Karel Lepka
Matyáš Lerch's work on number theory

Masarykova univerzita, Brno 1995, 78 str.

Persistent URL: http://dml.cz/dmlcz/501874

MASARYK UNIVERSITY, FACULTY OF SCIENCE

MATYÁŠ LERCH'S WORK ON NUMBER THEORY

Karel Lepka

Brno, 1995

The preparation of this text was supported by the Grant Agency of the Czech republic, Number Theory, its Algebraic Aspects and its Relationship to Computer Science, No. 201/93/2122.

Contents

1 Introduction

Matyáš Lerch (1860–1922), a significant Czech mathematician, published during his life about 250 articles from various fields of mathematics. The purpose of this publication is to inform the readers on Lerch's work in the number theory which deals above all with the number of classes of binar quadratic forms with integral coefficients. Other articles are devoted to Gauss's summs, Fermat quotient, quadratic residues and some other problems. Lerch's works were published in Czech, German, French and Polish.

His brief curricullum is published in chapter 2. There are mentioned Lerch's scientific and pedagogical activities above all.

Reviews of all Lerch's works on number theory are published in chapter 3; those were taken from [F. d. M.]. Papers No. 1, 41 and 51 from the list are without review. The complete list of Lerch's papers on number theory is published in the end of section 3.

Because paper No.1 is short and it is the first Lerch's paper on number theory, we publish it complete in section 4.

To enable the readers to become familiar with Lerch's methods and the way in he had published his results, in chapters 5 and 6 we present the papers No.42 and No. 44, which are devoted to Fermat quotient. Lerch presents in it not only already known results got in different ways but many new results as well. Paper No.42 contributed in a significant way to the development of number theory. Lerch's fundamental work "Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coeficients entiers" ist too large to be published here.

The paper No. 52 was found in Lerch's inheritance and published after his death thanks to Professor Borůvka and Professor Hostinský. This paper is interesting, both the method and results, that is why we published it's resume in detail in French in section 7 made by Professor Hostinský.

All given articles are published in the original form regardless present grammar rules and spelling. All Czech names are written according right Czech grammar rules. All papers mentioned in this publication are available at the Departement of Mathematics of Masaryk University Brno or at the author of this publication.

Acknowledgment. In the end I would like to thank all people who participated in this publication. Especially I would like to express my thanks to Professor Skula for reading the manuscript and valuable advice as to the selection of illustrations from Lerch's work. I thank Mgr. Machalová for her kind lending me her diploma thesis "About Matyáš Lerch" and other useful materials. I would like to thank to Doc. J. Kuben and Doc. V. Lešovský from the Military Academy in Brno for help as to graphic arrangement of the text.

2 Curriculum vitae.

M. Lerch was born on February 20, 1860 in Milínov (South-West Bohemia) in the family of a farmer. At the age of six he was seriously injured on his left leg. After his recovery the leg remained bent and he was able to move only on crutches. Owing to that started his education at the age of nine. In 1874–77 he attended the citizen school in Sušice and there his exclusive talent for mathematics became evident. František Scheinost, the owner of the factory in Sušice, offered him the position of the clerk in his factory. After a short working period as a clerk Lerch decided to continue his studies. In 1877 he passed the entrance exam and started the grammar school in Plzeň. Thanks to excellent study results he was given the exception and could continue with the fifth class. In the course of sixth class he moved to Rakovník where he passed his school-leaving examination with honours on July 13, 1880.

In 1880 he entered the Czech Technical College in Prague as the full-time student; he chose the building ingeneering branch. After three-years study he intended to pass the so-called "teacher exam" and to became a teacher at the grammar school, but he had to stop the carrier as a teacher because of his handicap. Having taken this fact into account he started to study mathematics at Professor Eduard Weyr and Professor Gabriel Blažek and geometry at Professor E. Weyr and Professor F. Tilšer. In those times he began to publish. His first paper "Příspěvek k teorii kuželoseček" (The contribution to the theory of the conical curves) was published in Časopis pro pěstování matematiky a fyziky **10** (1881), page 160–177. He fully devoted himself to studies. His living standard was very low, because he had no income.

In 1883–84 he became the external student at the Charles University at Professor F. J. Studnička. In May 1884 he gained the state grant of 800 golden for the studying at the University in Berlin. He was the student of Weierstrass, Kronecker, Fuchs and Runge. Although he left for Berlin mainly owing to Weierstrass, he returned as the Kronecker's student. He changed his subject from general analysis to the actual problems especially he studied special functions because he liked that best. Perfect mastering infinite series and analytic functions as well as his intuition enabled him to became the excellent mathematician well known all over the world. Professors Kronecker, Weierstrass and Fuchs gave Lerch excellent references about his talent, diligence and scientific outlook. During his stay in Berlin Lerch got acquainted with some young mathematicians, especially with Rusian mathematician Sonja Kowalewska and German mathematicians Heffter, Köhler and Runge.

Having returned from Berlin he habilitated and became the privat Docent at the Technical College in Prague. Because he wasn't graduated at the University, he couldn't gain the doctor's degree. In 1893 he was appointed the extra member both of the Czech Royal Society of science and Czech Academy. In 1886–96 he published at about 110 papers (almost half of the total items). Since 1885 Lerch published his papers also in many foreign magazines (see the list of magazins) and he became the world-known mathematician. The list of European and American mathematicians whom Lerch sent his offprints involves more than 100 adresses.

I would like to mention Lerch's relation with Ch. Hermite. This excellent French mathematician was enthusiastic by some of Lerch's papers and regarded highly his scientific work.

In spite of his excellent results he did not get the Professor's degree at the Czech Colleges or University so he in 1896 left for the University in Freiburg (Swiss). Thanks to Hermite he was appointed professor at the University. There he was teaching for 10 years. Those days Lerch's scientific activity culminated. He published at about 70 papers, the half of them written in Czech. In 1900 Lerch won the Prize of the Paris Academy for the work "Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers". In 1900–1901 he became the Dean of the Faculty of Natural Science of the University of Freiburg. Even Lerch's living conditions changed for the better. Besides increasing of his income he engaged his niece Růžena Sejpková to keep the household, so that he could concentrate on the pedagogic and scientific work. Later he got married his niece. In 1899 he had a surgery on the injured leg; after that he was able to move only with a stick, for short distances even without one.

Although he reached much success, he wanted to teach at the Czech Technical College or University. Therefore he accepted with pleasure the professorship at the Technical College in Brno where he taught till 1920. In that period published more than 30 papers, almost all of them was published in Czech magazines. In 1907 Lerch was given the honour membership of the Union of Czech mathematicians and physicists, in 1909 he gained the degree of doctor honoris causa at the Charles University. In 1908–1909 he became the Dean of the Technical College of machinery engineering. In 1910 Lerch was elected the President of the Technical College, but he had to give up due to this health (he suffered diabetes).

In 1920 Lerch was named Professor of the new established Masaryk's University in Brno and he began to organize its mathematical institute. Those years he reached the life satisfaction. In 1921 he was named a proper member of Czech Academy. Matyáš Lerch died on August 3, 1922 of pneumonia.

Lerch was an energetic man, straightforward in his dealings and he was really jokeful. He was able to concentrate on solving the problems. He used to work on several topics at the sme time, he regarded changes in topics stimulative. He took care about the style of his papers. Except Czech he spoke fluently German and French. He was endowed by impressive intuition. Lerch wrote about that: "I thank the very spontaneous inspiration, although it is usually imperfect in the beginning. I continuosly correct my style. This way I reach improving of my consideration."

For Lerch' teaching was typical high level of the lectures and strong examining. He recquired exact answes and made students read books from various branches of mathematics.

His scholar student and continuator Professor Borůvka wrote about Lerch: "Lerch's importance for scientists of all branches depends above all on the accuracz of thinking and the clear intrpretation. In addition to that Lerch had broad knowledge from the branches close to his and he was able to input his results into similar branches. He had big understanding for the application of other scientific results. His teaching at colleges and universities is very important as well, because

he educated a lot of successors."

The curriculum vitae was written by the following papers:
L. Frank: O životě Matyáše Lercha, Časopis pro pěstování matematiky a fyziky **78** (1953), 119–137
J. Škrášek: Život a dílo profesora Matyáše Lercha, Časopis pro pěstování matematiky a fyziky **85** (1960), 228–240.

The quotation of Professor Borůvka is published with agreement of his granddaughter Mrs. Machalová.

3 Reviews.

[1] Deux théorèmes d'arithmétique.

Prag. Ber. 683–688 F. d. M. **19** (1887), 168

Bezeichnet man die Anzahl der Teiler von α, welche grösser als β sind, mit $\psi(\alpha, \beta)$, so ist

$$\sum_{\varrho=0}^{[\frac{n}{2}]} \psi(n-\varrho, \varrho) = n$$

und

$$\sum_{\varrho=0}^{n} \psi(n+\varrho, \varrho) = 2n.$$

Sn.

[2] Sur une propriété des nombres.

Teixeira J. VIII. 161–163. F. d. M. **19** (1887), 168

Herr Lerch giebt folgenden Satz:

Die Summe aller möglichen Producte von der Form $q_1 q_2 q_3 \cdots q_n$, wo die q ganze positive Zahlen sind, die den Bedingungen $q_1 \leq 2, q_{a+1} \leq 1+q_a$ genügen, ist gleich dem Product $1{\cdot}3{\cdot}5 \cdots (2n{+}1)$. Dieser Satz ergiebt sich auf zwei verschiedene Weisen aus der Berechnung des Wertes der Ableitung $\left(\frac{d^{n+2}x}{du^{n+2}}\right)_{u=0}$, für $x = 1 - \sqrt{1-2u}$.

Tx. (Hch.)

[3] Modification de la troisième démonstration donnée par Gauss de la loi de réciprocité de Legendre.

Teixeira J. VIII. 137–146. F. d. M. **19** (1887), 180

Der Beweis, den Herr Lerch giebt, beruht auf demselben Princip wie die dritte von Gauss für das Legendre'sche Reciprocitätsgesetz gegebene. Er stützt sich im wesentlichen auf die Congruenz:

$$q^{\frac{1}{2}(p-1)} \equiv \operatorname{sgn} \prod_{\nu=1}^{\frac{1}{2}(p-1)} R\left(\frac{\nu q}{p}\right) \pmod{p},$$

wo p eine Primzahl > 2 und q eine ganze Zahl, die relativ prim zu p ist, bedeutet. $R\left(\frac{\nu q}{p}\right)$ ist der Wert, den man erhält, wenn man von der Grösse $\frac{\nu q}{p}$ die ihr am

nächsten liegende ganze Zahl abzieht, liegt also zwischen $\pm\frac{1}{2}k$.

Tx. (Hch.)

[4] Sur une formule d'arithmétique.

Darboux Bull. (2) XII. 100–108. F. d. M. **20** (1888), 184

[5] Théorèmes d'arithmétique.

Darboux Bull. (2) XII. 121–126. F. d. M. **20** (1888), 184

[6] Sur une formule d'arithmétique.

C.R. CVI. 186–187. F. d. M. **20** (1888), 184

Die Divisoren von p seien geteilt in solche, welche grösser als q und in solche, welche nicht grösser als q sind; die Anzahl der ersteren sei $\psi(p,q)$, die Anzahl der letzteren $\chi(p,q)$. Alsdann lautet die Formel des Herrn Lerch:

$$\sum_{a=0}^{(\frac{m}{a})}[\psi(m-\sigma a,k+\sigma-1)-\chi(m-\sigma a,a)]+\sum_{\lambda=1}^{\chi-1}[\psi(m+\lambda a,\lambda-1)-\chi(m+\lambda a,a)]=0.$$

Diese Formel wird abgeleitet aus der Gleichung:

$$\sum_{\nu=1}^{\infty}\frac{x^{\chi\nu}}{(1-x^{\nu})(1-x^{\alpha+\nu})}=\frac{1}{1-x^{\alpha}}\sum_{\nu=1}^{a}\frac{x^{\nu}}{1-x^{\nu}}-\sum_{\lambda=1}^{\chi-1}\sum_{\nu=1}^{\infty}\frac{x^{\lambda\nu}}{1-x^{\alpha+\nu}}$$

und anderseits zu der Formel des Herrn Hermite:

$$\sum_{\alpha=0}^{n-1}E(x+\frac{\alpha}{n})=E(nx)$$

in Beziehung gesetzt. Zahlreiche Specialisirungen ergeben besonders Eigenschaften der ψ -Function, sowie einen Beweis eines Satzes von Catalan, wonach die Gesamtanzahl der ganzzahligen, nicht negativen Lösungen der n Gleichungen

$$kx+(x+1)y=n-k$$
$$(k=1,2,\ldots,n)$$

genau gleich n ist.

Sn.

[7] Sur le développement en série de certaines fonctions arithmétiques.

C. R. CVIII. 171–174. F. d. M. **21** (1889), 251

Subtrahirt man von x die nächste ganze Zahl und nennt den Rest $R(x)$, so dass $-\frac{1}{2} \leq R(x) \leq \frac{1}{2}$ ist; bezeichnet $R^*(x)$ eine Function, die im allgemeinenen gleich $R(x)$ ist, jedoch sich von $R(x)$ dadurch unterscheidet, dass sie verschwindet, wenn $x - \frac{1}{2}$ gleich einer ganzen Zahl wird; bedeutet $\operatorname{sgn} R^*(x)$ den Wert $+1, 0, -1$, je nachdem $R^*(x)$ positiv, Null oder negativ ist, so giebt der Verfasser diesen Functionen das Argument $x + \frac{\alpha m}{n}$ und berechnet für $\alpha = 0, 1, 2, \ldots, n-1$ die Summen:

$$\sum R^*\left(x + \frac{\alpha m}{n}\right), \qquad \sum \operatorname{sgn} R^*\left(x + \frac{\alpha m}{n}\right), \qquad \sum \left|R\left(x + \frac{\alpha m}{n}\right)\right|.$$

Bezeichnet $\left(\frac{k}{n}\right)$ das durch Jacobi verallgemeinerte Legendresche Zeichen, so ergiebt sich weiter, dass die Summen

$$\sum \left(\frac{\alpha m}{n}\right) R^*\left(x + \frac{\alpha m}{n}\right), \qquad \sum \left(\frac{\alpha m}{n}\right) \operatorname{sgn} R^*\left(x + \frac{\alpha m}{n}\right),$$
$$\sum \left(\frac{\alpha m}{n}\right) \left|R\left(x + \frac{\alpha m}{n}\right)\right|$$

von der Zahl m unabhänging sind, vorausgesetzt, dass die ungerade positive Zahl n zu m relativ prim ist und keinen quadratischen Teiler besitzt.

Wz.

[8] Arithmetische Lehrsätze.

Časopis XXI. 90–95, 185–190. (Böhmisch.) F. d. M. **24** (1892), 186

Bezeichnet E (entier) das bekannte Symbol Legendre's, so ist

$$E\left(\frac{n}{k}\right) - E\left(\frac{n-1}{k}\right) = \begin{cases} 1 & \text{(divis. } k\text{)}, \\ 0 & \text{(non div. } k\text{)}; \end{cases} \tag{1}$$

daraus folgt dann

$$\sum_{k=1}^{n} \left[E\left(\frac{n}{k}\right) - E\left(\frac{n-1}{k}\right)\right] = \Theta(n),$$

wo $\Theta(n)$ die Divisorenanzahl von n bezeichnet,und

$$\sum_{k=1}^{n} \Theta(k) = \sum E\left(\frac{n}{k}\right). \tag{2}$$

Aus Formel (1) folgt weiter

$$\sum_{k=1}^{n} \Theta_1(k) = \sum kE\left(\frac{n}{k}\right), \tag{3}$$

wenn

$$\Theta_1(n) = \Theta(n) + 2,$$

und ebenso

$$\sum_{k=1}^{n} \Theta_s(k) = \sum k^s E\left(\frac{n}{k}\right), \tag{4}$$

wo $\Theta_s(n)$ die Summe der zur Potenz s erhobenen Divisoren von n bedeutet, so dass daraus für $s = 0, 1$ die Formeln (2), (3) sich ergeben.

Allgemein gilt dann, wenn

$$f(1), f(2), f(3), \ldots$$

beliebige Grössen bezeichnen und δ alle Divisoren vertritt, also

$$\sum_{\delta} f(\delta) = F(n),$$

wie z. B.

$$F(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12),$$

die Relation

$$\sum_{k=1}^{n} F(k) = \sum f(k) E\left(\frac{n}{k}\right). \tag{5}$$

Std.

[9] Sur quelques théorèmes d'arithmétique.

Prag. Ber. 11 S. (1894). F. d. M. **25** (1894), 274

Bezeichnet $\psi(p, q)$ die Zahl der Teiler von p, welche grösser als q sind, dagegen $\chi(p, q)$ die Zahl derselben kleiner als q, so ist:

$$\sum_{a=0}^{\left[\frac{m-1}{n}\right]} \psi(m - an, a) = \sum_{a=0}^{\left[\frac{m-1}{n}\right]} \chi(m - an, n);$$

wenn m und n verschiedene ganze positive, sonst beliebige Zahlen sind. Diese von dem Verfasser schon 1888 publicirte Formel (F. d. M. XX. 184) wird hier bewiesen und in ihre verschiedenen Consequenzen verfolgt.

Sn.

[10] Bemerkungen über eine Klasse arithmetischer Lehrsätze.

Prag. Ber. 1894. 20 S. (1894). F. d. M. **25** (1894), 274

[11] Ueber eine arithmetische Relation.

Prag. Ber. 1894. 16 S. (1894). F. d. M. **25** (1894), 274

Die Eigenschaften der zahlentheoretischen Functionen, welche diejenigen Anzahlen der Teiler von p bezeichnen, die entweder grösser oder auch nicht grösser als q sind, waren von dem Verfasser schon früher studirt worden und haben mittlerweile auch die Herren Schröder und Busche beschäftigt. Die ursprüngliche Quelle der gefundenen Formeln ist in den aus der Theorie der elliptischen Functionen entstammenden Reihen zu suchen.

Sn.

[12] Sur un théorème de Kronecker.

Prag. Ber. 1893, No IX. 17 S. F. d. M. **25** (1894), 312 (793)

Neuer, interessanter Beweis der Kronecker'schen Formel:

$$\lim_{\varrho=0}\left\{-\frac{1}{\varrho}+\frac{1}{2\pi}\sum_{m,n}\left(\frac{\sqrt{4ac-b^2}}{am^2+bmn+cn^2}\right)^{1+\varrho}\right\}=-2\Gamma'(1)+\log\frac{c}{\sqrt{4ca-b^2}}+$$
$$\frac{\pi\sqrt{4ac-b^2}}{6c}-2\log\prod_{n=1}^{\infty}\left(1-e^{2nw_1\pi i}\right)\left(1-e^{2nw_2\pi i}\right),$$

in der w_1 und w_2 die beiden Wurzeln der quadratischen Gleichung:

$$a+bw+cw^2=0 \quad (a>0, \quad c>0, \quad 4ac-b^2>0)$$

bedeuten.

St.

[13] Sur une intégrale définie qui représente la fonction $\zeta(s)$ de Riemann.

Chicago Congress, Math. papers. I. 165–166. F. d. M. **26** (1895), 216

Setzt man $(1-2^{-s})\zeta(s)=\lambda(s)$, so hat man für Werte von s, deren reeller Teil grösser als 1 ist,

$$\lambda(s)=1+\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\cdots,$$

und für jeden endlichen Wert von s wird $\lambda(s)$ durch die Gleichung

$$\lambda(s) = \frac{2^{s-2}}{s-1} - 2^{s-1} \int_0^{\frac{\pi}{2}} \frac{\sin s\varphi - e^{\frac{1}{2}\pi \operatorname{tg}\varphi} \cos s\varphi}{1 + e^{\pi \operatorname{tg}\varphi}} \cos^{s-2}\varphi \, d\varphi$$

dargestellt.

Hz.

[14] Sur diverses formules d'arithmétique.

Teixeira J. XII. 129–136. F. d. M. **26** (1895), 216

Der Verf. beweist zuerst die Formel:

$$\sum_{\alpha=1}^{\infty} E\left(\frac{m}{u+\alpha} - v\right) = \sum_{\alpha=1}^{\infty} E\left(\frac{m}{v+\alpha} - u\right),$$

wo $E(x)$ die grösste ganze Zahl bezeichnet, die nicht grösser als die positive Grösse x ist. Danach zieht er aus dieser Formel einige Folgerungen, insbesondere die Relation:

$$\sum_{\sigma} \left\{\psi\left(m - \sigma a, \frac{\sigma}{r}\right) + \psi(m - \sigma a, ra)\right\} = \sum_{\sigma} \left\{\psi\left(m - \sigma a, \frac{\sigma}{s}\right) + \psi(m - \sigma a, sa)\right\},$$

wo $\sigma > rsa$, und $\psi(p, q)$ die Anzahl der Divisoren von p bezeichnet, die q übersteigen; ferner auch die andere Formel:

$$\sum_{\sigma} \psi\left(m - \sigma a, \frac{\sigma}{r}\right) = \sum_{\sigma} \chi(m - \sigma a, ra),$$
$$\left(\sigma = 0, 1, 2, \ldots, \left[\frac{m-1}{a}\right]\right),$$

wo $\chi(p, q)$ die Anzahl der Divisoren von p bezeichnet, welche q nicht übertreffen.

Tx.(Lp.)

[15] Arithmetische Bemerkungen.

Časopis XXIV. 25–34, 118–124 (Böhmisch). F. d. M. **26** (1895), 217

[16] Arithmetische Notiz.

Časopis XXIV. 228–230 (Böhmisch). F. d. M. **26** (1895), 217

In beiden Artikeln handelt es sich um einige elementare Eigenschaften der ganzzahligen Functionen $\psi(a,b)$ und $\chi(a,b)$, von denen die erste die Anzahl der Teiler von a, die grösser als b sind, die zweite dagegen die Anzahl der Teiler von a, die nicht grösser als b sind, bedeutet.

Es möge hier bloss die Relation

$$\sum_{k=1}^{m} \chi(k,a) = aE\left(\frac{m}{a}\right) + \sum_{k=1}^{m} \psi\left(k, \frac{m}{a}\right)$$

Erwähnung finden. Speciell ist in der zweiten Note die Anzahl der Lösungen der Gleichung $E\left(\frac{n}{x}\right) = E\left(\frac{n}{x+1}\right)(x<n)$ durch den Ausdruck

$$\sum \psi(n-r,r) + \sum \chi(n-\varrho,\varrho),$$

$$\left(r \geq -\frac{1}{2} + \sqrt{n+\frac{1}{4}}, \varrho < -\frac{1}{2} + \sqrt{n+\frac{1}{4}}\right)$$

dargestellt worden.

Lh.

[17] Logarithmus der Factorielle n!.

Časopis XXIV. 129–132, (Böhmisch). F. d. M. **26** (1895), 225 (472)

Schliesst mit dem bemerkenswerten Resultat, dass

$$\frac{\log(n!)}{n\log n} = 1 + \delta_n;$$

wobei mit wachsendem n die Grösse δ_n abnimmt und das Product

$$\delta_n \cdot \log n$$

endlich bleibt.

Std.

[18] Sur le nombre des classes de formes quadratiques de déterminant négatif.

C. R. CXXI. 878–880. F. d. M. **26** (1895), 227

Es wird zunächst eine Thetaformel von Kronecker verallgemeinert. Zweitens wird, auf Grund der Kronecker'schen Formel, für die Klassenanzahl der definiten binären quadratischen Formen von einer negativen Determinante $-\Delta$, ohne quadratische Teiler und $\equiv 5 \pmod 8$, ein Ausdruck mittels Thetafunctionen gewonnen.

Mk.

[19] Sur une théorème de Zolotarev.

Bull. intern. de l'Ac. François Joseph. 1896. 4 S. F. d. M. **27** (1896), 141

Z o l o t a r e v hat im Jahre 1872 in den Nouv. Ann. (2) **9**, 354 einen Satz über die Permutationsklasse bewiesen, welche man erhält, wenn man in der Reihe (1) $k, 2k, 3k, \ldots, (p-1)k$, worin p eine Primzahl bedeutet und k nicht durch p teilbar ist, jedes Glied durch seinen kleinsten, in Bezug auf den Modul p genommenen positiven Rest ersetzt. Erteilt man einer Permutation als Charakter die Zahl +1 oder -1, je nachdem die Anzahl ihrer Inversionen gerade oder ungerade ist, so lautet der Satz von Z o l o t a r e v: "Die Permutation, auf welche sich die Reihe (1) reducirt, hat zum Charakter das Symbol $\left(\frac{k}{p}\right)$".— Verf. giebt folgende Verallgemeinerung dieses Satzes: "Ist k eine ganze zu $2m$ relativ prime Zahl, so hat die Permutation, welche entsteht, wenn man die Glieder der Reihe $k, 2k, 3k, \ldots, (2m-1)k$ nach dem Modul $2m$ reducirt, zum Charakter die Zahl $(-1)^{\frac{1}{2}(k-1)(m-1)}$. Ist ferner m eine ungerade positive Zahl und k relativ prim zu m, so hat die gebildete Permutation zum Charakter das Symbol $\left(\frac{k}{p}\right)$ in Sinne von J a c o b i."

Wbg.

[20] Ueber einen arithmetischen Satz von Zolotarev.

Rozpravy. **5,** No. 17. 8 S. (Böhmisch.) F. d. M. **27** (1896), 141

Jener Satz, auf Grund dessen von Z o l o t a r e v das L e g e n d r e'sche Gesetz der Reciprocität der quadratischen Reste bewiesen wurde, wird näher beleuchtet und in der Weise verallgemeinert, dass an Stelle der von Z o l o t a r e v angewandten Primzahl p eine beliebige ganze Zahl gesetzt wird.

Sda.

[21] Sur diverses formules d'arithmétique.

Teixeira J. **13,** 129–136. [1] F. d. M. **27** (1896), 159

Es werden die beiden folgenden Formeln bewiesen:

$$\sum_{\sigma}\left[\psi\left(m-\sigma a,\frac{\sigma}{r}\right)+\psi(m-\sigma a,ra)\right]= \sum_{\sigma}\left[\psi\left(m-\sigma a,\frac{\sigma}{s}\right)+\psi(m-\sigma a,sa)\right]; \quad (1)$$

$$\sum_{\sigma}\psi\left(m-\sigma a,\frac{\sigma}{r}\right)=\sum_{\sigma}\chi(m-\sigma a,ra). \quad (2)$$

[1] Reviews [15] and [21] concern the same paper

Hier bedeutet $\psi(p,q)$ die Anzahl der Teiler der positiven ganzen Zahl p, welche die positive Grösse q übertreffen, und $\chi(p,q)$ die Anzahl derjenigen Teiler von p, welche $\leq q$ sind. Ferner sind a, m, r, s irgend welche ganze positive Zahlen, während der Summationsbuchstabe σ in (1) alle ganzen Zahlen durchlaufen soll, die $> ars$ sind, in der zweiten Formel aber alle nicht negativen ganzen Zahlen, die $\frac{m-1}{a}$ nicht übertreffen.

Der Beweis beruht auf einer für die Function $E(x)$ bestehenden Identität, unter $E(x)$ die grösste, die Zahl x nicht übertreffende ganze Zahl verstanden. Der Uebergang zu den Teileranzahlen wird durch den Umstand gewonnen, dass die Differenz $E\left(\frac{n}{t}\right) - E\left(\frac{n-1}{t}\right)$ offenbar 1 oder 0 bedeutet, je nachdem t in n aufgeht oder nicht.

Fr.

[22] Sur quelques analogies des sommes de Gauss.

Prag. Ber. 1897, 16 S. F. d. M. **28** (1897), 176

Es werden hier (ganz dem Typus der G a u s s'schen Summen entsprechend) Summen von trigonometrischen Functionen betrachtet, welche sich auf die Multipla $k\pi/p$ (mit $k = 1, 2, \ldots, p-1$) des $(2p)^{\text{ten}}$ Teiles vom Vollwinkel 2π beziehen; dabei erscheint jedes Glied (wie bei den G a u s s'schen Summen) noch mit dem L e g e n d r e'schen Zeichen $(\frac{k}{p})$ behaftet; p bedeutet eine Primzahl. Die Summe der Reihe wird aber hier jedesmal durch die Klassenanzahl $Kl(-p)$ quadratischer Formen der Determinante $\Delta = -p$ ausgedrückt. Dies rührt daher, weil der Verf. seine Formeln durch analytische Umformung einer bekannten Gleichung D i r i c h l e t's gewinnt, welche für $\Delta > 4$ so lautet:

$$\sum_{k=1}^{\infty} \left(\frac{-\Delta}{k}\right) \frac{1}{k} = \frac{\pi}{\sqrt{\Delta}} Kl(-\Delta).$$

Ein einfaches, für $p > 3$ gültiges Beispiel der vom Verf. aufgestellten Summen ist $\sum_{a=1}^{p-1} \operatorname{ctg} \frac{\alpha^2 \pi}{p} = 2\sqrt{p}\, Kl(-p)$; für $p = 3$ ist rechts der Factor $\frac{2}{3}$ zuzufügen.

Fr.

[23] Sur quelques formules relatives au nombre des classes.

Darboux Bull. (2) **21,** 290–304. F. d. M. **28** (1897), 193

Die quadratischen Formen werden in der Gestalt $ax^2 + bxy + cy^2$ angesetzt. Die Discriminante $D = b^2 - 4ac$ ist dann entweder $\equiv 1$ oder $\equiv 0 \pmod 4$. Es sollen nur die D zugelassen werden, welche durch kein Quadrat ausser 4 teilbar sind, und im letzteren Falle soll $\frac{1}{4}D \equiv 2$ oder $3 \pmod 4$ zutreffen. $Cl(-\Delta)$ bedeutet die Klassenanzahl der Formen negativer Discriminante $D = -\Delta$, und unter τ wird

im allgemeinen der Wert 2, jedoch 6 für $\Delta = 3$ und 4 für $\Delta = 4$ verstanden. Unter Anknüpfung an die bekannte Relation:

$$Cl(-\Delta) = -\frac{\tau}{2\Delta} \sum_{\alpha=1}^{\Delta-1} \left(-\frac{\Delta}{\alpha}\right) \alpha \tag{1}$$

und unter Vermittelung der zahlentheoretischen Function $E(x)$ oder $[x]$ gelangt der Verf. für eine beliebige, durch Δ nicht teilbare ganze Zahl m zur Formel:

$$\frac{2}{\tau}\left[m - \left(\frac{-\Delta}{m}\right)\right] Cl(-\Delta) = -\sum_{\alpha=1}^{\Delta-1} \left(\frac{-\Delta}{\alpha}\right) E\left(\frac{\alpha m}{\Delta}\right),$$

welche er sodann in den Specialfällen $m = 2, 3, 4$ weiter discutirt. Es ergiebt sich z. B.

$$\sum_{\alpha=[\frac{\Delta}{4}]+1}^{[\frac{\Delta}{3}]} \left(-\frac{\Delta}{\alpha}\right) = \frac{1 - (\frac{\Delta}{2}) + (\frac{\Delta}{3}) + (\frac{\Delta}{4})}{2} \cdot Cl(-\Delta),$$

eine Formel, welche wegen der weit geringeren Gliederanzahl der Summe geeigneter zur Berechnung der Klassenanzahlen $Cl(-\Delta)$ erscheint, als (1).

Für eine weitere Art von Darstellungen der Function $Cl(-\Delta)$ diene das Beispiel:

$$Cl(-\Delta) = \frac{\tau\sqrt{\Delta}}{2\pi} \sum_{\nu=1}^{\infty} \left(-\frac{\Delta}{\nu}\right) \frac{\cos 2\nu x\pi}{\nu},$$

wo x eine dem Intervall $0 \leq x < \frac{1}{\Delta}$ angehörende Grösse ist. Für $x = 0$ entspringt eine wohlbekannte D i r i c h l e t'sche Gleichung.

Den Beschluss bilden einige mit den voraufgehenden Entwickelungen zusammenhängende Rechnungen im Anschluss an K r o n e c k e r's Untersuchungen über Modulfunctionen sowie insbesondere an dessen bekannte "Grenzformeln". (cf. F. d. M. **21,** 485, 1889 und **22,** 471, 1890).

Fr.

[24] Ueber die Gauss'schen Summen.

Časopis **28,** 1–24 (Böhmisch). F. d. M. **29** (1898), 168

Die Abhandlung ist eine Bearbeitung der bekannten Abhandlung K r o n e c k e r's (Berl. Monatsber. 1880; F. d. M **12,** 123, 1880); sie giebt zunächst eine strenge Begründung gewisser von K r o n e c k e r nur angedeuteten Grenzübergänge und führt die Auswertung der allgemeinen G a u s s'schen Summen zu Ende, indem sie sich auf die Identität

$$\sqrt{\frac{n}{n_1 i}} = (-1)^{\frac{1+\operatorname{sgn} n}{2} \cdot \frac{1-\operatorname{sgn} n_1}{2}} \frac{\sqrt{n}}{\sqrt{n_1}\sqrt{i}}$$

stützt.

Lh.

[25] Ueber die Anzahl der Klassen quadratischer Formen negativer Discriminante.

Rozpravy **7,** No. 4, 16 S. (Böhmisch.) F. d. M. **29** (1898), 174

Mit Hülfe von elementaren Betrachtungen werden die Summen $\sum F(4k)$ und $\sum F(4k-1)$, in welchen $F(\Delta)$ die Anzahl der Klassen quadratischer Formen der negativen Discriminante $b^2 - 4ac = -\Delta$ bezeichnet, auf Summation von gewissen grössten Ganzen zurückgeführt. Aehnliche Resultate hat vor Jahren H e r m i t e aus der Theorie der elliptischen Functionen (J. für Math. **100**) abgeleitet; dieselben beziehen sich auf Formen mit geradem mittleren Coefficienten und sind etwas einfacher als diejenigen des vorliegenden Aufsatzes.

Lh.

[26] Arithmetische Ableitung der zur Klassenanzahlbestimmung dienenden Lejeune - Dirichlet'schen Fundamentalformeln.

Rozpravy **7,** No. 5, 51 S. (Böhmisch.) F. d. M. **29** (1898), 175

[27] Ueber einen Zusammenhang des Legendre'schen Zeichens mit den Moebius'schen Zahlen.

Rozpravy **7,** No. 6, 12 S. (Böhmisch.) F. d. M. **29** (1898), 175

[28] Ueber die Summe der grössten Ganzen in einer gebrochenen arithmetischen Progression zweiter Ordnung und ihren Zusammenhang mit der Klassenanzahl quadratischer Formen negativer Discriminante.

Rozpravy **7,** No. 7, 8 S. (Böhmisch.) F. d. M. **29** (1898), 175

Die erste Abhandlung verfolgt bloss didaktische Zwecke, und zwar vor allen Dingen eine möglichst einfache Begründung der klassischen Reihe von D i r i c h l e t $\sum \left(\frac{D}{h}\right) h^{-1}$, die zur Klassenanzahlbestimmung dient. Dieselbe wurde nur deswegen gedruckt, um spätere Arbeiten des Verf. verständlich zu machen.

Die zweite Arbeit leistet die Auswertung der unendlichen Reihe

$$\sum \left(\frac{-\Delta}{\nu}\right) \frac{\cos 2\nu x\pi}{\nu}$$

vermittelst der Klassenanzahl und von grössten Ganzen gewisser Grössen, und zwar für eine beliebige negative Discriminante $-\Delta$. Durch geeignete Verknüpfung

der sich hier darbietenden Formeln gelangt man nach einigen Transformationen zu den Beziehungen

$$\sum_{\alpha=1}^{\Delta-1}\left(\frac{-\Delta}{\alpha}\right)d_\alpha = -\left(\frac{-\Delta}{n}\right)\varphi(\Delta),$$

$$\sum_{r=1}^{m=1}\left(\frac{r}{m}\right)\left(\frac{r+1}{m^2}\right) = (-1)^{\frac{m-1}{2}}\varepsilon_m,$$

in welchen d_α den grössten gemeinsamen Teiler von $n+\alpha$ und Δ, n eine positive ganze Zahl und $-\Delta$ eine negative Fundamentaldiscriminante bedeutet, und in der zweiten Formel ε_m die bekannten M o e b i u s'schen Zahlen sind, welche in vielen Fragen der analytischen Zahlentheorie auftreten, ferner m eine positive ungerade ganze Zahl ohne quadratische Teiler bedeutet.

Der Inhalt der dritten Abhandlung wird am besten durch die Formel charakterisirt:

$$\sum_{\alpha=1}^{n-1}\left\{\frac{\alpha^2 m}{n} - E\left(\frac{\alpha^2 m}{n}\right)\right\} = \frac{n-q}{2} - \sum_{n:d}\left(\frac{m}{d}\right)\frac{2}{\tau_d}\,Cl(-d),$$

in welcher m, n zwei teilerfremde positive ganze Zahlen sind, die zweite ausserdem ungerade und q^2 ihr grösster Quadratteiler; die Summation auf der rechten Seite bezieht sich auf alle negativen Teiler $-d$ von n, welche die Discriminantenform haben.

Lh.

[29] Résumé de trois notes d'arithmétique.

Bull. de l'Ac. d. Sciences de Bohème 1898. 6 S. F. d. M. **29** (1898), 176

Die erste Note giebt einen rein arithmetischen Beweis der Formel:

$$\left(\frac{Q^2}{l}\right)\sum_{(a,b,c)} N(l;a,b,c) = \tau\sum_{\lambda\lambda'=l}\left(\frac{-\Delta}{\lambda}\right)\left(\frac{Q^2}{\lambda'}\right),$$

welche nur eine andere Gestalt einer bekannten Formel D i r i c h l e t's vorstellt. Die Summe linker Hand bezieht sich auf die Klassen primitiver positiver Formen der negativen Determinante $-\Delta = b^2 - 4ac$, und es ist $\Delta = \Delta_0 Q^2$, wo Δ_0 die zugehörige Fundamentaldiscriminante ist. $N(l;a,b,c)$ bedeutet die Anzahl aller Lösungen von $am^2 + bmn + cn^2 = l$ in ganzen Zahlen m, n. Die Summe rechts ist auf die Factorenzerlegungen $l = \lambda\lambda'$ von l zu erstrecken; endlich ist $\tau = 2$ für $\Delta > 4$, während $\tau = 4$ und 6 für $\Delta = 4$, bez. 3 zu nehmen ist. Der Verf. beweist hier die fragliche Formel nicht, sondern berichtet über einige Anwendungen derselben, welche sich auf G a u s s'sche Summen, Klasssenanzahlen bei positiver Determinante und sogenannte P e l l'sche Zahlen beziehen.

Die zweite Note betrifft die sogenannten M ö b i u s'schen Zahlen ε_n, welche die Werte der sonst gewöhnlich durch $\mu(n)$ bezeichneten zahlentheoretischen Function darstellen (vergl. z. B. F. d. M. **28,** 177, 1897). Verf. beweist einen Zusammenhang dieser Zahlen mit dem L e g e n d r e'schen Zeichen, wie derselbe gegeben ist durch:

$$\sum_{r=1}^{m-1} \left(\frac{r}{m}\right)\left(\frac{r+1}{m^2}\right) = (-1)^{\frac{m-1}{2}}\varepsilon_m.$$

Die dritte Note handelt von Summen der Gestalt:

$$\sum_{\alpha=1}^{n-1} \left\{\frac{\alpha^2 m}{n} - E\left(\frac{\alpha^2 m}{n}\right)\right\},$$

wo m und n relativ prime ganze Zahlen sind. Es wird ein Zusammenhang zwischen solchen Summen und Klassenanzahlen aufgestellt. (Vergl. das vorangehende Referat.)

Fr.

[30] Sur la fonction $\zeta(s)$ pour les valeurs impaires de l'argument.

Teixeira J. **14,** 65–69. F. d. M. **31** (1900), 203

Der Verf. betrachtet in diesem Artikel die R i e m a n n'sche Function $\zeta(s) = \sum 1/m^s$ $(m = 1, 2, \ldots, \infty)$, um zu beweisen, dass man für $s = 4k-1$ ihre numerische Berechnung auf diejenige einer rasch convergirenden Reihe zurückführen kann vermittelst der Formel:

$$\sum_{m=1}^{\infty} \frac{1}{m^{4k-1}} = \frac{(2\pi)^{4k-1}}{(4k)!}\left[B_{2k} + (-1)^{k-1}\frac{1}{2}\binom{4k}{2k}B_k^2 + \sum_{\nu=1}^{k-1}(-1)^{\nu-1}\binom{4k}{2k}B_\nu B_{2k-\nu}\right] - 2\sum_{m=1}^{\infty}\frac{1}{m^{4k-1}}\cdot\frac{1}{e^{2m\pi}-1},$$

wo die B_ν die B e r n o u l l i'schen Zahlen bedeuten.

Tx.(Lp).

[31] Sur la formule fondamentale de Dirichlet qui sert à déterminer le nombre des classes de formes quadratiques binaires définies.

C. R. **135,** 1314–1315. F. d. M. **33** (1902), 222

Verf. hatte bei einer früheren Gelegenheit (vergl. F. d. M. **28,** 193 bis 194, 1897) aus der K r o n e c k e r schen Grenzformeln eine Folgerung gezogen, für welche er auch einen direkten Beweis in Aussicht gestellt hatte; diesen gibt er hier an.

Lnd.

[32] Démonstration élémentaire d'un théorème arithmétique.

Prague: Fr. Rivnac. Prag. Ber. 1903, Nr. 2, 3 S. F. d. M. **34** (1903), 205

Bedeutet m eine ganze Zahl, welche durch die Faktoren $a, b, c, \ldots, k, l$, von denen je zwei relativ prim sind, teilbar ist, so wird auf elementarem Wege der Satz bewiesen, daß die Anzahl derjenigen positiven ganzen Zahlen $a, b, c, \ldots k, l$ teilbar sind,

$$m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{l}\right)$$

ist.

F.

[33] Über den fünften Gaußschen Beweis des Reziprozitätsgesetzes für die quadratischen Reste.

Sep.-Abdr. a. d. Sitz.-Ber. d. Kgl. Böhm. Gesselsch. der Wissensch. 1903. Prag. 19 S. 8^0. [2] F. d. M. **34** (1903), 227

Verf. schlägt einen Weg ein, welcher sich an den fünften G a u ß schen Beweis des Reziprozitätsgesetzes anschließt, aber zugleich die Relationen

$$\left(\frac{m}{P}\right)\left(\frac{m'}{P}\right)=\left(\frac{mm'}{P}\right), \qquad \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right)=\left(\frac{m}{PQ}\right)$$

mitbeweist.

Lnd.

[34] Sur la cinquième démostration de Gauß de la loi de réciprocité de Legendre.

Teixeira J. **15,** 97–104. F. d. M. 34 (1903), 227

[2] See Prag. Ber.

Modifikation des fünften G a u ßschen Beweises für das Reziprozitätsgesetz, indem gleichzeitig die Gesetze aufgestellt werden (vergl. das vorstehende Referat):

$$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right), \qquad \left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right).$$

Tx. (Lp.)

[35] Bemerkung über die Theorie der Gaußschen Summen.

Sep.-Abdr. a. d. Sitz.-Ber. d. Kgl. Böhm. Gessellsch. der Wissensch. 1903. Prag. **4** S. 8^0.[3] F. d. M. **34** (1903), 227

ϱ, λ, μ seien drei ganze Zahlen und $\mu \gtrless 0$. Verf. betrachtet die Summe

$$\Phi(\varrho, \lambda, \mu) = \frac{1}{2} \sum_{\alpha=0}^{|2\mu|-1} e^{\frac{\alpha^2\lambda + \alpha\varrho}{\mu}\pi i},$$

welche für $\varrho = 0$ in die gewöhnliche G a u ßsche Summe übergeht. Er findet: wenn der größte gemeinsame Teiler von λ und μ nicht in ϱ aufgeht, ist $\Phi(\varrho, \lambda, \mu) = 0$. Sind λ und μ teilerfremd, so ist

$$\Phi(\varrho, \lambda, \mu)\Phi(\varrho, \lambda, -\mu) = \frac{1}{2}(1 + (-1)^{\varrho+\lambda\mu}) \mid \mu \mid,$$

also

$$\mid \Phi(\varrho, \lambda, \mu) \mid = \sqrt{\mid \mu \mid} \quad \text{oder} = 0.$$

Lnd.

[36] Zur Theorie der Gaußschen Summen.

Math. Ann. **57,** 554–567. F. d. M. **34** (1903), 228

C a u c h y hat die Gleichung bewiesen:

$$\sqrt{\frac{ri}{s}} \sum_{\nu=0}^{s-1} e^{-\frac{\nu^2 r\pi i}{s}} = \sum_{\nu=0}^{r-1} e^{\frac{\nu^2 s\pi i}{r}} \quad (r, s \text{ gerade}), \tag{1}$$

welche K r o n e c k e r als das Reziprozitätsgesetz der G a u ßschen Summen bezeichnete. Verf. beweist (1) und einige unwesentlich allgemeinere Relationen zunächst mit Hülfe einer durch zwei Funktionalgleichungen definierten ganzen

[3] See Prag. Ber.

transzedenten Funktion, dann auf direkterem Wege mit Hülfe der C a u c h y schen Formel

$$\sum_{n=-\infty}^{\infty} e^{-\frac{\pi}{a}(u+n)^2} = \sqrt{a} \sum_{n=-\infty}^{\infty} e^{-\alpha n^2 \pi + 2nu\pi i}. \tag{2}$$

Verf. kritisiert ferner zwei Beweisversuche, welche K r o n e c k e r (vergl. F. d. M. **12,** 123, 1880; s. auch B a c h m a n n, Lehrbuch der analytischen Zahlentheorie, 179–183, 1894), ausgehend von der G a u ßschen Summenformel mit, bezw. ohne Kenntnis der Vorzeichenbestimmung, für den Spezialfall $u = 0$ der Formel (2) angegeben hat; Verf. macht auf einen Fehlschluß aufmerksam und erklärt K r o n e c k e r s Entwicklungen für vollständig verfehlte Beweisversuche.

Lnd.

[37] Über die arithmetische Gleichung $Cl(-\Delta) = 1$.

Math. Ann. **57,** 568–570. F. d. M. **34** (1903), 242

Verf. beweist auf anderem Wege den Satz (vergl. das vorige Referat), daß die Klassenzahl $h = 1$ nur endlich vielen negativen Diskriminanten zukommt. In K r o n e c k e r scher Bezeichnungsweise (Form $ax^2 + bxy + cy^2$, Diskriminante $b^2 - 4ac$) bedeutet dies, daß die Klassenzahl 1 nur endlich vielen durch 4 teilbaren negativen Diskriminanten entspricht; ob sie überhaupt nur endlich vielen negativen Diskriminanten entspricht, kann leider nicht entschieden werden.

Lnd.

[38] Sur le nombre des classes de formes quadratiques binaires d'un discriminant positif fondamental.

Journ. de Math. (5) **9,** 337 bis 401. F. d. M. **34** (1903), 242

Es sei $Cl(D)$ die Klassenzahl der quadratischen Formen $ax^2 + bxy + cy^2$ der positiven Fundamentaldiskriminante $D = b^2 - 4ac$, $E(D)$ die Fundamentaleinheit $\frac{1}{2}(T + U\sqrt{D})$. Verf. beweist, auf die D i r i c h l e t schen Untersuchungen gestützt, die Relation

$$Cl(D) \log E(D) = 2\sqrt{\frac{D}{\pi}} \sum_{m=1}^{\infty} \left(\frac{D}{m}\right) \frac{1}{m} \int_{m\sqrt{\frac{u\pi}{D}}}^{\infty} e^{-x^2} dx + \sum_{m=1}^{\infty} \left(\frac{D}{m}\right) \int_{\frac{m^2\pi}{Du}}^{\infty} e^{-x} \frac{dx}{x},$$

wo u beliebig ist. Er bringt diese Formel noch auf eine einfachere Gestalt, welche — in der Annahme, daß $\log E(D)$ hinreichend genau bekannt ist — zur numerischen Berechnung der Klassenzahl auch für große Diskriminanten sehr geeignet ist. Der Kunstgriff liegt darin, daß man als Resultat eine ganze Zahl erhalten muß

und dementsprechend nur eine endliche, relativ kleine Anzahl von Gliedern in auftretenden unendlichen Reihen zu berechnen braucht.

Lnd.

[39] Sur quelqeues applications des sommes de Gauss.

Annali di Mat. (3) **11,** 79–91. F. d. M. **35** (1904), 209

Aus der G a u ß schen Summenformel leitet der Verf. den Wert des Ausdrucks

$$\sum_{\alpha=0}^{n-1} E^*\left(x+\frac{\alpha^2 m}{n}\right)$$

her, wo n ungerade und positiv, m zu n teilfremd ist und $E^*(x)$ für nicht ganze x gleich $E(x)$, für ganze x gleich $E(x)-\frac{1}{2}$ ist. Er findet, von der bekannten Gleichung

$$E^*(x) = x - \frac{1}{2} + \sum_{\nu=1}^{\infty} \frac{\sin 2\nu x\pi}{\nu\pi}$$

ausgehend,

$$\sum_{\alpha=0}^{n-1} \left\{ E^*\left(x+\frac{\alpha^2 m}{n}\right) - \left(x+\frac{\alpha^2 m}{n}\right)\right\} = -\frac{n}{2} + \sum_d \left(\frac{m}{d}\right) \Phi(d'x, d), \qquad (1)$$

wo d alle Divisoren von n durchläuft, $d' = \frac{n}{d}$ ist und $\Phi(z,d)$ durch die Gleichungen:

$$\Phi(z,d) = \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{\nu}{d}\right) \frac{\cos 2\nu z\pi}{\nu\pi} \quad \text{für } d \equiv -1 \pmod 4,$$

$$\Phi(z,d) = \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{\nu}{d}\right) \frac{\sin 2\nu z\pi}{\nu\pi} \quad \text{für } d \equiv 1 \pmod 4$$

definiert ist. Die rechte Seite von (1) läßt sich in geschlossener Form darstellen; daraus ergibt sich insbesondere, wenn $Cl(-\Delta)$ die Klassenzahl positiver primitiver quadratischer Formen der Diskriminante $-\Delta$ bezeichnet, wenn $\tau_\Delta = 2$ für $\Delta > 4$, $\tau_3 = 6$ ist, und wenn q^2 den größten quadratischen Faktor von n bezeichnet, für positive, teilfremde m, n (n ungerade):

$$\sum_{\alpha=1}^{n-1} E\left(\frac{\alpha^2 m}{n}\right) = m\left(\frac{n^3}{3} - \frac{n}{2} + \frac{1}{6}\right) - \frac{n-q}{2} + \sum_d \left(\frac{m}{d}\right) \frac{2}{\tau_d} Cl(-d),$$

wo d alle Teiler $4k+3$ von n durchläuft.

In Zusammenhang mit diesen Untersuchungen steht die Frage nach der Summe A der zwischen 0 und n gelegenen, zu n teilfremden quadratischen Reste von n. Verf. bestimmt A für ungerades n und findet speziell

$$A \equiv \frac{n}{3} \pmod{n},$$

falls n durch 3 teilbar ist und alle anderen Primfaktoren von n die Form $3k+2$ haben, dagegen

$$A \equiv 0 \pmod{n}$$

in allen anderen Fällen.

Lnd.

[40] Sur quelqes applications d'un théorème arithmétique de Jacobi.

Krakau Anz. 1904, 55–70. F. d. M. **35** (1904), 211

g sei eine primitive Wurzel der ungeraden Primzahl $p = 2m+1$, n eine positive ganze Zahl $< p-1$, α durch die Kongruenz

$$\alpha \equiv g^{p-1-n} \pmod{p}$$

bestimmt, und es werde die ganze Funktion von x

$$F_n(x) = \sum_{\nu=1}^{p-1} \alpha^{\operatorname{ind}\nu} x^\nu$$

betrachtet. J a c o b i (vgl. Werke, **6,** 254) hat die Kongruenz

$$F_n(1+y) \equiv -\frac{1}{n!} Y_n \pmod{p} \tag{1}$$

gefunden, wo Y_n die Summe der Glieder mit $y^n, y^{n+1}, \ldots, y^{p-1}$ in $\{\log(1+y)\}^n$ ist. Insbesondere ergibt sich für $n = m$

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) x^\nu \equiv -\frac{1}{m!} Y_m(x-1) \pmod{p}. \tag{2}$$

Verf. führt den Beweis von (1) aus und zieht dann einige Folgerungen aus (2). Z. B. ergibt sich, wenn

$$Y_m(y) = c_m y^m + \cdots + c_{2m} y^{2m}$$

ist und

$$-\frac{1}{m!} \sum_{\nu=m}^{2m} c_\nu (i-1)^\nu = A + iB$$

gesetzt wird, für alle Primzahlen $p = 4k + 1$

$$A \equiv B \equiv h \pmod{p},$$

wo h die Klassenzahl positiver quadratischer Formen der Diskriminante $-4p$ ist.

Lnd.

[41] Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$.

Math. Ann. **60,** 471–490. F. d. M. **36** (1905), 266

Setzt man

$$q(a) = \frac{a^{p-1} - 1}{p}$$

(p ungerade Primzahl), so genügt die Funktion $q(a)$ verschiedenen Kongruentzeigenschaften, die der Verf. in der vorliegenden Arbeit angibt. Die hauptsächlichsten Resultate sind die folgenden: Es wird

$$\sum_{a=1}^{p-1} q(a) \equiv \frac{(p-1)! + 1}{p} \pmod{p}.$$

Ist $[z]$ das größte Ganze von z, so ist:

$$q(a) \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu \cdot a} \left[\frac{\nu \cdot a}{p}\right] \pmod{p}$$

für jede zu p prime ganze Zahl a. Diese Kongruenz ergibt für $a = 2, 4, 8, \ldots$ interesante Anwendungen. Ferner führt sie auf

$$\sum_{\nu=1}^{p-1} aq(a) \equiv \frac{1}{2} \pmod{p}.$$

Mittels Einführung des L e g e n d r eschen Symbols $\left(\frac{\nu}{p}\right)$ beweist der Verf. die Relationen:

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu) \equiv 0 \pmod{p},$$

falls $p \equiv 3 \pmod 4$ ist, und

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu) \equiv (-1)^{\frac{p-5}{4}} \cdot 2 \cdot B_n \pmod{p},$$

falls $p \equiv 1 \pmod 4$ und B_n die n-te B e r n o u l l i sche Zahl ist. Ist $Cl(-p)$ die Klassenanzahl des quadratischen Körpers $(\sqrt{-p})$, so ist

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \nu q(\nu) \begin{array}{ll} \equiv 0 \pmod p, & \text{wenn } p \equiv 1 \pmod 4 \\ \equiv Cl(-p) \pmod p, & \text{wenn } p \equiv 3 \pmod 4. \end{array}$$

Eine Anwendung dieser Formel ist das Resultat, daß die unbestimmte Gleichung

$$ax - py = 1$$

gelöst wird durch

$$x = a - 12 \sum_{\nu=1}^{p-1} \nu \cdot \left[\frac{a\nu}{p}\right] \qquad (p \text{ Primzahl}).$$

Zum Schlusse werden ähnliche Kongruenzen auch für einen zusammmengesetzten Modul n gebildet durch Betrachtung der allgemeinen Funktion:

$$q(a) = \frac{a^{\varphi(m)} - 1}{m} \qquad (a \text{ prim zu } m).$$

Fu.

[42] Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers.

Acta Math. **29,** 333–424. F. d. M. **36** (1905), 288

Einleitung: Die vorliegende Arbeit ist ein Abdruck der Abhandlung, die 1900 den *Grand prix* der *Académie ès sciences* in Paris erhalten hat. Das Problem war, die Bestimmung der Klassenanzahl der quadratischen Formen zweier Variabeln mit ganzen, rationalen Koeffizienten zu fördern. Nach kurzer Angabe der D i r i c h l e t schen und K r o n e c k e r schen Entwicklungen für die Klassenanzahl wird auf die praktische Unbrauchbarkeit derselben, besonders im Falle positiver Diskriminanten, hingewiesen. Die Entwicklungen des Verf. hingegen bringen praktisch brauchbare Formeln. Die wichtigsten sind die folgenden: Es sei $C(l)D$ die Klassenanzahl der Diskriminante D, so ist

$$\frac{2}{\tau} Cl(-\Delta) = \frac{\sqrt{\Delta}}{\pi} \sum_{n=1}^{\infty} \left(\frac{-\Delta}{n}\right) \frac{1}{n} e^{-\frac{n^2\pi}{\Delta}} + \frac{2}{\sqrt{\pi}} \sum_{n=1}^{\infty} \left(\frac{-\Delta}{n}\right) \int_{n\sqrt{\frac{\pi}{\Delta}}}^{\infty} e^{-x^2}\, dx,$$

$$\frac{1}{\tau} Cl(-\Delta) = \sum_{1}^{\infty} \left(\frac{-\Delta}{m}\right) \frac{1}{1 + e^{\frac{m\pi\sqrt{2\Delta}}{\Delta}}} + \frac{1}{\sqrt{2}} \sum_{1}^{\infty} \left(\frac{-\Delta}{m}\right) \frac{1}{\sin \text{hyp} \frac{2m\pi}{\sqrt{2\Delta}}},$$

wo $\Delta > 0$ ist.

$$Cl(D)\lg E(D) = \frac{2\sqrt{D}}{\sqrt{\pi}}\sum_1^\infty \left(\frac{D}{n}\right)\frac{1}{n}\int_{\sqrt[n]{\frac{\pi}{D}}}^\infty e^{-x^2}dx + \sum_1^\infty\left(\frac{D}{n}\right)\int_{\frac{n^2\pi}{D}}^\infty e^{-x}\,\frac{dx}{x},$$

$$\frac{1}{2}Cl(D)\lg E(D) = \sqrt{D}\sum_1^\infty\left(\frac{D}{n}\right)\frac{1}{n}\cdot\frac{1}{e^{\frac{2n\pi}{\sqrt{2D}}}+1} + \sum_1^\infty\left(\frac{D}{n}\right)\lg\frac{1+e^{-\frac{n\pi\sqrt{2D}}{D}}}{1-e^{-\frac{n\pi\sqrt{2D}}{D}}},$$

wo

$$E(D) = \frac{T+U\sqrt{D}}{2} \text{ und } T^2 - DU^2 = 4.$$

Kap. 1. Zunächst werden die beiden bekannten Formeln

$$Cl(-\Delta) = \tau\sum_{h=1}^\infty\left(\frac{-\Delta}{h}\right)\frac{\sqrt{\Delta}}{2h\pi} \qquad (\Delta > 0),$$

$$Cl(D)\lg\frac{T+U\sqrt{D}}{2} = \sum_{h=1}^\infty\left(\frac{D}{h}\right)\frac{\sqrt{D}}{h}$$

auf einem wesentlich von H e r m i t e herrührenden Wege bewiesen. Die rechts stehenden Summen werden dann auf verschiedene Weise, z. B. mittels Gammafunktionen ausgewertet. Es entstehen so Vereinfachungen, die in speziellen Fällen mit Vorteil anzuwenden sind.

Kap. 2. Den Ausgangspunkt bildet die Relation:

$$\sum_{n=1}^\infty\left(\frac{D}{n}\right)e^{-\frac{n^2x\pi}{D}} = \frac{1}{\sqrt{x}}\sum_{n=1}^\infty\left(\frac{D}{n}\right)e^{-\frac{n^2\pi}{Dx}}.$$

Statt also das Integral über den Ausdruck links von 0 bis ∞ zu erstreckern, kann man dasselbe nur von 0 bis $z(>0)$ nehmen und dazu das Integral von z bis ∞ des Ausdruckes rechts addieren. Diese Summe ist von z unabhängig. Wendet man dieses Prinzip an, so gelangt man unmittelbar zu der ersten und dritten Einleitung angeführten Formeln.

Fu.

[43] Sur les théorèmes de Sylvester concernant le quotient de Fermat.

C. R. **142,** 35–38. F. d. M. **37** (1906), 225

Die Arbeit bezieht sich auf die M i r i m a n o f fschen Resultate betreffend die Sätze von S y l v e s t e r über den Quotienten

$$q(a) = \frac{a^{p-1}-1}{p} \qquad (p \text{ eine Primzahl}).$$

Dem Verf. gelingt es, die M i r i m a n o f fschen Resultate auf einen zusammengesetzten beliebigen Modul m zu erweitern. Er schließt daraus auf die für die Berechnung praktische Kongruenz:

$$\frac{a^{\varphi(m)}-1}{m} = q(a,m) \equiv \sum_{\nu} n_\nu n'_\nu \varphi(n_\nu) q(a, m_\nu) \pmod{m},$$

wo $m = m_1 \cdot m_2 \cdot m_3 \ldots$ (m_ν zu m_μ relativ prim), $m = m_\nu \cdot n_\nu$ und $n_\nu^2 \cdot n'_\nu \equiv 1 \pmod{m_\nu}$ ist.

Fu.

[44] Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers.

Acta Math. **30,** 203–293. F. d. M. **37** (1906), 247

Dies der Schluß der von der Pariser Akademie preisgekrönten Abhandlung (siehe F. d. M. **36,** 288, 1905). Der Verf. behandelt zunächst den Zusammenhang zwischen der Exponentialfunktion und den quadratischen Körpern. Setzt man:

$$A(x,D) = \prod_a \left(x - e^{\frac{2a\pi i}{|D|}}\right),$$
$$B(x,D) = \prod_b \left(x - e^{\frac{2b\pi i}{|D|}}\right),$$

wo die a alle Zahlen $1, 2, 3, \ldots, |D|-1$, für die $\left(\frac{D}{a}\right) = +1$ ist, und b alle Zahlen $1, 2, 3, \ldots, |D|-1$, für die $\left(\frac{D}{b}\right) = -1$ ist, durchläuft, so ist für positive D:

$$Cl(D) \lg E(D) = \lg \frac{B(1,D)}{A(1,D)}.$$

(Wegen der Bezeichnungen siehe F. d. M. **36,** 289, 1905). Es handelt sich also um Bestimmung von $A(1,D)$ und $B(1,D)$. Beide Größen werden durch Reihen und Produkte bestimmt. Die Ausdehnung dieser Resultate auf zusammengesetzte Moduln $D = D_1.D_2 \ldots$ ergibt verschiedene Sätze über den Rest der Klassenanzahlen nach 4 und 8, falls die $D_1, D_2, \ldots$ ungerade Primzahlen oder eine Potenz von 2 sind.

Zum Schluß geht der Verf. aus von der K r o n e c k e r schen Relation

$$\sum_{m=-\infty}^{+\infty} \frac{1}{\xi+m} \frac{e^{2\eta\pi i + \frac{2\pi i}{w}(v-\xi_0 v-\eta_0 w)(\xi+m)}}{e^{\frac{2v\pi i}{w}(\xi+m)+2\eta\pi i}-1} + \sum_{m=-\infty}^{+\infty} \frac{1}{\eta+n} \frac{e^{\frac{2\pi i}{v}(\xi_0 v+\eta_0 w)(\eta+n)}}{e^{\frac{2\pi i w}{v}(\eta+n)+2\xi\pi i}-1} =$$
$$\frac{2\pi i e^{2\eta\pi i}}{(e^{2\xi\pi i}-1)(e^{2\eta\pi i}-1)},$$

wo $0 < \xi_0 < 1, 0 < \eta_0 < 1$ und v, w komplexe Variabeln mit imaginärem Verhältnis, ξ, η reelle Variabeln sind. Diese Relation, andewendet auf die Reihen von D i r i c h l e t für die Klassenanzahl, hat schließlich das Ergebnis für positives D:

$$Cl(D) \lg E(D) = 2 \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \lg \frac{1 + e^{-\frac{n\pi}{x}}}{1 - e^{-\frac{n\pi}{x}}} + 2\sqrt{D} \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n} \frac{1}{e^{\frac{2nx\pi}{D}} - 1},$$

wo x eine beliebige Zahl ist.

Fu.

[45] Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers.

Mém. Sav. Étr. 1906. 244 S. 4^0 (vgl. das vorstehende Referat).

F. d. M. **37** (1906), 248

[46] Beiträge zu den Eigenschaften der Klassenanzahl der quadratischen Formen von negativer Diskriminante.

Rozpravy **17,** Nr. 6, 20 S. (Böhmisch.) F. d. M. **39** (1908), 275

Es werden zuerst zwei verschiedene Beweise der Formel

$$\sum_{k=1}^{\Delta-1} \left(-\frac{\Delta}{k}\right) \sum_{\alpha=1}^{k-1} (-1)^{E\left(\frac{\alpha\Delta}{k}\right)} = 4(1 - 2\varepsilon)K^2 - K$$

gegeben. Dabei ist $-\Delta$ eine negative ungerade Diskriminantenzahl, und K ist die Klassenanzahl der positiven quadratischen Formen $ax^2 + bxy + cy^2$ von der Diskriminante $-\Delta = b^2 - 4ac$; wenn $\Delta = 3$, ist $K = \frac{1}{3}$ zu setzen. Der zweite mehr elementare Beweis stützt sich auf die bekannte Formel des Verfassers

$$\left(m - \left(\frac{-\Delta}{m}\right)\right) K = -\sum_{\alpha=1}^{\Delta-1} \left(\frac{-\Delta}{\alpha}\right) E\left(\frac{\alpha m}{\Delta}\right)$$

(Darb. Bull. (2) **21,** 290–304; F. d. M. **28,** 193, 1897).

Dann werden verschiedene andere Formeln, welche der Verfasser in seinen früheren Arbeiten bereits angegeben hatte, bewiesen, so z. B. die Formel

$$\sum_{h=1}^{\Delta-1} \left(\frac{-\Delta}{n}\right) \operatorname{tg} \frac{h\pi}{\Delta} = (-1)^{\frac{\Delta}{8}-1} \frac{4\sqrt{\Delta}}{\tau} K \qquad (\Delta \equiv 0 \pmod 8).$$

Pe.

[47] Bestimmung gewisser arithmetischer Reihen.

Rozpravy **20,** Nr. 40, 14. S (Böhmisch.) F. d. M. **42** (1911), 224

Zuerst wird die Summe

$$H(D,m)=\sum_{\nu=1}^{\Delta-1}\left(\frac{D}{\nu}\right)e^{\frac{2\nu^2 m\pi i}{\Delta}}$$

betrachtet, wo $\Delta=|D|$ und D eine Diskriminante ist. Wenn $D=D_1D_2$, wo die Diskriminanten D_1, D_2 relativ prim sind, so ist

$$H(D_1D_2,m)=\varepsilon H(D_1,m\,\Delta_2)\cdot H(D_2,m\,\Delta_1);$$

$\varepsilon=\pm1$ und zwar ist nur dann $\varepsilon=-1$, wenn beide Diskriminanten D_1, D_2 negativ sind. Für $D=p$ (einer Primzahl von der Form $4k+1$) gewinnt der Verf. aus der Formel von E. J a c o b s t a h l (F. d. M. **37,** 226, 1906) folgende Beziehung

$$H^2(p,m)=2\left(\frac{2}{p}\right)\left[p+\left(\frac{m}{p}\right)a\sqrt{p}\right],$$

wo a eine ungerade, positive oder negative Zahl und durch die Gleichung

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

bestimmt ist.

Dann berechnet der Verf. verschiedene miteinander verwandte Summen, wie z. B.

$$\sum_{\nu=1}^{\Delta-1}\left(\frac{D}{\nu}\right)E\Big(\frac{s\nu^2}{\Delta}\Big)=\frac{s}{\Delta}\sum_{\nu=1}^{\Delta-1}\left(\frac{D}{\nu}\right)\nu^2.$$

Pe.

[48] Sur quelques formules concernant les formes quadratiques binaires d'un discriminant négatif.

Ann. sc. Ac. Pol. Porto **6**, 72–76. F. d. M. **42** (1911), 239

Anwendungen der Formel

$$\sum_{\alpha=1}^{\Delta}\left(\frac{-\Delta}{\alpha}\right)E\left(\frac{\alpha m}{\Delta}\right)=-\left[m-\left(\frac{\Delta}{m}\right)\right]h,$$

wo h die Klassenanzahl der binären quadratischen Formen

$$ax^2+bxy+cy^2$$

der negativen Determinante $b^2-4ac=-\Delta$ ist.

Fu.

[49] Eine Vereinfachung des Lejeune-Dirichletschen Vorganges bei der Ableitung von Formel für die Klassenanzahl der quadratischer Formen von negativer Diskriminante.

Časopis **40,** 425–446 (Böhmisch.) F. d. M. **42** (1911), 239

Der Verf. beweist mehrere teils von L e j e u n e - D i r i ch l et , teils von ihm selbst herrührende Beziehungen auf eine elementarere und einfachere Weise.

Pe.

[50] Études sur la théorie des résidues quadratiques suivivant un module premier. Relations nouvelles avec la théorie des formes quadratiques ayant un déterminant négatif et premier.

Publ. Univ. Masaryk, Nr. 34, 44 S. (1923)
(Tschechisch mit französischen Auszug auf 6 S.) F.d. M.**49** (1923), 93

Aus dem Nachlaß von Lerch (†1922) heransgegeben. Handelt von der Verteilung der Reste und in der Zahlenreihe $1, 2, \ldots, q-1$ wo q eine ungerade Primzahl ist. (II 7.)

Schr.

[51] Betrachtungen über die Theorie der quadratischen Reste nach einem Primmodul.

Spisy Brno, 1923, Nr. 34, 44 S. (Tschechisch, mit einem franz. Auszug). [4]
F. d. M. **49** (1923), 696

Aus dem Nachlaß des im Jahre 1922 verstorbenen Mathematikers. Verf. entdeckt neue Beziehungen zur Theorie der quadratischer Formen, deren Determinante eine negative Primzahl ist. Ist q ein Primmodul, so soll s_ν das Legendresche Symbol $\left(\frac{\nu}{q}\right)$ $\nu = 1, 2, \ldots, q-1$ bedeuten. Verf. untersucht dann die Permanenzen und Variationen, die sich in der Reihe der Zahlen s_ν darbieten. Anwendung von einigen unbestimmten Gleichungen.

By.

[4] Reviews [50] and [51] concern the same paper. Spisy Brno see Publ. univ. Masaryk.

The list of reviewers

By.	Prof. Bydžovský, Prag	Mk.	Prof. Minkowski, Zürich
F.	Dr. Faerber, Berlin	Schr.	Prof. Schrutka, Wien
Fr.	Prof. Fricke, Braunschweig	Sda.	Prof. Sucharda, Prag
Fu.	Prof. Fueter, Basel, (Karlsruhe)	Sn.	Dr. P. Simon, Berlin
Hch.	Dr. Henoch, Berlin	St.	Prof Stäckel, Kiel
Hz.	Prof. Hurwitz, Königsberg in Pr.	Std.	Prof. Studnička, Prag
Lh.	Prof. Lerch, Freiburg, Schweiz	Tx.	Prof. Teixeira, Porto
Lnd.	Dr. Landau, Berlin	Wbg.	Dr. Wallenberg, Berlin
Lp.	Prof. Lampe, Berlin	Wz.	Dr. Weltzien, Berlin

The list of magazines

Acta Math. Acta Mathematica, Stockholm

Annali di mat. Annali di matematica pure ed applicate, Milano

Ann. Sc. Ac. Pol. Porto Annaes da Academia polytechnica do Porto, Coimbra

Arch. der. Math. u. Phys. Archiv der Mathematik und Physik, Leipzig

Bull. intern. de l'Ac. François Joseph Bulletin international, Académie des sciences de l'empereur François Joseph, Praque

Bull. de l'Ac. d. Sciences de Bohème Bulletin international, Académie des sciences de l'empereur François Joseph, Praque

Chicago Congress, Math. papers I

C. R. Comptes Rendus hebdomadaires des séances de l'Académie des Sciences, Paris

Časopis Zeitschrift zur Pflege der Matematik und Physik, Prag, (Böhmisch)

Darboux Bull. Bulletin des sciences mathématiques et astronomiques, rédigé par G. Darboux, Paris

F. d. M. Jahrbuch über die Fortschritte der Mathematik, Berlin

Journ. de Math. Journal de Mathématiques pures et appliquées, fondé en 1836 et publié jusqu'en 1874 par j. Liouville, Paris

Krakau Anz. Bulletin international de l'Académie des Sciences de Cracovie

Math. Ann. Mathematische Annalen, Leipzig

Mém. Sav. Étr. Mémoires présentés par divers savants à l'Académie des sciences de l'Institut de France et imprimes par son ordre, Paris

Prace Prace matematyczno-fizyczne, Warszawa

Prag. Ber. Sitzungsberichte der Kgl. Böhmischen Geselschaft der Wissenschaften, Prag

Publ. Univ. Masaryk Publications de la Faculté des sciences de l'Université Masaryk, Brno

Rozpravy Rozpravy české Akademie císaře Františka Josefa pro vědy, slovesnost a umění, Prag (Böhmisch)

Teixeira J. Jornal de Sciences Mathematicas e Astronomicas publicado pelo Dr. F. Gomes Teixeira, Coimbra

The list of papers on number theory

1. **Expression analytique du plus grand commun diviseur de deux nombres entiers.** Prag. Ber. **1885**, 414–415. Without review.
2. **Deux théorèmes d'arithmétique.** Prag. Ber. **1887** 683–688. Review [1].
3. **Sur une propriétè des nombres.** Teixeira J. **8** 161–163. Review [2].
4. **Modification de la troisième démonstration donnée par Gauss de la loi de réciprocité de Legendre.** Teixeira J. **8** 137–146. Review [3].
5. **Sur une formule d'arithmètique.** Darboux Bull. (2) **12** 100–108. Review [4].
6. **Théorèmes d'arithmétique.** Darboux Bull. (2) **12** 121–126. Review [5].
7. **Sur une formule d'arithmétique.** C. R. **106** 186–187. Review [6].
8. **Sur le développement en série de certaines fonctions arithmétiques.** C. R. **108** 171–174. Review [7].
9. **Různé věty aritmetické.** (Arithmetische Lehrsätze.) Časopis **21** 90–95, 185–190. Review [8].
10. **Sur quelques thorèmes d'arithmétique.** Prag. Ber. 1894, 1–11. Review [9].
11. **Bemerkungen über eine Klasse arithmetischer Lehrsätze.** Prag. Ber. 1894. 1–20. Review [10].
12. **Ueber eine arithmetische Relation.** Prag. Ber. 1894, 1–16. Review [11].
13. **Sur une théorème de Kronecker.** Prag. Ber, 1893. NoIX. 1–17. Review [12].
14. **Sur une intégrale définie qui représente la fonction $\zeta(s)$ de Riemann.** Chicago Congress, Math. Papers. I, 165–166. Review [13].

15. **Sur diverses formules d'arithmétique.** Teixeira J. **12**. 129–136. Review [14], [21].

16. **Poznámky arithmetické.** (Arithmetische Bemerkungen.) Časopis **24**, 25–34, 128–124. Review [15].

17. **Poznámka arithmetická.** (Arithmetische Notiz.) Časopis **24**, 228–230. Review [16].

18. **Logarithmus faktorielly.** (Logarithmus der Factorielle.) Časopis **24**, 129–132. Review[17].

19. **Sur le nombre des classes de formes quadratiques de déterminant négatif.** C. R. **121**, 878–880. Review [18].

20. **Sur une théorme de Zolotarev.** Bull. intern. de l' Ac. Francois Joseph. 1896, 34–37. Review [19].

21. **O jisté arithmetické větě Zolotareva.** (Ueber einen arithmetischen Satz von Zolotarev.) Rozpravy **5**, No. 17. 1–8. Review [20]

22. **Sur quelques analogies des sommes de Gauss.** Prag. Ber. 1897, 1–16. Review [22].

23. **Sur quelques formules relatives au nombre des classes.** Darboux Bull. (2), **21**, 290–304. Review [23].

24. **O součtech Gaussových.** (Ueber die Gauss'schen Summen.) Časopis **28**, 1–24. Review [24].

25. **O počtu tříd kvadratických forem záporného diskriminantu.** (Ueber die Anzahl der Klassen quadratischer Formen negativer Discriminante.) Rozpravy **7**, No. 4, 1–16. Review [25].

26. **Arithmetické odvození Lejeune-Dirichletových výsledků o počtu tříd kvadratických forem.** (Arithmetische Ableitung der zur Klassenanzahlbestimmung dienenden Lejeune-Dirichlet'schen Fundamentalformen.) Rozpravy **7**, No.5, 1–51. Review [26].

27. **O souvislosti Legendreova znaménka s čísly Moebiovými.** (Ueber einen Zusammenhang des Legendre'schen Zeichens mit den Moebius'schen Zahlen.) Rozpravy **7.** No. 6, 1–12. Review [27].

28. **O součtu celých v lomené aritmetické posloupnosti druhého stupně a jeho souvislosti s počtem tříd kvadratické formy záporného diskriminantu.** (Ueber die Summe der grössten Ganzen in einer gebrochenen arithmetischen Progression zweiter Ordnung und ihren Zusammenhang mit der Klassenanzahl quadratischer Formen negativer Discriminante.) Rozpravy **7**, No. 7, 1–8. Review [28].

29. **Resume de trois notes d'arithmétique.** Bull. de l'Ac. d. Sciences de Bohème 1898. 33–38. Review [29].

30. **Sur la fonction $\zeta(s)$ pour les valeurs impaires de l'argument.** Teixeira J.**14**, 65–69. Review [30].

31. **Sur la formule fondamentale de Dirichlet qui sert à déterminer le nombre des classes de formes quadratiques binaires définies.** C. R. **135**, 1314–1315. Review [31].

32. **Démonstration élémentaire d'un théorème arithmétique.** Prag. Ber. 1903, Nr. 2, 1–3. Review [32].

33. **Über den fünften Gaußschen Beweis des Reziprozitätsgesetzes für die quadratischen Reste.** Prag. Ber. 1903, 1–19. Review [33].

34. **Sur la cinquième démonstration de Gauß de la loi de réciprocité de Legendre.** Teixeira J. **15**, 97–104. Review [34].

35. **Bemerkung über die Theorie der Gaußschen Summen.** Prag. Ber. 1–4. Review [35].

36. **Zur Theorie der Gaußschen Summen.** Math. Ann. **57**, 554–567. Review [36].

37. **Über die arithmetische Gleichung $Cl(-\Delta) = 1$.** Math. Ann. **57**, 568–570. Review [37].

38. **Sur le nombre des classes de formes quadratiques binaires d'un discriminant positif fondamental.** Journ. de Math. (5), **9** 337–401. Review [38].

39. **Sur quelques applications des sommes de Gauss.** Annali di Mat. (3) **11**, 79–91. Review [39].

40. **Sur quelques applications d'un théorème arithmétique de Jacobi.** Krakau Anz. 1904, 55–70. Review [40].

41. **O liczbie klas form kwadratowych dwójkowych o wyróżniku zasadniczym dodatnim.** (On the class number of primitive binary quadratic forms with positiv discriminant.) Prace **15**, 91–113. Without review.

42. **Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$.** Math. Ann. **60**, 471–490. Review [41].

43. **Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers.** Acta Math. **29**, 333–424. Review [42].

44. **Sur les théorèmes de Sylvester concernant le quotient de Fermat.** C. R. **142**, 35–38. Review [43].

45. **Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coeficients entiers.** Acta Math. **30**, 203–293. Review [44].

46. **Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coeficients entiers.** Mém. Sav. Étr. 1906. 1–244. Review [45].

47. **Příspěvky k vlastnostem počtu tříd kvadratických forem záporného diskriminantu.** (Beiträge zu den Eigenschaften der Klassenanzahl der quadratischen Formen von negativer Diskriminante.) Rozpravy **17**, Nr. 6, 1–20. Review [46].

48. **Stanovení jistých aritmetických součtů.** (Bestimmung gewisser arithmetischer Reihen.) Rozpravy **20**, Nr. 40, 1–14. Review [47].

49. **Sur quelques formules concernant les formes quaratiques binaires d'un discriminant négatif.** Ann. sc. Ac. Pol. Porto **6**, 72–76. Review [48].

50. **Zjednodušení Lejeune-Dirichletova postupu při odvozování vzorců pro počet tříd kvadratických forem záporného diskriminantu.** (Eine Vereinfachung des Lejeune-Dirischletschen Vorganges bei der Ableitung von Formel für die Klassenanzahl der quadratischer Formen von negativer Diskriminante.) Časopis **40**, 425–446. Review [49].

51. **Poznámky o počtu tříd kvadratických forem.** (Notes on the class number of quadratic forms.) Bull. intern. de l'Ac. François Joseph **20**, 120–144. Without review.

52. **Úvahy o theorii kvadratických zbytků pro kmenné moduly s novými vztahy k theorii kvadratických forem s kmennými zápornými determinanty.** Études sur la théorie des résidues quadratiques suivivant un module premier. Relations nouvelles avc la théorie des formes quadratiques ayant un déterminant négatif premier.) Spisy Brno, 1923 Nr, 34, 1–44. Review [50], [51].

4 Expression analytique du plus grand commun diviseur de deux nombres entiers.

Lu par **Matias Lerch** dans la séance du 13. Novembre 1885.

1. Si le nombre positif entier k supérieur à 3 est premier, l'expression

$$x = \prod_{\mu=0}^{k-3} \sin^2 \frac{k\pi}{\mu+2},$$

a pour valeur un nombre positif inférieur à l' unité et différent de zéro, tandis qu'elle a pour valeur zéro, si le nombre entier k est composé.

On en conclut que l'expression

$$\lim_{\nu=\infty}(1-(1-x)^\nu) = \lim_{\nu=\infty}\left(1-\left(1-\prod_{\mu=0}^{k-3}\sin^2\frac{k\pi}{\mu+2}\right)^\nu\right) \tag{2}$$

est égale à l' unité, si le nombre entier k est premier, et qu'elle est égale à zéro dans le cas contraire.

2. Considérons maintenant l' expression

$$\lim_{\nu=\infty}\left(1-\sin^2\frac{m\pi}{k}\right)^\nu\left(1-\sin^2\frac{n\pi}{k}\right)^\nu = \varphi(m,n,k), \tag{3}$$

où l' on entend par m, n, k des nombres entiers positifs quelconques; cette expression est évidemment égale à l' unité, si les deux nombres m, n sont en même temps divisibles par k, et égale à zéro dans le cas contraire. On en conclut que le produit des deux expressions (2) et (3), c'est à dire l'expression

$$\psi(m,n,k) = \lim_{\nu=\infty}\left(1-sin^2\frac{m\pi}{k}\right)^\nu\left(1-sin^2\frac{n\pi}{k}\right)^\nu\left(1-\left(-\prod_{\mu=0}^{k-3}\sin^2\frac{k\pi}{\mu+2}\right)^\nu\right)$$

a pour valeur l' unité, si k est un nombre premier supérieur à 3 divisant les deux nombres entiers m et n, et qu'elle est égale à zéro dans le cas contraire.

Il en résulte que l'expression

$$e^{\varphi(m,n,2)\lg 2+\varphi(m,n,3)\lg 3+\sum_{k=4}^{\zeta}\psi(m.n,k)\lg k} = div\,(m,n) \tag{5}$$

représente le plus grand commun diviseur des deux nombres entiers m et n, ζ désignant un nombre entier qeulconque égale ou supérieur au plus petit des nombres m, n.

On voit que cette expression (5) peut s'écrir sous la forme

$$e^{\sum_{\nu=0}^{\infty} f_\nu},$$

f_ν désignant une fonction entiére aux coefficients entiers des quantités

$$\begin{gathered}\sin^2\tfrac{m\pi}{2},\quad \sin^2\tfrac{m\pi}{3},\quad \sin^2\tfrac{n\pi}{2},\qquad \sin^2\tfrac{n\pi}{3},\\ \sin^2\tfrac{m\pi}{k},\quad \sin^2\tfrac{n\pi}{k},\quad \sin^2\tfrac{k\pi}{\mu+2},\quad \lg 2, \lg 3, \lg k,\\ (\mu = 0, 1, \ldots k-3,\quad k = 4, 5, \ldots \zeta),\end{gathered}$$

fonction qui est linéaire par rapport aux derniéres quantités logarithmiques $\lg 2$, $\lg 3$,$\ldots \lg \zeta$.

Écrit à Souchice en Bohême, fin du septembre 1885.

5 Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$.

Published in Math. Ann. **60** (1905), 471–490, section 3, [41]

Ist p eine ungerade Primzahl, a eine beliebige durch p nicht aufgehende ganze Zahl, so ist der Quotient

$$q(a) = \frac{a^{p-1} - 1}{p} \tag{1}$$

eine ganze Zahl, welche einige verhältnismäßig einfache Kongruenz-Eigenschaften besitzt, die hier entwickelt werden sollen. Die Art der Resultate ist aus den numerierten Formeln (Gleichungen oder Kongruenzen) leicht zu übersehen.

Zunächst setzen wir die Definitionsgleichung (1) in die Gestalt

$$a^{p-1} = 1 + pq(a), \tag{1^0}$$

und bilden das Produkt der Resultate, welche den Werten $a = 1, 2, \ldots, p-1$ entsprechen. Wird der Kürze wegen

$$P = 1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)! \tag{2}$$

gesetzt, so ensteht die Gleichung

$$P^{p-1} = \prod_{\alpha=1}^{p-1} (1 + pq(a)),$$

aus welcher sich durch Ausführung der Multiplikation rechterhand die Kongruenz

$$P^{p-1} \equiv 1 + p \sum_{a=1}^{p-1} q(a) \pmod{p^2} \tag{α}$$

erschließen läßt.

Um die linke Seite zu vereinfachen, bemerken wir, daß nach dem Wilsonschen Satze der Quotient

$$\frac{P+1}{p} = N \tag{3}$$

eine ganze Zahl ist; die Gleichung

$$P = -1 + pN$$

ergibt aber, wenn man auf beiden Seiten auf die $(p-1)^{\text{te}}$ Potenz erhebt, nach dem binomischen Lehrsatz offenbar

$$P^{p-1} \equiv 1 - p(p-1)N \pmod{p^2},$$

oder einfacher,

$$P^{p-1} \equiv 1 + pN \pmod{p^2}.$$

Diese Kongruenz hat mit (α) den gleichen Modul und die gleiche linke Seite; dies liefert unser erstes Resultat

$$\sum_{a=1}^{p-1} q(a) \equiv N \pmod{p}, \tag{4}$$

eine Kongruenz, welche die Summe der Fermatschen mit dem Wilsonschen Quotienten in Verbindung setzt.

Zu weiteren Betrachtungen bedürfen wir der bekannten Sätze

$$q(ab) \equiv q(a) + q(b) \pmod{p}, \tag{5}$$

$$q(c + pz) \equiv q(c) - \frac{z}{c} \pmod{p}, \tag{6}$$

welche man mit betreffenden Literaturangaben in Herrn P. B a c h m a n n s Niederer Zahlentheorie findet.

In der Letzten Kongruenz (6) tritt auf der rechten Seite ein Bruch $\frac{z}{c}$ auf, unter dem man in der Regel das Produkt von z mit dem sogenannten socius c^{-1} von $c \pmod{p}$ versteht. Ich finde übrigens vorteilhafter, den Kongruenzbegriff auf Brüche auszudehnen und mit letzteren systematisch im Sinne der Kongruenz zu rechnen, was übrigens in der Zahlentheorie längst geschieht.

Ich setze nun in (5) an Stelle von b der Reihe nach die Zahlen $\nu = 1, 2, 3, \ldots, p-1$ und addiere die Ergebnisse. So entsteht zunächst

$$\sum_{\nu=1}^{p-1} q(\nu a) \equiv (p-1)q(a) + \sum_{\nu=1}^{p-1} q(\nu) \pmod{p}$$

oder

$$\sum_{\nu=1}^{p-1} q(\nu a) \equiv -q(a) + \sum_{\nu=1}^{p-1} q(\nu) \pmod{p}. \tag{β}$$

In dieser Kongruenz wollen wir die linke Seite umformen, wodurch sich eine Darstellung von $q(a)$ modulo p ergeben wird.

Jeder Zahl ν der Reihe 1 bis $p-1$ enspricht eine Zahl c derselben Reihe, für welche

$$\nu a \equiv c \pmod{p}$$

oder also

$$\nu a = c + pz, \quad (0 < c < p)$$

wobei unter z eine ganze Zahl verstanden wird. Schreibt man diese Gleichung in der Gestalt

$$\frac{\nu a}{p} = \frac{c}{p} + z,$$

so läßt sich $\frac{c}{p}$ als der kleinste positive Rest und z als das größte Ganze der Größe $\frac{\nu a}{p}$, d. h.

$$z = \left[\frac{\nu a}{p}\right], \quad c = \nu a - pz,$$

charakterisieren.

Nun wird aber nach (6) für den Modul p

$$q(\nu a) \equiv q(c + pz) \equiv q(c) - \frac{z}{c}$$

oder

$$q(\nu a) \equiv q(c) - \frac{z}{\nu a - pz} \equiv q(c) - \frac{z}{\nu a},$$

d. h. also

$$q(\nu a) \equiv q(c) - \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}, \tag{7}$$

wenn $0 < c < p$ und

$$\nu a \equiv c \pmod{p}.$$

Wenn bei festem a die Zahl ν die sämtlichen Werte aus der Reihe von 1 bis $p-1$ durchläuft, so nimmt c die gleichen Werte in verschiedener Reihenfolge an, d. h. es ist

$$\sum q(c) = \sum_{1}^{p-1} q(\nu),$$

und wir erhalten demnach aus (7) durch Addition

$$\sum_{\nu=1}^{p-1} q(\nu a) \equiv \sum_{1}^{p-1} q(\nu) - \sum_{\nu=1}^{p-1} \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}.$$

Wird dies mit (β) vergleichen, so fällt in dem Resultat die Summe

$$\sum q(\nu)$$

heraus und *wir erhalten die Kongruenz*

$$q(a) \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}, \tag{8}$$

welche für sämtliche durch p nicht aufgehende ganze Zahlen a besteht. Man kann sie auch so schreiben:

$$\frac{a^p - a}{p} \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu} \left[\frac{\nu a}{p}\right] \pmod{p}. \tag{8*}$$

Bedient man sich der hier beizubehaltenden Bezeichnung

$$\frac{p-1}{2} = m,$$

so werden für $a = 2$ auf der rechten Seite von (8*) erst die Glieder

$$\nu = m+1, m+2, \ldots, 2m$$

von Null verschieden sein und zwar ist

$$\frac{2^p - 2}{p} \equiv \sum_{\nu=m+1}^{2m} \frac{1}{\nu} \equiv -\sum_{1}^{m} \frac{1}{\nu} \pmod{p}. \tag{9}$$

Die zweite Form ist nämlich eine unmittelbare Folge der ersten und des naheliegenden Umstandes, daß

$$\sum_{1}^{2m} \frac{1}{\nu} \equiv 0 \pmod{p}.$$

Das von S y l v e s t e r und S t e r n auf anderem Wege gewonnen Resultat (9) kann bekantlich vermöge der Idetität

$$\sum_{\nu=1}^{2m} c_\nu - 2\sum_{1}^{m} c_{2\nu} = \sum_{\nu=1}^{2m} (-1)^{\nu-1} c_\nu$$

auf die Gestalt

$$\frac{2^p - 2}{p} \equiv \sum_{1}^{p-1} (-1)^{\nu-1} \frac{1}{\nu} \pmod{p} \tag{9'}$$

gebracht werden.

Eine neue Darstellung des in Rede stehenden Restes fließt aus der Annahme $a = 4$; alsdann spalten sich die Indizes ν in drei Sektionen

$$\left(\frac{p}{4} \cdots \frac{p}{2}\right), \left(\frac{p}{2} \cdots \frac{3p}{4}\right), \left(\frac{3}{4}p \ldots p\right),$$

welchen beziehungweise die Werte 1, 2, 3 des größten Ganzen $\left[\frac{4\nu}{p}\right]$ entsprechen.

In den Termen der zweiten und dritten Sektion führe ich nun die Substitotion $\nu = p - \mu$ aus und beachte, daß alsdann

$$\frac{1}{\nu} = \frac{1}{p-\mu} \equiv -\frac{1}{\mu}$$

ist; es kommt

$$4q(4) \equiv \sum_{\frac{1}{4}p<\nu<\frac{1}{2}p} \frac{1}{\nu} - 2 \sum_{\frac{1}{4}<\nu<\frac{1}{2}p} \frac{1}{\mu} - 3 \sum_{1}^{\left[\frac{1}{4}p\right]} \frac{1}{\varrho};$$

die linke Seite ist

$$8q(2) = 4\frac{2^p - 2}{p},$$

während sich auf der rechten die zwei ersten Aggregate zusammenziehen, so daß man die Kongruenz erhält:

$$4\frac{2^p - 2}{p} \equiv - \sum_{\left(\frac{1}{4}p<\mu<\frac{1}{2}p\right)} \frac{1}{\mu} - 3 \sum_{\left(0<\varrho<\frac{p}{4}\right)} \frac{1}{\varrho} \pmod{p}$$

Die zahlen ϱ ergänzen die Zahlegruppe μ zur Gesamtheit der Zahlen ν des Intervalls $\left(0 \ldots \frac{1}{2}p\right)$, und demnach ensteht, wenn man das eine Aggregat

$$\sum \frac{1}{\varrho}$$

mit dem Aggregat

$$\sum \frac{1}{\mu}$$

vereinigt, die Kongruenz

$$4\frac{2^p - 2}{p} \equiv - \sum_{1}^{m} \frac{1}{\nu} - 2 \sum_{1}^{\left[\frac{1}{4}p\right]} \frac{1}{\varrho};$$

zieht man von hier das Resultat (9) ab, so kommt

$$3\frac{2^p - 2}{p} \equiv -2 \sum_{1}^{\left[\frac{1}{4}p\right]} \frac{1}{\varrho}$$

oder, unter der Annahme $p > 3$,

$$\frac{2^{p-1} - 1}{p} \equiv -\frac{1}{3} \sum_{\nu=1}^{\left[\frac{1}{4}p\right]} \frac{1}{\nu} \pmod{p}. \tag{10}$$

Indem wir nochmals auf (9)

$$\sum_{1}^{m} \frac{1}{\nu} \equiv -\frac{2^p - 2}{p}$$

zurückgreifen, spalten wir die Zahlen ν in gerade 2μ und ungerade λ, und erhalten

$$\sum_1^m \frac{1}{\nu} = \sum_{\lambda \le m} \frac{1}{\lambda} + \sum_1^{\left[\frac{p}{4}\right]} \frac{1}{\mu},$$

also mit Rücksicht auf (10)

$$\frac{2^{p-1}-1}{p} \equiv -2 \sum \frac{1}{\lambda} \pmod{p}, \tag{11}$$

$$(\lambda = 1, 3, 5, \ldots; \quad \lambda \le m).$$

Ähnlich findet man

$$\sum \frac{1}{\lambda'} \equiv \frac{2^{p-1}-1}{p} \pmod{p}, \tag{12}$$

$$(\lambda' = 1, 3, 5, \ldots, p-2).$$

Die Wahl $a = 8$ würde ferner ergeben

$$4\frac{2^p - 2}{p} \equiv -\sum \frac{1}{a} - \sum \frac{1}{b} \pmod{p} \tag{13}$$

$$\left(0 < a < \frac{p}{8}, \quad 0 < b < \frac{3p}{8}\right).$$

Ich notiere schließlich die ähnlich zu gewinnenden Resultate

$$\frac{3^p - 3}{p} \equiv -2 \sum_1^{\left[\frac{1}{3}p\right]} \frac{1}{\nu} \pmod{p}, \tag{14}$$

$$\frac{5^p - 5}{p} \equiv -2 \sum \frac{1}{a} - 2 \sum \frac{1}{b} \pmod{p} \tag{15}$$

$$\left(0 < a < \frac{p}{5}, \quad 0 < b < \frac{2p}{5}\right).$$

Wir kehren nun zu (8) zurück, indem wir nach a von 1 bis $p-1$ summieren; in der so enstandenen Kongruenz

$$\sum_1^{p-1} q(a) \equiv \sum_{\mu=1}^{p-1} \sum_{\nu=1}^{p-1} \frac{1}{\mu\nu} \left[\frac{\mu\nu}{p}\right] \pmod{p}$$

drückt sich die linke Seite vermöge (4), durch den Wilsonischen Quotienten N aus, während die rechte Seite, sich leicht in eine einfache Summe verwandelt.

Bedeutet nämlich $\psi(n)$ die Anzahl der Lösungen der unbestimmten Gleichung

$$\mu\nu = n; \quad (0 < \mu < p, \quad 0 < \nu < p),$$

so wird unser Resultat lauten

$$N \equiv \sum_{n=1}^{(p-1)^2} \frac{\psi(n)}{n} \left[\frac{n}{p}\right] \pmod{p}. \tag{16}$$

Die Zahl $\psi(n)$ kann aber einfacher gedeutet werden, wenn man die Bedingungen in die Form

$$n = \mu\nu, \quad 0 < \mu < p, \quad n < p\mu$$

setzt. Denn demnach ist für μ irgend ein Teiler von n zu setzen, der den Ungleichungen

$$\frac{n}{p} < \mu < p$$

genügt, und ν ist als Komplementärteiler unzweideutig bestimmt. Es ist also $\psi(n)$ die Anzahl der Teiler von n, welche innerhalb der Grenzen $\frac{n}{p}$ und p enthalten sind.

Ein viel einfacheres Resultat ergibt sich aus (8), wenn man auf beiden Seiten mit a multipliziert und dann über $a = 1, 2, \ldots, p-1$ summiert; es ergibt sich so

$$\sum_{a=1}^{p-1} aq(a) \equiv \frac{1}{2} \pmod{p}. \tag{17}$$

Dabei wird kein anderes neues Hilfsmittel gebraucht als die Gleichung

$$\sum_{a=1}^{p-1} \left[\frac{\nu a}{p}\right] = \sum_{a=1}^{p-1} \frac{a\nu}{p} - \sum_{b=1}^{p-1} \frac{b}{p} = \frac{(\nu-1)(p-1)}{2},$$

die unmittelbar ersichtlich ist.

Die Kongruenz (7) ist übrigens, wie manche andere Sätze, aus dem Spezialsatz

$$q(p-a) \equiv q(a) + \frac{1}{a} \pmod{p}, \tag{6^1}$$

der sich aus (6) vermöge Identität

$$q(-a) = q(a)$$

ergibt, leicht zu gewinnen.

Wir wollen ferner die Summe

$$S = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu)$$

betrachten, in welcher der Ausdruck

$$\left(\frac{\nu}{p}\right)$$

in üblicher Weise das aus der Theorie der quadratischen Reste bekannte Legendresche Zeichen ist. Wir machen erstens die Annahme, daßdie Primzahl p die Form $4x+3$ hat; alsdann gilt

$$\left(\frac{p-\nu}{p}\right) = -\left(\frac{\nu}{p}\right),$$

und daher verwandelt sich S, wenn man darin $\nu = p-\mu$ setzt, in

$$S = -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right) q(p-\mu),$$

und dies ist nach (6^1)

$$S \equiv -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right) q(\mu) - \sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right)\frac{1}{\mu} \pmod{p},$$

woraus unmittelbar

$$2S \equiv -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right)\frac{1}{\mu} \pmod{p}$$

folgt. Die Eulersche Kongruenz

$$\left(\frac{\mu}{p}\right) \equiv \mu^m \pmod{p}; \quad m = \frac{p-1}{2},$$

gestattet unsere letzte Kongruenz wie folgt zu schreiben:

$$2S \equiv -\sum_{\mu=1}^{p-1}\mu^{m-1} \pmod{p}.$$

Nun ist nach der bekannten Formel der Differenzrechnung,

$$u_0 + u_1 + \cdots + u_{n-1} = \sum_{\nu=0}^{n-1}\binom{n}{\nu+1}\Delta^\nu u_0,$$

also für

$$u_\nu = \nu^{m-1}, \quad n = p$$

$$\sum_{1}^{p-1}\mu^{m-1} = \sum_{\nu=0}^{p-1}\binom{p}{\nu+1}\Delta^\nu O^{m-1} = \sum_{\nu=0}^{m-1}\binom{p}{\nu+1}\Delta^\nu O^{m-1},$$

weil die m^{te} und die höheren Differenzen der $(m-1)^{\text{ten}}$ Potenzen natürlicher Zahlen sämtlich verschwinden. Hier ist nun jeder vorkommende Binomialkoeffizient

$$\binom{p}{\nu+1}$$

durch p teilbar, also

$$\sum \mu^{m-1} \equiv 0 \pmod{p}.$$

Demnach ist

$$S \equiv 0 \pmod{p},$$

d. h.

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu) \equiv 0 \pmod{p}, \tag{18}$$

falls die Primzahl p die Gestalt $4x+3$ hat.

Für Primzahlen der Gestalt $4x+1$ versagt die obige Betrachtung, und wir müssen uns nach anderen Hilfsmitteln umsehen, um den Rest der Summe S zu ermitteln.

Wegen der Eulerschen Kongruenz

$$\nu^m \equiv \left(\frac{\nu}{p}\right) \pmod{p}$$

ist die durch die Gleichung

$$\nu^m = \left(\frac{\nu}{p}\right)[1 + pq'(\nu)] \tag{19}$$

definierte Zahl $q'(\nu)$ eine ganze Zahl; dieselbe steht mit der Zahl $q(\nu)$ im engen Zusammenhange, und zwar ist, wie sich durch Quadrieren von(19) ergibt

$$1 + 2pq'(\nu) + p^2 q'(\nu)^2 = 1 + pq(\nu),$$

also

$$q(\nu) = 2q'(\nu) + pq'(\nu)^2, \tag{20}$$

woraus

$$q(\nu) \equiv 2q'(\nu) \pmod{p} \tag{20^0}$$

Ich setze nun für p eine Primzahl $4n+1$, so daß $m = 2n$ gerade ist, und bilde die Summe der Zahlen (19) für $\nu = 1, 2, \ldots, p-1$. Mit Rücksicht auf die Relation

$$\sum_{1}^{p-1} \left(\frac{\nu}{p}\right) = 0$$

ergibt sich in der Weise die Gleichung

$$\sum_{\nu=1}^{p-1} \nu^m = p \sum_{1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu).$$

Hier läßt sich die linke Seite mit der bekannten Formel

$$S_{2n}(x) = \frac{x^{2n+1}}{2n+1} - \frac{1}{2}x^{2n} + \sum_{\nu=1}^{n} (-1)^{\nu-1} \frac{B_\nu}{2\nu} \binom{2n}{2\nu-1} x^{2n-2\nu+1}$$

ausdrücken, und zwar ist

$$\sum_{\nu=1}^{p-1} \nu^m = S_{2n}(p), \quad 2n = m.$$

Wir erhalten daher

$$\sum_{\nu=1}^{n} (-1)^{\nu-1} \frac{B_\nu}{2\nu} \binom{2n}{2\nu-1} p^{2n-2\nu} + \frac{p^m}{m+1} - \frac{1}{2}p^{m-1} = \sum_{1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu).$$

Links enthält keine der auftreffenden Bernoullischen Zahlen B_ν den Faktor p im Nenner, und daher läßt sich hieraus die Kongruenz

$$(-1)^{n+1} B_n \equiv \sum_{1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu) \pmod{p}$$

erschließen; *dieselbe geht aber nach* (20^0) *über in*

$$S = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu) \equiv (-1)^{n-1} 2B_n \pmod{p}, \tag{21}$$

wobei die Primzahl $p = 4n+1$ *ist.*

Wir wollen ferner die Summe

$$H = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \nu q(\nu) \tag{22}$$

nach dem Modul p abschätzen.

Ist zunächst p der Gestalt $4x+1$, so wird

$$\left(\frac{p-a}{p}\right) = \left(\frac{a}{p}\right),$$

und wenn wir mit a Zahlen $\leq m$ bezeichnen, so zerfallen die $p-1$ Zahlen ν in die Zahlen a und $p-a$, so daß

$$H = \sum \left(\frac{a}{p}\right) a q(a) + \sum \left(\frac{p-a}{p}\right) (p-a) q(p-a)$$

also

$$H \equiv \sum \left(\frac{a}{p}\right) a[q(a) - q(p-a)] \pmod{p}$$

ist. Die Klammer ist aber nach (6^1) der Zahl

$$-\frac{1}{a}$$

kongruent, und *wir erhalten*

$$H \equiv -\sum_{a=1}^{m} \left(\frac{a}{p}\right) = 0,$$

also

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \nu q(\nu) \equiv 0 \pmod{p}, \qquad (22^1)$$

wenn $p = 4x + 1$.

Wenn dagegen $p = 4x + 3$ ist, so ergibt die Spaltung der Zahlen ν in a und $p - a$ zunächst

$$H = \sum \left(\frac{a}{p}\right) aq(a) + \sum \left(\frac{p-a}{p}\right) (p-a)q(p-a)$$

und also

$$H \equiv 2\sum \left(\frac{a}{p}\right) aq(a) + \sum \left(\frac{a}{p}\right) \pmod{p}. \qquad (\gamma)$$

Ferner lassen sich die Zahlen ν in gerade $2a$ und ungerade $p - 2a$ spalten; die Summe H nimmt dadurch die Gestalt an

$$H = \sum \left(\frac{2a}{p}\right) 2aq(2a) + \sum \left(\frac{p-2a}{p}\right) (p-2a)q(p-2a),$$

also

$$H \equiv 4\sum \left(\frac{2a}{p}\right) aq(2a) + \sum \left(\frac{2a}{p}\right) \pmod{p}.$$

Wegen

$$q(2a) \equiv q(a) + q(2)$$

läßt sich dies schreiben

$$H \equiv 4\left(\frac{2}{p}\right) \sum \left(\frac{a}{p}\right) aq(a) + \left(\frac{2}{p}\right) \sum \left(\frac{a}{p}\right) + 4\left(\frac{2}{p}\right) q(2) \sum \left(\frac{a}{p}\right) a.$$

Die Summe

$$\sum \left(\frac{a}{p}\right) a$$

hat eine aus der Theorie der quadratischen Formen bekannte Bedeutung; für uns kommt sie jedoch in Wegfall, weil sie durch p teilbar ist, und wir haben daher

$$H \equiv 4\left(\frac{2}{p}\right)\sum\left(\frac{a}{p}\right)aq(a) + \left(\frac{2}{p}\right)\sum\left(\frac{a}{p}\right). \qquad (\delta)$$

Multiplizieren wir nun (γ) mit 2, (δ) mit $\left(\frac{2}{p}\right)$ und ziehen ab, so ensteht

$$\left(2 - \left(\frac{2}{p}\right)\right) H \equiv \sum\left(\frac{a}{p}\right) \pmod{p}.$$

Nun ist aber nach bekannten Sätzen von D i r i c h l e t

$$\sum_{a=1}^{m}\left(\frac{a}{p}\right) = \left(2 - \left(\frac{2}{p}\right)\right) Cl(-p),$$

wenn mit $Cl(-\Delta)$ die Anzahl primitiver positiver Klassen quadratischer Formen $ax^2 + bxy + cx^2$ der negativen Diskriminante $b^2 - 4ac = -\Delta$ bezeichnet wird, und *also lautet unsere Resultat*

$$H \equiv Cl(-p) \pmod{p},$$

d. h.

$$\sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right)\nu q(\nu) \equiv Cl(-p) \pmod{p}, \qquad (22^2)$$

wenn die Primzahl p die Form $4x + 3$ hat.

Wir gehen nun auf die oben betrachtete Summe

$$A = \sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right) q(\nu) \qquad (23)$$

zurück. Die Kongruenz (7) oder

$$q(\nu b) \equiv q(\varrho) - \frac{1}{\nu b}\left[\frac{\nu b}{p}\right], \qquad (7')$$

wenn $0 < \varrho < p$, $\quad \nu b \equiv \varrho \pmod{p}$, verbunden mit dem Umstande, daß

$$\left(\frac{\nu b}{p}\right) = \left(\frac{\varrho}{p}\right),$$

liefert nach dem Satze $q(\nu b) \equiv q(\nu) + q(b)$ offenbar

$$\left(\frac{b}{p}\right)\left(\frac{\nu}{p}\right)q(\nu) + \left(\frac{b}{p}\right)q(b)\left(\frac{\nu}{p}\right) \equiv \left(\frac{\varrho}{p}\right)q(\varrho) - \left(\frac{\nu b}{p}\right)\frac{1}{\nu b}\left[\frac{\nu b}{p}\right] \pmod{p}.$$

Summiert man hier über die Werte $\nu = 1, 2, \ldots, p-1$, so nimmt ϱ die gleichen Werte an, und es kommt

$$\left(\frac{b}{p}\right) A \equiv A - \sum_{\nu=1}^{p-1} \left(\frac{b\nu}{p}\right) \left[\frac{b\nu}{p}\right] \frac{1}{b\nu} \pmod{p}$$

oder nach Kürzen durch $\left(\frac{b}{p}\right)$

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \left[\frac{b\nu}{p}\right] \frac{1}{\nu} \equiv -\left(1 - \left(\frac{b}{p}\right)\right) bA \pmod{p} \qquad (23^*)$$

Wenn also b quadratischer Rest von p ist, so ist die Summe

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \left[\frac{b\nu}{p}\right] \frac{1}{\nu}$$

durch p teilbar; sie ist es auch dann, wenn p die Gestalt $4n+3$ hat; ist dagegen p der Gestalt $4n+1$ und ist b ein Nichtrest von p, so ist unsere Summe nach dem Modul p der Zahl

$$(-1)^n 4 B_n b$$

kongruent, wobei B_n wie oben in (21) die n^{te} Bernoullische Zahl bedeutet.

Die Kongruenz (7') ergibt, wenn man sie mit

$$b^2\nu^2 \equiv \varrho^2$$

multipliziert, die folgende

$$b^2 q(b) \cdot \nu^2 + b^2 \cdot \nu^2 q(\nu) \equiv \varrho^2 q(\varrho) - b\nu \left[\frac{b\nu}{p}\right].$$

Wenn man hier über $\nu = 1, 2, \ldots, p-1$ summiert und beachtet, daß

$$\sum \nu^2 \equiv 0 \pmod{p},$$

so kommt

$$(b^2 - 1) \sum_{\nu=1}^{p-1} \nu^2 q(\nu) \equiv -b \sum_{\nu=1}^{p-1} \nu \left[\frac{b\nu}{p}\right] \pmod{p}. \qquad (\varepsilon)$$

Setzt man hier $b = 2$, so entsteht

$$3 \sum \nu^2 q(\nu) \equiv -2 \sum_{\nu=m+1}^{p-1} \nu = -2 \left(\sum_{1}^{p-1} \nu - \sum_{1}^{m} \nu \right),$$

also

$$3 \sum \nu^2 q(\nu) \equiv m(m+1) = \frac{p^2 - 1}{4} \equiv -\frac{1}{4};$$

dies gibt einrests das Resultat

$$\sum_{\nu=1}^{p-1} \nu^2 q(\nu) \equiv -\frac{1}{12} \pmod{p}, \tag{24}$$

anderseits, wenn man dies in (ε) einsetzt, die interessante Kongruenz

$$\sum_{\nu=1}^{p-1} \nu \left[\frac{b\nu}{p}\right] \equiv \frac{b^2-1}{12b} \pmod{p}. \tag{25}$$

Dieselbe liefert eine Darstelung der Zahl $\frac{1}{a} \pmod{p}$, in welcher die Zahl a nur "ganzen" Operationen wird, nämlich

$$\frac{1}{a} \equiv a - 12\sum_{\nu=1}^{p-1} \nu \left[\frac{a\nu}{p}\right] \pmod{p}. \tag{25*}$$

Dadurch wird auch für die unbestimmte Gleichung

$$ax - py = 1$$

eine Lösung

$$x = a - 12\sum_{\nu=1}^{p-1} \nu \left[\frac{a\nu}{p}\right]$$

gefunden, jedoch nur für den Fall, daß p eine Primzahl ist.

Diese Anwendung der Theorie Fermatscher Quotienten macht das Bedürfnis dringend, den Begriff der Zahlen $q(a)$ auf *zusammengesetzte Moduln* zu erweitern. Es sei also m ein ungerader Modul, $\varphi(m)$ die Anzahl der Zahlen, die kleiner als m und ohne gemeinsamen Teiler mit m sind; ist a zu m relativ prim, so besteht die Kongruenz

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

und demnach ist die durch die Gleichung

$$a^{\varphi(m)} = 1 + mq(a) \tag{26}$$

bestimmte Zahl $q(a)$ ganz.

Man findet leicht die Gesetze

$$\begin{cases} q(ab) & \equiv q(a) + q(b) \pmod{m}, \\ q(c+mz) & \equiv q(c) + \frac{\varphi(m)z}{c} \pmod{m}; \end{cases} \tag{27}$$

aus der zweiten läßt sich für $ab \equiv c \pmod{m}$, und $0 < c < m$ die weitere Kongruenz

$$q(ab) \equiv q(c) + \frac{\varphi(m)}{ab}\left[\frac{ab}{m}\right] \pmod{m} \tag{28}$$

ableiten. Multiplizieren wir beiderseits mit $a^2b^2 \equiv c^2$, und schreiben $q(a)+q(b)$ an Stelle von $q(ab)$, so kommt

$$a^2q(a)\cdot b^2 + a^2b^2q(b) \equiv c^2q(c) + \varphi(m)ab\left[\frac{ab}{m}\right].$$

Hier lassen wir b die sämtlichen $\varphi(m)$ zum Modul relativ primen Zahlen durchlaufen und addieren die Resultate; da alsdann c dieselben Zahlen wie b durchläft, so entsteht

$$a^2q(a)s_2 + (a^2-1)\sum_b b^2q(b) \equiv \varphi(m)a\sum_b b\left[\frac{ab}{m}\right] \pmod{m}, \qquad (\eta)$$

wobei s_2 die summe der Quadrate der zum Modul relativ primen Zahlen bedeutet.

Setzt man hier zunächst $a=2$, so kommt

$$4q(2)s_2 + 3\sum b^2q(b) \equiv 2\varphi(m)\sum b' \pmod{m}, \qquad (\zeta)$$

wobei in der letzten Summation die Bedinung

$$b' > \frac{m}{2}$$

zu erfüllen ist.

Nun ist aber

$$\sum b' \equiv -\sum \beta \pmod{m},$$

wenn β die relativen Primzahlen von m, welche zwischen 0 und $\frac{m}{2}$ liegen, durchläuft.

Bedeutet

$$f(n) = \sum_{\nu=1}^{\left[\frac{n}{2}\right]} \nu,$$

so ist

$$\sum \beta = \sum \mu(d) df\left(\frac{m}{d}\right),$$

wobei d die sämtlichen Teiler von m durchläuft und $\mu(d)$ die übliche Bezeichnung für die M o e b i u s schen Zahlen ist. Da m, also auch $\frac{m}{d} = d'$, ungerade ist, so hat man

$$f(d') = \sum_1^{\frac{d'-1}{2}} \nu = \frac{d'^2-1}{8},$$

also

$$\sum \beta = \frac{1}{8}\sum \mu(d)(md'-d). \qquad (29)$$

Hieraus folgt

$$\sum \beta \equiv -\frac{1}{8}\sum d\mu(d),$$

also, wenn die Bezeichning eingeführt wird

$$P(m) = (1-p)(1-p')(1-p'')\ldots, \tag{30}$$

wobei $p, p', p'', \ldots$ die verschiedenen Primfaktoren des Moduls m bedeuten,

$$\sum \beta \equiv -\frac{1}{8}P(m) \pmod{m}. \tag{31}$$

Ferner ist die Zahl s_2 zu ermitteln. Setzt man der Kürze wegen

$$F(n) = \sum_{1}^{n-1} \nu^2,$$

so wird

$$s_2 = \sum_{d} \mu(d) d^2 F\left(\frac{m}{d}\right),$$

wobei wieder d die sämtlichen Teiler von m anzunehmen hat.

Nun ist bekanntlich

$$F(n) = \frac{n^3}{3} - \frac{n^2}{2} + \frac{n}{6},$$

und daher

$$s_2 = \frac{m^2}{3}\sum \mu(d)\, d' - \frac{m^2}{2}\sum \mu(d) + \frac{m}{6}\sum d\,\mu(d),$$

oder da $\sum \mu(d) = 0$,

$$s_2 = \frac{m^2}{3}\varphi(m) + \frac{m}{6}P(m). \tag{32}$$

Ist nun m durch 3 nicht teilbar, so folgt aus (32)

$$s_2 \equiv 0 \pmod{m}$$

und das Resultat (ζ) lautet

$$\sum b^2 q(b) \equiv \frac{1}{12}\varphi(m)P(m) \pmod{m}, \tag{33}$$

wobei links die Summation sich über alle die $\varphi(m)$ zu m teilfremden Zahlen b zwischen Null und m erstreckt.

Setzt man dies in (η) ein, so kommt zunächst

$$\left(a - \frac{1}{a}\right)\frac{\varphi(m)P(m)}{12} \equiv \varphi(m)\sum_{b} b\left[\frac{ab}{m}\right].$$

Diese Kongruenz führt zu einem einfachen Resultate, wenn die Zahl $\varphi(m)$ zu m prim ist; dies findet statt, wenn m das Produkt von lauter verschiedenen Primzahlen ist, falls überdies das Produkt $P(m)$ durch keine derselben aufgeht. Alsdann wird man durch $\varphi(m)P(m)$ dividieren dürfen, und *es kommt*

$$\frac{1}{a} \equiv a - \frac{12}{P(m)}\sum_{b} b\left[\frac{ab}{m}\right] \pmod{m}, \tag{34}$$

wobei sich die Bedingung am bequemsten durch

$$(m, \varphi(m)) \sim 1 \tag{35}$$

ausdrückt, und die Summation sich über die $\varphi(m)$ relativen Primzahlen b von m des Intervalls $(0 \dots m)$ erstreckt.

Ist dagegen m durch 3 teilbar, und sollen die Zahlen m und $\varphi(m)$ relativ prim sein, so wird keine der Differenzen $p-1$ durch 3 aufgehen, also werden die sämtlichen Primfaktoren von m außer 3 die Form $3x+2$ haben. Alsdann ist

$$s_2 \equiv \frac{m}{6} P(m),$$

und es folgt aus (ζ)

$$3 \sum b^2 q(b) \equiv P(m) \left[\frac{1}{4}\varphi(m) - \frac{2}{3} m\, q(2) \right] \pmod{m}.$$

Die Kongruenz (η) kann alsdann unter die Form gebracht werden

$$\frac{a^2-1}{3} P(m) \left[\frac{1}{4}\varphi(m) - \frac{2}{3} m\, q(2) \right] + a^2 q(a) \cdot \frac{m}{6} P(m) \equiv \varphi(m) a \sum b \left[\frac{ab}{m} \right] \pmod{m}.$$

Multipliziert man mit 3, so fällt das zweite Glied links heraus, und das Glied

$$(a^2-1) P(m) \frac{2}{3} m\, q(2)$$

wird durch m teilbar sein, da a^2-1 durch 3 aufgeht. Demnach entsteht

$$\left(a - \frac{1}{a} \right) \frac{P(m)\varphi(m)}{4} \equiv \varphi(m) \cdot 3 \sum b \left[\frac{ab}{m} \right],$$

und hieraus wieder die Kongruenz (34).

Dieselbe ist daher bloß an die Bedingung

$$(m, \varphi(m)) \sim 1$$

gebunden.

Die Moduln m, welche die Bedingung (35) erfüllen, haben überhaupt die Eigenschaft, daß man auf sie die Theorie der Quotienten $q(a)$ ausdehnen kann. Namentlich erhält man analog wie im Falle des Primzahlmoduls

$$q(a) \equiv \sum_{\nu} \frac{1}{a\nu} \left[\frac{a\nu}{m} \right] \pmod{m}, \tag{36}$$

wobei ν die zu m relativen Primenzahlen des Intervalls $(0 \dots m)$ durchläuft. Speziell folgt hieraus eine Verallgemeinerung der S y l v e s t e r schen Kongruenz (9)

$$2 \frac{2^{\varphi(m)} - 1}{m} \equiv \sum\nolimits^{*} \frac{1}{m\nu} \equiv - \sum\nolimits^{*} \frac{1}{\mu} \pmod{m}$$

$$\left(\frac{m}{2} < \nu < m; \quad 0 < \mu < \frac{m}{2}\right),$$

wobei selbstverständlich ν und μ relativ prim zum Modul sein müssen.

Wir kehren zum einfacheren Falle des Primzahlmoduls p wieder zurück und betrachten die quadratischen Reste r des Moduls p. Werden dieselben in den Grenzen $0 \ldots p$ angenommen, so sind sie durch die Kongruenzen

$$\nu^2 \equiv r \pmod{p}$$

vollständig charakterisiert, und zwar wird jede der $\frac{p-1}{2}$ Zahlen r zweimal erzeugt, wenn ν die sämtlichen Werte 1 bis $p-1$ annimmt. Die Kongruenz (7) ergibt

$$q(\nu^2) \equiv q(r) - \left[\frac{\nu^2}{p}\right] \frac{1}{\nu^2};$$

summiert man über die sämtlichen ν von 1 bis $p-1$, und beachtet, daß

$$q(\nu^2) \equiv 2q(\nu),$$

so ensteht

$$2\sum_{\nu=1}^{p-1} q(\nu) \equiv 2\sum_{r} q(r) - \sum_{\nu=1}^{p-1} \frac{1}{\nu^2}\left[\frac{\nu^2}{p}\right] \pmod{p}.$$

Nun ist

$$\sum q(\nu) \equiv N,$$

ferner identisch

$$2\sum_{r} q(r) = \sum \left(1 + \left(\frac{\nu}{p}\right)\right) q(\nu),$$

also mit Benützung der Notation (23)

$$2\sum_{r} q(r) \equiv N + A,$$

und unser Resultat läßt sich schreiben

$$\sum_{\nu=1}^{p-1} \frac{1}{\nu^2}\left[\frac{\nu^2}{p}\right] \equiv A - N \pmod{p}. \tag{37}$$

Ist speziell $p = 4n+3$, so ist nach (18)

$$A \equiv 0$$

und die Kongruenz gibt eine *bemerkenswerte Darstellung des Restes des Wilsonschen Quotienten N.*

Ich werde bei einer anderen Gelegenheit zeigen, daß sich für jede ungerade Primzahl p der Wilsonische Quotient N nach dem Modul p durch eine Benoullische Zahl ausdrücken läßt, nämlich bei der früheren Bezeichnung $p = 2m+1$

$$N \equiv -1 + \frac{1}{p} - (-1)^m B_m \pmod{p}.$$

Im Falle $p = 4n + 1$ haben wir oben (21) gefunden, daß

$$A \equiv (-1)^{n-1} 2B_n \pmod{p},$$

und da hier

$$N \equiv -1 + \frac{1}{p} - B_{2n},$$

so lautet (37) für $p = 4n + 1$ wie folgt:

$$\sum_{1}^{p-1} \frac{1}{\nu^2} \left[\frac{\nu^2}{p}\right] \equiv 1 - (-1)^n 2B_n + B_{2n} - \frac{1}{p} \pmod{p} \qquad (37^1).$$

Die bisher angewandte Schlußweise ließe noch weitere Anwendungen zu; wir wollen jedoch den Gegenstand verlassen, und schließen mit einigen ähnlichen Formeln, in welchen sich nun die Summation entweder über die quadratischen Reste oder über die Nichtreste des Moduls erstrecken.

Wir bezeichnen mit a oder $a', a'', \ldots$ quadratische Reste, mit b, resp. $b', b'', \ldots$ Nichtreste von p und setzen

$$\sum_a q(a) = A, \quad \sum_b q(b) = B.$$

Nach (7) ist

$$aa' \equiv a' + pz, \quad z = \left[\frac{aa'}{p}\right],$$

$$q(aa') \equiv q(a'') - \frac{1}{aa'} \left[\frac{aa'}{p}\right] \equiv q(a) + q(a').$$

Summiert man über die a', so durchläuft a'' die gleichen Werte und es kommt

$$mq(a) \equiv -\sum_{a'} \frac{1}{aa'} \left[\frac{aa'}{p}\right]$$

oder

$$q(a) \equiv 2 \sum_{a'} \frac{1}{aa'} \left[\frac{aa'}{p}\right], \qquad (38)$$

wobei die Summation sich über die sämtlichen quadratischen Reste a' des Moduls p erstreckt, letztere natürlich in den Grenzen 0 und p vorausgesetzt.

Ferner ist bei der angenommen Bezeichnung

$$ab \equiv b' \pmod{p},$$

also

$$ab \equiv b' + pz$$

und

$$q(ab) \equiv q(b') - \frac{1}{ab}\left[\frac{ab}{p}\right] \equiv q(a) + q(b). \qquad (a)$$

Wird hier über die sämtlichen m Werte b summiert, so entsteht

$$m\,q(a) \equiv -\sum_b \frac{1}{ab}\left[\frac{ab}{p}\right],$$

oder

$$q(a) \equiv 2\sum_b \frac{1}{ab}\left[\frac{ab}{p}\right] \pmod{p}. \qquad (38^1)$$

Diese beiden Sätze (38) und (38^1) sind übrigens eine direkte Folge der Sätze (8) und (23^*).

Wird dagegen in (a) über die m Werte a summiert, so ensteht

$$m\,q(b) + A \equiv B - \sum_a \frac{1}{ab}\left[\frac{ab}{p}\right]$$

oder

$$q(b) \equiv 2A - 2B + 2\sum_a \frac{1}{ab}\left[\frac{ab}{p}\right] \pmod{p}. \qquad (39)$$

Ferner ist

$$bb' = a + pz$$

und demnach

$$q(b) + q(b') \equiv q(a) - \frac{1}{bb'}\left[\frac{bb'}{p}\right];$$

wird hier über die b' summiert, so ensteht

$$m\,q(b) + B \equiv A - \sum_{b'} \frac{1}{bb'}\left[\frac{bb'}{p}\right]$$

oder

$$q(b) \equiv -2A + 2B + 2\sum_{b'} \frac{1}{bb'}\left[\frac{bb'}{p}\right] \pmod{p}. \qquad (39')$$

Vergleicht man dies mit (39), so entsteht

$$\sum_a \frac{1}{ab}\left[\frac{ab}{p}\right] - \sum_{b'} \frac{1}{bb'}\left[\frac{bb'}{p}\right] \equiv 2(A - B) \pmod{m},$$

ein Resultat, das in (23^*) enthalten ist; denn hier bedeutet b einen Nichtrest, also

$$\left(\frac{b}{p}\right) = -1,$$

und der Buchstabe A in (23^*) ist

$$\sum_{1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu),$$

fällt also mit unserem jetztigen $A - B$ zusammen.

6 Sur les théorèmes de Sylvester concernant le quotient de Fermat.

Note de M. **LERCH**, présentèe par M. Émile Picard.

Published in C. R. 35 - 38, section 3, [44].

M. Mirimanov a donné un théorème qui rectife et restitueen partie quelques propositions de Sylvester concernant le quotient de Fermat *Comptes rendus,* t. LII)

$$q^{(a)} = \frac{a^{p-1} - 1}{p}$$

Pour généraliser le théorème de Mirimanov, j'envisage un module quelconque m, puis l'entier positif a premier avec m, et j'observe que l'on a identiquement

$$\frac{a^d - 1}{m} \equiv \sum_{\nu=1}^{d} \frac{\left(\frac{a^\nu}{m}\right) - a\left(\frac{a^{\nu-1}}{m}\right)}{a^\nu - m\left(\frac{a^\nu}{m}\right)} \pmod{m},$$

l'exposant d étant un diviseur de $\varphi(m)$ tel que

$$a^d \equiv 1 \pmod{m}.$$

Posant $de = \varphi(m)$, on aura, en effet,

$$q^{(a,m)} \equiv \frac{a^{\varphi(m)} - 1}{m} \equiv e\frac{a^d - 1}{m} \pmod{m},$$

et il s'ensuit

$$\frac{a^{\varphi(m)} - 1}{m} \equiv e \sum \frac{\alpha}{\beta}, \tag{1}$$

β parcourant les restes des différentes puissances de a, et les α étant déterminés par la condition

$$m\alpha + \beta \equiv 0 \pmod{a}, \qquad 0 \leq \alpha < a.$$

Mais la formule de Mirimanov ne possède le type des théorèmes de Sylvester que dans les cas particuliers. Afin de restituer les théorèmes du savant'anglais, j'ai établi la congruence

$$q^{(a,m)} \equiv \sum{}^{*} \frac{1}{a\nu}\left(\frac{a\nu}{m}\right) \pmod{m}, \tag{2}$$

ν parcourant les $\varphi(m)$ nombres premiers avec m et plus petits que m. Cette congruence se vérifie en développant le premier membre de l'équation identique

$$\prod_{\nu}\left[a\nu - m\left(\frac{a\nu}{m}\right)\right] = \prod \nu.$$

La formule (2) rend les mêmes services, et est peut-être plus commode que les formules de Sylvester, mais elle permet aussi d'établir ces dernières rectifiées. Les formules en question s'écrivent

$$q^{(a,m)} \equiv \sum \frac{r'_\nu}{\nu} \equiv -\sum \frac{r'_\nu}{\nu} \pmod m, \tag{3}$$

ν parcourant les mêmes valeurs que dans la formule (2), puis

$$mr_\nu + \nu \equiv 0, \quad mr'_\nu - \nu \equiv 0 \pmod a; \quad 0 \le r_\nu < a, \quad 0 < r'_\nu \le a.$$

Désignons ensuite par ξ les différentes racines de l'équation

$$\frac{x^{(\alpha)} - 1}{x - 1} = 0$$

posons

$$\Phi(x) = \sum_{\nu=1}^{m} \left(\frac{m^2}{\nu}\right) \frac{x^\nu}{\nu},$$

puis

$$Q(a,c) = \sum_\xi \frac{\Phi(\xi^c)}{\xi^m - 1},$$

les deux entiers de signes quelconques a et c étant supposés premiers avec m. Désignant enfin par $C(a,c)$ la quantité

$$\operatorname{sgn}(ac) \sum \frac{1}{\nu} \qquad \left(\begin{array}{c} 0 < \nu < m; \quad (\nu, m) \sim 1 \\ |c|\nu = |a|\alpha + m\beta \end{array} \right)$$

où l'on admet $\alpha, \beta = 1, 2, 3, \ldots$ et même $\beta = 0$ pour $c < 0$, on aura la congruence suivante

$$Q(a,c) \equiv aC(a,c) + cq(a) - cq(c) \pmod m \tag{4}$$

Pour $c = 1$ et m premier, cette dernière s'établit directement en multipliant entre eux les développements des binomes $(1 - \xi)^p$, ce qui est un procédé analogue à la méthode d'Eisenstein.

Mais il y a des procédés plus avantageux pour déterminer $q(a,m)$ lorsque m est un produit $m_1 m_2 m_3 \ldots$ de facteurs m_ν, premiers relatifs deux à deux. Posons à cet effet $m = m_\nu n_\nu$ et déterminons les n'_ν conformément aux congruences $n_\nu^2 n'_\nu \equiv 1 \pmod{m_\nu}$; alors on a comme cela se vérifie tout à l'heure

$$q(a,m) \equiv \sum_\nu n_\nu n'_\nu \varphi(n_\nu) q(a, m_\nu) \pmod m. \tag{5}$$

Ainsi la recherche directe du reste du quotient

$$q(2) \equiv \frac{2^{\varphi(385)} - 1}{385} = \frac{2^{240} - 1}{385} \pmod{385}$$

serait pénible. Mais comme ici $m = 5.7.11$, on a les valeurs respectives $m_\nu = 5, 7, 11$, $n'_\nu = -1, 1, 3$, $\varphi(n_\nu) = 60, 40, 24$, $q(2, m_\nu) = 3, 2, 5$ et l'on trouve sans aucune peine

$$q(2) \equiv 60 \pmod{385}.$$

Un procédé avantageux relatif aux modules puissances de nombres premiers reste cependant à découvrir.

7 Études sur la théorie des résidues quadratiques suivivant un module premier. Relations nouvelles avec la théorie des formes quadratiques ayant un déterminant négatif et premier.

Resume

Published in Publ. Univ. Masaryk, Nr. 34, 39–44, section 3, [50], [51].

I.

1. Le polynôme (1), où ε_ν est le symbole de Legendre:

$$\varepsilon_\nu = \left(\frac{\nu}{q}\right); \quad \nu = 1, 2, \dots q-1; \quad \varepsilon_0 = \varepsilon_q = 1,$$

et q un nombre premier de la forme $4a+3$, satisfait à la congruence algébrique

$$Q^2(x) + q \equiv 0 \pmod{\frac{x^q - 1}{x - 1}};$$

on peut écrire le premier membre de cette congruence sous la forme (α) (p.8), les nombres e_n étant définis au moyen des équations (2). On en déduit aisément les relations (4) et la formule (I).

2. La première des formules (4^4) donne immédiatement le théorème: *q ètant un module premier de la forme $4a+3$ la suite complète de symboles de Legendre (L) $\varepsilon_1, \varepsilon_2, \dots \varepsilon_{q-1}$ offre $\frac{1}{2}(q-3)$ permanences et $\frac{1}{2}(q-1)$ variations.*

L'expression

$$\sum_1^{q-2} \frac{(1+\varepsilon_\nu)(1+\varepsilon_{\nu+1})}{4}$$

(voir p. 10) est égale au nombre des cas où il y a, dans la suite (L), deux signes consécutifs positifs; le calcul de cette expression (au moyen des formules 4) donne le théorème suivant: *I ly a dans la suite $1, 2, 3, \dots q-1$ [q étant un nombre premier, $q \equiv 3 \pmod 4$], $\frac{1}{4}(q-3)$ résidus quadratiques suivis par un résidu et autant de non-résidus suivis par un non-résidu.*

On démontre d'une manière analogue en calculant les sommes (voir p. 10)

$$\sum_1^{q-2} \frac{1-\varepsilon_\nu}{2} \cdot \frac{1+\varepsilon_{\nu+1}}{2}, \quad \sum_1^{q-2} \frac{1+\varepsilon_\nu}{2} \cdot \frac{1-\varepsilon_{\nu+1}}{2} :$$

La suite $1, 2, \ldots, q-1$, *contient* $\frac{1}{4}(q+1)$ *résidus quadratiques suivis par un non-résidu et* $\frac{1}{4}(q-3)$ *non-résidus suivis par un résidu quadratique.*

3. Voici les théorèmes analogues pour la demi-suite de symboles de Legendre

$$\varepsilon_1, \varepsilon_2, \ldots \varepsilon_m \tag{M}$$

$$m = \frac{q-1}{2}, \quad q \equiv 3 \pmod 4.$$

Le nombre des variations contenues dans la demi-suite de symboles de Legendre de (M), suivant un module premier de la forme $4a+3$, *est égal au nombre des permanences.*

La suite $1, 2, \ldots \frac{1}{2}(q-1)$ *contient* $\frac{1}{8}(q-3)+\frac{1}{4}(1+\varepsilon_2)$ *résidus quadratiques mod* q *suivis par un non-résidu et* $\frac{1}{8}(q-3)-\frac{1}{2}(1+\varepsilon_2)$ *non-résidus suivis par un résidu.*

On démontre, en calculant les sommes

$$\sum_1^{m-1} \frac{1+\varepsilon_\mu}{2} \cdot \frac{1+\varepsilon_{\mu+1}}{2}, \quad \sum_1^{m-1} \frac{1-\varepsilon_\mu}{2} \cdot \frac{1-\varepsilon_{\mu+1}}{2}$$

(voir p. 13) le théorème suivant: *La suite* $1, 2, 3, \ldots \frac{q-1}{2}$, *relative à un module premier de la forme* $q = 4a+3$, *contient* $\frac{1}{8}(q-3) + \frac{1}{2}\left(H - \frac{1-\varepsilon_2}{2}\right)$ *paires de résidus quadratiques consécutifs et* $\frac{1}{8}(q-3) - \frac{1}{2}\left(H - \frac{1-\varepsilon_2}{2}\right)$ *paires de non-résidus consécutifs.* Ici H désigne le nombre des classes de formes quadratiques de Gauss $a_1x^2 + 2bx_1y_1 + c_1y^2$ ayant le déterminant $-q = {b_1}^2 - a_1c_1$.

4. La seconde des équations (4^4) donne le théorème: *Il y a, dans la suite* (L), *autant de termes qui séparent deux signes égaux, combien il y en qui séparent deux signes contraires.*

Eu calculant la somme

$$\sum_1^{q-3} \frac{1+\varepsilon_\mu}{2} \cdot \frac{1+\varepsilon_{\mu+2}}{2}$$

on démontre *la propriété suivante de la suite* $1, 2, \ldots q-1$*: Il y a* $\frac{1}{4}(q-3)$ *termes dont les deux voisins sont des résidus et* $\frac{1}{4}(q-3)$ *termes dont les deux voisins sont des non-résidus.*

De même, en employant la seconde équation (4^4) et la formule (6) on trouve que *la suite* $\varepsilon_3, \varepsilon_5, \ldots \varepsilon_{m-2}$ *contient autant de variations qu'il y a de permanences dans la suite* $\varepsilon_2, \varepsilon_4, \ldots \varepsilon_{m-3}$.

On démontre de la même manière, en calculant les sommes

$$\sum_1^{m-2} \frac{1+\varepsilon_\mu}{2} \cdot \frac{1+\varepsilon_{\mu+2}}{2}, \quad \sum_1^{m-2} \frac{1-\varepsilon_\mu}{2} \cdot \frac{1+\varepsilon_{\mu+2}}{2}$$

(voir p. 15) que *la suite* $1, 2, 3, \ldots m$ (où $m = \frac{q-1}{2}$ *et* q *est un nombre premier de la forme* $4a+3$*) contient* $\frac{m-3}{4} + \frac{1+\varepsilon_2}{4}\varepsilon_3 + \frac{1}{2}H$ *termes dont les deux voisins sont des résidus suivant le module* q *et* $\frac{m-1}{4} + \frac{1-\varepsilon_2}{4}\varepsilon_3 - \frac{1}{2}H$ *termes dont les deux voisins sont des non-résidus.*

La suite $1, 2, \ldots m$ (où $m = \frac{q-1}{2}$ et q est un nombre premier de la forme $4a+3$) *contient*

$$\frac{m-2-\varepsilon_2}{4} - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4} = \left[\frac{q}{8}\right] - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4}$$

termes précédés par un non résidu et suivis par un résidu quadratique; la même suite contient

$$\left[\frac{q}{8}\right] + \varepsilon_2 + \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}$$

termes précédés par un résidu quadratique et suivis par un non-résidu.

5. Substituons maintenant, dans la somme

$$A = \sum_{1}^{q-1} \varepsilon_{\nu^2-1}\varepsilon_\nu$$

la quantité $q-\mu$ à la place de ν; il vient $\nu^2 - 1 \equiv \mu^2 - 1$, d'où $A = 0$. Ce résultat, combiné avec les équations (4^4), nous permet de calculer les sommes

$$\sum_{1}^{q-3} \frac{1 \pm \varepsilon_\nu}{2} \cdot \frac{1 \pm \varepsilon_{\nu+1}}{2} \cdot \frac{1 \pm \varepsilon_{\nu+2}}{2};$$

on démontre ainsi le théorème: *La suite complète de symboles de Legendre* $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{q-1}$*, pour un module premier* q *de la forme* $4a+3$*, contient*

$$\frac{q-3-2(1+\varepsilon_2)}{8}$$

ternes du chacun des types $+++, -++, ---, --+$ *et*

$$\frac{q-3+2(1+\varepsilon_2)}{8}$$

ternes du chacan des types $+-+$, $-+-$, $++-$, $+--$.

II.

6. On obtient des résultats analogues pour un module premier p de la forme $4a+1$.

Le nombre des variations contenues dans la suite complète (L') *de symboles de Legendre* $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{p-1}$ *est plus grand d'une unitè que le nombre des permanences qui y sont contenues. Même théorème pour la demi suite*

$$\varepsilon_1, \varepsilon_2, \ldots \varepsilon_m \left(m = \frac{p-1}{2} \right). \qquad (M')$$

La demi-suite (M') *de symboles de Legendre pour un module p contient* $\left[\frac{p-2}{8}\right]$ *paires de termes consécutifs positifs et* $\left[\frac{p}{8}\right]$ *paires de termes consécutifs négatifs.*

Il y a, dans la suite (M')*, pour un module premier quelconque,* $\left[\frac{p}{8}\right]$ *groupes* $(-+)$ *et* $\left[\frac{p+3}{8}\right]$ *groupes* $(+-)$*.*

7. Appelons $+\pm-$, $-\pm+$ternes à une variation; $+\pm+$, $-\pm-$ternes à deux variations ou ternes sans variation. On a, pour les modules p: *Il y a, parmi les ternes à une variation de la suite* (M')

$$\left[\frac{p-2}{8}\right] + \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4}$$

ternes qui appartiennent à l'un ou à l'autre des types $-++$ *et* $--+$

$$\left[\frac{p+3}{8}\right] \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}$$

ternes qui appartiennent à l'un ou à l'autre des types $++-$, $+--$,

$$\left[\frac{p-2}{8}\right] - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{2}$$

ternes aux extrémités positives et

$$\left[\frac{p-2}{8}\right] + \varepsilon_2 + \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}$$

ternes aux extrémités négatives.

III.

8. Substituons $x = -1$ dans la formule (1), q étant un module de la forme $4a+3$. On obtient la formule (10^*) qui donne le nombre H de classes des formes primitives ayant le déterminant $-q$. Différentions l'èquation (I) et substituons y $x = 1$. On trouve la formule (11^*) qui donne le nombre $Cl(-q)$ des classes de formes positives ayant le discriminant $-q = b^2 - 4ac$.

9. On obtient une autre formule (12) pour H en substituant dans la formule (I), $\sqrt{-1}$ à la place de x: En combinant les équations (10) et (12) on trouve les formules (A).

IV.

10. Un module premier p de la forme $4a+1$ donne lieu à des résultats plus simples. L'équation (II) conduit aux équations $(16), (16^*), (16^1), (17)$ et (17^*).

11. En posant $Q(i) = A+iB$, on trouve $A = B = H$ où $H = -Cl(-\Delta p)$ désigne le nombre des classes de formes quadratiques ayant un déterminant négatif $-p$.

V.

12. Différentions l'equation (I) et substituons y $x = \Theta_n = e^{\frac{2h\pi i}{q}}$ (h et q étant des entiers sans diviseur commun); on obtient la formule III, et les équations (20), (21), (22), (22^*). L'équation (21^2) donne: *q étant un nombre premier de la forme $4a+3$, il y a*

$$N = \frac{m(m-1)}{4} - \frac{1+\varepsilon_2}{4} Cl(-q), \quad \left(m = \frac{q-1}{2}\right)$$

solutions de l'èquation indéterminée

$$xz^2 - x^2 z = y^2 + qu$$

qui satisfont aux conditions

$$0 < x < z \leq m, \quad 0 < y \leq m.$$

Il y a

$$\frac{m(m-1)}{4} + \frac{1+\varepsilon_2}{4} Cl(-q)$$

solutions de l'èquation indéterminée

$$xz^2 - x^2 z + y^2 = qu$$

qui satisfont aux mêmes conditions.

La formule (21^1)donne: *Il y a*

$$\frac{(q-1)(q-2)}{4} \pm \frac{3}{2} Cl(-q)$$

solutions de l'èquation indéterminée

$$xz^2 - x^2 z \pm y^2 = qu$$

qui satisfont aux conditions

$$0 < x < z < q, \quad 0 < y \leq m.$$

13. Posons

$$A = \sum_{n=1}^{q-1} n s_{n-1} \varepsilon_n, \quad s_k = \sum_{1}^{k} \varepsilon_\nu;$$

on déduit l'identitè (23) et la formule (23*).

14. L'équation (21) conduit (voir les équations $20, \alpha, 23, 24$) à l'identité (24^0) et aux équations (25) et (26).

15. Applications. L'équation (a) conduit immédiatement au résultat suivant: *Il y a n_ν solutions de la congruence*

$$x^2 + y^2 \equiv \nu^2 \pmod{q}$$

qui satisfont aux conditions

$$-\nu < x < \nu, \quad 0 < y \leq m.$$

Il résulte des équations (a) et (13) que

$$\sum_{1}^{m} n_\nu = \frac{H^2 + m^2}{2},$$

done: *Il y a $\frac{1}{2}(H^2 + m^2)$ solutions de la congruence*

$$x^2 + y^2 \equiv z^2 \pmod{q}$$

qui satisfont aux conditions

$$0 < y \leq m, \quad 0 < x < z \leq m, \quad \left(m = \frac{q-1}{2}\right).$$

L'expression

$$\frac{2\nu - 1 - c_{2\nu}}{2} = n'_\nu$$

est égale au nombre de solutions de la congruence $x^2 - y^2 \equiv \nu^2, 0 < y \leq m, |x| < \nu$; remarquons encore que

$$\sum_{1}^{m} n'_\nu = \frac{1}{2}(m^2 - H^2).$$

On a les théorèmes suivants: *Il y a $\frac{1}{2}(m^2 - H^2)$ solutions de la congruence $x^2 \equiv y^2 + z^2$ qui satisfont aux conditions $0 < y \leq m, 0 < z \leq m, -z < x < z$.*

Il y a $\frac{1}{4}(m^2 - H^2)$ solutions de la congruence $x^2 \equiv y^2 + z^2$ qui satisfont aux conditions $0 < y \leq m, 0 < z \leq m, 0 < x < z$.

Appelons "solutions fondamentales" de la congruence

$$x^2 + y^2 \equiv z^2 \pmod{q} \qquad (P)$$

toute solution composé des nombres $x, y, z = 1, 2, \ldots m$.

Il y a $\frac{1}{2}m(m-1)$ *solutions fondamentales de la congruence (P);* $\frac{1}{4}(m^2 - H^2)$ *solutions avec* $x > z$, *et* $\frac{1}{4}(m^2 - 2m + H^2)$ *solutions avec* $x < z$.

q étant un nombre premier de la forme $8k+3$, *le nombre des solutions fondamentales de la congruence (P) qui satisfont aux conditions* $z < x < y$ *surpasse de* $\frac{1}{4}(m-H)^2$ *unités celui des solutions fondamentales qui satisfont aux conditions* $x < y < z$

q étant un module premier de la forme $8k+7$, *le nombre des solutions fondamentales de la congruence (P) qui satisfont aux conditions* $x \leq y < z$ *surpasse de* $\frac{1}{4}(H^2 + m)$ *unités celui des solutions fondamentales qui satisfont aux conditions* $z < x < y$.

16. Enfin, les équations (27) et (28) qui résultent de la relation (a)
nous donnent les théorèmes suivants:

La somme des valeurs de x qui figurent dans les solutions fondamentales de la congruence (P) avec la condition $x > z$ *est égale à*

$$\sum x = \frac{(q-2)(q^2-1)}{48} - \frac{1-\varepsilon_2}{4}\, q\, Cl(-q)^2$$

La somme des valeurs de z qui figurent dans les solutions fondamentales de la congruence (P) avec la condition $z > x$ *est égal à*

$$\sum z = \frac{(q^2-1)(q-4)}{48} + \frac{1-\varepsilon_2}{4}\, q\, Cl(-q)^2.$$

8 Index

English	**German**	**page and number of review**
modular function	Modulfunktion	20, [23]
Pell number	Pellsche Zahl	22, [28]
primitive root	primitiver Wurtzel	18, [40]
quadratic field	quadratischer Körper	30, 32, [40], [43]
quadratic residue (non residue)	quadratischer Rest (Nichtrest)	18, 24, 28, 35, 50, 55, 60, 61, 69, 70, 71, [20], [33], [50], [51]
Riemann zeta-function	Riemannn'sche Funktion	15, 23, [13], [30]
Sylvester's theorem	Satz von Sylvester	31, 65, [43]
Wilson quotient	Wilsonscher Quotient	43, 44, 48, 60
Wilson's theorem	Wilsonscher Satz	43
Zolotarev's theorem	Zolotarevscher Satz	18, [19], [20]

Title: Matyáš Lerch's work on number theory
Author: Karel Lepka
Adress: 618 00 Brno, Jiránkova 49, Czech republic, email lepka@scova.vabo.cz
Published: Masaryk University, Faculty of Science, Departement of Mathematics
Adress: 662 95 Brno, Janáčkovo nám. 2a, Czech republic
Printed: Grafex, 67801 Blansko, Těchov 152
Impression: 600 copies