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

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

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots + \cfrac{1}{a_n}}}} \tag{1}$$

by $[a_0, a_1, ..., a_n]$. For $0 \leqq m \leqq n$ 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

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

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 res-