Karel Rychlík
Anmerkungen

In: Bernard Bolzano (author); Karel Rychlík (other): Bernard Bolzano's Schriften. Band 2. Zahlentheorie. (German). Praha: Královská česká společnost nauk v Praze, 1931. pp. 1–7.

Persistent URL: http://dml.cz/dmlcz/400164

ANMERKUNGEN.

Bolzanos Zahlentheorie sollte ebenso wie die „Functionenlehre" einen Teil eines größeren Werkes über Mathematik bilden, das „Größenlehre" betitelt wurde. Das Manuskript eines Teiles dieser Größenlehre, das auch die Zahlentheorie enthält, befindet sich in der National- (früher Hof-) Bibliothek in Wien.

Nach Mitteilung des H. Jašek, der Bolzanos Handschriftlichen Nachlaß in der Wiener Nationalbibliothek durchgesehen und sich um die Sichtung dieses Nachlasses große Verdienste erworben hat, ist die Zahlentheorie in drei Bearbeitungen erhalten. Die erste Bearbeitung ist eigenhändig von Bolzano geschrieben, die zweite und dritte hat Bolzano durchgelesen und eigenhändig verbessert. Die vorliegende Ausgabe schließt sich an die vollkommenste, die dritte Bearbeitung an. Sie besteht aus 99 Blättern in 4°. Der Titel „Zahlentheorie" wurde vom Herausgeber gewählt. Bei Bolzano selbst führt sie als Teil der Größenlehre den Titel: „Zweiter Abschnitt: Verhältniß der Theilbarkeit unter den Zahlen." (In der ersten Bearbeitung: „Vierter Artikel: Von den Verhältnissen unter den Zahlen, welche auf den bisher betrachteten Rechnungsarten des Addirens, Subtrahirens, Multiplicirens und Dividirens beruhen.")

Wie die „Functionenlehre" wurde auch die Zahlentheorie von Bolzano in (mit dem Zeichen §. bezeichnete) Paragraphen eingeteilt; die Numerierung wurde vom Herausgeber durchgeführt. Die Zitate wurden von Bolzano durch ein beigefügtes Zeichen §. angedeutet. In den Fällen, wo sich dieses Zeichen auf die vorliegende Ausgabe bezieht, wurde die entsprechende Nummer ergänzt. In den anderen Fällen wurde das Zeichen §. ohne Nummer gelassen. Dem Verständnis wird dies hoffentlich nicht schaden.

§. 1.—9. *Teilbarkeit, gemeinsame Vielfache und gemeinsame Teiler. kleinstes gemeinsames Vielfache und größter gemeinsamer Teiler.*

§. 3. Unter einer wirklichen Zahl wird eine natürliche (ganze rationale positive) Zahl verstanden. Ein Produkt aus n natürlichen Zahlen, die >1, also $\geqq 2$ sind, ist $\geqq 2^n \geqq n$ (und $>n$ für $n>1$). Diese Ungleichung, die eine Folge der Ungleichung $(1+h)^n \geqq 1+nh$, h reell und >0, n rational ganz $\geqq 0$, ist, kann leicht durch vollständige Induktion bewiesen werden.

§. 7. Ist $\mathfrak{M}$ eine nach oben (nach unten) beschränkte Menge von ganzen rationalen Zahlen, d. h. gibt es eine reelle Zahl G, so daß alle Zahlen aus $\mathfrak{M} \leqq G$ ($\geqq G$) sind, so existiert in $\mathfrak{M}$ eine größte Zahl M (eine kleinste Zahl m), d. h. ist x irgendeine Zahl aus $\mathfrak{M}$, so ist $x \leqq M$ ($x \geqq m$). M und m existieren, falls $\mathfrak{M}$ endlich ist. Sind alle Zahlen aus $\mathfrak{M} \geqq 0$, so existiert m.

§. 10, 11. *Wann ist $a-b$ durch m teilbar?*

§. 10. Einer der bedeutendsten Fortschritte, die Gauß in seinen „Disquisitiones arithmeticae" gegenüber seinen Vorgängern erzielte, besteht in der Einführung des Begriffes der Kongruenz oder vielmehr in einer zweckmäßigen Bezeichnung für diesen Begriff. Bolzano benützt diese Bezeichnung nicht. Statt $a \equiv b \pmod{m}$ sagt er, daß a und b denselben „Rest" in bezug auf m liefern. Unter dem „Rest" von a in bezug auf m wird der kleinste, nicht negative Rest von a durch m verstanden. Hiedurch wird die etwas schwerfällige Formulierung vieler Sätze verursacht. (Vergl. §. 24, 86—102, 113—122).

§. 12. *Existenz des absolut kleinsten Restes.*

§. 12. Es wird die Existenz des absolut kleinsten Restes von a in bezug auf b bewiesen (a, b ganze positive Zahlen, a nicht durch b teilbar).

§. 13. *Euklidischer Algorithmus.*

§. 13. Das geschilderte Verfahren wird als Euklidischer Algorithmus (Euklid, Elemente 7, Satz 2) bezeichnet. (Siehe auch §. 49).

§. 14—15. *Zwei Lehrsätze.*

§. 14. Es wird bewiesen, daß $\left[\frac{a}{b}\right] \geqq n\left[\frac{a}{nb}\right]$ ist (a, b, n ganze positive Zahlen). Es gilt aber schärfer $\left[\frac{\left[\frac{a}{b}\right]}{n}\right] = \left[\frac{a}{nb}\right]$. Ist x eine beliebige reelle Zahl, n positiv ganz, so gilt die Gleichung $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$. (Landau, Primzahlen I., §. 17, S. 74.)

§. 16—26. *Lehrsätze über die Teilbarkeit der Summe und des Produktes ganzer Zahlen.*

§. 27—42. *Primzahlen und relative Primzahlen.*

§. 43—45. *Zerlegung einer ganzen Zahl in Primfaktoren.*

§. 46—47. *Die Menge der Primzahlen ist unendlich.*

§. 46. Der Satz und sein Beweis befindet sich schon in Euklids Elementen 9, Satz 20).

§. 48. *Alle Primzahlen außer 2 und 3 sind von der Form* $6n \pm 1$.

§. 49—54. *Folgerungen aus dem Euklidischen Algorithmus.*

§. 51. Ist d der größte gemeinsame Teiler der ganzen Zahlen a, b, so kann man zwei ganze Zahlen x, y derart bestimmen, daß $ax+by=d$ ist. Daraus folgt, daß jeder gemeinsame Teiler von a und b ein Teiler ihres größten gemeinsamen Teilers d ist.

Man kann leicht den allgemeineren Satz beweisen:

Ist d der größte gemeinsame Teiler der Zahlen $a, b, c, \ldots, l$, so kann man immer ganze Zahlen $x, y, z, \ldots, w$ bestimmen, so daß $ax+by+cz+\ldots$ $\ldots+lw=d$ gilt. Daraus folgt, daß jeder gemeinsame Teiler der Zahlen $a, b, c, \ldots, l$ auch Teiler ihres größten gemeinsamen Teilers d ist (§. 77).

§. 55—70. *Lehrsätze über relative Primzahlen.*

§. 62. Dieser Satz, der als Grundlage des Eindeutigkeitssatzes der Zerlegung in Primfaktoren (§. 71) dient, wird in Lejeune-Dirichlets Zahlentheorie auf folgende Weise bewiesen:

Da a und α relative Primzahlen sind, so kann man zwei ganze Zahlen m, n bestimmen, so daß $am+\alpha n=1$ ist (§. 53). Daraus folgt $b=abm+\alpha bn$. Da ab durch α teilbar ist, so sind beide Glieder der rechten Seite durch α teilbar. Es ist also auch b durch α teilbar.

§. 71—73. *Eindeutigkeit der Zerlegung in Primfaktoren.*

§. 74—79. *Sätze über den größten gemeinsamen Teiler.*

§. 80—83. *Sätze über das kleinste gemeinsame Vielfache.*

§. 84—85. *Das assoziative Gesetz für den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache.*

§. 84. Es wird das assoziative Gesetz für die Berechnung des größten gemeinsamen Teilers ausgesprochen.

§. 85. Desgleichen für das kleinste gemeinsame Vielfache.

§. 86—102. *Die zahlentheoretische Funktion* $\varphi(m)$.

§. 100. Die Anzahl der positiven Zahlen, die kleiner als eine gegebene Zahl m (>1) und zugleich teilerfremd zu m sind, wird mit $\varphi(m)$ bezeichnet (nach Gauß, Disquisitiones arithmeticae, art. 38). Es wird $\varphi(1)=1$ gesetzt. Man kann dann sagen, daß $\varphi(m)$ die Anzahl derjenigen positiven Zahlen bedeutet, welche teilerfremd zu m (m positiv ganz) und nicht größer als m sind.

Ist eine Zahl der Restklasse (mod m) teilerfremd zu m, so sind alle Zahlen dieser Restklasse zu m teilerfremd; die Restklasse wird dann als teilerfremd zu m bezeichnet. $\varphi(m)$ gibt also die Anzahl der zu m teilerfremden Restklassen an.

Die Anzahl $\varphi(m)$ wurde zuerst von Euler bestimmt (in Verbindung mit der Verallgemeinerung des Fermat'schen Satzes). (Euler: Eneströmsches Verzeichnis 271; Opera omnia (1) 2, S. 531—555).

Dirichlet (Zahlentheorie §. 11) gibt folgende Verallgemeinerung an:

Ist die ganze positive Zahl N durch die ganzen positiven Zahlen $a, b, \ldots, l$ teilbar, die paarweise teilerfremd sind, so ist

$$N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{l}\right)$$

die Anzahl der positiven Zahlen, die $<N$ und durch keine dieser Zahlen teilbar sind.

Zum Beweise dieses Satzes könnte man gelangen, indem man Bolzanos Gedankengang weiter verfolgt.

Der im §. 96 ausgesprochene Satz ist nämlich ein Spezialfall des Satzes von Dirichlet:

Sind $a, b, \ldots, l$ paarweise teilerfremde (positive) Zahlen, so ist die Anzahl der ganzen positiven Zahlen, die durch keine dieser Zahlen teilbar und $<ab\ldots l$ sind,

$$(a-1)(b-1)\ldots(l-1).$$

Auf dieselbe Weise, wie der Satz aus §. 99 abgeleitet wird, könnte man allgemeiner beweisen:

Sind $a, b, \ldots, l$ ganze positive Zahlen, die paarweise teilerfremd sind, und ist n eine ganze positive Zahl, so ist die Anzahl der ganzen positiven Zahlen, die durch keine dieser Zahlen teilbar und $<n\,.\,ab\ldots l$ sind,

$$n(a-1)(b-1)\ldots(l-1).$$

Setzt man jetzt $N=nab\ldots l$, so ist

$$n(a-1)(b-1)\ldots(l-1)=N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{l}\right).$$

Wie leicht ersichtlich, ist dieser Satz mit dem angeführten Satze von Dirichlet identisch.

§. 103—105. *Anzahl und Summe der Teiler einer ganzen Zahl.*

§. 106—111. *Zur Zerlegung einer ganzen Zahl in Primfaktoren.*

§. 109. Es soll eine Menge von ganzen rationalen Zahlen bestimmt werden, deren kleinstes gemeinsames Vielfache eine gegebene Zahl ist.

§. 111. Kennen wir den größten gemeinsamen Teiler m der Zahlen a, b, so ist das kleinste gemeinsame Vielfache dieser Zahlen $\frac{ab}{m} = \frac{a}{m} \cdot \frac{b}{m} \cdot m$. Bolzano verallgemeinert unrichtig diese Formel für den Fall von mehreren Zahlen. Das kleinste gemeinsame Vielfache der Zahlen 12, 24, 30, 42 ist 840.

§. 113—115. *Jede ganze positive Zahl kann als Summe von höchstens vier Quadratzahlen dargestellt werden.*

Dieser Satz war vielleicht schon Diophantos bekannt, Bachet de Méziriac spricht ihn als erster klar aus. (Vergl. dazu Dickson, History of the theory of numbers, II S. 275—6).

Fermat erwähnt diesen Satz in mehreren Briefen. (Vergl. Oeuvres Bd. 2 S. 403 und 433, Bd. 3 S. 314.) Der erste veröffentlichte Beweis dieses Satzes stammt von Lagrange (Démonstration d'un théorème d'arithmétique, Nouv. mém. de l'Ac. royale d. Sc. et B.-L. de Berlin (1770), 1772, S. 123).

§. 113. Bolzano versucht den Hilfssatz von Lagrange in der Richtung zu verallgemeinern, daß er für c zusammengesetzte Zahlen zulässt. Aber dann ist der Satz unrichtig:

Es ist $x^2+y^2+1 \equiv 1, 2, 3 \pmod 4$, aber nie $\equiv 0 \pmod 4$.

Die richtige Fassung des Satzes lautet:

Sind a, b zwei ganze Zahlen und a durch die ungerade Primzahl $p\ (>0)$ nicht teilbar, so kann man zwei ganze Zahlen x, y bestimmen derart, daß $0 \leqq x < \frac{p}{2}$, $0 \leqq y < \frac{p}{2}$ und $x^2 - ay^2 - b \equiv 0 \pmod p$ gilt.

Bolzanos Beweis kann leicht richtig gestellt werden.

Betrachten wir das System A der Zahlen x^2 für $x = 0, 1, 2, \ldots, \frac{p-1}{2}$ und das System B der Zahlen ay^2+b für $y = 0, 1, 2, \ldots, \frac{p-1}{2}$. Weder irgend zwei Zahlen aus dem System A noch irgend zwei Zahlen aus B sind kongruent $(\mathrm{mod}\ p)$. Die Anzahl der Zahlen des Systems A und ebenso des Systems B beträgt $\frac{p+1}{2}$. Es muß wenigstens eine Zahl aus dem System A mit einer Zahl aus B kongruent sein $(\mathrm{mod}\ p)$, da es sonst $p+1$ inkongruente Zahlen $(\mathrm{mod}\ p)$ gäbe. Daraus folgt unmittelbar die Behauptung.

Der angeführte Beweis befindet sich in der Abh. von Daudlebsky v. Sterneck: Über die Darstellung der Zahlen als Summe von vier Quadraten, Monatshefte 15, 1904, S. 235—238.

Daublebsky v. Sterneck berichtet darin, daß er gelegentlich einer Durchsicht des handschriftlichen Nachlasses von Bolzano eine Notiz fand, die sich auf die Darstellbarkeit der Zahlen als Summe von vier Quadraten bezieht. Vergl. auch Bachmann, Niedere Zahlentheorie II, S. 323.

§. 114. Es genügt zu beweisen, daß eine ungerade Primzahl p (>0) als Summe von höchstens vier Quadratzahlen dargestellt werden kann. Für $p=2$ ist nämlich $2=1^2+1^2$.

Man kann zuerst den Satz aussprechen:

a) Es existieren vier ganze Zahlen x, y, w, z (nicht $=0$) und eine ganze Zahl p_1 derart, daß

$$pp_1 = x^2+y^2+w^2+z^2$$

und

$$1 \leqq p_1 < p \text{ ist.}$$

Es genügt, den Hilfssatz des vorigen Paragraphen auf x^2+y^2+1 anzuwenden. Man kann x, y so bestimmen, daß $0 \leqq x < \frac{p}{2}$, $0 \leqq y < \frac{p}{2}$ und $x^2+y^2+1 \equiv 0 \pmod p$ gilt. Setzen wir $w=1$, $z=0$, so ist $x^2+y^2+w^2+z^2 = pp_1$. Aus $0 \leqq x < \frac{p}{2}$, $0 \leqq y < \frac{p}{2}$, $w=1$, $z=0$ folgt $x^2+y^2+w^2+z^2 < 2\frac{p^2}{4}+1 = \frac{p^2}{2}+1 < p^2$, also $pp_1 < p^2$, $p_1 < p$. Dabei ist sicher $p_1 \neq 1$.

Weiter gilt der Satz:

b) Aus $pp_1 = x^2+y^2+w^2+z^2$ (x, y, w, z ganz und nicht $=0$, p_1 ganz und $1 < p_1 < p$) folgt $pp_2 = x_2^2+y_2^2+w_2^2+z_2^2$ (x_2, y_2, w_2, z_2 ganz und nicht $=0$, p_2 ganz und $1 \leqq p_2 < p_1$).

Bei ungeradem p_1 ist Bolzano's Beweis richtig. Dann ist nämlich jede ganze Zahl kongruent (mod p_1) einer ganzen Zahl r aus der Reihe

$$-\frac{p_1-1}{2}, -\frac{p_1-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p_1-3}{2}, \frac{p_1-1}{2}.$$

Für r gilt also $|r| < \frac{p_1}{2}$. Es ist also $x \equiv x_1$, $y \equiv y_1$, $w \equiv w_1$, $z \equiv z_1 \pmod{p_1}$

$$x_1 < \frac{p_1}{2}, \quad y_1 < \frac{p_1}{2}, \quad w_1 < \frac{p_1}{2}, \quad z_1 < \frac{p_1}{2}.$$

Man setze

$$x_1 = x - \alpha p_1, \quad y_1 = y - \beta p_1, \quad w_1 = w - \gamma p_1, \quad z_1 = z - \delta p_1.$$

Da

$$x^2+y^2+w^2+z^2 \equiv 0 \pmod{p_1},$$

so ist auch

$$x_1^2+y_1^2+w_1^2+z_1^2 \equiv 0 \pmod{p_1},$$

also

$$x_1^2+y_1^2+w_1^2+z_1^2 = p_1p_2.$$

Es ist zunächst $p_2 \neq 0$. Denn sonst müsste $x_1=y_2=w_1=z_1=0$, also $x \equiv y \equiv w \equiv z \equiv 0 \pmod{p_1}$ gelten. Weiter wäre $x^2+y^2+w^2+z^2 \equiv 0 \pmod{p_1^2}$, d. h. $pp_1 \equiv 0 \pmod{p_1^2}$ und $p \equiv 0 \pmod{p_1}$ entgegen der Voraussetzung, daß p eine Primzahl ist.

Aus

$$x_1 < \frac{p_1}{2}, \quad y_1 < \frac{p_1}{2}, \quad w_1 < \frac{p_1}{2}, \quad z_1 < \frac{p_1}{2}$$

folgt

$$x_1^2+y_1^2+w_1^2+z_1^2 < 4\frac{p_1^2}{4} = p_1^2,$$

d. h.

$$p_1p_2 < p_1^2,$$

also

$$1 \leqq p_2 < p_1.$$

Auf

$$(x^2+y^2+w^2+z^2)(x_1^2+y_1^2+w_1^2+z_1^2)=pp_1^2p_2$$

wenden wir die Eulersche Identität an.*)

Wir erhalten dann nach kurzer Zwischenrechnung, die leicht der Bolzano's Darstellung zu entnehmen ist:

$$\begin{aligned} pp_2 &= x_2^2+y_2^2+w_2^2+z_2^2,\\ x_2 &= p-\alpha x-\beta y-\gamma w-\delta z,\\ y_2 &= \alpha y-\beta x+\gamma z-\delta w,\\ w_2 &= \alpha w-\beta z-\gamma x+\delta y,\\ z_2 &= \alpha z+\beta w-\gamma y-\delta x. \end{aligned}$$

Für gerades p_1 ist $x+y+w+z\equiv 0 \pmod 2$. Man kann dann voraussetzen, daß $x+y\equiv 0,\ w+z\equiv 0 \pmod 2$ ist.

(Sind x, y, w, z sämtlich gerade oder sämtlich ungerade, so gilt dies ohne weiteres, sind zwei gerade und zwei ungerade, so muß man allenfalls erst eine geeignete Vertauschung vornehmen.)

Dann ist

$$p\,p_1=\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+\left(\frac{w+z}{2}\right)^2+\left(\frac{w-z}{2}\right)^2,$$

d. h.

$$pp_2=x_2^2+y_2^2+w_2^2+z_2^2,$$

wo x_2, y_2, w_2, z_2 ganz sind und $p_2=\frac{p_1}{2}$, also $1\leqq p_2<p_1$ gilt.

Die beste moderne Darstellung des Bolzanoschen Beweises findet man bei Landau, Vorlesungen, Bd 1, S. 107—109. Dieser Darstellung habe ich die ergänzenden Bemerkungen entnommen.

§. 116—118. *Satz von Fermat.*

Für jede durch p (p eine Primzahl >0) nicht teilbare ganze Zahl a ist

$$a^{p-1}\equiv 1 \pmod p.$$

Für jede beliebige ganze Zahl a daher

$$a^p\equiv a \pmod p.$$

Dieser Satz wird nach seinem Entdecker der Fermatsche Satz genannt. Fermat hat ihn ohne Beweis am 18. Okt. 1640 brieflich an Frenicle de Bessy mitgeteilt; veröffentlicht wurde dieser Brief erst in den Varia opera mathematica von Fermat, Tolosae 1679, S. 162—164. (Vergl. Oeuvres de Fermat 2 S. 206—212.)*)

Der erste veröffentlichte Beweis rührt von Euler her (Enestr. Verz. 54, Op. omn. (1) 2, S. 33—37).

Der Binomialkoeffizient $\binom{p}{k}$, $1\leqq k\leqq p-1$, ist nämlich durch p teilbar. Aus dem binomischen Lehrsatze folgt $(a+1)^p\equiv 1+a^p \pmod p$. Aus $a^p\equiv a \pmod p$ ergibt sich weiter $(a+1)^p\equiv a+1 \pmod p$. Da $1^p\equiv 1 \pmod p$ richtig ist, folgt durch vollständige Induktion allgemein $a^p\equiv a \pmod p$.

*) Siehe S. 31 Z. 18. Vergl. Euler, Enestr. Verz. 42, Op. omn. (1) 2, S. 369.

*) Über die Entdeckung und den Beweis des Satzes von Fermat und Wilson in den Manuskripten von Leibniz s. Dickson, History of the Theory of numbers I, S. 59

Der Satz aus §. 116

$$a^{\varphi(b)} \equiv 1 \pmod{b} \quad (a \text{ teilerfremd zu } b)$$

und der hier mitgeteilte Beweis stammt von Euler (Enestr. Verz. 262. Op. omn. (1), S. 493—518).

§. 119—122. *Satz von Wilson.*

Der Satz, daß

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

ist, wenn p eine Primzahl (> 0) bedeutet, wurde ohne Beweis von Waring, Meditationes algebraicae (Cantabrigiae 1770, S. 208; III. Aufl., Cantabrigiae 1782, S. 380), veröffentlicht, der die Entdeckung Wilson zuschreibt.

Den ersten Beweis veröffentlichte Lagrange (Nouv. Mém. de l'ac. r. d. sc. et b.-l. Berlin (1771), 1773, S. 125—137, Oeuvres 3, 1869, S. 425—438).

Lagrange benützt zum Beweise die identische Kongruenz

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-p+1) \pmod{p},$$

aus der für $x = 0$ der Satz von Wilson unmittelbar folgt.

Der hier mitgeteilte Beweis stammt von Gauß, Disqu. aritm. art. 77, wo in Art. 78 eine Verallgemeinerung für zusammengesetzte Moduln angegeben wird. Ist x eine Zahl aus der Reihe $1, 2, 3, \ldots, p-1$, so existiert eine und nur eine Zahl y in dieser Reihe von der Eigenschaft, daß $xy \equiv 1 \pmod{p}$ gilt (Numerus socius nach Gauß, Disqu. arithm. art. 77). 1 und $p-1$ sind „socii" ihrer selbst. Es gibt auch keine weiteren Zahlen dieser Art, da für sie $x^2 \equiv 1 \pmod{p}$ gelten müsste. Daraus folgt:

Die Zahlen

$$2, 3, \ldots, p-2$$

zerfallen in $\frac{1}{2}(p-3)$ Zahlenpaare

$$x_1, y_1;\ x_2, y_2;\ \ldots\ x_{\frac{1}{2}(p-3)},\ y_{\frac{1}{2}(p-3)},$$

für die

$$x_1 y_1 \equiv 1,\ x_2 y_2 \equiv 1, \ldots, x_{\frac{1}{2}(p-3)} y_{\frac{1}{2}(p-3)} \equiv 1 \pmod{p}$$

gilt. Die Zahlen

$$x_1, y_1, x_2, y_2, \ldots, x_{\frac{1}{2}(p-3)}, y_{\frac{1}{2}(p-3)}$$

sind also bis auf die Reihenfolge gleich den Zahlen $2, 3, \ldots, p-2$. Es ist also

$$x_1 y_1 x_2 y_2 \ldots x_{\frac{1}{2}(p-3)} y_{\frac{1}{2}(p-3)} \equiv 1 \pmod{p},$$

d. h.

$$2 \cdot 3 \ldots (p-2) \equiv 1 \pmod{p}.$$

Multipliziert man mit $p-1 \equiv -1 \pmod{p}$, so erhält man

$$(p-1)! \equiv -1 \pmod{p}.$$

Der Satz über „numeri socii" befindet sich ohne Beweis in der Abhandlung von Franz von Schaffgotsch (Abhandlung über einige Eigenschaften der Prim- und zusammengesetzten Zahlen, Abh. d. Böhmischen Gesell. d. Wiss. in Prag, 1786, S. 123—129). Daselbst wird mit Hilfe dieses Satzes auch der Satz von Wilson bewiesen.