

4. The Construction of Gauss

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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 $(2n)! A_m^2 - (2n)! p B_m^2 \equiv (p B_m B_{m-1} - A_m A_{m-1}) \pmod{p}$, so that by (3) and (4) we get

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

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

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

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

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

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)

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

Let $b^2 \equiv r \pmod{p}$, $|r| < \frac{p}{2}$, so that $(r, p) = 1$. Then in terms of α ,

β , and r , $x \equiv \alpha r \pmod{p}$ and $y \equiv \beta r \pmod{p}$. There are unique integers K and L such that $x = \alpha r + Kp$, $y = \beta r + Lp$. 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

$$(8) \quad \{L^2p^2 + 2r\beta pL + (\alpha^2 + \beta^2)r^2 - p\} \{t^2 + 2r\alpha pt + p\{L^2p^2 + 2r\beta pL + (\alpha^2 + \beta^2)r^2 - p\}\} = 0$$

The discriminant of the quadratic function

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

is $4p^2\{p - (pL + \beta r)^2\}$ 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

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

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 $(\alpha^2 + \beta^2)r^2 - p = Lu$ and (9) vanishes when

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

so that

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

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

$$(11) \quad (\alpha^2 + \beta^2)r^2 - p = 0$$

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 $\frac{(2n)!}{2(n!)^2}$ which we denote by a_n for $n = 1, 2, 3, \dots$