Gauss' unpublished Section Eight of the Disquisitiones arithmeticae: The Beginning of the Theory of Function Fields over a Finite Field. (Lecture delivered in Oberwolfach on June 21, 2001)

Günther Frei

24th of June, 2001

Contents

1 Introduction

1. The starting point for my investigations, done in March 1999, on the largely unknown unpublished **Section Eight** of Gauss' ***Disquisitiones arithmeticae*** was a study of how *Emil Artin* was led to his reciprocity law in abelian extensions of algebraic number fields.[1] For that reason I had to begin with Artin's thesis on the theory of quadratic extensions of *Function Fields over a Finite Field of Constants.* Artin in his thesis is referring to a paper of *Dedekind* of 1857, and Dedekind himself said in the introduction of his paper that the subject, the *Theory of Function Fields over a Finite Field of Constants*, was initiated (angeregt) by Gauss. An examination of the *Disquisitiones arithmeticae* of Gauss showed that the subject is not treated there, but instead, that Gauss makes many references to an as yet unpublished Section Eight.√This Section Eight, written in Latin in 1797, V was found after Gauss' death (1855) in his papers under the title ***Disquisitiones generales de congruentiis.*** It was published by Dedekind in 1863 in the second volume of Gauss' Werke. A second printing of this Volume II appeared in 1876.

2. In the next section (**Section 2**) we will discuss the relation of the *Disquisitiones generales de congruentiis* with the *Disquisitiones arithmeticae.* In **Section 3** we try to put the *Disquisitiones generales de congruentiis* into the historic perspective, and in the last section (**Section 4**) we will present the content of the *Disquisitiones generales de congruentiis* and translate it into modern mathematical terminology and concepts.[2]

[1] This paper is a by-product of a project, jointly with Peter Roquette, on the Artin-Hasse correspondence and on the work of Helmut Hasse. It is a pleasure to thank *Peter Roquette* for his hospitality, his support and for the many interesting discussions. My thanks go also to the University of Heidelberg and to the Deutsche Forschungsgemeinschaft for their generous practical and financial support.

[2] A more detailed discussion of the mathematical content of the *Disquisitiones generales de congruentiis* will appear in a forthcoming paper entitled "On the Development of the Theory of Function Fields over a Finite Field from Gauss to Dedekind and Artin", see [Fr-2001].

2 The *Disquisitiones arithmeticae* and the *Disquisitiones generales de congruentiis*

2.1 The *Disquisitiones arithmeticae*

1. It is well known that Gauss laid the foundation of modern number theory in his fundamental treatise *Disquisitiones arithmeticae.* This treatise is divided up into seven sections.[3]

In the first section Gauss introduces congruences, and in the second he solves linear congruences and systems of linear congruences. In the third section he treats power residues, Fermat's theorem, primitive roots with respect to a prime number and the calculus of indices. The content of the first three sections can be called 'Elementary Number Theory' and was essentially known before Gauss, but Gauss discovered most of it independently.[4] It goes back to Euclid's Elements, to Fermat, Euler, Lagrange and Legendre. The next four sections are of a higher level. They are the work of Gauss who was building on various results of his predecessors P. de Fermat, L. Euler, L. Lagrange and A. M. Legendre. The **Section Four** is dedicated to congruences of the second degree: *quadratic residues* and the quadratic reciprocity law together with Gauss' *First Proof of the Quadratic Reciprocity Law.* The largest and most difficult, but also the most important section is **Section Five** where Gauss develops in detail the *Theory of binary quadratic forms*, including his *Second Proof of the Quadratic Reciprocity Law* by means of his theory of genera.[5] **Section Six** gives some applications. Fundamental is also **Section Seven**, the last section, where Gauss develops essentially the Galois Theory of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$, where p is a prime number, by means of his periods.

2. Sometimes it has been said that Section Seven is alien to the other sections since it is not arithmetic in character but rather algebraic or even analytic. But we will see that this is not so. In fact, the *Theory of Cyclotomy*, that is, the theory of the division of the circle which algebraically can be reduced to the solution of the equation $f(x) = x^n - 1 = 0$, treated in Section Seven, has been initiated by Gauss' investigations in number theory on the congruence $x^n - 1 \equiv 0$ modulo p, in particular $x^{p-1} - 1 \equiv 0$ modulo p, where

[3] see [Ga-1801], or [Ma-1889] for a German translation, or [Ga-1966] for an English translation.

[4] see [Ma-1889], pp. VI-VII; or [Ga-1966], p. xviii.

[5] Gauss began his investigations on quadratic forms on the 22nd of June 1796, stimulated by the work of Euler, Lagrange and Legendre; see [Ba-1911], p. 17.

p is an odd prime number.[6] Gauss noticed that the set of solutions of the congruence $x^{p-1} - 1 \equiv 0$ modulo p, and the set of permutations that send a fixed primitive root of the equation $F(x) = \frac{x^p - 1}{x-1} = x^{p-1} + \ldots + x + 1 = 0$ to another, that is, the Galois group of $F(x)$, both form a cyclic group of order $p-1$, a fact Gauss used in Section Seven to present the $p-1$ roots of F(x) in a purely abstract algebraic-arithmetic way without using complex numbers in the form introduced by Euler.[7] The cyclic structure of the roots of $F(x)$ and the possibility of grouping them into (Gaussian) periods in a way to allow to solve the equation $F(x) = 0$ became clear to Gauss on the 29th of March 1796. That was one day before he made the great discovery on the construction of the 17-gon with straightedge and compass, the discovery that made him start his diary on the same day.[8] This can be deduced from a letter of Gauss, written on the 6th of January 1819, to his former student Christian Ludwig Gerling, where Gauss writes, referring to the 29th of March 1796:[9]

> "Schon früher war alles was auf die Zertheilung der Wurzeln der Gleichung $\frac{x^p-1}{x-1} = 0$ in *zwei* Gruppen sich bezieht, von mir gefunden, wovon der schöne Lehrsatz D. A. p. 637 unten[10] abhängt u[nd] zwar im Winter 1796 (meinem ersten Semester in Göttingen), ohne dass ich den Tag aufgezeichnet hätte. Durch angestrengtes Nachdenken über den Zusammenhang aller Wurzeln unter einander nach arithmetischen Gründen, glückte es mir bei einem Ferienaufenthalt in Braunschweig, am Morgen des gedachten Tages[11] (ehe ich aus dem Bette aufgestanden war) diesen Zusammenhang auf das klarste anzuschauen, so dass ich die specielle Anwendung auf das 17-Eck und die numerische Bestätigung auf der Stelle machen konnte."

> "Already earlier I had found everything related to the separation of the roots of the equation $\frac{x^p-1}{x-1} = 0$ into two groups on which the beautiful theorem in the D. A. on p. 637 depends,[12] namely in Winter 1796 (during my first semester in Göttingen), without having recorded the day. By thinking with great effort about the relation of all the roots

[6] see for instance [Ba-1911], p. 33.

[7] see *Disquisitiones arithmeticae*, art. 343.

[8] see [Ga-1985], Entry 1.

[9] see Gauss, Werke, vol. X/1, p. 125.

[10] that is, *Disquisitiones arithmeticae*, art. 357; see [Ma-1889], pp. 427-428.

[11] that is, on the 29th of March 1796.

[12] that is, *Disquisitiones arithmeticae*, art. 357; see [Ga-1966], p. 439.

> to each other with respect to their arithmetic properties, I succeeded, while I was on a vacation in Braunschweig, on that day[13] (before I got off my bed) in seeing with utmost clarity this relation, so that I was able to make on the spot the special application to the 17-gon and to verify it numerically."

The "beautiful theorem in the D. A. on p. 637" refers to art. 357 of the *Disquisitiones arithmeticae*, where Gauss found, that the two (Gaussian) periods ω_1 and ω_2 of length $\frac{p-1}{2}$ of the roots of the cyclotomic polynomial $F(x) = \frac{x^p-1}{x-1}$, where p is an odd prime number, allow to split $F(x)$ into two factors with integral rational coefficients in ω_1 and ω_2, and yield the decomposition $4F(x) = G(x)^2 - p^*H(x)^2$, where $G(x)$ and $H(x)$ are two polynomials with integral rational coefficients and $p^* = +p$ if $p = 4t+1$ and $p^* = -p$ if $p = 4t-1$. Furthermore Gauss discovered that ω_1 and ω_2 are the two (quadratic) roots of the polynomial $x^2 + x + \frac{1}{4}(1-p^*)$,[14] and that on this fact a third and completely new proof of the Quadratic Reciprocity Law can be based. It is remarkable that Gauss announced his beautiful theorem on the decomposition of $F(x)$ already in art. 124 of the *Disquisitiones arithmeticae* where he was analysing the quadratic character of 7 and -7 modulo p.

3. That Section Seven must be seen as an integral part of the *Disquisitiones arithmeticae* is also stressed by Gauss himself who says in article 335, the first article of Section Seven:[15]

> "Der Leser könnte sich wundern, dass eine solche Untersuchung [über die Teilung des Kreises] gerade in diesem Werke, das einem beim ersten Anblick ganz heterogenen Gegenstande vorzugsweise gewidmet ist, angestellt wird; doch wird die Abhandlung selbst hinreichend klarlegen, in welchem innigen Zusammenhange dieser Gegenstand mit der höheren Arithmetik steht."

> "The reader might be surprised to find such an investigation [on the division of the circle] (exactly) in the present work which deals with a subject apparently so unrelated; but the treatment itself will make it abundantly clear that there is an intimate connection between this subject and higher Ar✓tihmetic."

(precisely)

✓ t

In the next section we will see that Section Seven served mainly as a preparation for an unpublished Section Eight and for a Third Proof of the

[13] that is, on the 29th of March 1796.

[14] see *Disquisitiones arithmeticae*, art. 356; [Ma-1889], p. 426; [Ga-1966], p. 438.

[15] see [Ma-1889], p. 397; respectively [Ga-1966], p. 407.

Quadratic Reciprocity Law that Gauss planned to extend to Higher Reciprocities by means of a detailed theory of function fields with coefficients in a finite field of order p.

2.2 The *Disquisitiones generales de congruentiis*

1. For this reason and in order to fully understand the ***Disquisitiones arithmeticae*** one has to know that Gauss had planned the publication of a second volume containing a detailed treatment of the *Theory of function fields over a finite field of constants*, called by Gauss *"Theory of higher congruences with respect to a prime number"* or *"Theory of double congruences"*. A draft of the beginning of this second volume was already written up in 1797, first planned as a Section Eight of an early version of the *Disquisitiones arithmeticae*. But, by lack of time, and also because Gauss intended to develop it further, it was not included in the final version of the *Disquisitiones arithmeticae* in order to leave space for a more detailed treatment of sections Five and Seven.

A hint to this can be found in the **Preface** of the *Disquisitiones arithmeticae* where Gauss says:

> "Schliesslich habe ich, da das Buch besonders wegen der grossen Ausdehnung des fünften Abschnittes bei weitem umfangreicher geworden war, als ich erwartet hatte, mehreres, was anfänglich für dasselbe bestimmt war, und unter andern den ganzen achten Abschnitt (welcher in diesem Bande bereits an einigen Stellen erwähnt wird und eine allgemeine Abhandlung über die algebraischen Congruenzen jeden Grades enthält) weglassen müssen. Alles dieses, welches mit Leichtigkeit einen mit dem vorliegenden gleichstarken Band ausfüllen wird, werde ich veröffentlichen, sobald sich die Gelegenheit dazu bietet."[16]

> "Finally, since the book came out much larger than I expected, owing to the size of Section V, I shortened much of what I first intended to do and, especially, I omitted the whole of Section *Eight* (even though I refer to it at times in the present volume; it was to contain a general treatment of algebraic congruences of indeterminate rank [better: algebraic congruences of any degree]). All the treatises which complement the present volume [better: All this which will easily fill another

[16] see [Ma-1889], p. VIII.

> volume of equal size as the present volume] will be published at the first opportunity."[17]

And in a **Letter to Bolyai** (dated the 29th of November 1798), we read regarding the *Disquisitiones arithmeticae*[18]:

> "Der sechste [Abschnitt] ist von keinem grossen Umfange; der 7^{te} (der die Theorie der Polygone enthält) etwas grösser aber im Wesentlichen schon fertig, u[nd] nur der letzte wird mich noch eine beträchtliche Zeit beschäftigen da er die schwersten Materien enthält."

> "[Section] Six is not of big size; [Section] Seven (which contains the Theory of Polygons) is somewhat larger but essentially already finished, and only the last will still keep me occupied for a considerable time, since it contains the most difficult matters."[19]

2. This unpublished manuscript by Gauss on the planned Section Eight of the *Disquisitiones arithmeticae*, entitled *Disquisitiones generales de congruentiis* (General Treatise on Congruences) was only found after his death among his papers as a *Chapter Eight* of a manuscript, entitled *Analysis residuorum* (Theory of Residues), which was composed of three chapters, running from a Chapter Six to a Chapter Eight. It was edited by Dedekind in 1863, second printing in 1876, in the second volume of Gauss' collected works under the title ***Disquisitiones generales de congruentiis. Analysis residuorum: Caput Octavum.*** (*Allgemeine Untersuchungen über die Congruenzen. Theorie der Reste: Kapitel acht.* General Investigations on the Congruences. Theory of Residues: Chapter Eight.)[20] It is divided up into articles running from art. 330 up to art. 375, in a way similar to those in the *Disquisitiones arithmeticae.* This seems to indicate that it must have belonged to an earlier version of a part of the *Disquisitiones arithmeticae.* This is, in fact, confirmed by a careful mathematical analysis of the content of the *Disquisitiones arithmeticae* and of the *Disquisitiones generales de*

[17] see [Ga-1966], p. xix. We have given here the translation by Clarke, but we have added in brackets another translation from the original Latin text which seems to us to be more appropriate.

[18] see [Ga-1899], pp. 11-12.

[19] My translation.

[20] see [Ga-1863]; or [Ga-1876], pp. 212-240; or [Ma-1889], pp. 602-629.

congruentiis, furthermore by Gauss' diary and by several remarks made by Gauss himself in the *Disquisitiones arithmeticae*, namely in the *Preface* and in artt. 11, 44, 61, 62, 65, 84, and by a remark he made in the *Disquisitiones generales de congruentiis* in art. 338.[21]

3. Section Eight contains a theory of Gauss on functions, that is polynomials modulo p and was planned to run completely analogously to the theory of rational integral numbers as treated in the sections One to Seven of the *Disquisitiones arithmeticae.* In particular, it was also to contain a theory of cyclotomy modulo p. For these reasons, many proofs in the *Disquisitiones arithmeticae* are formulated in such a way that they are not only valid for the domain of rational integers but also for the domain of polynomials over the integers or rationals or over a finite field of order p, that is, as we would say today, for integral domains. This is one reason why the *Disquisitiones arithmeticae* appeared so advanced and abstract for the readers of the last two centuries and still do so for many readers of our generation.

4. One also has to understand that *Section Seven on Cyclotomy* of the *Disquisitiones arithmeticae* served only as a preparation for the planned *Section Eight* which was to contain a *Third Proof of the Quadratic Reciprocity Law,* a proof Gauss planned to generalize to *Higher Reciprocity.* It was the discovery of this third proof, made on or before the 2nd of September 1796,[22] which stimulated Gauss to go deeper into the theory of polynomials over a finite field. The connection of the Quadratic Reciprocity Law with his theory of polynomials modulo p, however, was discovered by Gauss already three weeks earlier, on the 13th of August 1796.[23]

What Gauss noticed was that – what he called – the two periods of length $\frac{p-1}{2}$, belonging to the *cyclotomic congruence* $x^p - 1 \equiv 0$ modulo q, where p and q are odd prime numbers, furnish a *third proof* and a *fourth proof* of the Quadratic Reciprocity Law. These proofs are presented in the artt. 360-366 of the *Disquisitiones generales de congruentiis.*[24] On the other hand, the two periods also give, as Gaussian sums belonging to the *cyclotomic equation* $x^p - 1 = 0$, still another new proof for the quadratic character $\left(\frac{-1}{p}\right)$ of -1, that is, for the First Complementary Law of the Quadratic Reciprocity, a proof Gauss included in art. 356 of the *Disquisitiones arithmeticae.* The other proofs were given in artt. 108, 109 and 262 of the *Disquisitiones arithmeticae.*

two distinct

[21] for more details see [Fr-2001].

[22] see [Ga-1985], Entry 30.

[23] see [Ga-1985], Entry 23.

[24] see Section 4.5 below.

It is remarkable that it was exactly this theorem on the quadratic character $\left(\frac{-1}{p}\right)$ which led Gauss, according to his own testimony, to his investigations on number theory in the beginning of the year 1795.[25] From the letter to Gerling, dated the 6th of January 1819 and cited above in Section 2.1, art. 2, we learned that Gauss had discovered the structure and importance of the two periods of length $\frac{p-1}{2}$, belonging to the cyclotomic equation $x^p - 1 = 0$, already on or before the 29th of March 1796. Later, in 1811, Gauss found another proof of the Quadratic Reciprocity Law based on Gaussian sums,[26] and in 1817/8 still another, closely related to the theory of polynomials modulo p.[27]

So we see that, from the beginning, Gauss' study of the theory of polynomials modulo p was the driving force for his investigations and discoveries in number theory.

5. (Similarly)as Gauss' discovery of the *third proof* of the *Quadratic Reciprocity Law* has given rise to a detailed theory on functions modulo p, Gauss' discovery of his *second proof* of the Quadratic Reciprocity Law by means of his theory of the genus of quadratic forms, made on the 27th of June 1796,[28] had been the stimulus for Gauss to elaborate again and again on a detailed theory of quadratic forms in Section Five of the *Disquisitiones arithmeticae.* From the letter to Bolyai cited above we know that Gauss had rewritten this Section Five four times, each time improving on the former version in a way which "exceeded his most audacious expectations".[29] Let us recall that Gauss had found the *Quadratic Reciprocity Law*, called by him *"theorema fundamentale"* , already in March 1795.[30] The *first proof* for it was found by Gauss a year later on the 8th of April 1796.[31] It is the one he presented in artt. 131-144 of the *Disquisitiones arithmeticae.* That he considered the Quadratic Reciprocity Law as being the central theorem of number theory is also underlined by the fact that he turned back to the theorem again and again, finally leaving eight different proofs, most of them completely different from the others.

In a very simila

6. Gauss in his *Disquisitiones generales de congruentiis* first establishes

[25] see [Ga-1966], Preface, p. xviii; or [Ma-1889], p. VI.

[26] see [Ma-1889], pp. 463-495; in particular p. 493.

[27] see [Ma-1889], pp. 496-510; in particular pp. 501-505. See also [Fr-1994], pp. 79-81.

[28] see [Ba-1911], p. 25.

[29] see [Ga-1899], p. 11.

[30] see [Ba-1911], p. 5; and [Ga-1801], p. 475, Zu Art. 131.

[31] see [Ga-1985], Entry 2 of Gauss' Diary; and [Ga-1801], p.475, Zu Art. 130 and Zu Art. 131; see also [Ba-1911], pp. 15-16.

the fundamental theorem of arithmetic on unique factorization for polynomials modulo p, that is, for the ring $\mathbb{F}_p[x]$, via the existence of a Euclidean algorithm, thus following his presentation given in the *Disquisitiones arithmeticae* for the ring of integers. Then he passes to what he calls the main problem, the explicit determination of the number and of the form of all monic irreducible polynomials modulo p. This gives rise to - expressed in modern terminology - the determination of the structure of finite fields, that is, the determination of all finite algebraic extensions of the prime field $\mathbb{F}_p$ of characteristic p as ground field. Thereby the *Frobenius automorphism*, as we call it today, plays a key rôle. By an argument on the degree of the subfield $\mathbb{F}_p(\sqrt{q^*})$ constructed within $\mathbb{F}_p(\zeta_q)$ by means of Gaussian periods of length $\frac{q-1}{2}$, Gauss obtains his *Third Proof* of the *Quadratic Reciprocity Law* for two different odd rational prime numbers p and q, where ζ_q denotes a primitive q-th root of unity over $\mathbb{F}_p$. He encounters difficulties while extending the theory to Gaussian periods of length $\frac{q-1}{e}$, where e divides $q-1$, when $e > 2$. He starts to overcome this difficulty by passing to congruences modulo higher powers of p, hence by going to p-adic numbers, whereby he proves *Hensel's Lemma*. Very unfortunately, Gauss stops after this point in the middle of an article, even in the middle of a formula, and it seems that he never found the time to develop the theory further. So Gauss remained with his theory of function fields, strictly speaking, always in the ground field $\mathbb{F}_p(x)$. But there can be no doubt that he had envisaged also a theory of quadratic forms over the ring $\mathbb{F}_p[x]$, and as such a theory of quadratic extensions over $\mathbb{F}_p(x)$, as well as a theory of cyclotomy over $\mathbb{F}_p(x)$ in analogy to his Section Seven of the *Disquisitiones arithmeticae.*

3 Origin and Influence of the *Disquisitiones generales de congruentiis*

3.1 Origin of the *Disquisitiones generales de congruentiis*

1. The theory of functions, that is polynomials, over a prime field of characteristic p must be seen as a genuine creation by Gauss. However, Gauss might have been motivated for such a theory by the *Theorem of Lagrange* as-

serting that a polynomial of degree n, whose coefficient of the term of highest degree is not divisible by the prime number p, has at most n roots modulo p. Gauss proves this theorem in the *Disquisitiones generales de congruentiis* in art. 338 by showing that if a polynomial $f(x)$ with integer coefficients has the integer a as a root modulo p, then $f(x)$ is divisible modulo p by $x - a$,[32] a theorem which goes back to Descartes in the ordinary case where $f(x)$ is a polynomial and a is a root, say belonging to the rational, real or complex numbers. And Gauss adds in this art. 338 of the *Disquisitiones generales de congruentiis*, after having given his proof, that "this is the proof of this theorem he had promised".

2. By this Gauss is referring to the *Disquisitiones arithmeticae*, art. 43, where he proved the same theorem by induction on the degree n and then added that he will give a different proof in Section Eight. In his commentaries in the next article, art. 44 of the *Disquisitiones arithmeticae*, Gauss attributes the theorem to Lagrange.[33] Lagrange had proved the theorem in essentially the same way as Gauss has done in art. 43 of the *Disquisitiones arithmeticae*, that is, by induction, and this already in 1768 in volume XXIV of the Mémoire de l'Académie royale des Sciences et Belles-Lettres de Berlin, which was published in 1770.[34] The theorem in art. 43 of the *Disquisitiones arithmeticae* is one of several theorems appearing in the *Disquisitiones arithmeticae* under the heading "*Theoremata varia*" (various theorems), which includes art. 38 up to art. 44. Lagrange's theorem is the very last theorem proved in Section Two. By this fact and by Gauss' commentaries made in art. 44, it appears that Gauss must have considered it a key theorem for the theory of polynomials modulo p, a theory he would eventually develop later. For, he also mentions Euler who proved the theorem in the particular case where the polynomial is $f(x) = x^n - 1$ in a paper presented to the St.Petersburg Academy on the 18th of May 1772 and published in the proceedings of the St.Petersburg Academy in 1774. Euler was then already blind and for that reason did not know the more general result by Lagrange published two years earlier.[35] An even more special case of it had been considered by Euler in 1754 in connection with his proof of Fermat's theorem asserting that every prime number p of the form $4n+1$ is the sum of two squares.[36]

3. That Lagrange's theorem might have been a motivation for Gauss'

[32] see [Ma-1889], p. 607.

[33] see [Ma-1889], p. 29, art. 44.

[34] see [La-1770], p. 667, art. 10, Cor. V.

[35] see [Eu-1774], art. 28; Op. Om. 1, III, p. 248.

[36] see [Eu-1760].

theory of functions modulo p is also indicated by what Gauss says in art. 338 of the *Disquisitiones generales de congruentiis* following his second proof of Lagrange's theorem:[37]

> "Aber zugleich ersieht man hieraus, dass die Lösung der Congruenzen nur einen Teil einer viel höheren Untersuchung bildet, nämlich der Untersuchung über die Zerlegung der Functionen in Factoren."

> "But at the same time one sees from this that the solution of congruences constitutes only a part of a much higher [more advanced] investigation, namely the investigation on the decomposition of functions [i. e., polynomials] into factors."

A remark made by Gauss in art. 44 of the *Disquisitiones arithmeticae* seems to hint into the same direction where Gauss says regarding this theorem of Lagrange that it is considered here in art. 44 only as a lemma and that there is here not the place for a detailed elaboration of it. This seems to indicate that Gauss was thinking of a more detailed treatment eventually to be given in the planned Part Two of the *Disquisitiones arithmeticae* on the theory of polynomials.

4. It is also noteworthy that Gauss proved under the same heading "*Theoremata varia*" in art. 42 of the *Disquisitiones arithmeticae*, right before the theorem of Lagrange, another isolated important theorem on polynomials which later plaid a fundamental rôle for Kronecker's theory of divisors, namely the theorem asserting that if a monic polynomial $f(x)$ with integral coefficients is decomposable into two monic polynomials $g(x)$ and $h(x)$ with rational coefficients, then necessarily the coefficients of $g(x)$ and $h(x)$ must be integers. So we might guess that an elaboration on this theorem was also to be part of a detailed theory of polynomials reserved for the planned Part Two of the *Disquisitiones arithmeticae.*

3.2 Influence of the *Disquisitiones generales de congruentiis*

3.2.1 Dedekind

1. Gauss' *Disquisitiones generales de congruentiis* have remained without direct influence on the future development of the theory of function fields. The

[37] see [Ma-1889], p. 607.

reason is that they were published only in 1863 (by Dedekind in the second volume of Gauss' collected works) after papers by Galois (1830), Schönemann (1846) and Dedekind (1857) on the same subject had appeared. In addition, they were published in Latin (under the title *Disquisitiones generales de congruentiis. Analysis residuorum: Caput Octavum.*), a language not used any more for mathematical papers after 1850. They were translated into a modern language only in 1889 by H. Maser under the German title *Allgemeine Untersuchungen über die Congruenzen.*[38] By that time the main interest in number theory had shifted to the fundamental works of Kummer, Dedekind and Kronecker on the new theory of algebraic number fields. Later authors, such as Kornblum and Artin only refer to Dedekind's paper of 1857, *Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus,*[39] as regards the theory of higher congruences modulo a prime number p. (Hence)Gauss' posthumously published treatise remained practically unnoticed up to our days.

(Thus)

2. Dedekind in the introduction of his paper of 1857 referred to Gauss by saying that Gauss initiated the subject of functions modulo p. He also mentioned that *E. Galois, I. A. Serret* and *Th. Schönemann* had taken it up afterwards.

Let us cite what exactly Dedekind did say in his introduction:[40]

> "Es ist meine Absicht, dem in der Überschrift bezeichneten Gegenstand, welcher, von *Gauß*[41] zuerst angeregt, später mit Erfolg von *Galois, Serret, Schönemann*[42] wieder aufgenommen ist, eine einfache zusammenhängende Darstellung zu widmen, welche sich streng an die Analogie mit den Elementen der Zahlentheorie binden soll. Diese ist in der Tat so durchgreifend, daß es mit Ausnahme einiger unserem Gegenstand eigentümlicher Untersuchnungen nur einer Wortänderungen in den Beweisen der Zahlentheorie bedarf. Ich folge genau dem Gange, welchen *Dirichlet*

[38] see [Ma-1889], pp. 602-629.

[39] see [De-1857].

[40] see [De-1857], p. 1; or Werke, Band 1, p. 40.

[41] Ore in his commentary refers to C. F. Gauß' Werke, Bd. 2, S. 212-240. But it is very doubtful, as we will see, that Dedekind already knew the notes *Disquisitiones generales de congruentiis* by Gauss in October 1856 when Dedekind wrote his paper

[42] Ore in his commentary refers to E. Galois: Oeuvres mathématiques, pp. 15-23. I. A. Serret: Cours d'algèbre, 2e édition, pp. 343-370. Th. Schönemann, Journ. f. reine angew. Math. 31 (1846), S. 269-325 and 32 (1846), S. 93-105.

in seinen Vorlesungen über die Zahlentheorie[43] (oder in seiner kurzen Darstellung der Theorie der komplexen Zahlen im 24. Band dieses Journals[44]) eingeschlagen hat. In Rücksicht hierauf wird man es nicht tadeln, daß ich meist nur die Hauptmomente der Beweise hervorhebe, da größere Ausführlichkeit für den Kenner der Zahlentheorie, welche hier vorausgesetzt wird, ermüdend sein müßte."

"It is my intention to give a simple and coherent presentation of the subject called in the title, which was first initiated by Gauss[45] and later taken up with success by *Galois, Serret, Schönemann*,[46] a presentation which shall be strongly tied to the analogy with the elements of number theory. This analogy is, in fact, so thorough, that only a change of words are needed in the proofs of the number theory, except for some investigations which are particular for our subject. I follow exactly the path taken by *Dirichlet* in his lectures on number theory[47] (or in his short presentation of the theory of complex numbers in volume 24 of this journal[48]). Taken this into account, one will not blame me for stressing mostly only the main moments of the proofs, since a more detailed presentation will be tiring for the expert in number theory, a theory which is assumed here."

3. The reference Dedekind made to Gauss could not have meant the *Disquisitiones generales de congruentiis* for various reasons.

Firstly, by October 1856 Dedekind could not have seen the unpublished Section Eight *Disquisitiones generales de congruentiis* by Gauss who had died only 20 months before on the 23rd of February 1855. In fact, a letter from

[43] see [DD-1869]. Dirichlet in his lectures had, of course, followed the presentation of Gauss' *Disquisitiones arithmeticae.*

[44] that is, Journ. f. reine angew. Math., see [Di-1842], *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes*, Journ. f. reine angew. Math. 24 (1842), 291-371; or Dirichlet, Werke, Erster Band, XXXII, pp. 533-618.

[45] Ore in his commentary refers to C. F. Gauß' Werke, Bd. 2, S. 212-240. But it is very doubtful, as we will see, that Dedekind already knew the notes *Disquisitiones generales de congruentiis* by Gauss in October 1856 when Dedekind wrote his paper

[46] Ore in his commentary refers to E. Galois: Oeuvres mathématiques, pp. 15-23. I. A. Serret: Cours d'algèbre, 2e édition, pp. 343-370. Th. Schönemann, Journ. f. reine angew. Math. 31 (1846), S. 269-325 and 32 (1846), S. 93-105.

[47] see [DD-1869]. Dirichlet in his lectures had, of course, followed the presentation of Gauss *Disquisitiones arithmeticae.*

[48] that is, Journ. f. reine angew. Math.; see [Di-1842], *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes*, Journ. f. reine angew. Math. 24 (1842), 291-371; or Dirichlet, Werke, Erster Band, XXXII, pp. 533-618.

Dedekind to Jacob Henle, dated the 29th of February 1860, seems to indicate that Dedekind saw Gauss' unpublished paper for the first time in the spring of 1860.[49]

Secondly, Dedekind's paper treats the subject in a way so similar to Gauss, that it is quite clear that Dedekind would not have published it had he known the paper by Gauss already in 1856. Also from the content of Dedekind's paper itself it is obvious that Dedekind did not yet know at that time Gauss' Section Eight, since he reproves several theorems that had already been proved by Gauss in his unpublished manuscript. Also in the paper *Beweis der Irreduktibilität der Kreisteilungsgleichungen*,[50] written at the same time, namely in October 1856, Dedekind refers to Schönemann's paper *Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist*[51] for a theorem which corresponds to the theorem stated by Gauss in artt. 348-350 of the *Disquisitiones generales de congruentiis.*

4. Dedekind had been Gauss' student in Göttingen from 1850 until 1852, where he heard among other things Gauss' lectures on the method of least squares. In 1852 he graduated under the direction of Gauss with the doctoral thesis *Über die Theorie der Eulerschen Integrale* (On the Theory of Eulerian Integrals), and in 1854 he wrote his habilitation paper *Über die Transformationsformeln für rechtwinklige Koordinaten* (On the Transformation Formulae for Rectangular Coordinates), and on the 30th of June in the same year Dedekind presented his habilitation lecture *Über die Einführung neuer Funktionen in der Mathematik* (On Introducing New Functions in Mathematics), both examined by Gauss. In the winter term 1854/55 Dedekind gave his first lecture "Probability and Geometry" as a Privatdocent (lecturer) in Göttingen. So it might a priori be possible, although it is very unlikely, that Gauss had told him at that time about his investigations on polynomials modulo a prime number p. It is, however, much more likely that Dedekind was inspired for his paper by the many references Gauss made in the *Disquisitiones arithmeticae* to the unpublished Section Eight *Disquisitiones generales de congruentiis* on higher congruences. Also the reference given to Gauss by

[49] From this letter we learn that Wilhelm Weber, Professor of Physics in Göttingen, had asked Dedekind through Jacob Henle, Professor of Anatomy in Göttingen, to collaborate on the edition of Gauss' Work and that Dedekind should come to Göttingen in order to look over Gauss' manuscripts and perhaps take upon part of them for the edition. See [De-1985], pp. 335-336. I would like to thank Ralph Haubrich for bringing this letter to my attention.

[50] see [De-1857b].

[51] see [Sch-1845].

Galois in *Sur la théorie des nombres* (1830)[52] might have had some influence on Dedekind. However, there are also some reasons to believe that the direct motivation for Dedekind's paper might have come from the series of papers by Kummer on ideal numbers in cyclotomic fields which appeared in Crelle's Journal (Journal für die reine und angewandte Mathematik) in the years 1846 and 1847.[53]

5. Gauss in his *Disquisitiones generales de congruentiis* and Dedekind in his paper [De-1857], both first establish the fundamental theorem for polynomials modulo p, that is, for the ring $\mathbb{F}_p[x]$, via the existence of a Euclidean algorithm, thus following the presentation given by Gauss in the *Disquisitiones arithmeticae* for the ring of rational integer numbers.

v of arithmetic

We have seen in Section 2.2, art. 6 that Gauss passes then to the explicit determination of the number and of the form of all monic irreducible polynomials modulo p and that this gives rise to the determination of the structure of finite fields by means of the *Frobenius automorhism.* By an argument on the degree of the subfield $\mathbb{F}_p(\sqrt{q^*})$ constructed within $\mathbb{F}_p(\zeta_q)$ by means of Gaussian periods of length $\frac{q-1}{2}$, Gauss deduces then his Third Proof of the Quadratic Reciprocity Law for two odd rational prime numbers p and q. We have also mentioned that Gauss theory of function fields modulo p remained, strictly speaking, always in the ground field $\mathbb{F}_p(x)$, but that there can be no doubt that he was also considering an extension of this theory.

v distinct

6. Also Dedekind does not leave the ground field $\mathbb{F}_p(x)$. After having proved the fundamental theorem for the ring $\mathbb{F}_p[x] = \mathcal{R}$, Dedekind treats the theory of congruences in $\mathcal{R}$ and then the theory of quadratic residues in $\mathcal{R}$. He then deduces the analogue in $\mathcal{R}$ of the *Gaussian Lemma* and sketches how to obtain the analogue of the *Quadratic Reciprocity Law* in $\mathcal{R}$ by following Gauss' fifth proof of the Quadratic Reciprocity for the rational numbers, published by Gauss in 1818 under the title *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplificationes novae.*[54]

v of arithmetic

3.2.2 Galois

1. We have mentioned that Dedekind referred to Galois in his article [De-1857] written in 1856. Let us cite what Galois said at the beginning of

[52] see [Gal-1897], p. 15.

[53] see [De-1878], p. 1; Werke, Band 1, p. 202; and [Ku-1975], pp. 193-251.

[54] see [Ga-1876], pp. 51-54; or the German translation in [Ma-1889], pp. 497-501.

his paper *Sur la théorie des nombres*, published in 1830 in the *Bulletin des Sciences mathématiques de M. Férussac*, volume XIII, p. 428:[55]

> "Quand on convient de regarder comme nulles toutes les quantités qui, dans les calculs algébriques, se trouvent multipliées par un nombre premier donné p, et qu'on cherche, dans cette convention, les solutions d'une équation algébrique $F(x) = 0$,[56] ce que M. Gauss désigne par la notation $F(x) \equiv 0$, on n'a coutume de considérer que les solutions entières de ces sortes de questions. Ayant été conduit par des recherches particulières à considérer les solutions incommensurables, je suis parvenu à quelques résultats que je crois nouveaux."

> "If one agrees to consider, in the algebraic calculations, as zero all quantities which are multiples of a given prime number p, and if one looks for the solutions of an algebraic equation $F(x) = 0$[57] with respect to this convention, what Gauss denotes by $F(x) \equiv 0$, then one is used to consider only the integer solutions of this kind of questions. After having been led by special investigations to consider the incommensurable [that is, irrational] solutions, I arrived at some results which I believe are new."

Of course, Galois refers to Gauss' *Disquisitiones arithmeticae*, since in 1830 he could not have known Gauss' unpublished *Disquisitiones generales de congruentiis*. And further down Galois writes after having proposed to introduce imaginary symbols for the incommensurable, that is, irrational solutions of $F(x) \equiv 0$ modulo p:[58]

> "C'est la classification de ces imaginaires, et leur réduction au plus petit nombre possible, qui va nous occuper."

> "It is the classification of these imaginaries and their reduction to the smallest number possible which will occupy us [in this paper]."

2. Galois then sets out to establish the additive and multiplicative structure of the finite algebraic field extensions of the prime field $\mathbb{F}_p$ of characteristic p. A field extension is viewed as generated by - what Galois calls -

[55] see [Gal-1897], pp. 15-23, in particular p. 15.

[56] Galois writes Fx instead of $F(x)$.

[57] Galois writes Fx instead of $F(x)$.

[58] see [Gal-1897], p. 15.

an (imaginary) root of an irreducible polynomial $F(x)$ of a certain degree ν over $\mathbb{F}_p$. Galois then illustrates his theory in detail with the example where $p = 7$ and $\nu = 3$. Galois' discoveries are essentially the same as those made by Gauss and presented by Gauss in artt. 351-352 of the *Disquisitiones generales de congruentiis*. Gauss, however, works with the irreducible polynomial $F(x)$ itself instead of an (imaginary) root of $F(x)$. Gauss explicitly says in art. 338 of the *Disquisitiones generales de congruentiis* that he could have shortened considerably his investigations, had he wanted to introduce such imaginary quantities; but nevertheless, he had preferred to deduce everything from first principles.[59] Also in the *Disquisitiones arithmeticae*, in Section Seven on Cyclotomy, Gauss had avoided to work exlicitly with complex numbers, but instead represented them arithmetically in a formal way as roots of the cyclotomic polynomial.[60]

3.2.3 Schönemann

1. Next to Galois, Dedekind also referred to Schönemann in his article of 1857. Similarly as Galois, Schönemann also mentions Gauss in the Preface (Vorwort) of his treatise *Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist*, written on the 16th of February 1845 and published in volume 31 of Crelle's Journal, namely as follows:[61]

> "Der berühmte Verfasser der *Disquisitiones Arithmeticae* hatte für den achten Abschnitt seines Werkes eine allgemeine Theorie der höheren Congruenzen bestimmt. Da indessen dieser achte Abschnitt nicht erschienen, und auch, so viel ich weiss, über diesen Gegenstand sonst nichts von dem Herrn Verfasser bekannt gemacht oder nur bestimmt angedeutet worden ist (denn die Untersuchungen über imaginäre Moduln gehören in ein anderes Gebiet), so wage ich nicht, zu entscheiden, ob und wie weit die vorliegende Arbeit mit den Untersuchungen des berühmten Meisters in Berührung stehe. Sollte ich vielleicht zum Theil denselben Sätzen meine Forschung gewidmet haben, wie der tiefsinnige Begründer der Lehre von den Congruenzen, so würde mich über

[59] see section 4.2 below for the exact citation.

[60] see Section 2.1, art. 2 above.

[61] see [Sch-1845], p. 270. Schönemann had published his paper already a year before, in 1844, in the Programme of the Brandenburg Gymnasium (College) at Brandenburg on the Havel.

> die Einbusse der ersten Entdeckung das Bewusstsein schadlos halten, auf selbstständigem Wege mit dem Streben eines solchen Geistes zusammengetroffen zu sein."

> "The famous author of the *Disquisitiones Arithmeticae* had intended a general theory of higher congruences for the Section Eight of his work. Since, however, this Section Eight did not appear, and also, as far as I know, the author did not publish anything on this subject, nor indicate anything concretely, I do not dare to decide, whether and how far this present paper is related to the investigations of the famous master. In case I have perhaps dedicated my research partially to the same theorems as the profound creator of the theory of congruences, then the loss of the first discovery would be compensated by my knowing of having met on my own way the endeavor of such a [great] spirit."

2. Schönemann, who was a professor at the Brandenburg Gymnasium (College) at Brandenburg on the Havel, also mentions in his preface that he was led to his investigations by the discovery of the theorem asserting, that the polynomial $F(x)$, having as roots modulo p the p-th powers of the roots modulo p of a given polynomial $f(x)$ with integral coefficients, is congruent to this given polynomial $f(x)$ modulo p, if p is a prime number, a theorem he proved in §13.[62] This is the theorem Gauss proved in art. 350 of the *Disquisitiones generales de congruentiis.*[63] But contrary to Gauss, Schönemann does not realize the importance of the corresponding Frobenius automorphism for the structure of finite fields. Schönemann finds essentially all the properties of finite fields in terms of congruences modulo a prime number p and modulo an "expression" $f(\alpha)$, where $f(x)$ is an irreducible polynomial modulo p and α is a root of $f(x)$ modulo p; Schönemann calls it a congruence according to the module (p, α). But Schönemann's presentation lacks the clarity and precision of the one's given by Gauss who essentially works in $\mathbb{F}_p[x]$ modulo $f(x)$ or by Galois who considers α as being an algebraic irrational and works in $\mathbb{F}_p(\alpha)$. Schönemann's principal result is the following *Hauptsatz* in §18 that we will translate into modern terms and terminology:[64]

If $f(x)$ is an irreducible monic polynomial of degree n modulo a prime number p, that is, $f(x) \in \mathbb{F}_p[x]$, and if α is a root of $f(x)$, then $f(x)$ splits in the algebraic extension $\mathbb{F}_p(\alpha)[x]$ as follows:
$f(x) = (x - \alpha)(x - \alpha^p)(x - \alpha^{p^2}) \dots (x - \alpha^{p^{n-1}})$.

[62] see [Sch-1845], p. 269 and p. 287.

[63] see Theorem 3 in section 4.2 below.

[64] see [Sch-1845], p. 292.

Furthermore: $\alpha^{p^n-1} = 1$ in $\mathbb{F}_p(\alpha)$.

Schönemann views this principal result as a generalization of *Lagrange's Theorem:*[65] $x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-(p-1))$ modulo p,
which can also be written as
$x^{p-1} - 1 \equiv (x-a)(x-a^2)\dots(x-a^{p-1})$ modulo p, if a is a primitive root modulo p,
and of *Fermat's Theorem:* $a^{p-1} \equiv 1$ modulo p.

3. Schönemann then goes on to study - what we call today - the polynomial ring $\mathbb{F}_p(\alpha)[x]$ for which he proves the fundamental theorem of arithmetic on the unique decomposition of polynomials into irreducible polynomials,[66] where α is the root of an irreducible monic polynomial $f(x)$ in $\mathbb{F}_p[x]$. Then he passes to iterated algebraic extensions $\mathbb{F}_p(\alpha)(\beta)$, where β is a root of an irreducible monic polynomial $g(x) = g(x, \alpha) \in \mathbb{F}_p(\alpha)[x]$.[67] He then determines the number of irreducible polynomials of degree q^ν in $\mathbb{F}_p(\alpha)[x]$, where q is a prime number and α is the root of an irreducible monic polynomial $f(x)$ in $\mathbb{F}_p[x]$.[68] Finally, Schönemann essentially finds part of Kummer's decomposition law, in terms of congruences modulo p, of a prime number p in the cyclotomic field $\mathbb{Q}(\zeta_q)$, where q is a prime number not necessarily different from p; namely, if $q \neq p$ and f is the smallest natural number such that $p^f \equiv 1$ modulo q, then $\psi(x) = x^{q-1} + x^{q-2} + \dots + x + 1$ splits modulo p into $\frac{q-1}{f} = e$ irreducible factors of degree f; and if $q = p$, then $\psi(x) \equiv (x-1)^{p-1}$ modulo p.[69] From there he obtains, by means of Dirichlet's theorem on primes in an arithmetic progression, the theorem that the polynomial $\psi(x) = x^{q-1} + x^{q-2} + \dots + x + 1$ is irreducible in $\mathbb{Q}[x]$, the theorem Gauss proved in art. 341 of the *Disquisitiones arithmeticae.*[70]

4. In a subsequent paper with the title "*Von denjenigen Moduln, welche Potenzen von Primzahlen sind*" published in the following volume of Crelle's Journal, Schönemannn extends his investigations from a prime number p to a power p^m of p.[71] Thereby he discovers a forerunner version of *Hensel's Lemma.*[72] He then obtains a new and simple proof for the cyclotomic polynomial $\psi(x) = x^{q-1} + x^{q-2} + \dots + x + 1$ to be irreducible in $\mathbb{Q}[x]$ if q is a

[65] see [Sch-1845], p. 288.
[66] see [Sch-1845], p. 297.
[67] see [Sch-1845], pp. 302-305.
[68] see [Sch-1845], p. 319
[69] see [Sch-1845], p. 323-325; and [Ku-1847], p. 321.
[70] see [Sch-1845], p. 325.
[71] see [Sch-1846].
[72] see [Sch-1846], §§ 58/59, pp. 97-98.

prime number.[73]

3.2.4 Later authors: Kühne, Kornblum, Artin, F. K. Schmidt

1. Kühne

1. From the later authors working on function fields $\mathbb{F}_q[x]$ of characteristic p, $q = p^m$, we first mention H. Kühne from Dortmund[74], who in a paper, entitled "*Eine Wechselbeziehung zwischen Functionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt*" and published in 1902 in volume 124 of Crelle's Journal,[75] proved the general n-th power Reciprocity Law in $\mathbb{F}_q[x]$, for $n = 3$ and $n = 4$, and for general n in the case where the constant field $\mathbb{F}_q$ contains the n-th roots of unity. This theorem was rediscovered and reproved later in 1925 independently by F. K. Schmidt. Kühne does not give any reference to his predecessors, but surely he must have been aware at least of Dedekind's paper of 1857. It seems to me also very likely that he knew Schönemann's article, and also Gauss' *Disquisitiones generales de congruentiis* which had been published in the meantime in 1863 and 1876. One reason for this is that the papers by Kühne, Dedekind and Schönemann all appeared in Crelle's Journal. Another reason is that Kühne does not repeat anything contained either in the paper of Dedekind or in the treatise of Gauss or in the article of Schönemann, but rather starts right where these three authors have left. For example, Kühne's iterated construction of the finite algebraic extension $K = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{F}_p$ resembles and resumes the one given by Schönemann. But from there, Kühne goes on to study the polynomials in $K[x]$.

2. Kühne first introduces the domain $\mathcal{B} = \mathbb{Z}[x_1, \ldots, x_n]$ modulo the "prime module system" $P = (p, f_1(x_1), f_2(x_2; x_1), \ldots, f(x_n; x_1, \ldots, x_{n-1})$, where p is a prime number and $f_1(x_1)$ is a monic irreducible integral polynomial modulo p, $f_2(x_2; x_1)$ is a monic irreducible integral polynomial modulo $(p, f_1(x_1))$, etc. That is, he is considering the finite algebraic extension $\mathbb{F}_q = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ of $\mathbb{F}_p$, where $f_1(\alpha_1) = 0, f_2(\alpha_2; \alpha_1) = 0$, etc. Then he deduces the *General n-th Power Reciprocity Law* in $\mathbb{F}_q[x]$ for n dividing $q-1$,

[73] see [Sch-1846], § 61, p. 100.

[74] *Hermann* Ernst Gustav Eduard **Kühne** was born on the 25th of November 1867 in Berlin and died on the 21st of May 1907 in Dortmund. He studied from 1886 until 1892 in Berlin where he got his Dr. phil. with a paper on n-manifolds. From 1898 until his early retirement in 1907 he was Oberlehrer at the Maschinenbauschule in Dortmund. His papers, published between 1892 and 1904 in the *Mathemtische Annalen* and the *Archiv der Mathematik und Physik* concern the theory of manifolds.

[75] see [Kü-1902].

that is, when the field $\mathbb{F}_q$ contains the n-th roots of unity; namely if f and g are two different monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree μ and ν respectively, then[76]

$$\left(\frac{f}{g}\right)_n = \left(\frac{g}{f}\right)_n (-1)^{\mu\nu\frac{q-1}{n}},$$

where $\left(\frac{-}{g}\right)_n$ is the n-th power Legendre symbol of g in $\mathbb{F}_q[x]$.

Kühne then derives also the cubic and biquadratic reciprocity law in the cases where $n = 3, 4$ is not a divisor of $q - 1$. He obtains in both cases, that is, for $n = 3$ and $n = 4$ and $n \not| q - 1$ that:[77]

$$\left(\frac{f}{g}\right)_n = \left(\frac{g}{f}\right)_n.$$

3. In a subsequent paper entitled "*Angenäherte Auflösung von Congruenzen nach Primmodulsystemen in Zusammenhang mit den Einheiten gewisser Körper*", published a year later in volume 126 of the same journal,[78] Kühne studies the units in $\mathbb{F}_q[x]$ and obtains the analogue of *Dirichlet's Unit Theorem* for $\mathbb{F}_q[x]$.[79] For that purpose he also states and proves *Hensel's Lemma.*[80] We have seen in Section 2.2, art. 6 that Gauss had already stated and proved Hensel's Lemma in his *Disquisitiones generales de congruentiis*,[81] and that Schönemann found a forerunner version of it in his paper [Sch-1846]. As it is very likely that Kühne did know the *Disquisitiones generales de congruentiis* and also the paper by Schönemann, we might guess that Kühne got the idea for this lemma directly from Gauss. Now remember that Hensel was the editor of Crelle's Journal from 1903 up to 1936, starting with volume 125. We know that Hensel used to read all the submitted articles, so he must have known Kühne's paper. Whether this might have influenced Hensel's work on p-adic numbers, started in 1899, in particular Hensel's discovery of Hensel's Lemma, remains to be analysed. So it is possible that Hensel's Lemma, in fact, goes back directly to Gauss *Disquisitiones generales de congruentiis*, even so neither Kühne nor Hensel mention any predecessors related to this lemma.

4. According to what Kühne says on p. 130 in his paper of 1902, he had the intention to study also the theory of quadratic forms over $\mathbb{F}_q[x]$, probably

[76] see [Kü-1902], p. 129.
[77] see [Kü-1902], pp. 132-133.
[78] see [Kü-1903].
[79] see [Kü-1903], p. 115.
[80] see [Kü-1903], p. 105.
[81] see Section 4.6, art. 10 below.

following the exposition given by Gauss in Section Five of the *Disquisitiones arithmeticae*, but it seems that Kühne did not publish anything on this subject.[82]

2. Kornblum

Another author we have to mention, although he is not directly influenced by Gauss, is *Heinrich Kornblum* who in a paper entitled "*Über die Primfunktionen in einer arithmetischen Progression*" carries Dirichlet's Theorem on primes in an arithmetic progression from the ring of integers $\mathbb{Z}$ over to the ring $\mathbb{F}_p[x]$ of integral polynomials modulo p. Heinrich Kornblum (1890-1914) was a student of Landau in Göttingen. He fell in the First World War in October 1914 at the age of 24 near Poël-Capelle. Kornblum's paper is based on his doctoral dissertation on prime functions in arithmetical progressions and was edited in 1919 after the war by Landau in volume 5 of the Mathematische Zeitschrift. Kornblum's starting point was also Dedekind's paper of 1857. Kornblum discovered, after having introduced L-functions for $\mathbb{F}_p[x]$, that the classical proof of Dirichlet for the non-vanishing of $L(s, \chi)$, at $s = 1$ and for non-principal characters χ, $\chi \neq \chi_0$, can be adapted to function fields $\mathbb{F}_p(x)$. However, Kornblum does not introduce algebraic extensions of $\mathbb{F}_p(x)$.

3. Artin

An important step in the theory of function fields of characteristic p was done by *Emil Artin* in his thesis *Quadratische Körper im Gebiete der höheren Kongruenzen I, II*,[83] where Artin introduces and studies systematically the arithmetic of a quadratic extension $\mathcal{K}$ of the function field $\mathbb{F}_p(x)$ over a finite field of prime order $p \neq 0$, that is, the theory of hyper-elliptic curves over a finite prime field $\mathbb{F}_p$. The center of his study was the analytic class number formula for $\mathcal{K}$ which led him to introduce the ζ-function for the function field $\mathcal{K}$ and to formulate and conjecture the Riemann Hypothesis for $\mathcal{K}$. The thesis was sent for publication to the *Mathematische Zeitschrift* on the 14th of October 1921, but appeared only in 1924. Like Kornblum, Artin in his dissertation does not mention Gauss but refers to Dedekind's article of 1857, and also to Kornblum's paper which had appeared just two years before Artin's thesis was written and finally published in the same journal as Kornblum's. It is very likely that it was Artin's thesis advisor *Gustav Herglotz* who suggested to Artin to study, in his thesis, quadratic algebraic exten-

[82] Kühne retired in 1907 at the age of 40, probably because of bad health, and died the same year. His last paper appeared in 1904. So it seems that he could not realize his plan to publish a paper on the theory of quadratic forms over congruence function fields.

[83] see [Ar-1924].

sions of a function field $\mathbb{F}_p(x)$, after having seen Kornblum's thesis in the Mathematische Zeitschrift of which Herglotz was a wissenschaftlicher Beirat (scientific adviser). For more details on Artin's thesis we refer to [Fr-2001] and [Fr-2002].

4. F.K. Schmidt

1. Finally, let us mention *F. K. Schmidt* who took over the theory of function fields of characteristic p where Artin had left it in 1924, by generalizing Artin's theory from quadratic extensions over $\mathbb{F}_p(x)$ to arbitrary finite algebraic extensions $\mathcal{K}$ of $\mathbb{F}_q(x)$, where q is a power of p. This was done first in Schmidt's thesis, written in 1925 under the title "*Allgemeine Körper im Gebiet der höheren Kongruenzen*",[84] where Schmidt derives the fundamental arithmetical properties of the ring of integers $\mathcal{R} = \mathfrak{o}_{\mathcal{K}}$ in $\mathcal{K}$, that is, properties of the discriminant, of the units and of the class number of $\mathcal{R}$. However, the thesis was never published, probably because similar results had been obtained at the same time and independently by *P. Sengenhorst* and *H. Rauter*, a doctoral student of Hasse.[85] We have already mentioned that the n-th Power Reciprocity Law in $\mathbb{F}_q[x]$, found by Schmidt in his thesis, had already been obtained by Kühne in 1902. In his next papers, however, Schmidt goes into completely new territory by deriving class field theory for function fields of characteristic p,[86] in analogy to and by following Hasse's report on class field theory of algebraic number fields.[87] For doing this Schmidt had first to develop the analytic theory of the ζ-function and of the L-functions of $\mathcal{K}$ in order to obtain the first inequality of class field theory. Thereby Schmidt discovered that the functional equation of the ζ-function, introduced by him in 1926 for the field $\mathcal{K}$,[88] is equivalent to the *Theorem of Riemann-Roch* in $\mathcal{K}$.[89] This theorem had been translated by Schmidt from the case of characteristic zero, studied by Dedekind and Weber in their fundamental treatise of 1882,[90] to the case of characteristic p.

2. F.K. Schmidt's theory was fundamental for Hasse's investigations on the Riemann Hypothesis for function fields in one variable over finite fields and for Hasse's proof in the elliptic case (1933),[91] for Weil's proof of the

[84] see [Sm-1925].

[85] see [Ro-2001], p. 564.

[86] see [Sm-1931b].

[87] see [Ha-1926].

[88] see [Sm-1926].

[89] see [Sm-1931a].

[90] see [DW-1882].

[91] see [Ha-1933].

general case (1948)[92] and for the proof of the Weil conjectures (1949) by Dwork (1960), Grothendieck and Deligne (1973).[93] For more details on the work of F. K. Schmidt we refer to Roquette's paper [Ro-2001].

[92] see [We-1948], pp. 60-70.

[93] see [Did-1985], pp. 151-158. IX, 123-139.

4 Content of the *Disquisitiones generales de congruentiis*

4.1 Fundamental Theorem and Main Problem

Let us now indicate the content of the *Disquisitiones generales de congruentiis* in short form.[94] We will number the important theorems from 1 to 10.

art. 330. Gauss insists strongly on the **analogy** between **Number Fields** and **Function Fields**, that is, between $\mathbb{Z}$ and $\mathbb{Q}[x]$, or $\mathcal{R} = \mathbb{F}_p[x]$, an analogy he had stressed many times before (see Section 2.2, art. 3.)

art. 333. Then Gauss begins his treatise with what sometimes is called **"Descartes' Theorem"**, namely:
If a is a root of a polynomial $P(x) \in \mathcal{R} = \mathbb{F}_p[x]$, then $P(x)$ is divisible in $\mathcal{R}$ by $x - a$.

art. 334. Gauss develops the **Euclidean algorithm** in $\mathcal{R}$.

art. 335. Gauss proves what sometimes is called **"Bezout's Theorem"** which states that, given two polynomials $A(x)$ and $B(x)$ in $\mathcal{R}$, prime to each other, there exist $P(x)$ and $Q(x)$ in $\mathcal{R}$ such that
$A(x)P(x) + B(x)Q(x) = 1.$
(→ D 27; 19. 8. 1796).[95]

art. 340. From there Gauss gets the **Fundamental Theorem of arithmetic** on unique factorization in $\mathcal{R}$.

artt. 341-347. Gauss treats what he calls the **Main problem:** Determine the number of monic[96] prime functions $P(x)$ in $\mathcal{R}$ of a given degree m.

He first gets this number by combinatorial counting arguments and by

[94] A detailed discussion of the mathematical content of the *Disquisitiones generales de congruentiis* will appear in a forthcoming paper entitled "On the Development of the Theory of Function Fields over a Finite Field from Gauss to Dedekind and Artin", see [Fr-2001].

[95] By (→ D 27; 19. 8. 1796) we refer to Gauss' Diary, Entry 27, dated the 19th of August 1796. In the sequel we shall always refer in this way to Gauss' Diary.

[96] By "monic" we denote a polynomial whose leading coefficient is one.

recursion going from polynomials of degree one to polynomials of higher degree (*artt. 343-346*).

Then he obtains an explicit formula (*art. 347*). (→ D 75; 26.8.1797).

4.2 Detailed study of the prime functions $P(x)$ in $\mathbb{F}_p[x]$ of a given degree m: Theory of finite fields

art. 348. Gauss opens the next section with the following question: Given an equation $P(x) = 0$, where $P(x)$ is a polynomial of degree m in $K[x]$ with roots $\alpha_1, \ldots, \alpha_m$, where K is any field, or where K is replaced by a ring of integers I in K, to find the polynomial $P^{(t)}(x)$ whose roots are $\alpha_1^t, \ldots, \alpha_m^t$, that is, the t-th powers of the roots of $P(x)$.
(→ D 28; 21.8.1796)

Gauss uses two different methods.

The first applies *Newton's formulae* relating the coefficients of $P(x)$ with the sums s_ν of the ν-th powers of the roots, $s_\nu = \alpha_1^\nu + \ldots + \alpha_m^\nu$, $\nu = 1, 2, 3, \ldots$ He deduces:

1. $P^{(t)}(x) \in K[x]$.

The second method makes use – for the first time – of *cyclotomy* (Section Seven of the *Disquisitiones arithmeticae.* See Section 2.1 above). If ϑ is a primitive t-th root of unity, then Gauss forms the product $\prod(x - \vartheta^\tau \alpha_i)$ over all $\tau = 1, \ldots, t$ and $i = 1, \ldots m$ and puts $x^t = y$. This yields $P^{(t)}(y)$ from which he deduces:

2. $P^{(t)}(x) \in I[x]$, if $P(x) \in I[x]$.

art. 350. Next Gauss proves the remarkable property:

3. $P^{(t)}(x) = P(x)$, if $P(x) \in \mathbb{F}_t[x]$, and t is a prime number.

This means that, applying the t-th power induces a permutation of the roots of $P(x) \in \mathbb{F}_t[x]$. In modern terms that is to say:

3'. The map $\sigma : \alpha_i \mapsto \alpha_i^t$, where α_i is a root of $P(x)$, induces a relative automorphism of the field $E = \mathbb{F}_t(\alpha_1, \dots, \alpha_m)$ with respect to the base field $\mathbb{F}_t$.

3". That is, Gauss introduces the **Frobenius automorphism**
$\sigma : \alpha_i \mapsto \alpha_i^t$ of $E/\mathbb{F}_t$.
(→ D 26; 18. 8. 1796).

According to his Diary, Gauss introduced the Frobenius automorphism (on the 18th of August 1796) in order to establish his **Third Proof (Proof VII) of the General Quadratic Reciprocity Law**. He got the **Principal idea** for this proof five days before, namely on the 13th of August, 1796.
(→ D 23; 13. 8. 1796).

That Gauss, indeed, was thinking of the Frobenius automorphism in the modern sense and of the theory of finite fields in terms of **algebraic numbers over $\mathbb{F}_p$ and adjoined to $\mathbb{F}_p$** can be inferred from the following remark made by Gauss in *art. 338* where he proves *Lagrange's Theorem* asserting, that a polynomial $P(x) \in \mathbb{F}_p[x]$ of degree m cannot have more than m distinct roots, a theorem he deduces from Descartes' Theorem:

> "Hieraus geht hervor, dass die Anzahl der Wurzeln die Dimension der Congruenz nicht übersteigen kann; dies ist der von uns versprochene Beweis des Satzes.
>
> Aber zugleich ersieht man hieraus, dass die Lösung der Congruenzen nur einen Teil einer viel höheren Untersuchung bildet, nämlich der Untersuchung über die Zerlegung der Functionen in Factoren. Es ist klar, dass die Congruenz $\xi \equiv 0$ keine reellen Wurzeln hat, wenn ξ keine Factoren von *einer* Dimension besitzt; aber es hindert nichts, dass ξ in Factoren von zwei, drei oder mehr Dimensionen zerlegt werden kann, wonach jener gewissermassen *imaginäre* Wurzeln zugeschrieben werden können. In der That hätten wir, wenn wir uns einer ähnlichen Freiheit, wie sie neuere Mathematiker sich erlaubt haben, bedienen und derartige imaginäre Grössen einführen wollten, alle unsere nachfolgenden Untersuchungen unvergleichlich zusammenziehen können; nichtsdestoweniger haben wir es vorgezogen, Alles aus den Prinzipien abzuleiten. Vielleicht werden wir bei anderer Gelegenheit unsere Ansicht hierüber ausführlicher darlegen."[97]

[97] The last sentence appears as a footnote in Gauss. This and all the subsequent German citations are taken from [Ma-1889].

> "From this it becomes clear that the number of roots [of a polynomial congruence] cannot exceed the dimension [i. e., degree] of the congruence; this is the proof of the theorem [in art. 44 of the *Disquisitiones arithmeticae*] we promised.
>
> But at the same time one sees from this how the solution of congruences constitutes only a part of a much higher [more advanced] investigation, namely on the decomposition of functions [i. e., polynomials] into factors. It is clear that the congruence $\xi \equiv 0$ does not have real roots, if ξ has no factors of dimension[98] one; but nothing prevents us from decomposing ξ, nevertheless, into factors of two, three or more dimensions, whereupon, in some sense, *imaginary* roots could be attributed to them. Indeed, we could have shortened incomparably all our following investigations, had we wanted to introduce such imaginary quantities by taking the same liberty some more recent mathematicians have taken; but nevertheless, we have preferred to deduce everything from the [first] principles. Perhaps, we will explain our view on this matter in more detail on another occasion."[99] [100]

4.3 Properties of a finite field and its sub-fields by means of the *Frobenius automorphism*

artt. 351-352. Next Gauss proves:

4. Every prime function $P(x) \neq x$ of degree m in $\mathbb{F}_p[x]$ is a divisor of $x^{p^m-1} - 1$ in $\mathbb{F}_p[x]$.

This means that

4'. All roots of $P(x)$ are $p^m - 1$-th roots of unity with respect to $\mathbb{F}_p$.

Hence, by the theory of cyclotomy of Section Seven of the *Disquisitiones arithmeticae*, any root of an irreducible polynomial $P(x) \in \mathbb{F}_p[x]$ (of degree m) is contained in some "universal" field (of $p^m - 1$-th roots of unity).

[98] "dimension" here always means "degree".

[99] The last sentence appears as a footnote in Gauss.

[100] My English translation, here and in the sequel, is based on the original Latin text and not on Maser's German translation.

art. 353. Furthermore:

5. $x^{p^m-1}-1$ is equal to the product over all monic prime functions in $\mathbb{F}_p[x]$ whose degree d is a divisor of m.

This theorem determines all the sub-fields of $\mathbb{F}_p(\vartheta)$, where ϑ is a root of an irreducible polynomial $P(x) \in \mathbb{F}_p[x]$.
(→ D 30; 2. 9. 1796).

4.4 Study of the residue field $\mathbb{F}_p[x]/P(x)$ with respect to the base field $\mathbb{F}_p$, where $P(x)$ is a prime function in $\mathbb{F}_p[x]$ and p is a prime number

art. 356. Another important property of the Galois Theory over $\mathbb{F}_p$ is:

6. If $P(x)$ is a prime function in $\mathbb{F}_p[x]$ of degree m and $Q(x)$ is another function in $\mathbb{F}_p[x]$ which is invariant under the permutations of $x, x^p, x^{p^2}, x^{p^3}, \ldots, x^{p^{m-1}}$, then $Q(x) \equiv a \pmod{P(x)}$ with a constant a in $\mathbb{F}_p$.
(→ D 76; 30. 8. 1797; → D 77; 31. 8. 1797).

This means (in modern terminology):

6'. Let ϑ be a root of $P(x)$ and $E = \mathbb{F}_p(\vartheta)$. If $Q(\vartheta)$ is invariant under the *Frobenius automorphism* $\sigma : x \mapsto x^p$ of $E/\mathbb{F}_p$, then $Q(\vartheta)$ lies in the ground field $\mathbb{F}_p$.

art. 357. From this, Gauss deduces (in modern terminology):

7. If $P(x) = x^m - a_1x^{m-1} + a_2x^{m-2} - a_3x^{m-3} + \ldots + a_m$ is a prime function in $\mathbb{F}_p[x]$ of degree m and $E_i(x)$ is the i-th elementary symmetric function of $x, x^p, x^{p^2}, x^{p^3}, \ldots, x^{p^{m-1}}$, then $E_i(\vartheta) = a_i \in \mathbb{F}_p$, for all $i = 1, \ldots m$, if ϑ is a root of the irreducible polynomial $P(x)$.

artt. 358-359. Also the following theorem is quite remarkable and shows that Gauss had a deep insight into the structure of finite fields and their Galois Theory:

8. Let $P(x)$ be a prime function in $\mathbb{F}_p[x]$ and x^ν be the smallest power of x, such that $x^\nu \equiv 1 \pmod{P(x)}$. If $P(x) = P^{(n)}(x)$, then $n \equiv p^t \pmod{\nu}$ for some t.

This means:

8'. If ϑ^n is a cònjugate of ϑ, then there is a certain power σ^t of the Frobenius automorphism σ, which maps ϑ onto $\vartheta^{p^t} = \vartheta^n$. Or else:

8''. The group of automorphisms of $\mathbb{F}_p(\vartheta)/\mathbb{F}_p$ is cyclic and is generated by the Frobenius automorphism σ.

4.5 Gauss' *Third Proof* of the Quadratic Reciprocity Law

The last part of the *Disquisitiones generales de congruentiis* (*artt. 360-375*) is entitled
On finding the prime divisors of the function $x^\nu - 1$ with respect to a prime modulus.
Determine all the prime factors of $F(x) = x^\nu - 1$ in $\mathbb{F}_p[x]$ means to **Determine all the sub-fields of the normal closure of $F(x) = x^\nu - 1$ over $\mathbb{F}_p$.**

artt. 362-364. Gauss sketches the **Theory of Cyclotomy** for the polynomial $F(x) = x^\nu - 1 \in \mathbb{F}_p[x]$ over the field $\mathbb{F}_p$ with $\nu \in \mathbb{N}$, where ν is not divisible by p, in analogy to the Section Seven of the *Disquisitiones arithmeticae.*
That is, Gauss develops *Galois Theory* over the finite field $K = \mathbb{F}_p$ by explicit construction of the sub-fields of the normal closure of $F(x) = x^\nu - 1$ over $\mathbb{F}_p$ by means of **Gaussian Periods.**

art. 365. If $\nu = q$ is a prime number, Gauss obtains a new proof for the **General Quadratic Reciprocity Law** in $\mathbb{Q}$, his **Third Proof** (**Proof VII** in the official counting).

art. 366. Gauss comments as follows.

> "Dies ist also der dritte vollständige Beweis des Fundamentaltheorems im vierten Kapitel, der um so mehr beachtenswert ist, weil

> die Prinzipien, aus denen er abgeleitet ist, von denen, deren wir uns zu den früheren Beweisen bedient haben, völlig verschieden sind. Aus eben dieser Quelle aber, jedoch auf dem entgegengesetzten Wege, wollen wir einen vierten Beweis ableiten."

> "Thus this is the third complete proof of the fundamental theorem of Chapter IV [Section IV of the *Disquisitiones arithmeticae*] which is all the more noteworthy, since the principles, from which it is derived, are completely different from those we have used before. From the very same source [that is, with the same method], but going in the opposite direction, we will deduce a fourth proof."

The **principal idea** of the proof, from the modern point of view, is that: The field $\mathbb{F}_p(\sqrt{q^*})$ is viewed as contained in the cyclotomic field $\mathbb{F}_p(\zeta_q)$, $q^* = q(\frac{-1}{q})$, where $(\frac{\cdot}{q})$ is the Legendre symbol for the prime number q, and where ζ_q is a primitive q-th root of unity over $\mathbb{F}_p$. Then the reciprocity law follows from the fact that the degree t of $\mathbb{F}_p(\zeta_q)$ over $\mathbb{F}_p(\sqrt{q^*})$ is a divisor of $\frac{q-1}{2}$. The subfield $\mathbb{F}_p(\sqrt{q^*})$ is constructed within $\mathbb{F}_p(\zeta_q)$ by means of Gaussian periods of length $\frac{q-1}{2}$.

Hence this proof has some similarity with Gauss' Sixth Proof of the Quadratic Reciprocity Law presented in Gauss' paper "*Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplificationes novae*" (1817),[101] where Gauss uses Gaussian sums in $\mathbb{Q}[x]$ modulo $G(x) = x^{q-1} + \ldots + x + 1$;[102] or (as *Eisenstein* has pointed out[103]) in $\mathbb{Q}(\zeta_q)$, q a prime.[104]

4.6 Generalizations

In the remaining articles, Gauss goes on to generalize his investigations in different directions.

art. 367. First, he says that analogous theorems hold for ν **composite**: (→ D 77; 31. 8. 1797) and (→ D 78; 4. 9. 1797)

[101] see [Ga-1876], pp. 55-59; or [Ma-1889], pp. 501-505.

[102] see [Fr-1994].

[103] see [Ei-1847], p. 274.

[104] That $\mathbb{Q}[x]$ modulo $G(x) = x^{q-1} + \ldots + x + 1$ is isomorphic to $\mathbb{Q}(\zeta_q)$ was also clear to Gauss.

> "Obwohl wir uns hier auf den Fall, wo ν eine Primzahl ist, beschränkt haben, können doch auch, wenn ν eine zusammengesetzte Zahl ist, analoge Sätze ohne grosse Mühe aufgestellt werden, was wir jetzt der Kürze halber nicht ausführlicher auseinandersetzen können."

> "Although we have restricted ourself here to the case where ν is a prime number, analogous theorems, however, if ν is composite, can be established without much effort, which, for the sake of brevity, we cannot discuss now in more detail."

Then Gauss starts to prepare a proof of **Higher Reciprocity** by means of **Periods of arbitrary length**. He first considers a prime q of the form $q = 3t + 1$ and constructs in $\mathbb{F}_p(\zeta_q)$ Gaussian periods of length $\frac{q-1}{3}$.
(→ D 39; 1. 10. 1796).

In that context he says:

> "Es würde uns nicht schwer fallen, dieses Kapitel noch mit vielen andern Bemerkungen zu bereichern, wenn nicht die Grenzen, auf welche wir uns beschränken müssen, dies verbieten würden. Denjenigen, welche weiter vorgehen möchten, werden diese Prinzipien wenigstens den Weg andeuten können."

> "It would not be difficult for us to enrich this Chapter with many other observations, if the limits imposed on us did not forbid it. For those who want to advance further, these principles will at least indicate the way."

artt. 368-369. Then he goes further by studying the case where $P(x) \in \mathbb{F}_p[x]$ has **multiple roots**.
(→ D 68; 1. 7. 1797).

He first proves:

9. $P(x) \in \mathbb{F}_p[x]$ has no multiple roots, if $P(x)$ and its derivative $P'(x) \in \mathbb{F}_p[x]$ have no common non trivial factor in $\mathbb{F}_p[x]$.

artt. 373-375. Next he studies the case where the modulus is a **power of a prime** p^k.
(→ D 77; 31. 8. 1797) and (→ D 78; 4. 9. 1797).

10. As a preparation he proves **Hensel's Lemma**:
(→ D 79; 9.9.1797)

Obtain a factorization of a polynomial $P(x)$ modulo p^k for any $k \in \mathbb{N}$, once a factorization of $P(x)$ is known modulo p, under the hypothesis that the factors of $P(x)$ are relatively prime modulo p.

art. 374. He goes on by saying:

> "Aus diesem ersieht man, dass, wenn die Funktion X nach dem Modul p keine gleichen Factoren hat, dieselbe nach dem Modul p^k in ähnlicher Weise in Factoren zerlegt werden kann, wie nach dem Modul p. Wenn aber X gleiche Factoren hat, so wird die Sache bei weitem complicierter und lässt sich sogar mittelst der vorhergehenden Prinzipien nicht vollständig erledigen. Daher wollen wir, da wir nicht Alles, was hierher gehört, mitteilen können, nur einen einzigen Fall betrachten, welcher am häufigsten vorkommt und dessen Entwicklung zur Lösung einiger im Vorhergehenden übriggebliebener Zweifel erforderlich ist. Dieser Fall ist der, wo nur gleiche Factoren von einer Dimension in Betracht kommen. Dieser kann in zweckmässiger Weise auch zur Auffindung der Wurzeln der Congruenzen benutzt werden. Bei anderer Gelegenheit werden wir diesen Gegenstand allgemein behandeln."

> "From this one sees that, if the function [i. e., the polynomial] X does not have equal [i. e., multiple] factors with respect to the modulus p, it can be decomposed into factors modulo p^k in a similar way as modulo p. But if X has equal [i. e., multiple] factors, then things get much more complicated and cannot be completely settled, even by means of the preceding principles. For this reason, since we cannot communicate everything pertinent to this subject, we will consider only a single case, the one which occurs most often and whose clarification is necessary in order to resolve certain doubts [that might have remained] in the preceding [articles]. Namely the case, where only equal factors of dimension one [i. e., of degree one] will be considered. This case can also be applied in an appropriate way to find the roots of congruences [i. e., polynomials]. We will treat this subject in a general way on another occasion."

art. 375. In the last article Gauss stops in the middle of his exposition, even in the middle of a formula.

Chronology

1777 (April 30) **Gauss**, born in Braunschweig.

1797 Gauss, *Disquisitiones generales de congruentiis.*

1801 Gauss, Publication of the *Disquisitiones arithmeticae.*

1830 Galois, *Sur la théorie des nombres.*

1845 (February) **Schönemann**, *Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist.*

1855 (February 23) **Gauss**, died in Göttingen.

1856 (October) **Dedekind**, *Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus.*

1863 Gauss, *Disquisitiones generales de congruentiis*, edited by Dedekind.

1889 Maser, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik.*

1902 Kühne, *Eine Wechselbeziehung zwischen Functionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt.*

1919 (April 10) **Kornblum**, *Über die Primfunktionen in einer arithmetischen Progression.*

1921 (June 20) **Artin's Thesis**, *Quadratische Körper im Gebiete der höheren Kongruenzen I, II.*

1925 F. K. Schmidt' Thesis, *Allgemeine Körper im Gebiet der höheren Kongruenzen.*

References

[Ar-1924] Artin, Emil: *Quadratische Körper im Gebiete der höheren Kongruenzen I, II.* Math. Zeitschrift 19 (1924), 153-246.

[Ba-1911] Bachmann, Paul: *Über Gauß zahlentheoretische Arbeiten.* Teubner, Leipzig, 1911. Materialien für eine wissenschaftliche Biographie von Gauß. Gesammelt von F. Klein und M. Brendel. Durchgesehener Abdruck in Carl Friedrich Gauss, Werke, Vol. X/2, Abhandlung 1, Göttingen, 1922-1933.

[De-1857] Dedekind, Richard: *Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus.* J. Reine Angew. Math. 54 (1857), 1-26. Ges. math. Werke, Band 1, V, pp. 40-67.

[De-1857b] Dedekind, Richard: *Beweis für die Irreduktibilität derKreisteilungs-Gleichungen.* J. Reine Angew. Math. 54 (1857), 27-30), Ges. math. Werke, Band 1, VI, pp. 68-71.

[De-1878] Dedekind, Richard: *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen.* Abh. Königl. Ges. Wiss. Göttingen 23 (1878), 1-23; Ges. math. Werke, Band 1, XV, pp. 202-232.

[De-1985] Dedekind, Richard: *Vorlesung über Differential- und Integralrechnung 1861/62 in einer Mitschrift von Heinrich Bechtold*, bearbeitet von Max-Albert Knus und Winfried Scharlau. Vieweg, Braunschweig, Wiesbaden,1985.

[DW-1882] Dedekind, Richard; Weber, Heinrich: *Theorie der algebraischen Funktionen einer Veränderlichen.* J. Reine Angew. Math. 92 (1882; datiert Oktober 1880), 181-290; Dedekind, Ges. math. Werke, Band 1, XVIII, pp. 238-350.

[Di-1842] Dirichlet, G. Lejeune: *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes.* Journ. f. reine angew. Math. 24 (1842), 291-371; Werke, Erster Band, XXXII, Berlin, 1889, pp. 533-618.

[Did-1985] Dieudonné, Jean: *History of Algebraic Geometry.* Wadsworth, Monterey, California, 1985. [Translation of *Cours de géométrie algébrique I*, Presses Universitaires de France, Paris, 1974.]

[Ei-1847] Eisenstein, Gotthold: *Genaue Untersuchung der unendlichen Doppelproducte, aus welchen die elliptischen Functionen als Quotienten zusammengesetzt sind, und der mit ihnen zusammenhängenden Doppelreihen (als eine neue Begründungsweise der Theorie der elliptischen Functionen, mit besonderer Berücksichtigung ihrer Analogie zu den Kreisfunctionen).* J. Reine Angew. Math. 35 (1847), 153-274; Math. Werke, Band 1, [28f], pp. 357-478.

[Eu-1760] Euler, Leonhard: *Demonstratio theorematis FERMATIANI omnem numerum primum formae* $4n+1$ *esse summam duorum quadratorum.* Novi. comm. acad. sci. Petrop. 5 (1754/5) 1760, pp. 3-13; Opera Omnia, Series Prima, II, E. 241, pp. 328-337.

[Eu-1774] Euler, Leonhard: *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.* Novi. comm. acad. sci. Petrop. 18 (1773) 1774, pp. 85-135; Opera Omnia, Series Prima, III, E. 449, pp. 240-281.

[Fr-1994] Frei, Günther: *The Reciprocity Law from Euler to Eisenstein.* In: The Intersection of History and Mathematics (Editors: Sasaki Ch., Sugiura M., Dauben J.W.). Birkhäuser, Basel (1994), pp. 67-88.

[Fr-2001] Frei, Günther: *On the Development of the Theory of Function Fields over a Finite Field from Gauss to Dedekind and Artin.* Preprint, December 2001.

[Fr-2002] Frei, Günther: *On the History of the Artin Reciprocity Law in Abelian Extensions of Algebraic Number Fields: How Artin was led to his Reciprocity Law.* Preprint, April 2002. To appear in the "Abel-Book" of the Abel Bicentennial Conference 2002, Oslo, June, 2002.

[Ga-1801] Gauss, Carl Friedrich: *Disquisitiones arithmeticae.* Werke, Erster Band, Göttingen, 1863. (German translation in [Ma-1889]; English translation in [Ga-1966], Second corrected printing, Springer, Heidelberg, 1986.)

[Ga-1863] Gauss, Carl Friedrich: *Werke.* Zweiter Band. Göttingen, 1863.

[Ga-1876] Gauss, Carl Friedrich: *Werke.* Zweiter Band, Zweiter Abdruck. Göttingen, 1876.

[Ga-1899] Gauss, Carl Friedrich: *Briefwechsel zwischen Carl Friedrich*

Gauss und Wolfgang Bolyai. Herausgegeben von Franz Schmidt und Paul Stäckel. Teubner, Leipzig, 1899.

[Ga-1966] Carl Friedrich Gauss: *Disquisitiones arithmeticae.* Translated by Arthur A. Clarke. Yale University Press, New Haven, 1966.

[Ga-1985] Gauss, Carl Friedrich: *Mathematisches Tagebuch 1796-1814.* Mit einer historischen Einführung von Kurt-R. Biermann. Ins Deutsche übertragen von Elisabeth Schuhmann. Durchgesehen und mit Anmerkungen versehen von Hans Wußing und Olaf Neumann. 4. Auflage. Ostwalds Klassiker der exakten Wissenschaften 256. Akademische Verlagsgesellschaft Geest & Portig, Leipzig, 1985.

[Gal-1897] Galois, Évariste: *Oeuvres mathématiques.* Gauthier-Villars, Paris, 1897.

[Gr-1984] Gray, J. J.: *A commentary on Gauss's mathematical diary, 1796-1814, with an English translation.* Expo. Math. 2 (1984), pp. 97-130.

[Ha-1926] Hasse, Helmut: *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I; Ia; II.* J.-ber. Deutsch. Math. Ver. 35 (1926), 1-55; 36 (1927), 233-311; Ergänzungsband 6 (1930), 1-204.

[Ha-1933] Hasse, Helmut: *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufige Mitteilung.* Nachrichten Ges. Wiss. Göttingen I, Nr. 42 (1933), 253-262.

[Ko-1919] Kornblum, Heinrich: *Über die Primfunktionen in einer arithmetischen Progression.* Math. Zeitschrift 5 (1919), 100-111.

[Kü-1902] Kühne, H.: *Eine Wechselbeziehung zwischen Functionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt.* J. Reine Angew. Math. 124 (1902), 121-133.

[Kü-1903] Kühne, H.: *Angenäherte Auflösung von Congruenzen nach Primmodulsystemen in Zusammenhang mit den Einheiten gewisser Körper.* J. Reine Angew. Math. 126 (1903), 102-115.

[Ku-1847] Kummer, Ernst Eduard: *Zur Theorie der complexen Zahlen.*

J. Reine Angew. Math. 35 (1847), 319-326.

[La-1770] Lagrangre, *Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers.* Mémoire de l'Académie royale des Sciences et Belles-Lettres de Berlin, vol. XXIV, 1770; Oeuvres (publiées par J.-A. Serret), tome deuxième, Gauthier-Villars, Paris, 1868, pp. 655-726.

[Ma-1889] Maser, H.: *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik.* Julius Springer, Berlin, 1889.

[Ro-2001] Roquette, Peter: *Class Field Theory in Characteristic p, its Origin and Development.* In: Class Field Theory – Its Centenary and Prospect, edited by K. Miyake, Advanced Studies in Pure Mathematics 30, Tokyo (2001), pp. 549-631.

[Sch-1845] Schönemann: *Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist.* J. Reine Angew. Math. 31 (1846), 269-325.

[Sch-1846] Schönemann: *Von denjenigen Moduln, welche Potenzen von Primzahlen sind.* J. Reine Angew. Math. 32 (1846), 93-105.

[Sm-1925] Schmidt, F. K.: *Allgemeine Körper im Gebiet der höheren Kongruenzen.* Inauguraldissertation zur Erlangung der Doktorwürde. Naturw. Math. Fakultät der Universität Freiburg (1925), 52 p.

[Sm-1926] Schmidt, F. K.: *Zur Zahlentheorie in Körpern der Charakteristik p. Vorläufige Mitteilung.* Sitz.-ber. phys. med. Soz. Erlangen 58/59 (1926/27), 159-172.

[Sm-1931a] Schmidt, F. K.: *Analytische Zahlentheorie in Körpern der Charakteristik p.* Math. Zeitschrift 33 (1931), 1-32.

[Sm-1931b] Schmidt, F. K.: *Die Theorie der Klassenkörper über einem Körper algebraischer Funktionen in einer Unbestimmten und mit endlichem Koeffizientenbereich.* Sitz.-ber. phys. med. Soz. Erlangen 62 (1931), 267-284.

[We-1948] Weil, André: *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités scientifiques et industrielles, 1041. Publications de l'Institut de Mathématique de l'Université de Strasbourg, VII. Hermann, Paris, 1948.

Acknowledgement

I would like to thank *Peter Roquette*, *Urs Stammbach* and *Franz Lemmermeyer* for their commentaries and suggestions on the first draft of my manuscript, and the editors of this volume for asking me to enlarge the first draft.

Hombrechtikon, the 18th of July, 2002.

Günther Frei
Lützelstrasse 36
CH-8634 Hombrechtikon
Switzerland

E-mail: g.frei@active.ch