Gauss: The Last Entry

by Frans Oort*

Introduction

We present one of the shortest examples of a statement with a visionary impact: we discuss an expectation by Gauss. His idea preludes developments only started more than a century later. Several proofs were given for the prediction by Gauss. We show where this statement fits into modern mathematics. We give a short proof, using methods, developed by Hasse, Weil and many others. Of course this is history upside down: instead of seeing the Last Entry as a prelude to modern developments, we give a 20-th century proof of this 19-th century statement.

I thank Norbert Schappacher for discussions and suggestions on this topic.

(1) Carl Friedrich Gauss (1777–1855) kept a mathematical diary (from 1796). The last entry he wrote was on 7 July 1814. A remarkable short statement.

Observatio per inductionem facta gravissima theoriam residuum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta, si $a + bi$ est numerus primus, $a - 1 + bi$ per $2 + 2i$ divisibilis, multitudo omnium solutionum congruentiae $1 = x x + y y + x y y$ (mod $a + bi$) inclusis $x = \infty$, $y = \pm i$, $x = \pm i$, $y = \infty$ fit $= (a - 1)^2 + bb$.

The text of the “Tagebuch” was rediscovered in 1897 and edited and published by Felix Klein, see [9], with the Last Entry on page 33. A later publication appeared in [5]. For a brief history see [6], page 97. In translation:

A most important observation made by induction which connects the theory of biquadratic residues most elegantly with the lemniscatic functions. Suppose, if $a + bi$ is a prime number, $a - 1 + bi$ divisible by $2 + 2i$, then the number of all solutions of the congruence $1 = x x + y y + x y y$ (mod $a + bi$) including $x = \infty$, $y = \pm i$, $x = \pm i$, $y = \infty$, equals $(a - 1)^2 + bb$.

Remarks. In the original we see that Gauss indeed used the notation $xx$, as was used in his time. In [4] for example we often see that $x^2$ and $x'x'$ are used in the same formula.

The terminology “Tagebuch” used, with subtitle “Notizenjournal”, is perhaps better translated by “Notebook” in this case. In the period 1796–1814 we see 146 entries, and, for example, the Last Entry is the only one in 1814. Gauss wrote down discoveries made. The first entry on 30 March 1796 is his famous result that a regular 17-gon can be constructed by ruler and compass.

A facsimile reproduction and a transcript we find in [5].

(2) We phrase the prediction by Gauss in other terms. We write $\mathbb{F}_p = \mathbb{Z}/p$ for (the set, the ring) the field of integers modulo a prime number $p$. Suppose $p \equiv 1$ (mod 4). Once $p$ is fixed we write

$$N = \# \{(x,y) \in \mathbb{F}_p \mid 1 = x^2 + y^2 + x^2 y^2\} + 4.$$ 

A prime number $p$ with $p \equiv 1$ (mod 4) can be written as a sum of two squares of integers (as Fermat predicted, possibly proved by Fermat, and as proved by Euler). These integers are unique up to sign and up to permutation. Suppose we write

$$p = a^2 + b^2,$$

with $b$ even and $a - 1 \equiv b$ (mod 4); this fixes the sign of $a$. In this case Gauss predicted

$$N = (a - 1)^2 + b^2$$

for every $p \equiv 1$ (mod 4).

(3) Some history. In [9] we find the original formulation edited and published by Klein. In [7] we find the first proof for this expectation by Gauss. More historical details and descriptions of the Last Entry can be found in [14]; [10]; Chapter 10; [3], page 86; [8], 11.5.
We see the attempt and precise formulation of Gauss of this problem as the pre-history and a prelude of the Riemann hypothesis in positive characteristic as developed by E. Artin, F. K. Schmidt, Hasse, Deuring, Weil and many others; a historical survey and references can be found in [12] and [11].

(4) We give some examples. For \( p = 5 \) we obtain \( a = -1 \), and \( b = \pm 2 \) and \( N = 8 \). Indeed, \( (x = \pm 1, y = \pm 1) \) are the only solutions for \( y^2 = x(x-1)(x+1) \) (see Proposition 2(a) for an explanation).

We easily show that \( \#(E_{13}) = 8 \), as predicted by Gauss.

For \( p = 17 \) we obtain \( a = +1 \) and \( b = \pm 4 \) and \( N = 16 \). Here are the 12 solutions of \( y^2 = x(x-1)(x+1) \): the point 0, the three 2-torsion points and \( x = 4, 5, 7, 10, 12, 13 \); the points \( (x = 4, y = \pm 3) \) and \( (x = 13, y = \pm 5) \) we will encounter below as \( (x = -e, y = 1 + e) \) with \( e^2 = -1 \).

We explain below in which way the condition “divisible by 2 + 2\( n \)” mentioned by Gauss enters the discussion, and in which way, once \( p \equiv 1 \) (mod 4) is fixed, this determines the choice of \( a \). Also we explain the four values “at infinity” as observed by Gauss.

(5) Notation. In this paper we consider fields of characteristic zero or of characteristic \( p \neq 2 \). We will consider an elliptic curve denoted by \( E_K \) once a base field \( K \) is given, to be described below. These base fields will be \( \mathbb{Q} \), \( \mathbb{Q}(\sqrt{-T}) \) or \( \mathbb{F}_p \). The equation \( 1 = XX + YY + XXXY \) studied by Gauss gives a nonsingular, affine curve and the corresponding projective curve
\[
\mathcal{Z}(Z^4 + X^2Z^2 + Y^2Z^2 + X^2Y^2) \subset \mathbb{P}^2
\]
has two singularities at infinity, both ordinary double points; it follows that the normalization has genus one (we will make this explicit below); moreover the curve does have rational points, e.g. \( (x = 0, y = \pm 1) \), hence \( E \) is an elliptic curve:

the curve \( E \) minus a finite set of points will be an affine curve isomorphic with the curve
\[
\mathcal{Z}(-1 + X^2 + Y^2 + X^2Y^2) \subset \mathbb{A}^2,
\]
where \( \mathcal{Z}(-) \) stands for the set of zeros.

When saying for example “\( E \) is given by \( Y^2 = X^3 + 4X \)”, we intend to say that \( E \) is this unique projective, non-singular curve containing this affine curve; in this case we see that

\[
E = \mathcal{Z}(-Y^2Z + X^3 + 4XZ^2) \subset \mathbb{P}^2
\]
over any field of characteristic not equal to 2.

We see in the statement by Gauss four points “at infinity”. Here is his explanation. Consider the projective curve
\[
C = \mathcal{Z}(-Z^4 + X^2Z^2 + Y^2Z^2 + X^2Y^2) \subset \mathbb{P}^2
\]
over a field \( K \) of characteristic not equal to 2. For \( Z = 0 \) we have points \( P_2 = [x = 0 : y = 1 : z = 0] \) and \( P_3 = [x = 1 : y = 0 : z = 0] \). Around \( P_2 \) we can use a local chart given by \( Y = 1 \), and \( \mathcal{Z}(-Z^4 + X^2Z^2 + Z^2 + X^2) \); we see that the tangent cone is given by \( \mathcal{Z}(Z^2 + X^2) \) (the lowest degree part); hence we have a ordinary double point, rational over the base field \( K \) and the tangents to the two branches are conjugate if \(-1 \) is not a square in \( K \), respectively given by \( X = \pm Z \) with \( e^2 = -1 \) in \( L \).

This is what Gauss meant by \( x = \infty \), \( y = \pm i \). Analogously for \( P_3 \) and \( y = \infty \), \( x = \pm i \).

Explanation. Any algebraic curve (an absolutely reduced, absolutely irreducible scheme of dimension one) \( C \) over a field \( K \) is birationally equivalent over \( K \) to a non-singular, projective curve \( C' \), and \( C' \) is uniquely determined by \( C \). The affine curve \( \mathcal{Z}(-1 + X^2 + Y^2 + X^2Y^2) \subset \mathbb{A}^2_K \), over a field \( K \) of characteristic not equal to 2 determines uniquely a curve, denoted by \( E_K \) in this note. This general fact will not be used: we will construct explicit equations for \( E_K \) (over any field considered) and for \( E_L \) over a field with an element \( e \in L \) satisfying \( e^2 = -1 \).

In the present case, we write \( C \subset \mathbb{P}^2_K \) as above (the projective closure of the curve given by Gauss), \( E \) for the normalization. We have a morphism \( h : E \to C \) defined over \( K \). On \( E \) we have a set \( S \) of 4 geometric points, rational over any field \( L \supset K \) in which \(-1 \) is a square, such that the induced morphism
\[
E \setminus S \to \mathcal{Z}(-1 + X^2 + Y^2 + X^2Y^2) \subset \mathbb{A}^2_K
\]
is an isomorphism.

(6) Normal forms.

Proposition 1. Suppose \( K \) is a field of characteristic not equal to 2.

(a) The elliptic curve \( E \) can be given by \( Y^2 = 1 - X^4 \).

(b) The elliptic curve \( E \) can be given by \( U^2 = V^3 + 4V \).

(c) There is a subgroup \( \mathbb{Z}/4 \to E(K) \).

Proof. (a) From \( 1 = X^2 + Y^2 + X^2Y^2 \) we see
\[
\frac{1 - X^2}{Y^2} = 1 + X^2, \quad \text{and we write } T = \frac{1 - X^2}{Y}.
\]

(b) Starting from \( T^2 = 1 - X^4 \) with the substitutions
\[
U = \frac{(V + 2)^2 T}{4}, \quad X = \frac{V - 2}{V + 2} \quad \text{we arrive at } U^2 = V^3 + 4V.
\]

(c) The point \( P := (v = 2, u = 4) \) is on the curve \( \mathcal{Z}(-U^2 + V^3 + 4V) \); the line \( U = 2V \) passes through \((0, 0)\), a 2-torsion point, and substituting \( U = 2V \) we obtain: \((-25)^2 + S^2 + 4S = S(S - 2)^2 \), hence this line is tangent at \( P \), hence \( 2P \) is 2-torsion, hence \( P \) is a 4-torsion point.

\]

Explanation. Starting with the equation given by Gauss we take the \( 2 : 1 \) covering given by \( 1/Y \), and
Remark. We see that two rational branch points: \( x = \pm 1 \). We see that \((x = \pm 1, y = 0)\) correspond with \((x = \pm 1, t = 0)\) and \((x = 0, y = \pm 1)\) with \((x = 0, t = \pm 1)\). See [17], page 298.

We take one of these, the point with \( x = 1 \) and make a coordinate change transporting this to infinity in the \( \mathbb{Z} \)-coordinate, and make a further coordinate change in order to obtain this Weierstrass equation; this gives (b). The point \((x = 1, y = 0)\) gives \( v = \infty \) and \((x = -1, y = 0)\) gives \( (v = 0, u = 2) \). For \( x = 0 \) we obtain \( v - 2v + 2 = 0 \) hence \( v = 2 \) and \( u = \pm 4 \).

In this form (c), or in the form in (b), we recognize that the 4 obvious zeros \((x = \pm 1, y = 0), (x = 0, y = \pm 1)\) in the equation in (a) give a subgroup cyclic of order 4.

**Proposition 2.** Suppose \( L \) is a field of characteristic not equal to 2. Suppose there is an element \( e \in L \) with \( e^2 = -1 \).

(a) The elliptic curve \( E_L \) can be given by \( y^2 = X(X - 1)(X + 1) \).

(b) There is a subgroup \((\mathbb{Z}/4 \times \mathbb{Z}/2) \hookrightarrow E(L)\).

We will study this in case either \( L = \mathbb{Q}(\sqrt{-1}) \) or \( L = \mathbb{F}_p \) with \( p \equiv 3 \pmod{4} \) (as Gauss did in his Last Entry).

**Proof.** (a) Note that in \( L \) we have

\[
(1 + e)^2 = 2e; \quad \text{hence } ((1 + e)^3)^2 = (2e)^3. 
\]

Starting from \( U^2 = V^3 + 4V \), hence \( U^2 = V(V + 2e)(V - 2e) \), after dividing by \( (2e)^3 \), we write \( V/(2e) = X \) and \( Y = U/(1 + e)^3 \) and arrive at \( Y^2 = X(X - 1)(X + 1) \).

(b) There is a 4-torsion point, see Proposition 1(c); in fact \((x = -e, y = 1 + e) \in L^2 \) is such a point. Also all 2-torsion points are rational over \( L \), and we arrive at the conclusion (b).

**Explanation.** Starting from \( U^2 = V^3 + 4V \) as in Proposition 1(b) we see that over \( L \) all 2-torsion is rational and we change the Weierstrass form to a Legendre normal form by moving the branch points to \(-1, 0, +1\) and observing that we can already make the necessary coordinate change over \( L \).

**Remark.** We see that \( E_L \) defined by \( U^2 = V^3 + 4V \) has complex multiplication by \( \sqrt{-1} \) given by the map \( v \mapsto -v, u \mapsto eu \) with \( e \in L \) with \( e^2 = -1 \). Tracing back through the coordinate transformations this gives on the equation as proposed by Gauss, with \((x = +1, y = 0)\) as zero-point on \( E \), the transformation

\[
1 = x^2 + y^2 + x^2 y^2, \quad x = \frac{v - 2}{v + 2} \mapsto \frac{-v - 2}{v + 2} = \frac{1}{x}, \quad y \mapsto eu. 
\]

(7) The case \( p \equiv 3 \pmod{4} \) (not mentioned by Gauss).

**Theorem 3.** The elliptic curve \( E \) over \( \mathbb{F}_p \) with \( p \equiv 3 \) (mod 4) has:

\[
\#(E(\mathbb{F}_p)) = p + 1. 
\]

**First proof.** The elliptic curve \( E \) can be given by the equation \( Y^2 = X^3 + 4X \). We define \( E' \) by the equation \(-Y^2 = X^3 + 4X \). We see:

\[
\#(E(K)) + \#(E'(K)) = 2p + 2; \quad E \equiv_K E'. 
\]

Indeed, any \( x \in \mathbb{P}^1(K) \) giving a 2-torsion point contributes +1 to both terms, and any possible \((x, \pm y)\) with \( y \neq 0 \) contributes +2 to exactly one of the terms. The substitution \( X \mapsto -X \) shows the second claim. Hence \( \#(E(K)) = (2p + 2)/2 \).

**Second proof.** Partly taken from [10], page 318. We note that \( E \) can be given by the equation as in Prop. 1(a). We write

\[
\begin{align*}
C^0 &= \mathbb{Z}(-Y^2 + 1 - X^4) \subset \mathbb{A}^2, \\
D^0 &= \mathbb{Z}(-Y^2 + 1 - X^4) \subset \mathbb{A}^2 \\
D &= \mathbb{Z}(-Y^2 + 1) \subset \mathbb{A}^2.
\end{align*}
\]

**Lemma.** The images

\[ 2\exp(\mathbb{F}_p) = 4\exp(\mathbb{F}_p) \]

are equal.

Here \( a \exp \) stands for the map \( x \mapsto x^a \), and here \( p \equiv 3 \pmod{4} \). Note that \((p - 1)/2 \) is odd.

**Proof of the Lemma.** The isomorphism

\[
((\mathbb{F}_p)^*, +) \cong (\mathbb{Z}/(p - 1), +) \cong (\mathbb{Z}/2) \times (\mathbb{Z}/((p - 1)/2))
\]

translates \( a \exp \) in multiplication by \( a \). Both under \( 2 \exp \) and \( 4 \exp \) the image is \( \{0\} \times \mathbb{Z}/((p - 1)/2) \).

We have:

Step one;

\[ E(\mathbb{F}_p) = C^0(\mathbb{F}_p). \]

The transformation \( Y = \eta/\xi^2 \) and \( X = 1/\xi \) gives the model \( \eta^2 = \xi^4 - 1 \). Hence the points \( \xi = 0, \eta^2 = 1 \) are not rational over \( \mathbb{F}_p \).

Step two;

\[ \#(C^0(\mathbb{F}_p)) = \#(D^0(\mathbb{F}_p)). \]

This follows from the lemma.

Step three;

\[ D^0(\mathbb{F}_p) = D(\mathbb{F}_p). \]

Analogous proof as in Step one.

Step four;

\[ \#(D(\mathbb{F}_p)) = p + 1. \]

Over any field \( L \) a conic \( D \) with a rational point we have a bijection \( D(L) = L \cup \{\infty\}. \)
Note that $\mathbb{Z}/4 \cong E(\mathbb{F}_3)$ and $\mathbb{Z}/4 \not\subseteq E(\mathbb{F}_p)$ for $p > 3$.

It is not difficult to show that $E(\mathbb{Q}) \cong \mathbb{Z}/4$.

(8) Frobenius and formulas. We recall some theory developed by Emil Artin, F. K. Schmidt, Hasse, Deuring, Weil and many others, now well-known, and later incorporated in the general theory concerning "the Riemann Hypothesis in positive characteristic"; for a survey of the history, and for references see [12] and [11]. For proofs in the case of elliptic curves used and described here one can consult [15]. Notions in this section are not fully explained nor documented here.

The Frobenius morphism. For a variety $V$ over a field $\mathbb{F}$ we construct $V^{(p)}$ over $\mathbb{F}$ instead of defining polynomials $\alpha a_i x_i$ (multi-index notation, local equations) for $V$ we use the polynomials $\Sigma a_i x_i$ in order to define $V^{(p)}$. There exists a morphism

$$\text{Frob} = F : V \rightarrow V^{(p)},$$

defined by "raising all coordinates to the power $p$". Note that if $(x_\alpha | \alpha)$ is a zero of $f = \Sigma a_i x_i$, then indeed $(x_\beta | \alpha)$ is a zero of $\Sigma a_i x_i$, because

$$f(x)^p = (\Sigma a_i x_i)^p = \Sigma a_i x_i^p.$$

Suppose $\mathbb{F} = \mathbb{F}_q$ with $q = p^n$. Then there is an identification $V^{(p)} = V$, and the $n$-times repeated Frobenius morphism gives:

$$F^n = \text{Frob}_V : V \rightarrow V^{(p^n)} = \left( \pi : V \rightarrow V^{(p)} \rightarrow V^{(p^2)} \rightarrow \ldots \rightarrow V^{(p^n)} = V \right).$$

This morphism was considered by Hasse in 1930. In the case in this note we only consider $\mathbb{F}_p$, i.e. $n = 1$ and $F = \pi$.

A little warning. The morphism $\pi : V \rightarrow V$ induces a bijection $\pi(k) : V(k) \rightarrow V(k)$ for every algebraically closed field $k \supset \mathbb{F}_q$; however (in case the dimension of $V$ is at least one) $\pi : V \rightarrow V$ is not an isomorphism.

Here is where the central idea starts: note that the map $x \mapsto x^q$ is the identity on $\mathbb{F}_q$, and the set of fixed points of this map on any field $k \supset \mathbb{F}_q$ is exactly the subset $\mathbb{F}_q$.

Along these lines one shows that sets of invariants (fixed points) of $\pi(k) : V(k) \rightarrow V(k)$ is exactly the set of rational points $V(\mathbb{F}_q)$. On an elliptic curve $V = E$, using the addition, we see that

$$\text{Ker} (\pi - 1 : E \rightarrow E) = E(\mathbb{F}_q).$$

We can consider $\pi \in \text{End}(E)$ as a complex number. A small argument shows that

$$\text{Norm}(\pi - 1) = \#(E(\mathbb{F}_q)) = N.$$

Moreover for the complex conjugate $\overline{\pi}$ we have $\pi \cdot \overline{\pi} = q$. Write $\beta := \pi + \overline{\pi}$, the trace of $\pi$. We see that $\beta$ is a zero of

$$T^2 - \beta T + q,$$

$$N = \text{Norm}(\pi - 1) = (\pi - 1)(\overline{\pi} - 1) = 1 - \beta + q;$$

$$|\beta| = \sqrt{q}.$$

This is the first form of the characteristic $p$ analogue of the Riemann Hypothesis for elliptic curves; the proof above is the second proof by Hasse (in 1934) for elliptic curves, generalized by Weil for curves of arbitrary genus, for abelian varieties, and further generalized in the Weil conjectures, and proved by Grothendieck, Deligne and many others; for a survey and references see [12], [11].

Remark. Not used in this note. Suppose $C$ is an elliptic curve over $K = K_1 = \mathbb{F}_q$ with $\text{Frob}_C/\mathbb{F}_p = \rho$. For every $m \in \mathbb{Z}_{>0}$ we can compute the number of rational points on $C$ over $K_m := \mathbb{F}_q^m$ by:

$$\#(C(K_m)) = \text{Norm}(\rho^m - 1).$$

The statements usually indicated by "the Riemann hypothesis in positive characteristic" I tend to indicate by pRH, in order to distinguish this from the classical Riemann hypothesis RH. For any elliptic curve $C$ over a finite field $\mathbb{F}_q$ one can define its zeta function (as can be done for more general curves, and more general varieties over a finite field). As E. Artin and F. K. Schmidt showed, for an elliptic curve we have

$$\zeta(C, T) = \frac{(1 - \rho T)(1 - \overline{\rho} T)}{(1 - T)(1 - q T)}.$$

As is usual, the variable $s$ is defined by $T = q^{-s}$. The theorem proved by Hasse is

$$|\rho| = \sqrt{q}; \quad \text{this translates into } s = \frac{1}{2} \quad \text{(pRH)},$$

and we see the analogy with the classical RH, which explains the terminology pRH.

Third proof of Theorem 3. (But not all concepts used are explained). A prime number $p \equiv 3 \pmod{4}$ is inert in $\mathbb{Z}[i] = \text{End}(E_K)$; write $K = \mathbb{F}_p$. This implies that $E_K$ is supersingular. Its Frobenius homomorphism $\pi = \text{Frob}_{E/K}$ is a zero of $T^2 - \beta T + p \in \mathbb{Z}[T]$. In the supersingular case we know that $p$ divides $\beta$. As $p > 2$ and $\beta^2 - 4p \leq 0$ we conclude either $\beta = 0$ or $p = 3$ and $\beta = \pm 3$. The last case would imply $N = 1 - 3 + 3 = 1$ or $N = 1 + 3 + 3 = 7$, in contradiction with the fact that $E$ has a $K$-rational 2-torsion point. Hence $\beta = 0$ and

$$N = \#(E(K)) = 1 - \beta + p = p + 1.$$

(9) A proof for the statement by Gauss in his Last Entry. We analyze the condition

$$N = \#(E(K)) = 1 - \beta + p = p + 1.$$

\[\square\]
$a + bi$ is a prime number in $\mathbb{Z}[i]$, with $i = \sqrt{-1}$ and $a - 1 + bi$ divisible by $2 + 2i$.

Claim. This implies $a^2 + b^2 = p$, a prime number with $p \equiv 1 \pmod{4}$.

We use the fact (already known by Gauss) that prime elements (up to units) of $\mathbb{Z}[i]$ are:

(2) $\pi = \pm 1 \pm i$,
(3) or a rational prime number $\ell$ with $\ell \equiv 3 \pmod{4}$,
(4) or $a + bi$ with $a^2 + b^2 = p$, a rational prime number with $p \equiv 1 \pmod{4}$.

Suppose $\pi = a + bi \in \mathbb{Z}[i]$, a prime. If $\pi = \pm 1 \pm i$, then $2 + 2i$ does not divide $\pi - 1$.

If $\ell \equiv 3 \pmod{4}$, then $\ell - 1 \equiv 2 \pmod{4}$ is not divisible by $2 + 2i$; also $\ell - 1$ is not divisible by $2 + 2i$ because $\text{Norm}(\ell - 1) \equiv 2 \pmod{4}$. The cases (2) and (3) are excluded, hence we are in case (4).

Theorem 4 ([Gauss, Herglotz], [9], [7]). Suppose $K = \mathbb{F}_p$ with $p \equiv 1 \pmod{4}$. Let $E = E_K$ be the elliptic curve given by the equation Gauss gave in his Last Entry. Then

(a) $8$ divides $\#(E(\mathbb{F}_p))$;
(b) $\#(E(\mathbb{F}_p)) = \text{Norm}(\pi - 1) = (a - 1)^2 + b^2$;
(c) either $p \equiv 1 \pmod{8}$, and $p = a^2 + b^2$ with $b$ even and $a \equiv 1 \pmod{4}$, or $p \equiv 5 \pmod{8}$, with $b$ even and $a \equiv 3 \pmod{4}$.

Proof. (a). We have seen that for $K = \mathbb{F}_p$ with $p \equiv 1 \pmod{4}$ we have $(\mathbb{Z}/4 \times \mathbb{Z}/2) \hookrightarrow E(K)$.

(b) and (c). For $K = \mathbb{F}_p$, we know by the pRH for $E$, that $\pi \equiv \pi_p$; hence $\pi = \text{Frob}_{E/\mathbb{F}_p} = a + bi$ with $a^2 + b^2 = p$, and

\[ \text{Norm}(\pi - 1) = \#(E(\mathbb{F}_p)) = 2N. \]

Using the condition given by Gauss, or using that $8$ divides $N$, we see that $(a - 1)^2 \equiv b^2 \pmod{8}$, hence $a - 1 \equiv b \pmod{4}$. Note that

\[ N = (a - 1)^2 + b^2 = (a^2 + b^2) - 2a + 1 = p - 2a + 1. \]

If $p \equiv 1 \pmod{8}$ we obtain $2a \equiv 2 \pmod{8}$; if $p \equiv 5 \pmod{8}$ we obtain $2a \equiv 6 \pmod{8}$. Hence (c) follows.

What a precision in the statement by Gauss in his Last Entry to to formulate the statement in this exact form.

Remark. For any prime number $p$ with $p > 13$ and for the elliptic curve $E$ in this note we have $8 < \#(E(\mathbb{F}_p))$ and $\#(E(\mathbb{F}_{13})) = 8$. (However, there does exist an elliptic curve $C$ over $\mathbb{F}_{13}$ with $\#(C(\mathbb{F}_{13})) = 7$.)

Remark. Several other cases finding rational points over a finite field (solving an equation modulo $p$) were considered by Gauss; see [4], §358, [14], (2.1)-(2.5), [3], §14C.

Remarks. We have seen that for $p \equiv 1 \pmod{4}$ and $E = E_\mathbb{F}_p$, the Frobenius morphism is $\pi = a \pm bi$. One can wonder whether $-a \pm bi$ is also the Frobenius of an elliptic curve.

(a) For $E = E_K$ over a field $K$ given by $Y^2 = X^3 + 4X$ we choose $\delta \in K$ with $\delta$ not a square in $K$. We write $E$ for the elliptic curve over the field $K$ given by $\delta Y^2 = X^3 + 4X$. For any finite field $K = \mathbb{F}_q$ we see that

\[ \#(E(K)) + \#(E'(K)) = 2q + 2. \]

(b) Choose $p \equiv 1 \pmod{4}$, with $K = \mathbb{F}_p$ and $\pi' = -a \pm bi$. General theory tells us that this indeed is the Frobenius of an elliptic curve, see Honda-Tate theory [16]; the proof in the general case, using analytic parametrization, is non-trivial; for a purely algebraic proof see [2]. However in this particular case we see:

\[ \text{Frob}_{E'/K} = -a \pm bi. \]

Indeed, we see that $\beta = 2a$ and

\[ \#(E'(K)) = 2p + 2 - (1 - \beta + p) = 1 - (2a) + p \]

and we conclude

\[ \text{Frob}_{E'/K} = -a \pm bi, \]

a zero of $T^2 + 2aT + p$. Note that $E$ and $E'$ are non-isomorphic over $K = \mathbb{F}_p$, in this case $p \equiv 1 \pmod{4}$, but that they become isomorphic over the quadratic extension $\mathbb{F}_p^2$ of $K$; also we see that $(a + bi)^2 = (-a - bi)^2$.

Remarks. The quartic equation given by Gauss in his Last Entry originates in the theory of the lemniscate functions. We refer to [1], Section 3, and to [13] for details. The lemniscate functions $sl(t)$ and $cl(t)$ give a parametrization

\[ t \mapsto (x = cl(t), y = sl(t)) \]

of the curve given by $x^2 + y^2 + x^2y^2 = 1$; these functions are analogous of the usual sine and cosine functions, with the circle replace by the lemniscate of Bernouilli. For example see [1], Section 3. Addition theorems and other aspects of this uniformization are a rich source of beautiful mathematics, but not the focus of this note.

This parametrization of this particular elliptic curve was generalized by Abel, Jacobi and Weierstrass for all elliptic curves uniformized by elliptic functions and by Koebe and Poincaré (1907) for arbitrary curves of genus at least two.

Gauss used the lemniscate functions in his work. However it is not so clear in which way this was of inspiration for him to consider modulo $p$ solutions for this equation. Certainly his interest in biquadratic residues and his thoughts and results about primes in the ring $\mathbb{Z}[i]$ are connected with the topic discussed.
Even so it is remarkable the precision in which he found the right conditions and statement in the Last Entry.

In [17], on page 106 André Weil comments on the Last Entry. The statement “Observatio per inductionem” could be translated by “empirically”. We see comments on the connection with biquadratic residues: the number of solutions of the equation in this case is the analogue of pRH. On page 106 of [17] we see how the “two memoirs on biquadratic residues” were the cradle for the “generalized Riemann Hypothesis”.

Gauss considered solution of this equation modulo \( p \). Only much later \( E_{p} \) was considered as an independent mathematical object, not necessarily a set of modulo \( p \) solutions of a characteristic zero polynomial. What did Gauss consider? Note that in his Last Entry Gauss wrote \( \cdots = \cdots (\bmod a+bi) \); we see in work by Gauss that he knew very well when to use “\( = \)” and when to use “\( \equiv \)”. Was he foreshadowing the later use of geometric objects in characteristic \( p \)? Note that Felix Klein in [9] made the “correction” replacing the sign by \( \equiv \).

In the beginning \( E_{p} \) was seen as the set of values of a function field, as in the PhD-thesis by Emil Artin, 1921/1924. For elliptic curves this was an accessible concept, but for curves of higher genus (leave alone for varieties of higher dimensions) this was cumbersome. A next step was to consider instead a geometric object over a finite field; a whole new aspect of (arithmetic) algebraic geometry had to be developed, by Weil, Grothendieck and many others, before we could proceed. Each of these new insights was not easily derived; however, as a reward we now have a rich theory, and a thorough understanding of the impact of ideas as in the Last Entry of Gauss.

References


Figure 1. Carl Friedrich Gauss, 1777–1855.
Catalogum precedentem per falsa irigae iterum interruptam
initio anno 1812 restituius. In occasu Nov. 1811 conficiat
deformationem theorematis fundamentalis in doctrina arbitra
hominum pure analythicam complebat redire, sed quoque multiplici
cartis soratum fuerit, pars quaedam memoriae perhibet
excidit. Huc per salis longum tentorum interna
frustra quaestam tandem solvitur redemunans 1812 febr
Theoriam Anachonis Sphaeris Alphabii in paucis
extra solidum abe prius noua inventionem
Regez. 1812, May 26
Eadem partis reliquiis, idem theoriam
nouamu neocimphotis abstilius 1812 Oct. 15. Gob.
Fundamentum theoriae residuum liquaescentium
per generalis, per septem-propromolum annos summa con-
tentione ad sempem frustra quaestionem tamen solvit
etiam ordinem ut quod filius notis nobis est, 1813 Oct. 20. Gob.
Sublissimum hoc est omnium cumus quae quinquem
perfecimus. Vide itaque opera pruxm est, his in formis
minimorum quaestum simplificationem ad calculum
ordinem, parallicum pastorecum
Observabile per inductionem falso pronunciam, theorematis fundamentalis
hominum van functionibus teantibus ad integrum redit. Pute si ab tri est
numerus primus a = b, et a = b, est multis ordinibus, multibus ordinibus
comperidum: x = 0, y = 0, (a = t) + b, b
a = ±1, y = 0, f(x) = (a-i) + b, b

Figure 2. Facsimile in [5].
Figure 3. Handwritten notes by Gauss.
Fundamentum theoricum residuum biquadraticorum generalis, per septem propemodum annos summa contentione sed semper frustra que situm tandem feliciter deteximus eodem die, quo filius \(^*\) nobis natus est.


Subtilissimum hoc est omnium corum, quae unquam perfectionem. Vix itaque operae pretium est, bis intermiscere mentionem quarumdam simplificationum ad calculum orbitorum parabolicorum pertinentium.


KLEIN: BRENDEL.

Observatio per inductionem facta gravissima theorem residuum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si \(a+bi\) est numerus primus, \(a-i+bi\) per \(2+2i\) divisibilis, multando omnium solutionum congruentiae

\[
1 = x(x+y^2+ixy) \text{ mod. } a+bi \quad (**),
\]

inclusis

\[
x = \infty, \quad y = \pm i; \quad x = \pm i, \quad y = \infty,
\]

fit

\[
(a-1)^2+bb.
\]

1814 Iul. 9.

(*) Dieser am 21. Oktober 1813 geborene zweite Sohn des GAUSS zweite Ehe mit Minna WALDECK hieß WILHELM, widmete sich der Landwirtschaft und folgte später seinem älteren Bruder ENDER nach Amerika.

(**) In der Handschrift steht statt des Kongruenzzeichens \(\equiv\) das Gleichheitszeichen \(=\).
Die Anzahl Lösungen der Kongruenz \( \mod \cdot a + b \) ist die gleiche wie die der Kongruenz
\[
x \equiv (x^2 + y^2) \mod m,
\]
wo \( m = a + b \), in reellen ganzen Zahlen nach Dedekind, Brief an Klein. Man hat also zu suchen, wie groß die Anzahl der Lösungen von
\[
x \equiv n \mod m
\]
ist, bei denen gleichzeitig \( n \equiv 1 \mod 4 \) quadratische Reste von \( y \) sind. Dedekind hat für alle Primzahlen \( p \equiv 1 \mod 4 \) auf diese Weise die Gleichung bestätigt gefunden. Andererseits hat R. Eicker (Brief an Klein) darauf hingewiesen, daß die Gleichung
\[
x = n^2 - y^2 + a^2 y
\]
die zwischen
\[
x = \text{einlesm n, } y = \text{einlesm n}
\]
bestehende Beziehung ist. Der Zusammenhang aber der Theorie der biquadratischen Reste mit den hemisphärischen Funktionen, der durch die Anzahl der Lösungen jener Kongruenz vermittelt wird, bleibt aufzuklären.

---

SCHLUSSBEMERKUNG *.

Hinter der Nr. 145, mit der die Aufzeichnungen des Tagebuchs als solche schließen, sowie noch zwischen- durch eingefügt, finden sich in der Handschrift noch einige Blätter, die mit verschiedenartigen, teils mathematischen, teils nicht mathematischen Aufzeichnungen beschrieben sind **. Auf der Innenseite der Einband- decke endlich stehen in eine Folge hineingeschrieben die folgenden Syllepsen
Nihil Desperare.
Habeant sibi.
QVA EXEAS HABES.

*) Diese Schlussbemerkung und das folgende Nachverzeichnis sind mit einigen geringfügigen Änderungen aus der ersten Ausgabe des Tagebuchs übernommen worden.

**) Eine dieser Aufzeichnungen mathematischen Inhalts ist oben S. 513 in der Bemerkung zu der Nr. 145 wiedergegeben.

Figure 5. See [5], page 572.