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.
Kapitel: 3. The Quadratic Character of $\frac{(2n)!}{2(n!)^2}$
DOI: https://doi.org/10.5169/seals-46891

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 13.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

by $[a_0, a_1, \ldots, a_n]$. For $0 \leq m \leq n$ we denote the numerator and denominator of the mth approximant to $[a_0, a_1, \ldots, a_n]$ 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 $\dfrac{A_m}{B_m}$ is the mth 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 $\dfrac{(2n)!}{2(n!)^2}$ is a quadratic residue of p.

Proof. We use Euler's criterion. Thus if we suppose that $\dfrac{(2n)!}{2(n!)^2}$ is a quadratic nonresidue of p we have $\left\{\dfrac{(2n)!}{2(n!)^2}\right\}^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 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 res-

pect 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 $\frac{(2n)!}{2(n!)^2}$ 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 $\frac{(2n)!}{2(n!)^2}$ and $(2n)!\,\beta$ modulo p, so that $|\alpha| < \frac{p}{2}$, $|\beta| < \frac{p}{2}$. 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 $\left\{\frac{(2n)!}{2(n!)^2}\right\}^{\frac{p-1}{2}} \equiv 1 \pmod p$ 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 $\left(\frac{x}{p}\right) = \left(\frac{2}{p}\right)$; 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