 13$ we have $y = -3$, $\beta = -3$; when $p = 29$, $y = -5$, $\beta = 5$, and when $p = 41$, $y = 5$, $\beta = 5$. Hence the sign of y, determined by the approximants to a continued fraction depends on the integer m, the number of terms in the finite segment of (2) which is used, can agree with that of β or be opposite that of β. The same applies to x and α. In [1], Theorem 1, we gave a construction which always gives positive values for x and y. Other various constructions, as we have seen, do not have this property.

Finally we comment on the numbers $\dfrac{(2n)!}{2(n!)^2}$ which we denote by a_n for $n = 1, 2, 3, \ldots$.

The members of the sequence $\{ a_n \}$ are related to the numbers $b_{n+1} = \frac{(2n)!}{(n+1)!\,n!}$, $n = 0, 1, 2, \ldots$, which, as mentioned by Becker [2], have a variety of applications. Birkhoff [3] pointed out that b_n is an integer for every positive integer n, and noted the recurrence relation $b_n = \sum_{i=1}^{n-1} b_i b_{n-i}$; a relation which was also obtained by Wedderburn [10].

The results of this note depend on the fact that a_n is an integer, at least when $p = 4n + 1$ is a prime. Although it is known that a_n is an integer for every positive integer n, we can see that this also follows readily from [3]. For we have $2a_n = (n+1)\,b_{n+1}$. If n is even, it follows that b_{n+1} is even since $(2, n+1) = 1$. Therefore $a_n = (n+1)\frac{b_{n+1}}{2}$ is an integer. If n is odd then $2 \mid (n+1)$ and in this case also $a_n = \frac{n+1}{2} b_{n+1}$ is an integer. A list of values for a_n can be obtained from the second column of a table in [2], page 699, headed N_n, by multiplying the $(n+1)$st member by $\frac{n+1}{2}$.

REFERENCES

[1] Barnes, C. W. The Representation of Primes of the Form $4n + 1$ as the Sum of Two Squares, *L'Enseignement Mathématique, 18* (1972), pp. 289-299.

[2] Becker, H. W. Discussion of Problem 4277, *American Mathematical Monthly, 56* (1949), pp. 697-699.

[3] Birkhoff, Garrett. Problem 3674, *American Mathematical Monthly, 42* (1935), pp. 518-521.

[4] Cauchy, A. *Sur les Formes quadratiques de certaines Puissances des Nombres Premiers ou du quadruple de ces Puissances,* Œuvres complètes 1re série, tome 3, pp. 390-437.

[5] Davenport, H. *The Higher Arithmetic,* Hutchinson's University Library, London, 1952.

[6] Gauss, C. F. Werke Bd. 2, S. 90-91.

[7] Jacobsthal, Ernst. Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe Zweier Quadrate, *Journal für die Reine und Angewandte Mathematik,* Band 132, (1907), pp. 238-245.

[8] Legendre, A. M. *Théorie des Nombres.* Troisième édition, Paris, 1830.

[9] Perron, Oskar. *Die Lehre von den Kettenbrüchen.* Chelsea, New York, 1951.

[10] Wedderburn, J. H. M. The Functional Equation $g(x^2) = 2\alpha x + [g(x)]^2$, *Annals of Mathematics, (2), 24,* (1922-1923), pp. 121-140.

(Reçu le 1er mai 1973)

C. W. Barnes
Department of Mathematics
University of Mississippi
Mississippi, 38677, USA

vide-leer-empty