

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: 2. Continued Fractions
DOI: <https://doi.org/10.5169/seals-46891>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. 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. [Siehe Rechtliche Hinweise.](#)

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. [Voir Informations légales.](#)

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. [See Legal notice.](#)

Download PDF: 03.04.2025

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

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

$$(1) \quad a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n}}}$$

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

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

$$(2) \quad \sqrt{p} = [a_0, \overline{a_1, \dots, a_m, a_m, \dots, a_1}, 2a_0]$$

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

$$(3) \quad x = pB_m B_{m-1} - A_m A_{m-1}$$

$$(4) \quad y = A_m^2 - pB_m^2$$

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

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

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 $\left\{ \left(\frac{p-1}{2} \right)! \right\}^2 \equiv -1 \pmod{p}$; 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 $\left\{ \frac{(2n)!}{2(n!)^2} \right\}^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and thus $\left\{ (2n)!^2 \right\}^{\frac{p-1}{4}} \equiv - \left\{ 2(n!)^2 \right\}^{\frac{p-1}{2}} \pmod{p}$. 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-