Vega, Primes, Cryptography and the Fields Medal

Vega, praštevila, kriptografija in Fieldsova medalja

Dr. Tomaž Pisanski, Dr. Marko Boben, Dr. Alen Orbanić, Boris Horvat

University of Ljubljana
Faculty of Mathematics and Physics
Jadranska 19, Ljubljana
Slovenia

Abstract

Prime numbers have been studied since the ancient times. This seemingly theoretical part of mathematics forms the basis for cryptographic algorithms which secure the communications in the modern world. The list of famous mathematicians who were involved in the study of primes is very long. It ranges from Euclid, Eratosthenes, Fermat, Gauss, Legendre, Hadamard to Erdős. Jurij Vega can proudly take place on this list. By publishing the table of primes up to 400,031 in 1797 he enabled further research in this area done by Gauss and Legendre who formulated the Prime number theorem.

Povzetek

Praštevila so predmet raziskav že vse od antike. To na videz teoretično področje v okviru matematike je osnova za kriptografske algoritme, ki služijo varovanju komunikacij v sodobnem svetu. Seznam matematikov, ki so raziskovali praštevila, je zelo dolg, obsega imena od Evklida in Eratostena, prek Fermata, Gaussa, Legendra in Hadamarda, do Erdősa. Na ta seznam se lahko s ponosom uvrsti tudi Jurij Vega. Njegova objava praštevil do 400.031 iz leta 1797 je omogočila nadaljnje raziskovanje področja tudi Gaussu in Legendru, ki je oblikoval Izrek o praštevilih.

Introduction

Vega accomplished many very important achievements in mathematics. He published several editions of logarithmic, trigonometric, and ballistic tables, lectures (on geometry, land surveying, infinitesimal calculus), handbooks (*Logarithmisch-trigonometrisches Handbuch*, etc.). However, it is not well known that he was also interested in problems in number theory. He published a table of prime numbers and tables of decompositions of numbers not divisible by 2, 3, or 5.

Prime numbers

A prime number, or simply a "prime," is a positive integer $p > 1$ that has no positive integer divisors other than 1 and p itself. For example, 13 is a prime and $15 = 3 \cdot 5$ is not. The history of primes is very long. The ancient Greeks knew of primes and Euclid proved in his *Elements* (Book IX) that there were infinitely many of them. In about 200 BC Eratosthenes devised an algorithm for calculating primes called the *Sieve of Eratosthenes*.

After a large gap during the Dark Ages, the next important results about prime numbers were made by Fermat. Among them, the result which is known under the name *Little Fermat Theorem* is best known. It states that if p is a prime number and a is a natural number then $a^p \equiv a \pmod{p}$.

The first known table of primes is a table of the least prime factors of the positive integers up to 800. This table was created by Cataldi in 1603. The least prime factor of n is the least integer greater than 1 that divides n. Cataldi's table was soon followed by others; see Table 1.

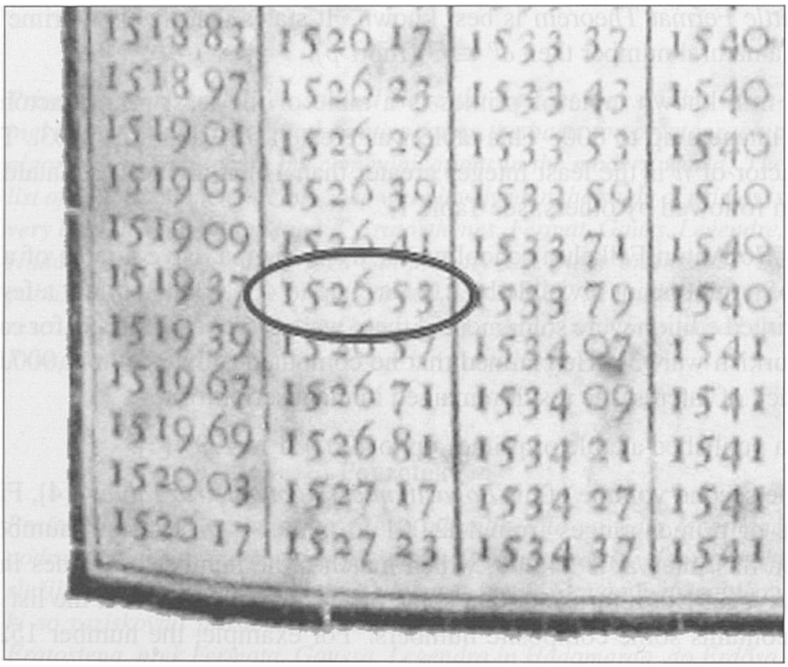
In 1776 Anton Felkel, a schoolmaster from Vienna, gave a table of all prime factors of numbers not divisible by 2, 3, or 5 up to 408,000. But only a few copies of the printed edition were sold; most of them were scrapped and used for cartridges in the Turkish war [3]. He claimed that he computed primes up to 2,000,000, but due to lack of interest the result remained in manuscript form.

Vega published a table of primes up to 400,031 in 1797 [4].

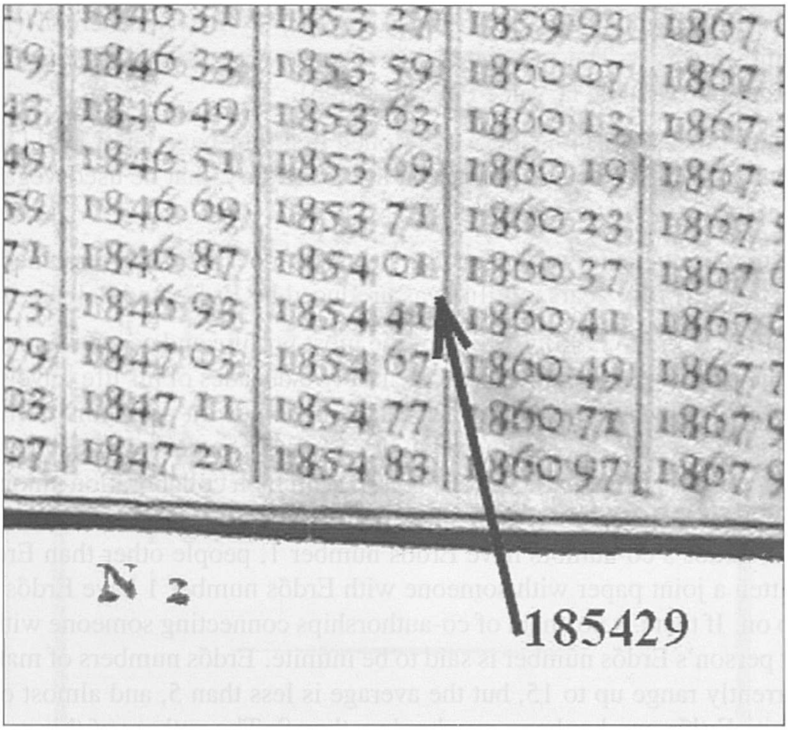
In the second volume of his *Logarithmic-Trigonometric Tables* ([4], Figure 3), the table of primes ranges from 102,001 to 400,031. The actual number of all primes in this interval is 24,096, which matches the number of primes in the list given by Vega. But it turns out that some primes are missing from the list and that the list contains some composite numbers. For example, the number $152{,}653 = 293 \cdot 521$ is listed in the table (page 99 of [4]); see Figure 1. An example of a missing prime is 185,429. It should be listed between 185,401 and 185,441 but it is not; see Figure 2. The list of primes of this extent can be nowadays obtained in a few seconds using the computer program *Mathematica*. This was how the authors were able to detect errors in Vega's tables.

Limit	Who	When	Type of table
800	Cataldi	1603	least prime factor
100,000	Brancker	1668	least prime factor
100,000	Kruger	1746	primes
102,000	Lambert	1770	least prime factor
408,000	Felkel	1776	least prime factor
400,031	**Vega**	**1797**	**primes**
1,020,000	Chernac	1811	least prime factor
3,036,000	Burkhardt	1816/17	primes
6,000,000	Crelle	1856	primes
9,000,000	Dase	1861	primes
100,330,200	Kulik	1863 ?	least prime factor
10,007,000	D. N. Lehmer	1909	least prime factor
10,006,721	D. N. Lehmer	1914	primes

TABELA / TABLE 1. Tabele praštevil pred elektronsko računalniško dobo (iz [**2**]) / Tables of prime numbers before the electronic computer age (from [**2**])



SLIKA / FIGURE 1. **Številka 152.653 ni praštevilo, saj je produkt številk 293 in 521 (str. 95). / The number 152,653 is not a prime since it is a product of 293 and 521 (page 95).**



SLIKA / FIGURE 2. Na seznamu manjka praštevilo 185.429 (str. 99). / The prime number 185,429 is missing from the list (page 99).

Vega's tables were known as very reliable. Vega himself offered a prize of one *ducat* to anyone that could find an imperfection in his *Thesaurus logarithmorum* [5], which would lead to an error in computation. Gauss, who reviewed *Thesaurus* [1], reported that he did not find any errors after checking some values of logarithms in the first part but that there are several in the second part. Gauss also remarked that Vega was probably not aware of what kinds of imperfections could actually occur, but also said that he was not informed of any case that the reward had actually been paid out. At that time, there were many authors of various tables that used the same stimulation. According to Gauss [1], only Köhler had requested rewards for four errors.

Using the tables of primes by Lambert and Vega, the great mathematicians like Gauss and Legendre were able to guess the prime number theorem.

Gauss carefully checked the tables of Lambert and caught several errors. This shows that probably no tables of that time were error-free. The *prime number theorem* gives an asymptotic formula for the prime counting function $\pi(n)$, which counts the number of primes less than n. In 1791, Gauss suggested the formula

$\pi(n) \sim n/\ln n$, which was later refined to $\pi(n) \sim Li(n)$, where $Li(n)$ is the logarithmic integral. The prime number theorem was proved independently by Hadamard (1896) and de la Valée Poussin (1896).

On December 24, 1849, Gauss mentioned in a four-page letter [**10**],[**11**] to his student Johann Franz Encke, a lieutenant in the artillery, that he used Vega's tables to confirm his estimate (see Figure 4).

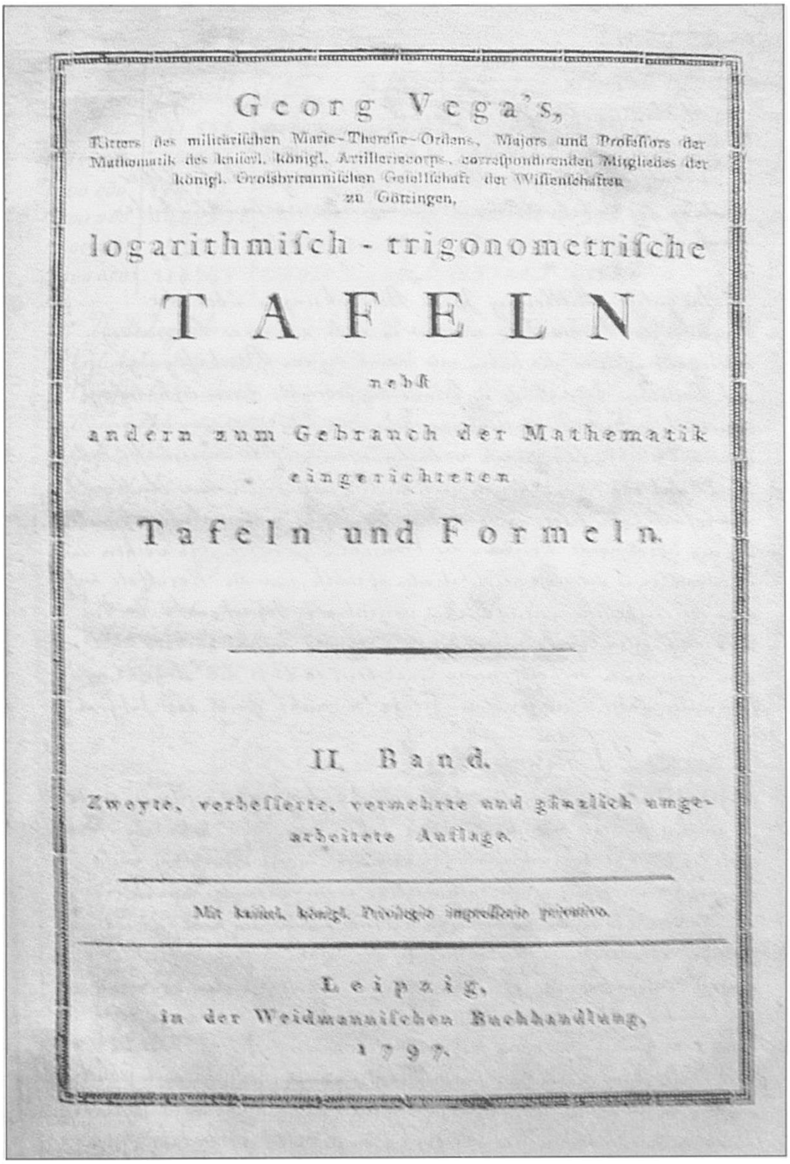
Finding an elementary proof of the Prime number theorem remained a challenge for the next fifty years, until it was produced by Erdős and Selberg in 1949.

Paul Erdős (1913–1996) was one of the most prolific and eccentric mathematicians of the past century [**6**]. He spent the last two decades of his life traveling from university to a university to work with mathematicians on problems in many different areas. He wrote or co-authored 1,475 academic papers. His extensive work with many people gave him the idea to start research on collaboration among mathematicians. An *Erdős number* is defined in the following way [**9**]: Erdős has Erdős number 0, Erdős's co-authors have Erdős number 1, people other than Erdős who have written a joint paper with someone with Erdős number 1 have Erdős number 2, and so on. If there is no chain of co-authorships connecting someone with Erdős, then that person's Erdős number is said to be infinite. Erdős numbers of mathematicians currently range up to 15, but the average is less than 5, and almost everyone with a finite Erdős number has a number less than 8. The authors of this paper have Erdős numbers 2, 3, 3, respectively.

Back to the prime number theorem. There is an interesting story about the proof of Erdős and Selberg. Erdős sent a postcard to some friend informing him about the proof. When Selberg met this friend, he told him that Erdős and some "what's-his-name" had an elementary proof of the prime number theorem. Selberg felt offended and published the result alone. Among other work, this proof brought him the Fields Medal, which is considered the premier award in mathematics, often called the "Nobel Prize in Mathematics" (although its monetary value of about $9,500 cannot compare to the Nobel Prize).

Prime numbers today have an important application in cryptography. They are the basis of the RSA encryption system [**7**]. The system uses the fact that determining whether some large number is a prime is a computationally hard problem. Until recently, all algorithms for determining whether some number is prime were of exponential time complexity. In [**8**] a polynomial algorithm was found. (Un)fortunately the algorithm has still large time complexity ($O(n^{12})$).

Because Vega was also a soldier, we may consider the role of primes in wars. The first known use of primes in battles was the use of Felkel's tables for cartridges, as mentioned before. In the last century and nowadays, cryptography plays an essential role in communications in the army.



Georg Vega's,

Ritters des militärischen Marie-Theresie-Ordens, Majors und Professors der Mathematik des kaiserl. königl. Artilleriecorps, correspondirenden Mitgliedes der königl. Grossbritannischen Gesellschaft der Wissenschaften zu Göttingen,

logarithmiſch - trigonometriſche

TAFELN

nebst

andern zum Gebrauch der Mathematik eingerichteten

Tafeln und Formeln.

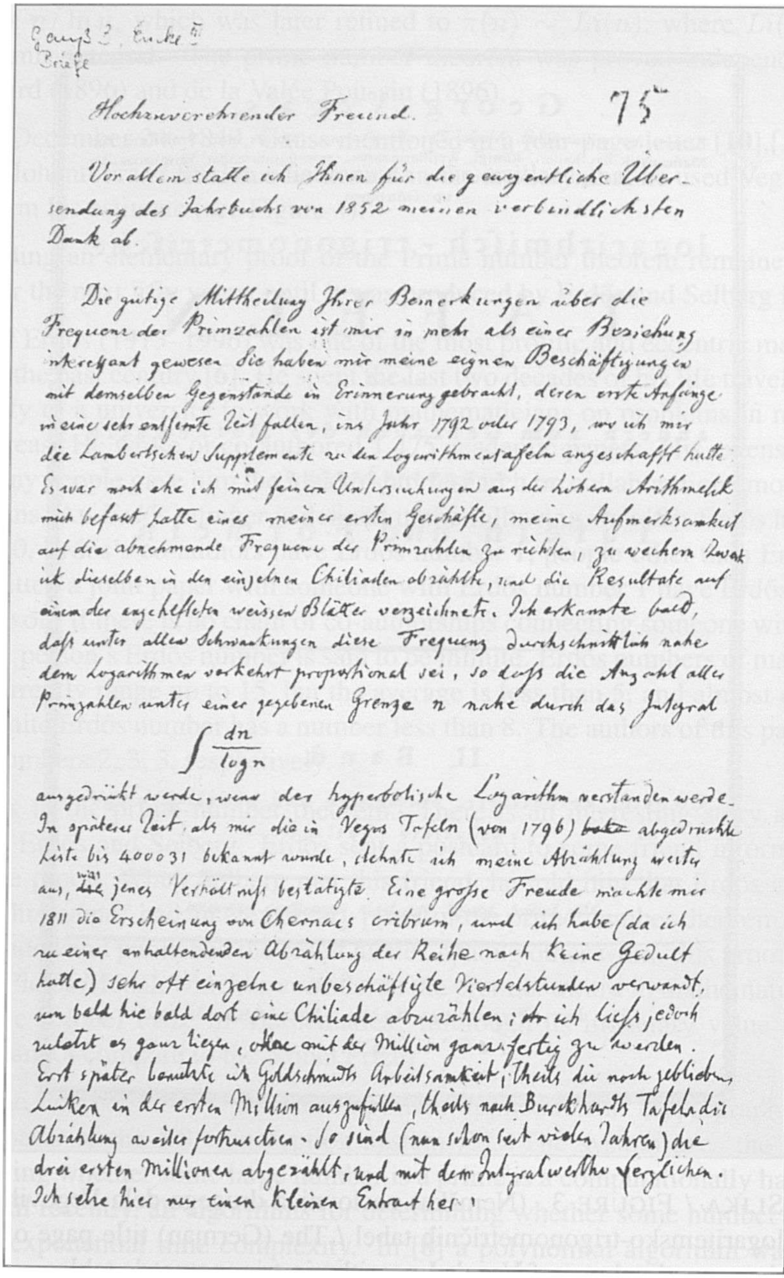
II. Band.

Zweyte, verbesserte, vermehrte und gänzlich umgearbeitete Auflage.

Mit kaiserl. königl. Privilegio impressorio privativo.

Leipzig,
in der Weidmannischen Buchhandlung,
1797.

SLIKA / FIGURE 3. (Nemška) naslovnica drugega dela Vegovih logaritemsko-trigonometričnih tabel / The (German) title page of the second volume of Vega's Logarithmic-trigonometric tables



Gauß 3, Encke III
Briefe

Hochzuverehrender Freund. 75

Vor allem statte ich Ihnen für die gewogentliche Übersendung des Jahrbuchs von 1852 meinen verbindlichsten Dank ab.

Die gütige Mittheilung Ihrer Bemerkungen über die Frequenz der Primzahlen ist mir in mehr als einer Beziehung interessant gewesen. Sie haben mir meine eignen Beschäftigungen mit demselben Gegenstande in Erinnerung gebracht, deren erste Anfänge in eine sehr entfernte Zeit fallen, ins Jahr 1792 oder 1793, wo ich mir die Lambertschen Supplemente zu den Logarithmentafeln angeschafft hatte. Es war noch ehe ich mit feinern Untersuchungen aus der höhern Arithmetik mich befaßt hatte eines meiner ersten Geschäfte, meine Aufmerksamkeit auf die abnehmende Frequenz der Primzahlen zu richten, zu welchem Zweck ich dieselben in den einzelnen Chiliaden abzählte, und die Resultate auf einem der angehefteten weissen Blätter verzeichnete. Ich erkannte bald, daß unter allen Schwankungen diese Frequenz durchschnittlich nahe dem Logarithmen verkehrt proportional sei, so daß die Anzahl aller Primzahlen unter einer gegebenen Grenze n nahe durch das Integral

$$\int \frac{dn}{\log n}$$

ausgedrückt werde, wenn der hyperbolische Logarithm verstanden werde. In späterer Zeit, als mir die in Vegas Tafeln (von 1796) ~~bata~~ abgedruckte Liste bis 400031 bekannt wurde, dehnte ich meine Abzählung weiter aus, ~~die~~ was jenes Verhältniß bestätigte. Eine große Freude machte mir 1811 die Erscheinung von Chernacs cribrum, und ich habe (da ich zu einer anhaltenden Abzählung der Reihe nach keine Geduld hatte) sehr oft einzelne unbeschäftigte Viertelstunden verwandt, um bald hie bald dort eine Chiliade abzuzählen; ich ließ jedoch zuletzt es ganz liegen, ohne mit der Million ganz fertig zu werden. Erst später benutzte ich Goldschmidts Arbeitsamkeit, theils die noch gebliebenen Lücken in der ersten Million auszufüllen, theils nach Burckhardts Tafeln die Abzählung weiter fortzusetzen. So sind (nun schon seit vielen Jahren) die drei ersten Millionen abgezählt, und mit dem Integralwerthe verglichen. Ich setze hier nur einen kleinen Extract her:

SLIKA / FIGURE 4. Gaussovo pismo svojemu študentu Johannu Franzu Enckeju, 1. stran / Gauss' letter to his student Johann Franz Encke, page 1

Unter	gibt es Primzahlen	Integral $\int \frac{dn}{\log n}$	Differ	Ihre Formel	Abweich.
500 000	41 556	41606,4	+50,4	41596,9	+40,9
1000 000	78 501	78627,5	+126,5	78672,7	+171,7
1500 000	114 112	114263,1	+151,1	114374,0	+264,0
2000 000	148883	149054,8	+171,8	149233,0	+350,0
2500 000	183016	183245,0	+229,0	183495,1	+479,1
3000 000	216745	216970,6	+225,6	217308,5	+563,6

Dass Legendre sich auch mit diesem Gegenstande beschäftigt hat, war mir nicht bekannt; auf Veranlassung Ihres Briefes habe ich in seiner Theorie des Nombres nachgesehen, und in der zweiten Ausgabe einige darauf bezügliche Seiten gefunden, die ich früher übersehen (oder seitdem vergessen) haben muss. Legendre gebraucht die Formel

$$\frac{n}{\log n - A}$$

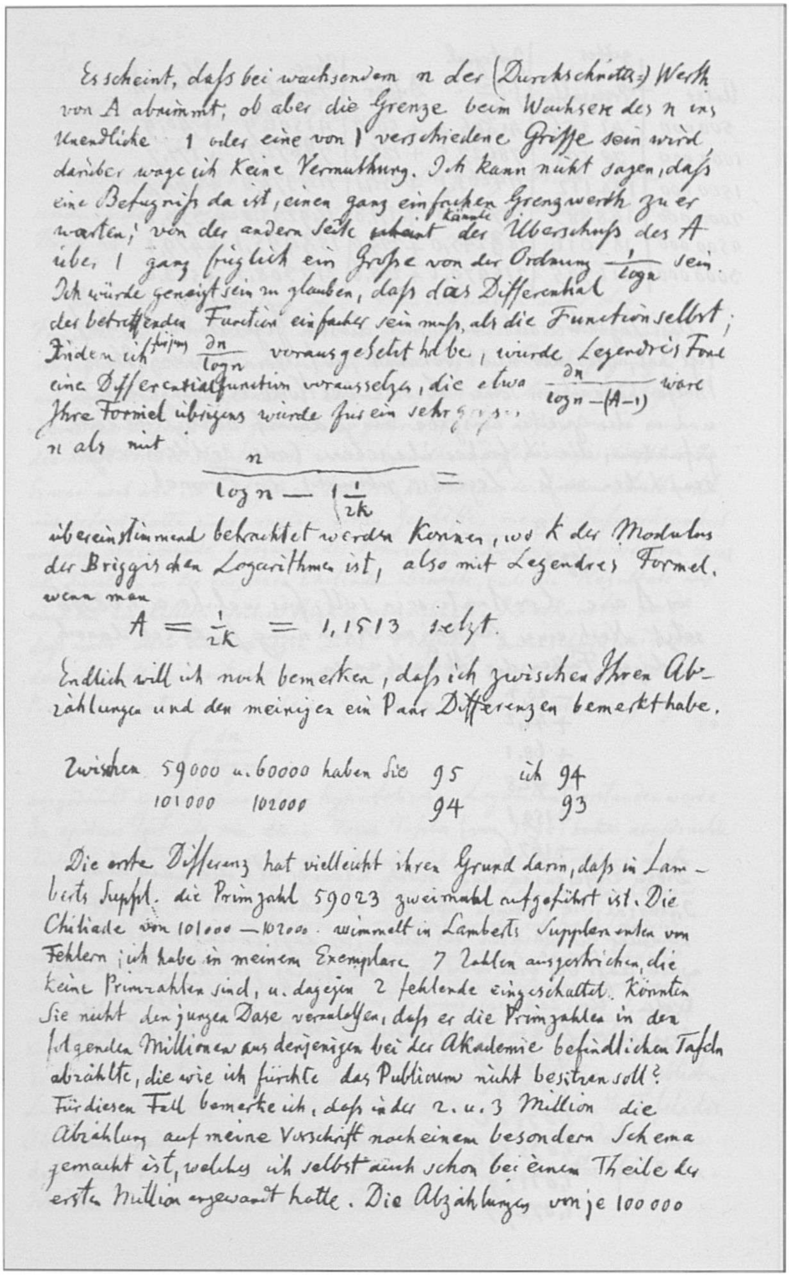
wo A eine Constante sein soll, für welche er 1,08366 setzt. Nach einer flüchtigen Rechnung finde ich danach in diesen Fällen die Abweichungen

−23,3
+42,2
+68,1
+92,8
+159,1
+167,6

Diese Differenzen sind noch kleiner als die mit dem Integral, sie scheinen aber bei zunehmendem n schneller zu wachsen als diese, so dass leicht möglich wäre, dass bei viel weiterer Fortsetzung jene die letztern überträfen. Um Zählung und Formel in Übereinstimmung zu bringen müsste man respective anstatt $A = 1,08366$ setzen

1,09040
1,07682
1,07582
1,07529
1,07179
1,07297

SLIKA / FIGURE 5. Gaussovo pismo svojemu študentu Johannu Franzu Enckeju, 2. stran / Gauss' letter to his student Johann Franz Encke, page 2



Es scheint, dass bei wachsendem n der (Durchschnitts-) Werth von A abnimmt; ob aber die Grenze beim Wachsen des n ins Unendliche 1 oder eine von 1 verschiedene Grösse sein wird, darüber wage ich keine Vermuthung. Ich kann nicht sagen, dass eine Befugniss da ist, einen ganz einfachen Grenzwerth zu erwarten; von der andern Seite ~~schaut~~ könnte der Überschuss des A über 1 ganz füglich eine Grösse von der Ordnung $\frac{1}{\log n}$ sein. Ich würde geneigt sein zu glauben, dass das Differential der betreffenden Function einfacher sein muss, als die Function selbst; Indem ich für jene $\frac{dn}{\log n}$ vorausgesetzt habe, würde Legendre's Formel eine Differentialfunction voraussetzen, die etwa $\frac{dn}{\log n - (A-1)}$ wäre. Ihre Formel übrigens würde für ein sehr gross n als mit

$$\frac{n}{\log n - \frac{1}{2k}} =$$

übereinstimmend betrachtet werden können, wo k der Modulus der Briggischen Logarithmen ist, also mit Legendre's Formel, wenn man

$$A = \frac{1}{2k} = 1,1513 \text{ setzt.}$$

Endlich will ich noch bemerken, dass ich zwischen Ihren Abzählungen und den meinigen ein Paar Differenzen bemerkt habe.

Zwischen	59000 u.	60000	haben Sie 95	ich	94
	101000	102000	94		93

Die erste Differenz hat vielleicht ihren Grund darin, dass in Lamberts Suppl. die Primzahl 59023 zweimahl aufgeführt ist. Die Chiliade von 101000 – 102000 wimmelt in Lamberts Supplementen von Fehlern; ich habe in meinem Exemplare 7 Zahlen ausgestrichen, die keine Primzahlen sind, u. dagegen 2 fehlende eingeschaltet. Könnten Sie nicht den jungen Dase veranlassen, dass er die Primzahlen in den folgenden Millionen aus denjenigen bei der Akademie befindlichen Tafeln abzählte, die wie ich fürchte das Publicum nicht besitzen soll? Für diesen Fall bemerke ich, dass in der 2. u. 3 Million die Abzählung auf meine Vorschrift nach einem besondern Schema gemacht ist, welches ich selbst auch schon bei einem Theile der ersten Million angewandt hatte. Die Abzählungen von je 100000

SLIKA / FIGURE 6. Gaussovo pismo svojemu študentu Johannu Franzu Enckeju, 3. stran / Gauss' letter to his student Johann Franz Encke, page 3

stehen auf einer (Klein) Octavseite in 10 Columnen, jede sich auf
eine Myriade beziehend; dazu kommt noch eine Columne
davor (links) und eine dahinter (rechts); ~~jene zeigten~~ als Beispiel
hier eine Verticalcolumne u. die beiden Zusatzcolumnen aus dem
Zehnmill 1000000 — 1100000

	0	1	2	....	9	
1	1					1
2						4
3						21
4	2					54
5	11					114
6	14					171
7	26					217
8	19					164
9	11					126
10	8					71
11	6					39
12	1					12
13	1					6
14						
15						
16						
	752					7210

Zur Erläuterung diene ich die ~~1te horizontal~~ Verticalreihe
In der Myriade 1000000 bis 1010000 sind 100 Hecatontaden; darunter ist 1 die nur eine Primzahl enthält; gar keine mit 2 oder 3; 2 Stück mit je 4 Primzahlen; 11 Stück mit je 5 u.s.w. alle zusammen geben 752. = 1.1 + 4.2 + 5.11 + 6.14 + u.s.w. Die letzte Columne ~~ist~~ enthält die Aggregate aus den 10 einzelnen. Die Zahlen 14.15.16 in der ersten Verticalreihe

stehen hier nur zum Überfluss, da keine Hecatontaden mit so vielen Primzahlen vorkommen; sie aber auf den folgenden Blättern bekommen sie Geltung. Zuletzt werden wieder die 10 Seiten in 1 vereinigt, u. umfassen so die ganze 2te Million.

Doch es ist Zeit abzubrechen. Ich sage noch meinen herzlichen Dank für Ihre Mittheilungen über die Färbungen der dortigen öffentl. Zustände. Noch sieht man keinen Ausweg aus dem Labyrinth, in das uns die Nachäfferei der Franzosen gezerrt hat. Unter herzlichen Wünschen für Ihr Wohlbefinden

Stets der Ihrige
C. F. Gauss

Göttingen 24 ~~Decb~~ December
1849

SLIKA / FIGURE 7. Gaussovo pismo svojemu študentu Johannu Franzu Enckeju, 4. stran / Gauss' letter to his student Johann Franz Encke, page 4

References

[1] C. F. Gauss, *Einige Bemerkungen zu Vega's Thesaurus Logarithmorum*, Astronomische Nachichten 756, 1851.

[2] The Prime Glossary, http://primes.utm.edu/glossary/page.php?sort=TablesOfPrimes.

[3] http://www.scs.uiuc.edu/~mainzv/exhibitmath/exhibit/felkel.htm.

[4] G. Vega, Logaritmisch – trigonometrische Tafeln, Leipzig, 1797.

[5] G. Vega, *Thesaurus logarithmorum completus*, Leipzig, Weidmann, 1794.

[6] P. Hoffman, *The Man Who Loved Only Numbers*, Hyperion, New York, 1998.

[7] A. J. Menzes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of Applied Crytograph*, CRC press, 1997.

[8] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, http://www.cse.iitk.ac.in/users/manindra/index.html.

[9] The Erdős Number Project, http://personalwebs.oakland.edu/~grossman/erdoshp.html.

[10] Y. Tschinkel, *About the cover: On the distribution of primes – Gauss' tables*, Bulletin (new series) of the AMS, Vol. 43, No. 1, 89–91, 2006.

[11] L. J. Goldstein, *A history of the prime number theorem*, Amr. Math. Monthly 80 (1973), 599–615.