Die Chronologie in ihrem ganzem Umfange, mit vorzüglicher Rücksicht auf ihre Unwendung in der Astronomie, Weltgeschichte und Urkundenlehre

Vorbegriffe [zur Chronologie I. - XXII.]. Allgemeine Säze der Höheren Arithmetik, welche in der Chronologie vielfache Anwendung finden

In: Wilhelm Matzka (author): Die Chronologie in ihrem ganzem Umfange, mit vorzüglicher Rücksicht auf ihre Unwendung in der Astronomie, Weltgeschichte und Urkundenlehre. (German). Wien: Fr. Beck'schen Universitätsbuchhandlung, 1844. pp. [1]--62.

Persistent URL: http://dml.cz/dmlcz/400373

Vorbegriffe

zur

Chronologie.

Vorbegriffe.

Allgemeine Säze der höheren Arithmetik, welche in der Chronologie vielfache Anwendung finden.

I.

Annahmen.

In der vorliegenden arithmetiſchen Darſtellung der Chronologie werden häufig Lehren der höheren Arithmetik oder der vorzugsweiſe ſo genannten »Theorie der Zahlen« angewendet, deren die Lehrbücher der Algebra nicht gedenken; deswegen ſollen ſie hier in Kürze zuſammengeſtellt und begründet werden.

Die in dieſer Zuſammenſtellung zu betrachtenden allgemeinen, durch Buchſtaben vorgeſtellten, Zahlen werden ohne Ausnahme ganze Zahlen, mit Einſchluß der Nulle, oder blos Anzahlen andeuten, daher ihr Beiname »ganze« entbehrlich iſt. Dabei können ſie entweder abſolute, oder algebraiſch relative, und im lezteren Falle entweder poſitive oder negative Zahlen ſein.

Sehr oft wird eine allgemeine Zahl a nur gewiſſe beſondere Zahlen, von einer beſtimmten kleinſten α an ununterbrochen bis zu einer angegebenen größten β vorſtellen dürfen; dann gibt man dieſe Einſchränkung gewöhnlich durch folgenden Anſaz

$$a = \alpha, \alpha+1, \alpha+2, \ldots . \beta,$$

oder zuweilen in umgekehrter Ordnung

$$a = \beta, \beta-1, \beta-2, \ldots . \alpha$$

zu erkennen. Für algebraiſch größer als eine andere gilt hiebei eine Zahl, wenn jene, von dieſer abgezogen, einen poſitiven Reſt gibt.

Manchmal müſſen jedoch alle zuläſſigen Werthe der allgemeinen Zahl, durch Beiſtriche getrennt, nach einander hingeſtellt werden; insbeſondere dann immer, wenn ſie nicht in der natürlichen Folge der Zahlen fortlaufen.

So z. B. zeigt $a = 0, 1, 2, \ldots . 18$ an, daß a je eine der Zahlen von 0 bis 18 vorſtellt, und $a = 2, 5, 1, 4$, daß a der Reihe nach den Zahlen 2, 5, 1, 4 gleich werde.

II.

Congruenz der Zahlen.

Ist der Unterschied zweier Zahlen, a und α, durch eine dritte Zahl, m, theilbar; so nennt man jene zwei Zahlen einander congruent nach dieser dritten, m, diese selbst den Modul der Congruenz, und schreibt nach Gauß, der diesen folgereichen Begriff und das Zeichen der Congruenz, (≡), in die Zahlenlehre einführte, $a \equiv \alpha$, mod m.

In einer Congruenz kommt demnach blos bei den zwei congruenten Zahlen, nicht aber bei ihrem Unterschiede und Modul, zu beachten, ob sie positiv oder negativ seien. Im Verlaufe der vorliegenden Abhandlung wird der Modul sogar immer absolut genommen werden.

So ist z. B. $17 \equiv 3$, mod 7, weil $17 - 3 = 14 = 7.2$,

$8 \equiv -14$, mod 11, weil $8-(-14) = 22 = 11.2$.

Ist eine Zahl insbesondere der Null congruent, so heißt dies eigentlich, sie selbst ist durch den Modul theilbar; z. B. $96 \equiv 0$, mod 4 sagt, 96 ist durch 4 theilbar. Mithin läßt sich die Theilbarkeit einer Zahl durch eine andere mittels des Congruenzzeichens andeuten.

III.

Lehrsäze über die Congruenz der Zahlen.

1. Gleiche Zahlen sind nach jedem Modul congruent, weil ihr Unterschied Null, daher durch jede Zahl theilbar ist.

Die Gleichheit zweier Zahlen kann demnach als ein besonderer Fall ihrer Congruenz nach beliebigem Modul angesehen werden.

2. Sind zwei Zahlen einer dritten nach einerlei Modul congruent, so sind sie auch unter sich congruent. Ist nemlich $a \equiv c$, mod m und $b \equiv c$, mod m; so ist auch $a \equiv b$, mod m.

Denn nach der Annahme sind die Unterschiede a—c und c—b durch den Modul m theilbar, daher auch ihre Summe a—c + c—b, die sich auf den Unterschied a—b zusammenzieht.

3. Von zwei congruenten Zahlen wird jede erhalten, wenn man die andere um ein Vielfaches des Moduls entweder vermehrt oder vermindert. Wenn nemlich $a \equiv b$, mod m ist, läßt sich $a = b \pm h\,m$ sezen und darin h beliebig groß annehmen.

Denn von den congruenten Zahlen a und b muß der Unterschied a — b ein positives oder negatives Vielfaches, allgemein das h fache, des Moduls m, nemlich $a - b = \pm h\,m$ sein; mithin ist $a = b \pm h\,m$.

4. Die Congruenz $a \equiv b$, mod m drückt daher, in so fern aus ihr $a = b \pm h\,m$ folgt, auch aus, daß die Zahl a jedes Glied derjenigen nach beiden

Richtungen in's Unendliche auslaufenden arithmetischen Progression vorstelle, deren ein Glied b und beständiger Unterschied der Modul m ist.

5. Addirt man, bei einerlei Modul, congruente Zahlen zu congruenten, so sind die Summen congruent; und

6. Zieht man congruente Zahlen von congruenten ab, so sind die Unterschiede congruent.

Ist nemlich $a \equiv \alpha$, mod m und $b \equiv \beta$, mod m, so ist eben sowohl $a+b \equiv \alpha+\beta$, mod m als $a-b \equiv \alpha-\beta$, mod m.

Denn nach den Annahmen sind die Unterschiede $a-\alpha$ und $b-\beta$ durch den Modul m theilbar, sonach auch ihre Summe $a-\alpha+b-\beta$ sowohl, als ihr Unterschied $a-\alpha-b+\beta$, oder dort der Unterschied $a+b-(\alpha+\beta)$ und hier $a-b-(\alpha-\beta)$.

7. Da sämmtliche Vielfachen des Moduls der Null und unter sich congruent sind, so bleibt es immer gestattet, jeder aus zwei congruenten Zahlen was immer für Vielfachen ihres Moduls zuzugeben oder zu entziehen, indem man diese Vielfachen gleichsam als Nullen ansieht. Man benüzt dieses Verfahren vorzüglich dann, wenn die congruenten Zahlen zusammengesezte Ausdrücke sind; um sowohl die einzelnen Glieder derselben, als auch sie selbst auf die möglich einfachste Gestalt zurück zu führen.

So ist z. B. $3+76-5 \equiv 15+4-22$, mod 7,

also auch $3+76-70-5 \equiv 15-14+4-22+21$, mod 7,

oder $3+6-5 \equiv 1+4-1$, mod 7.

8. Multiplicirt man, bei einerlei Modul, congruente Zahlen mit congruenten — oder insbesondere mit gleichen — Zahlen, so sind auch die Producte congruent. Ist $a \equiv \alpha$, mod m und $b \equiv \beta$, mod m, so ist auch $ab \equiv \alpha\beta$, mod m.

Denn vermöge der Voraussezung sind die Unterschiede $a-\alpha$ und $b-\beta$ durch den Modul m theilbar, daher auch, wenn man den ersteren Unterschied mit b, und den anderen mit α multiplicirt, die Producte $ab-\alpha b$ und $\alpha b-\alpha\beta$; folglich ist auch ihre Summe $ab-\alpha b+\alpha b-\alpha\beta$, d. h. der Unterschied $ab-\alpha\beta$, durch m theilbar.

9. Erhebt man congruente Zahlen zu einerlei Potenz nach einem ganzen absoluten Exponenten, so sind auch die Potenzen nach demselben Modul congruent. Ist $a \equiv \alpha$, mod m, so ist auch $a^n \equiv \alpha^n$, mod m.

Denn solche Potenzen sind Producte gleich vieler, durchgängig gleicher Factoren, daher (nach 8) congruent.

10. Sind zwei congruente Zahlen, a und b, durch zwei andere, nach demſelben Modul, m, congruente Zahlen, α und β, von denen jede gegen den Modul relativ prim iſt, einzeln theilbar; ſo ſind auch ihre Quotienten, a: α und b: β, nach eben dieſem Modul congruent.

Denn ſei $a \equiv b$, mod m und $\alpha \equiv \beta$, mod m, ferner $a:\alpha = a'$ und $b:\beta = b'$, folglich $a = a'\alpha$ und $b = b'\beta$. Dann ſind durch den Modul m theilbar die Unterſchiede a—b und $\alpha-\beta$, alſo auch $a'\alpha - b'\beta$ und ſowohl $a'(\alpha-\beta) = a'\alpha - a'\beta$, als $b'(\alpha-\beta) = b'\alpha - b'\beta$; folglich wenn man von jenem dieſe beiden abzieht, die Unterſchiede $a'\beta - b'\beta$ und $a'\alpha - b'\alpha$, oder die ihnen gleichen Producte $(a'-b')\beta$ und $(a'-b')\alpha$. Hat aber, nach der Annahme, in dieſen Producten weder α noch β mit dem Modul m einen Theiler gemeinſchaftlich, ſo können die Producte nur dazumal durch m theilbar ſein, wenn ihr anderer Factor $a' - b'$ durch m theilbar, alſo $a' \equiv b'$, mod m, oder $a:\alpha \equiv b:\beta$, mod m iſt.

11. Hat eine aus zwei congruenten Zahlen mit dem Modul einen Theiler gemeinſchaftlich, ſo muß dieſer auch der anderen Zahl zukommen.

Denn ſei $a \equiv b$, mod m, und t ein gemeinſchaftlicher Theiler von b und m. Da die andere Zahl $a = b + (a-b)$, und ſowohl die Zahl b als auch der Modul m, daher auch der durch dieſen Modul theilbare Unterſchied a—b durch t theilbar iſt; ſo muß die Summe $b+(a-b)$, oder die Zahl a, gleichfalls durch den gemeinſchaftlichen Theiler t theilbar ſein.

12. Eine Congruenz bleibt beſtehen, wenn man die congruenten Zahlen und den Modul durch einerlei Zahl multiplicirt oder durch einen gemeinſchaftlichen Theiler theilt. Iſt nemlich $a \equiv \alpha$, mod m, ſo iſt auch $ap \equiv \alpha p$, mod mp und wofern a, α, m durch p theilbar ſind, auch $a:p \equiv \alpha:p$, mod $(m:p)$. Z. B. Weil $21 \equiv 9$, mod 12, iſt auch $42 \equiv 18$, mod 24 und $7 \equiv 3$, mod 4.

Denn nach der Vorausſezung iſt der Quotient $(a-\alpha):m$ eine ganze Zahl, daher auch, wenn man Dividend und Theiler desſelben mit einerlei Zahl p multiplicirt oder durch den gemeinſchaftlichen Theiler p dividirt, jeder der ihm gleichen Quotienten $(ap-\alpha p):mp$ und $\left(\frac{a}{p} - \frac{\alpha}{p}\right) : \frac{m}{p}$.

13. Sind zwei Zahlen nach einem Modul congruent, ſo ſind ſie auch nach jedem Modul congruent, der ein Theiler jenes Moduls iſt. Wenn nemlich $a \equiv b$, mod m, und μ ein Theiler von m iſt, ſo muß auch $a \equiv b$, mod μ ſein.

Denn der Annahme zu Folge iſt der Unterſchied a—b durch die Zahl m theilbar, daher auch durch jeden ihrer Theiler μ.

14. Zwei Zahlen, welche nach mehreren Moduln congruent sind, müssen auch nach dem kleinsten gemeinschaftlichen Vielfachen dieser Moduln congruent sein. Ist nemlich $a \equiv b$, mod (m, m′, m″, . . .) und μ die kleinste durch m, m′, m″, . . . theilbare Zahl, so ist auch $a \equiv b$, mod μ.

Denn da der Unterschied a—b durch die Zahlen m, m′, m″, . . . einzeln theilbar ist, so muß er auch durch ihr kleinstes gemeinschaftliches Vielfaches μ theilbar sein.

IV.

Betrachtungen über das Theilen der Zahlen.

Bei dem Theilen einer Zahl — Dividend — durch eine andere — Theiler oder Divisor — verlangt man eigentlich diejenige, ganze oder gebrochene, Zahl — Quotient —, welche, mit der lezteren, dem Theiler, multiplicirt, die erstere, den Dividend, zum Producte liefert. Sehr oft, und in den Rechnungen der Zeitkunde fast immer, wo man mit lauter ganzen Zahlen rechnet, fordert man, bei dem Theilen eines Dividends durch einen Theiler, diejenige ganze Zahl — zur Unterscheidung zu nennen der **Quotus** — welche, mit dem Theiler multiplicirt, ein Product gibt, das sich von dem Dividend um eine positive oder negative Zahl — Rest — unterscheidet, die absolut genommen kleiner, oder höchstens ausnahmsweise so groß, als der absolut genommene Theiler ist.

Soll nemlich d durch t getheilt zum Quotus d′ und zum Reste d″ geben, so muß der Rest

$$(1) \qquad d - t\,d' = d'' \leqq t$$

sein, wofern man von den Zeichen des Theilers und Restes absieht. Daraus folgt der bekannte Saz

$$(2) \qquad d = t\,d' + d'',$$

d. h. Man erhält den Dividend, wenn man zum Producte aus Theiler und Quotus den Rest addirt.

Dieselbe Form (2) werden wir auch benüzen, um kurz anzudeuten, daß eine Zahl d, durch eine andere t getheilt, d′ zum Quotus und d″ zum Reste gebe.

Fordert man, daß der Rest, dem Zahlwerthe nach, so klein als möglich, mithin höchstens so groß als der halbe Theiler genommen werde; dann heißt er der kleinste (mögliche) Rest, und ist bald positiv, bald negativ.

Bemerkt mag hier noch werden, daß wir im Folgenden nie veranlaßt sein werden, andere als absolute Theiler in Rechnung zu bringen.

V.

Bezeichnung der Quoti und positiven Reste.

Gewöhnlich wird verlangt, daß bei der Theilung einer Zahl d durch eine andere t der Rest d'' nur positiv genommen werde.

1. Soll der Rest d'' dabei auch noch stets kleiner als der Theiler t, also der kleinste positive Rest sein: so bezeichnet man den Quotus gewöhnlich durch $\mathfrak{q}\frac{d}{t}$ oder zuweilen durch $d:t$,

lesend: »Quotus von d (getheilt) durch t",
oder: »Quotus der Theilung von d durch t";

und den Rest gewöhnlich durch $\mathfrak{r}\frac{d}{t}$ oder zuweilen durch $d:t$,

lesend: »Rest von d (getheilt) durch t",
oder: »Rest der Theilung von d durch t".

Dann ist im Vergleich mit der obigen Bezeichnung in IV

$$d' = \mathfrak{q}\frac{d}{t} = d:t,$$

$$d'' = \mathfrak{r}\frac{d}{t} = d:t = 0, 1, 2, \ldots .t-1$$

und nach den Gleichungen (1) und (2)

$$(3) \qquad d - t\,\mathfrak{q}\frac{d}{t} = \mathfrak{r}\frac{d}{t} = 0, 1, 2, \ldots . t-1,$$

$$(4) \qquad d = t\,\mathfrak{q}\frac{d}{t} + \mathfrak{r}\frac{d}{t}.$$

Z. B. So ist $23 = 7.3 + 2$, d. h. 23 durch 7 getheilt gibt 3 zum Quotus und + 2 zum Reste (IV); also ist

$$\mathfrak{q}\frac{23}{7} = 23:7 = 3, \text{ und } \mathfrak{r}\frac{23}{7} = 23:7 = 2,$$

dagegen ist $-23 = 7.-4+5$, d. h. -23 durch 7 getheilt gibt -4 zum Quotus und + 5 zum Reste; daher ist

$$\mathfrak{q}\frac{-23}{7} = -23:7 = -4, \text{ und } \mathfrak{r}\frac{-23}{7} = -23:7 = 5.$$

2. Soll aber der Rest d'' nie Null, sondern damals dem Theiler t selbst gleich genommen werden, so oft der Dividend d durch den Theiler t theilbar, folglich der kleinste Rest Null ist; so sollen dergleichen Quoti und Reste außerordentliche oder ausnahmsweise genannt, und zu ihrer Bezeichnung, anstatt der kleinen Charaktere $\mathfrak{q}$ und $\mathfrak{r}$, die großen $\mathfrak{Q}$ und $\mathfrak{R}$ verwendet werden.

In einem solchen Falle ist, nach der obigen Bezeichnung in IV,

$$d' = \mathfrak{Q}\frac{d}{t} = d:t,$$

$$d'' = \mathfrak{R}\frac{d}{t} = d : t = 1, 2, 3, \ldots\ldots t,$$

und vermöge der Gleichungen (1) und (2)

$$(5) \qquad d - t\,\mathfrak{Q}\frac{d}{t} = \mathfrak{R}\frac{d}{t} = 1, 2, 3, \ldots\ldots t,$$

$$(6) \qquad d = t\,\mathfrak{Q}\frac{d}{t} + \mathfrak{R}\frac{d}{t}.$$

So z. B. ist $21 = 7.3 + 0 = 7.2 + 7$, also

$$\mathfrak{q}\frac{21}{7} = 3 \text{ und } \mathfrak{r}\frac{21}{7} = 0, \text{ dagegen } \mathfrak{Q}\frac{21}{7} = 2 \text{ und } \mathfrak{R}\frac{21}{7} = 7.$$

Allein $-21 = 7.-3+0 = 7.-4+7$, daher

$$\mathfrak{q}\frac{-21}{7} = -3 \text{ und } \mathfrak{r}\frac{-21}{7} = 0, \text{ hingegen } \mathfrak{Q}\frac{-21}{7} = -4 \text{ und } \mathfrak{R}\frac{-21}{7} = 7.$$

Anmerkung. *Cisa de Cresi* gebraucht die leicht zu mißdeutenden Bezeichnungen $\mathbf{Q}.\frac{d}{t}$ und $\mathbf{R}.\frac{d}{t}$; *de Ciccolini* bezeichnet den Quotus mit $\left(\frac{d}{t}\right)_i$, *Delambre* durch $\left(\frac{d}{t}\right)_e$, beide den Rest durch $\left(\frac{d}{t}\right)_r$; ich selbst folgte früher*) dem Lezteren, weil ich zur Bezeichnung des außerordentlichen Quotus den undeutlichen Buchstaben I oder J nicht brauchen konnte. Bei den lezteren Bezeichnungen kommt jedoch, gegen die mathematische Grundregel, das Hauptrechnungszeichen erst ganz am Ende, und die sich häufenden Klammern (Parentheſen) verundeutlichen die Rechnungsausdrücke; dies bewog mich, obige Zeichen in Vorschlag zu bringen.

VI.

Zusammenhang der gewöhnlichen und außerordentlichen Quoti und Reste.

Zwischen den gewöhnlichen und außerordentlichen Quotis und Resten bestehen einfache Beziehungs- und Verwandlungs-Gleichungen, die sich leicht aus folgenden Betrachtungen ergeben.

1. Zieht man von beiden Theilen der Gleichung

$$(6) \qquad d = t\,\mathfrak{Q}\frac{d}{t} + \mathfrak{R}\frac{d}{t}$$

die Zahl 1 ab, so erhält man

$$d - 1 = t\,\mathfrak{Q}\frac{d}{t} + \mathfrak{R}\frac{d}{t} - 1.$$

Nun ist $\mathfrak{R}\frac{d}{t} = 1, 2, \ldots\ldots t,$

also $\mathfrak{R}\frac{d}{t} - 1 = 0, 1, 2, \ldots t-1;$

daher findet man, nach dem Begriffe und der Bezeichnung des gewöhnlichen Quotus und Restes (IV und V, 1), aus der lezten Gleichung

*) Crelle Journal für Mathematik, 3. Bd., S. 337.

(7) $\mathfrak{Q}\frac{d}{t} = \mathfrak{q}\frac{d-1}{t}$,

$\mathfrak{R}\frac{d}{t} - 1 = \mathfrak{r}\frac{d-1}{t}$,

daher

(8) $\mathfrak{R}\frac{d}{t} = \mathfrak{r}\frac{d-1}{t} + 1$.

2. Addirt man zu beiden Theilen der Gleichung

(4) $d = t\,\mathfrak{q}\frac{d}{t} + \mathfrak{r}\frac{d}{t}$

die Zahl 1, so erhält man

$$d + 1 = t\,\mathfrak{q}\frac{d}{t} + \mathfrak{r}\frac{d}{t} + 1.$$

Es ist aber $\mathfrak{r}\frac{d}{t} = 0, 1, 2, \ldots . t-1$,

daher $\mathfrak{r}\frac{d}{t} + 1 = 1, 2, 3, \ldots . t$;

mithin gibt die lezte Gleichung, nach den Begriffen von den außerordentlichen Theilungsergebnissen, (IV und V, 2) die Beziehungen

(9) $\mathfrak{q}\frac{d}{t} = \mathfrak{Q}\frac{d+1}{t}$,

$\mathfrak{r}\frac{d}{t} + 1 = \mathfrak{R}\frac{d+1}{t}$,

also

(10) $\mathfrak{r}\frac{d}{t} = \mathfrak{R}\frac{d+1}{t} - 1$.

Anmerkung 1. Aus den Gleichungen (7) und (8) können (9) und (10) gewonnen werden, wenn man d in d + 1 verwandelt; umgekehrt aus diesen jene, wenn man d in d — 1 übergehen läßt.

Anmerkung 2. Sowohl aus der Erklärung der außerordentlichen Theilungsergebnisse (V, 2), als aus den Gleichungen (7) bis (10) ist ersichtlich, daß beide Arten der Theilungsergebnisse ganz einerlei sind, so lange der Dividend durch den Theiler untheilbar ist, und daß sie sich blos da, wo der Dividend durch den Theiler theilbar ist, von einander in der Weise unterscheiden, daß der außerordentliche Quotus numerisch um 1 kleiner oder größer ist, je nachdem man es mit einem positiven oder negativen Dividende zu thun hat, und daß der außerordentliche Rest der Theiler, der gewöhnliche dagegen Null ist. So hat man z. B.

$\mathfrak{Q}\frac{16}{7} = \mathfrak{q}\frac{16}{7} = 2$, $\mathfrak{R}\frac{16}{7} = \mathfrak{r}\frac{16}{7} = 2$, $\mathfrak{R}\frac{-16}{7} = \mathfrak{r}\frac{-16}{7} = 5$; hingegen ist

$\mathfrak{Q}\frac{14}{7} = 1, \mathfrak{q}\frac{14}{7} = 2$; $\mathfrak{Q}\frac{-14}{7} = -3, \mathfrak{q}\frac{-14}{7} = -2$ und $\mathfrak{R}\frac{\pm 14}{7} = 7, \mathfrak{r}\frac{\pm 14}{7} = 0$.

Anmerkung 3. Nach den hier aufgestellten Verwandlungsgleichungen könnte man allerdings blos mit einer Art von Theilung sich behelfen; allein wer die Einfachheit und Zierlichkeit der Rechnungsformen nicht überhaupt

gering schäzt, wird es uns im Folgenden gewiß billigen, wenn wir stets diejenige Theilungsweise wählen, bei welcher die Rechnungsformen am einfachsten und am zierlichsten sich ergeben.

VII.

Vertauschung der positiven und negativen Dividende.

Negative Dividende lassen sich, wofern, wie hier immer bedungen wird, die Reste positiv genommen werden, durch positive und umgekehrt ersezen, wenn man sich an folgende Verwandlungsgleichungen hält.

1. Aendert man in der Gleichung

$$(4) \qquad d = t\,\mathfrak{q}\tfrac{d}{t} + \mathfrak{r}\tfrac{d}{t}$$

alle Zeichen, so ergibt sich

$$-d = -t\,\mathfrak{q}\tfrac{d}{t} - \mathfrak{r}\tfrac{d}{t},$$

und wenn man im zweiten Theile t abzieht und addirt,

$$-d = -t\left(\mathfrak{q}\tfrac{d}{t} + 1\right) + t - \mathfrak{r}\tfrac{d}{t}.$$

Nun ist $\mathfrak{r}\frac{d}{t} = 0, 1, 2, \ldots . t-1,$

daher $t - \mathfrak{r}\frac{d}{t} = t, t-1, t-2, \ldots . 1,$

und somit ergeben sich nach den Begriffen von den außerordentlichen Theilungsergebnissen (V, 2), zur Verwandlung der negativen Dividende in positive, die Gleichungen

$$(11) \qquad \mathfrak{Q}\tfrac{-d}{t} = -\left(\mathfrak{q}\tfrac{d}{t} + 1\right) = -\mathfrak{q}\tfrac{d}{t} - 1,$$

$$(12) \qquad \mathfrak{R}\tfrac{-d}{t} = t - \mathfrak{r}\tfrac{d}{t}.$$

Z. B. $\mathfrak{Q}\frac{-19}{7} = -\mathfrak{q}\frac{19}{7} - 1 = -2 - 1 = -3,$

$\mathfrak{R}\frac{-19}{7} = 7 - \mathfrak{r}\frac{19}{7} = 7 - 5 = 2.$

2. Behandelt man auf gleiche Weise die Gleichung

$$(6) \qquad d = t\,\mathfrak{Q}\tfrac{d}{t} + \mathfrak{R}\tfrac{d}{t},$$

oder vertauscht man in den gefundenen Gleichungen (11) und (12) die kleinen Charaktere $\mathfrak{q}$ und $\mathfrak{r}$ mit den großen $\mathfrak{Q}$ und $\mathfrak{R}$, so findet man die ferneren Verwandlungsgleichungen:

$$(13) \qquad \mathfrak{q}\tfrac{-d}{t} = -\mathfrak{Q}\tfrac{d}{t} - 1,$$

$$(14) \qquad \mathfrak{r}\tfrac{-d}{t} = t - \mathfrak{R}\tfrac{d}{t}.$$

3. Will man bei diesen Verwandlungen der negativen Dividende die nemliche Theilungsweise beibehalten, so darf man blos mit den eben gefundenen

vier Gleichungen jene des vorhergehenden Artikels verbinden. Dann findet man noch die Gleichungen:

$$(15)\quad \mathfrak{q}_t^{-d} = -\mathfrak{q}_t^{d-1} - 1,$$

$$(16)\quad \mathfrak{r}_t^{-d} = t - 1 - \mathfrak{r}_t^{d-1},$$

$$(17)\quad \mathfrak{Q}_t^{-d} = -\mathfrak{Q}_t^{d+1} - 1,$$

$$(18)\quad \mathfrak{R}_t^{-d} = t + 1 - \mathfrak{R}_t^{d+1}$$

4. Zum Uebergange von positiven Dividenden auf negative erhält man aus den gefundenen acht Gleichungen die folgenden vier doppelten:

$$(19)\quad \mathfrak{q}_t^{d} = -\mathfrak{Q}_t^{-d} - 1 = -\mathfrak{q}_t^{-d-1} - 1,$$

$$(20)\quad \mathfrak{r}_t^{d} = t - \mathfrak{R}_t^{-d} = t - 1 - \mathfrak{r}_t^{-d-1},$$

$$(21)\quad \mathfrak{Q}_t^{d} = -\mathfrak{q}_t^{-d} - 1 = -\mathfrak{Q}_t^{-d+1} - 1,$$

$$(22)\quad \mathfrak{R}_t^{d} = t - \mathfrak{r}_t^{-d} = t + 1 - \mathfrak{R}_t^{-d+1}.$$

VIII.

Aufwärtiges Theilen. Negative Reste.

Das bisher besprochene, gewöhnliche und außerordentliche Theilen, welches auch in der Folge immer verstanden werden muß, wofern nicht eine Ausnahme bestimmt ausgesprochen wird, setzt voraus, daß der Divisionsrest jederzeit positiv sei, folglich daß der Quotus andeutet, das Wievielfache des Theilers, im algebraischen Sinne, nächst kleiner oder höchstens so groß als der Dividend ist, nemlich, vom Dividende abgezogen, einen positiven, den Theiler nicht übersteigenden, Rest gibt. Zuweilen sieht man sich jedoch veranlaßt, dergestalt zu theilen, daß der Quotus angibt, das Wievielfache des Theilers, im algebraischen Sinne, nächst größer oder mindestens so groß als der Dividend ist, nemlich, vom Dividende abgezogen, einen negativen, numerisch den Theiler nicht übersteigenden, Rest liefert. Ein solches Theilen mit negativen Resten kann man ein aufwärtiges, mithin das Theilen mit positiven Resten das abwärtige nennen; und auch bei jenem, wie bei diesem, ein gewöhnliches und außerordentliches unterscheiden.

Die Vergleichung der Ergebnisse beider Theilungsweisen liefern die Gleichungen:

$$(4)\quad d = t\,\mathfrak{q}_t^{d} + \mathfrak{r}_t^{d},$$

$$(6)\quad d = t\,\mathfrak{Q}_t^{d} + \mathfrak{R}_t^{d},$$

wenn man in ihren zweiten Theilen t addirt und abzieht, wodurch sie in

$$d = t\left(\mathfrak{q}\tfrac{d}{t}+1\right)-\left(t-\mathfrak{r}\tfrac{d}{t}\right),$$

$$d = t\left(\mathfrak{Q}\tfrac{d}{t}+1\right)-\left(t-\mathfrak{R}\tfrac{d}{t}\right)$$

sich verwandeln, und folgende Säze lehren.

1. Theilt man eine Zahl d durch eine andere t aufwärts, so daß der Rest, mit Ausschluß der Nulle, negativ und numerisch höchstens so groß als der Theiler ausfällt, und benüzt man die Verwandlungsgleichungen (11) und (12), so ist

der außerordentliche aufwärtige Quotus von d durch $t = \mathfrak{q}\tfrac{d}{t}+1 = -\mathfrak{Q}\tfrac{-d}{t}$,

» » » Rest $= -\left(t-\mathfrak{r}\tfrac{d}{t}\right) = -\mathfrak{R}\tfrac{-d}{t}$,

$= -1, -2, -3, \ldots -t.$

2. Theilt man dagegen eine Zahl d durch eine andere t dergestalt aufwärts, daß der Rest, mit Einschluß der Nulle, negativ und numerisch kleiner als der Theiler ausfällt, und verwendet man die Verwandlungsgleichungen (13) und (14); so ist

der gewöhnliche aufwärtige Quotus von d durch $t = \mathfrak{Q}\tfrac{d}{t}+1 = -\mathfrak{q}\tfrac{-d}{t}$,

» » » Rest $= -\left(t-\mathfrak{R}\tfrac{d}{t}\right) = -\mathfrak{r}\tfrac{-d}{t}$,

$= 0, -1, -2, \ldots -(t-1).$

Die Zahlwerthe der negativen Reste sind demnach die Ergänzungen der positiven Reste zum Theiler. Und der kleinste negative Rest von d durch t ist $= -\left(t-\mathfrak{R}\tfrac{d}{t}\right) = -\mathfrak{r}\tfrac{-d}{t}$, weil er stets kleiner als der Theiler sein muß.

Im Zusammenhange lassen sich die Ergebnisse der viererlei Theilungen mittels folgender Betrachtung aufstellen. Sei d eine positive oder negative Zahl; durch die absolute Zahl t getheilt gebe sie d′ zum Quotus und d″ zum Reste, welche mit dem Dividende d gleichzeitig entweder positiv oder negativ sein sollen. Sezt man ihnen demnach ihr gemeinschaftliches Qualitätszeichen vor, so sind $\pm d$, $\pm d'$, $\pm d''$ entschieden positiv. Man hat aber allgemein

$$(2) \qquad d = t.\,d' + d'',$$

daher auch

$$\pm d = \pm t.\,d' \pm d'',$$

und dabei immer $\pm d'' \gtreqless t$.

Somit findet man bei der gewöhnlichen Theilung, wo

$$\pm d'' = 0, 1, \ldots t-1 \text{ ist},$$

$$\pm d' = \mathfrak{q}\tfrac{\pm d}{t},\quad \pm d'' = \mathfrak{r}\tfrac{\pm d}{t},$$

also wie in V, 1 und VIII, 2,

(23) $d' = \pm \mathfrak{q}^{\frac{\pm d}{t}}$, $d'' = \pm \mathfrak{r}^{\frac{\pm d}{t}}$;

und bei der außerordentlichen Theilung, wo

$\pm d'' = 1, 2, \ldots t$ ist,

$\pm d' = \mathfrak{Q}^{\frac{\pm d}{t}}$, $\pm d'' = \mathfrak{R}^{\frac{\pm d}{t}}$,

also wie in V 2, und VIII, I,

(24) $d' = \pm \mathfrak{Q}^{\frac{\pm d}{t}}$, $d'' = \pm \mathfrak{R}^{\frac{\pm d}{t}}$.

IX.

Besondere Betrachtung des Theilens durch 2.

Ein sehr oft in Anwendung kommendes Theilen ist jenes durch 2, nemlich das Zerfällen einer Zahl, n, in zwei Theile, x und y, die sich um nicht mehr als 2 von einander unterscheiden. Sei der Theil x mindestens so groß, wenn nicht größer, als der andere y, und ihr Unterschied d, so ist

(25) $x + y = n$,

$x - y = d$,

folglich, wenn man addirt und abzieht,

$2x = n + d$,

$2y = n - d$.

Hieraus folgt einerseits

(26) $x = \frac{n}{2} + \frac{d}{2}$,

$y = \frac{n}{2} - \frac{d}{2}$,

andrerseits

(27) $n = 2x - d = 2y + d$.

Läßt sich nun die Zahl n in zwei gleiche Theile zerfällen, so daß ihr Unterschied d keiner oder Null ist; so nennt man diese Zahl n gerade, und jeden ihrer beiden gleichen Theile x und y ihre Hälfte, so daß

$x = y = \frac{n}{2}$ ist.

Kann man dagegen die Zahl n nicht in zwei gleiche, sondern höchstens in zwei möglichst wenig, nur um 1, von einander verschiedene, ungleiche Theile zerfällen; so nennt man diese Zahl n ungerad, und den größeren Theil x die größere Hälfte, den kleineren Theil y die kleinere Hälfte; so daß man hat:

größere Hälfte $x = \frac{n}{2} + \frac{1}{2} = \frac{n+1}{2}$,

kleinere Hälfte $y = \frac{n}{2} - \frac{1}{2} = \frac{n-1}{2}$.

1. Will man demnach eine Zahl n in zwei, entweder gleiche, oder höchstens nur um 1 verschiedene, Theile x und y zerlegen, mithin beide Zerfällungsweisen durch obige Gleichungen (27) auf einmal ausdrücken, so gibt man diesen die Gestalt

$$n + 1 = 2x + 1 - d,$$
$$n = 2y + d.$$

Je nachdem nun n gerade oder ungerade ist,

hat man $d = 0$ oder 1,

also $1 - d = 1$ oder 0;

daher, nach der Erklärung der gewöhnlichen Theilung (in IV),

$$x = \text{ɢ}\frac{n+1}{2}, \quad y = \text{ɢ}\frac{n}{2},$$

$$1 - d = \text{ꝛ}\frac{n+1}{2}, \quad d = \text{ꝛ}\frac{n}{2}.$$

Daraus folgt nun, nach den Gleichungen (25) und wenn man die zwei lezten Gleichungen addirt,

$$(28) \qquad \text{ɢ}\frac{n+1}{2} + \text{ɢ}\frac{n}{2} = n,$$
$$\text{ɢ}\frac{n+1}{2} - \text{ɢ}\frac{n}{2} = \text{ꝛ}\frac{n}{2}$$

und

$$(29) \qquad \text{ꝛ}\frac{n+1}{2} + \text{ꝛ}\frac{n}{2} = 1.$$

Je nachdem also

die Zahl n entweder gerade, oder ungerade ist,

muß der Rest $\text{ꝛ}\frac{n}{2} = 0$ oder 1 und

der Rest $\text{ꝛ}\frac{n+1}{2} = 1$ oder 0,

also die Summe beider Reste jeden Falls 1 sein; ferner sind die zwei, entweder gleichen oder höchstens um 1 verschiedenen Theile von n die Quoti $\text{ɢ}\frac{n}{2}$ und $\text{ɢ}\frac{n+1}{2}$; und zwar ist

α) der Quotus $\text{ɢ}\frac{n}{2}$ entweder genau die Hälfte,
oder nur die kleinere Hälfte, und

β) der Quotus $\text{ɢ}\frac{n+1}{2}$ entweder genau die Hälfte,
oder schon die größere Hälfte.

2. Will man dagegen eine Zahl n in zwei ungleiche, möglichst wenig von einander verschiedene, Theile x und y zerfällen; so muß, je nachdem n gerade oder ungerade ist, der Unterschied $d = 2$ oder 1, folglich nach Gleichung (26)

der größere Theil $x = \frac{n}{2} + 1$ oder $= \frac{n}{2} + \frac{1}{2} = \frac{n+1}{2}$,

der kleinere „ $y = \frac{n}{2} - 1$ oder $= \frac{n}{2} - \frac{1}{2} = \frac{n-1}{2}$,

und nach den Gleichungen (27)

$$n = 2(x-1) + 2 - d,$$
$$n = 2y + d$$

sein.

Je nachdem nun n gerade oder ungerade ist,

hat man $d = 2$ oder 1,

also $2 - d = 0$ oder 1;

daher nach der Erklärung des gewöhnlichen und außerordentlichen Theilens (in IV und V),

$$x - 1 = \mathfrak{q}\tfrac{n}{2}, \quad x = \mathfrak{q}\tfrac{n}{2} + 1, \quad y = \mathfrak{Q}\tfrac{n}{2},$$

$$2 - d = \mathfrak{r}\tfrac{n}{2}, \quad d = \mathfrak{R}\tfrac{n}{2}.$$

Daraus folgt nun, nach den Gleichungen (25), und wenn man die beiden lezten Gleichungen addirt,

$$(30) \qquad \left(\mathfrak{q}\tfrac{n}{2} + 1\right) + \mathfrak{Q}\tfrac{n}{2} = n,$$
$$\left(\mathfrak{q}\tfrac{n}{2} + 1\right) - \mathfrak{Q}\tfrac{n}{2} = \mathfrak{R}\tfrac{n}{2},$$

und

$$(31) \qquad \mathfrak{r}\tfrac{n}{2} + \mathfrak{R}\tfrac{n}{2} = 2.$$

Je nachdem also

die Zahl n entweder gerade oder ungerade ist,

muß der Rest $\mathfrak{r}\frac{n}{2} = 0$ oder 1,

und der Rest $\mathfrak{R}\frac{n}{2} = 2$ oder 1,

also die Summe beider Reste jeden Falls 2 sein; ferner sind die zwei, möglichst wenig von einander verschiedenen, Theile von n der außerordentliche Quotus $\mathfrak{Q}\frac{n}{2}$ und der aufwärtige Quotus $\mathfrak{q}\frac{n}{2} + 1$; und zwar ist

α) der Quotus $\mathfrak{Q}\frac{n}{2} = \mathfrak{q}\frac{n-1}{2}$ entweder um 1 kleiner als die Hälfte,
oder die kleinere Hälfte selbst, und

β) der Quotus $\mathfrak{q}\frac{n}{2} + 1$ entweder um 1 größer als die Hälfte,
oder die größere Hälfte selbst.

Anmerkung. Die Gleichungen (30) und (31) fließen auch aus den früheren (28) und (29), wenn man darin n mit $n - 1$ vertauscht, und die Gleichungen (7), (8) berücksichtiget.

X.

Kleinſte Reſte.

Kennt man den gewöhnlichen poſitiven Reſt der Theilung einer Zahl d durch eine andere t, nemlich $\mathfrak{r}\frac{d}{t}$, ſo läßt ſich leicht der ihm angehörige negative Reſt $-\left(t-\mathfrak{r}\frac{d}{t}\right)=-\mathfrak{R}\frac{-d}{t}$, vermöge Gleichung (12), finden, wenn man jenen von dem Theiler t abzieht, und den entfallenden Unterſchied negativ anſezt. Sobald aber beide Reſte, der kleinſte poſitive $\mathfrak{r}\frac{d}{t}$ und der ihn zum Theiler ergänzende negative $-\left(t-\mathfrak{r}\frac{d}{t}\right)=-\mathfrak{R}\frac{-d}{t}$, bekannt ſind, ſo iſt der kleinere aus ihnen, oder, falls ſie gleich groß wären, jeder von ihnen der kleinſte Reſt der Theilung von d durch t.

1. Der kleinſte Reſt iſt demnach poſitiv, folglich $=\mathfrak{r}\frac{d}{t}$, wenn $\mathfrak{r}\frac{d}{t}\leqq t-\mathfrak{r}\frac{d}{t}$, alſo $2\,\mathfrak{r}\frac{d}{t}\leqq t$, und $\mathfrak{r}\frac{d}{t}\leqq\frac{1}{2}t$, d. h. wenn $\mathfrak{r}\frac{d}{t}$ nicht größer als der halbe Theiler iſt; nemlich wenn, vermöge IX, $\mathfrak{r}\frac{d}{t}\leqq\mathfrak{q}\frac{t}{2}$, d. h. nicht $>\mathfrak{q}\frac{t}{2}$, folglich $<\mathfrak{q}\frac{t}{2}+1$, und ſomit

$$\mathfrak{r}\frac{d}{t}=0,\ 1,\ 2,\ \ldots\ \mathfrak{Q}\frac{t}{2},\ \mathfrak{q}\frac{t}{2}$$

iſt. Dann wird auch

der kleinſte Reſt $=0,\ 1,\ 2,\ \ldots\ \mathfrak{Q}\frac{t}{2},\ \mathfrak{q}\frac{t}{2}$.

2. Der kleinſte Reſt iſt dagegen negativ, folglich $=-\left(t-\mathfrak{r}\frac{d}{t}\right)$, wenn $\mathfrak{r}\frac{d}{t}\geqq t-\mathfrak{r}\frac{d}{t}$, alſo $2\,\mathfrak{r}\frac{d}{t}\geqq t$, und $\mathfrak{r}\frac{d}{t}\geqq\frac{1}{2}t$, d. h. wenn $\mathfrak{r}\frac{d}{t}$ nicht kleiner als der halbe Theiler iſt; nemlich wenn, vermöge IX, $\mathfrak{r}\frac{d}{t}\geqq\mathfrak{q}\frac{t+1}{2}$, d. h. nicht $<\mathfrak{q}\frac{t+1}{2}$, folglich $>\mathfrak{Q}\frac{t}{2}$, und ſomit

$$\mathfrak{r}\frac{d}{t}=\mathfrak{q}\frac{t+1}{2},\ \mathfrak{q}\frac{t}{2}+1,\ \ldots\ t-1$$

iſt. Dann wird

der kleinſte Reſt $=-\mathfrak{q}\frac{t}{2},-\mathfrak{Q}\frac{t}{2},\ \ldots\ -1$.

3. Der kleinſte Reſt iſt endlich eben ſowohl poſitiv $=\mathfrak{r}\frac{d}{t}$ als negativ $=-\left(t-\mathfrak{r}\frac{d}{t}\right)$, wenn $\mathfrak{r}\frac{d}{t}=t-\mathfrak{r}\frac{d}{t}$, alſo $2\mathfrak{r}\frac{d}{t}=t$, und $\mathfrak{r}\frac{d}{t}=\frac{1}{2}t$, d. h. wenn $\mathfrak{r}\frac{d}{t}$ die Hälfte des Theilers iſt; was vorausſezt, daß der Theiler t eine gerade Zahl ſei. Dann iſt

der kleinſte Reſt eben ſowohl $=\pm\mathfrak{q}\frac{t}{2}$, als $\pm\mathfrak{q}\frac{t+1}{2}$.

Anmerkung. Man kann auch den kleinsten positiven Rest $\mathfrak{r}\frac{d}{t}$ mit dem kleinsten negativen $-\mathfrak{r}\frac{-d}{t}$ vergleichen, und aus ihnen den kleinsten möglichen bestimmen.

XI.

Zusammenhang der Zahlen mit ihren Resten.

1. Jeder Zahl sind alle ihre Reste, daher auch diese einander, congruent, wenn man den Theiler, oder einen Factor desselben, zum Modul nimmt.

Denn gibt d durch t getheilt d′ zum Quotus und d″ zum Reste, mag dieser wie immer beschaffen sein, so ist, vermöge IV, Gleichung (2),

$$d = td' + d''.$$

Nimmt man demnach den Theiler t, oder einen Factor Θ desselben, zum Modul; übergeht nach III, 1 von der Gleichheit auf die Congruenz; und wirft nach III, 7 das durch den Modul theilbare Product td′ weg: so erhält man vermöge III, 13

$$d \equiv d'', \text{ mod } (t, \Theta).$$

So ist insbesondere

$$(32) \quad d \equiv \mathfrak{r}\tfrac{d}{t} \equiv -\left(t - \mathfrak{r}\tfrac{d}{t}\right) \equiv -\mathfrak{R}\tfrac{-d}{t}$$
$$\equiv \mathfrak{R}\tfrac{d}{t} \equiv -\left(t - \mathfrak{R}\tfrac{d}{t}\right) \equiv -\mathfrak{r}\tfrac{-d}{t}, \text{ mod } (t, \Theta).$$

Z. B. Wenn man 147 durch 30 theilt, ist

$$147 \equiv 27 \equiv -3, \text{ mod } (30, 15, 10, 6, 5, 3, 2).$$

2. Soll demnach eine Zahl x irgend einer der Reste einer anderen Zahl d, nach einem Theiler oder Modul t, sein; so kann man dies am einfachsten allgemein durch die Congruenz

$$(33) \qquad x \equiv d, \text{ mod } t$$

andeuten. Obschon diese Bezeichnung unbestimmt ist, weil sie x nur als irgend eine nach dem Modul t mit d congruente Zahl, folglich vermöge III, 4 als jedes Glied der arithmetischen Progression angibt, deren ein Glied d und Unterschied t ist; so kann man sie doch, wegen ihrer besonderen Bequemlichkeit, überall verwenden, wo man aus dem Zusammenhange der Rede oder aus der Bedeutung der Zahl x bereits weiß, ob selbe Null, nur positiv oder auch negativ, blos kleiner oder auch so groß als der Modul, oder wohl gar noch größer als derselbe sein darf; folglich ob man sie dem positiven oder negativen, gewöhnlichen oder außerordentlichen, oder — was meistens der Fall sein wird — dem kleinsten möglichen Reste der Zahl d durch t, oder sonst einem Gliede obiger arithmetischer Progression gleich zu stellen hat. Um mehr Bestimmtheit in den Ausdruck

zu bringen, kann man nebenbei den Umfang der Werthe der gesuchten Zahl ansezen, folglich den gewöhnlichen Rest

$$x = \mp\frac{d}{t} \text{ durch } x \equiv d, \mod t = 0, 1, \ldots t-1,$$

den außerordentlichen Rest

$$x = \mathfrak{R}\frac{d}{t} \text{ durch } x \equiv d, \mod t = 1, 2, \ldots t,$$

und den möglich kleinsten Rest durch

$$x \equiv d, \mod t = -\mathfrak{f}\frac{t-1}{2}, \ldots \mathfrak{f}\frac{t}{2}$$

andeuten.

3. Wird demnach von einem zusammengesezten Ausdrucke, d. i. von der Summe oder dem Unterschiede mehrerer theils zu addirender, theils abzuziehender Zahlen, welche selbst wieder zum Theil Producte oder Potenzen sein können, ein Rest nach einem angegebenen Theiler oder Modul gesucht; so darf man, zur Vereinfachung der Rechnung, zu Folge III, 5 und 6, anstatt jedes Gliedes, mag es zu addiren oder abzuziehen sein, oder vermöge III, 8 statt jedes Factors eines Gliedes, oder endlich, vermöge III, 9, statt der in einem Gliede zu potenzirenden Zahl, einen Rest nach demselben Modul, am vortheilhaftesten den kleinsten, in Rechnung bringen; folglich von jedem Gliede, oder von einem Factor oder einer zu potenzirenden Zahl in demselben, den Theiler oder Modul, so oft es angeht, wegwerfen. Erhält man endlich für den Dividend eine negative den Theiler nicht erreichende Zahl, und soll der Rest positiv ausfallen, so wird man blos noch den Zahlwerth des negativen Restes zum Theiler ergänzen.

4. Congruente Zahlen geben, durch den Modul oder durch einen Theiler des Moduls getheilt, gleiche Reste derselben Art, welche nemlich beide gewöhnlich oder außerordentlich, positiv oder negativ sind.

Denn ist $d \equiv \delta$, mod m, und geben die Zahlen d und δ durch einen Theiler μ des Moduls m, dem er auch gleich sein kann, auf einerlei Weise getheilt die Reste r und ρ; so ist, vermöge III, 13, $d \equiv \delta$, mod μ, vermöge XI, 1, $d \equiv r$, und $\delta \equiv \rho$, mod μ; daher auch, zu Folge III, 2,

$$r \equiv \rho, \mod \mu,$$

d. h. die Reste r und ρ der congruenten Zahlen d und δ sind nach jedem Theiler μ des Moduls m congruent, nemlich der Unterschied jener Reste ist durch diesen Theiler μ theilbar. Weil nun die Zahlwerthe der Reste r und ρ nie größer als der Theiler μ, und beide Reste gleichzeitig entweder positiv oder negativ, gewöhnlich oder außerordentlich sind; so muß ihr Unterschied $r - \rho$ oder $\rho - r$, kleiner als der Theiler μ ausfallen, mithin Null, und sofort der Rest $r = \rho$ sein; da durch eine Zahl keine kleinere außer Null theilbar ist.

So ist z. B. $131 \equiv -93 \bmod 28$, beide Zahlen geben durch den Modul 28 und seine Theiler 14, 7, 4, 2 getheilt die positiven Reste 19, 5, 5, 3, 1 und die negativen Reste — 9, — 9, — 2, — 1, — 1.

5. Insbesondere muß, weil vermöge XI, 1,

$$d \equiv \mathfrak{r}\frac{d}{t} \equiv \mathfrak{R}\frac{d}{t}, \bmod t$$

ist, auch

$$(34) \qquad \mathfrak{r}\frac{d}{t} = \mathfrak{r}\frac{\mathfrak{r}\frac{d}{t}}{t} = \mathfrak{r}\frac{\mathfrak{R}\frac{d}{t}}{t},$$

$$\mathfrak{R}\frac{d}{t} = \mathfrak{R}\frac{\mathfrak{r}\frac{d}{t}}{t} = \mathfrak{R}\frac{\mathfrak{R}\frac{d}{t}}{t}$$

sein.

XII.

Verwandlung der Quoti und Reste.

1. Ein Quotus bleibt ungeändert, wenn man den Dividend und Theiler mit einerlei Zahl multiplicirt oder durch einen gemeinschaftlichen Theiler dividirt.

2. Ein Rest bleibt derselbe, wenn man entweder den Dividend und Theiler mit einerlei Zahl multiplicirt und den neuen Rest durch diesen Multiplicator theilt, oder wenn man den Dividend und Theiler durch einen gemeinschaftlichen Theiler dividirt und den neuen Rest mit diesem Divisor multiplicirt.

Denn wenn man d durch t theilt, ist

$$(4) \qquad d = t\mathfrak{q}\frac{d}{t} + \mathfrak{r}\frac{d}{t} \text{ und}$$

$$\mathfrak{r}\frac{d}{t} = 0, 1, 2, \ldots t-1;$$

folglich, wenn man mit der Zahl n beide Theile dieser Gleichungen multiplicirt,

$$nd = nt\,\mathfrak{q}\frac{d}{t} + n\,\mathfrak{r}\frac{d}{t}$$

und

$$n\,\mathfrak{r}\frac{d}{t} = 0, n, 2n, \ldots . nt - n.$$

Mithin ist, nach der Erklärung der gewöhnlichen Theilung in IV,

$$(35) \qquad \mathfrak{q}\frac{nd}{nt} = \mathfrak{q}\frac{d}{t},$$

$$(36) \qquad \mathfrak{r}\frac{nd}{nt} = n\,\mathfrak{r}\frac{d}{t} \text{ und } \mathfrak{r}\frac{d}{t} = \mathfrak{r}\frac{nd}{nt} : n.$$

Aus denselben Gründen ist

$$(37) \qquad \mathfrak{Q}\frac{nd}{nt} = \mathfrak{Q}\frac{d}{t},$$

$$(38) \qquad \mathfrak{R}\frac{nd}{nt} = n\,\mathfrak{R}\frac{d}{t} \text{ und } \mathfrak{R}\frac{d}{t} = \mathfrak{R}\frac{nd}{nt} : n.$$

z. B. $\mathfrak{q}\frac{17}{7} = 2 = \mathfrak{q}\frac{102}{42} = \mathfrak{q}\frac{51}{21}$,

$$\text{r}\frac{17}{7} = 3 = \text{r}\frac{102}{42} : 6 = 18 : 6,$$
$$\text{r}\frac{102}{42} = 2\,\text{r}\frac{51}{21} = 2.9 = 18.$$

XIII.

Das Theilen durch ein Product. Nach einander folgendes Theilen.

Sei die Zahl d zuerst durch m zu theilen, und der entfallende Quotus wieder durch p, so findet man

$$d = m\,\text{q}\frac{d}{m} + \text{r}\frac{d}{m},$$

$$\text{q}\frac{d}{m} = p\,\text{q}\frac{\text{q}\frac{d}{m}}{p} + \text{r}\frac{\text{q}\frac{d}{m}}{p},$$

daher, wenn man substituirt,

$$d = mp\,\text{q}\frac{\text{q}\frac{d}{m}}{p} + m\,\text{r}\frac{\text{q}\frac{d}{m}}{p} + \text{r}\frac{d}{m}.$$

Nun ist

$$\text{r}\frac{d}{m} = 0, 1, \ldots . m-1,$$

$$\text{r}\frac{\text{q}\frac{d}{m}}{p} = 0, 1, \ldots . p-1,$$

also

$$m\,\text{r}\frac{\text{q}\frac{d}{m}}{p} + \text{r}\frac{d}{m} = 0, 1, \ldots . mp-1;$$

mithin liefert die gewöhnliche Theilung

$$\text{q}\frac{d}{mp} = \text{q}\frac{\text{q}\frac{d}{m}}{p},$$

$$\text{r}\frac{d}{mp} = m\,\text{r}\frac{\text{q}\frac{d}{m}}{p} + \text{r}\frac{d}{m}.$$

Verwechselt man in diesen Gleichungen m und p, so findet man

$$\text{q}\frac{d}{pm} = \text{q}\frac{\text{q}\frac{d}{p}}{m},$$

$$\text{r}\frac{d}{pm} = p\,\text{r}\frac{\text{q}\frac{d}{p}}{m} + \text{r}\frac{d}{p},$$

daher, wegen $mp = pm$, auch

$$(39) \qquad \text{q}\frac{d}{mp} = \text{q}\frac{\text{q}\frac{d}{m}}{p} = \text{q}\frac{\text{q}\frac{d}{p}}{m},$$

$$(40) \qquad \text{r}\frac{d}{mp} = m\,\text{r}\frac{\text{q}\frac{d}{m}}{p} + \text{r}\frac{d}{m} = p\,\text{r}\frac{\text{q}\frac{d}{p}}{m} + \text{r}\frac{d}{p}.$$

Die erste dieser Gleichungen enthält folgende Sätze:

1. Ist eine Zahl durch das Product zweier Zahlen zu theilen, so erhält man den Quotus, wenn man die Zahl zuerst durch den einen Theiler und den entfallenden Quotus durch den zweiten Theiler dividirt.

2. Anstatt eine Zahl durch zwei andere der Reihe nach zu theilen, kann man sie auch sogleich durch das Product derselben theilen.

3. Die Ordnung des nach einander folgenden Theilens ist beliebig.

Z. B. Ist $d = 87$ durch $m = 4$ und $p = 5$ nach einander oder durch das Product $mp = 20$ auf einmal zu theilen, so hat man

$$87 = 20.\ 4 + 7 = 4.\ 21 + 3 = 5.\ 17 + 2,$$
$$21 = 5.\ 4 + 1,\quad 17 = 4.\ 4 + 1,\quad 7 = 4.\ 1 + 3 = 5.\ 1 + 2.$$

Soll die Theilung durch das Product eine außerordentliche sein, so muß man zuerst durch den einen Factor außerordentlich und nachher durch den anderen gewöhnlich theilen. Denn aus

$$d = m\, \mathfrak{Q}^{d}_{m} + \mathfrak{R}^{d}_{m},$$

$$\mathfrak{Q}^{d}_{m} = p\, \mathfrak{q}\frac{\mathfrak{Q}^{d}_{m}}{p} + \mathfrak{r}\frac{\mathfrak{Q}^{d}_{m}}{p}$$

folgt

$$d = mp\, \mathfrak{q}\frac{\mathfrak{Q}^{d}_{m}}{p} + m\, \mathfrak{r}\frac{\mathfrak{Q}^{d}_{m}}{p} + \mathfrak{R}^{d}_{m};$$

zugleich ist

$$m\, \mathfrak{r}\frac{\mathfrak{Q}^{d}_{m}}{p} + \mathfrak{R}^{d}_{m} = m\,(0, 1, \ldots p-1) + (1, 2, \ldots m)$$
$$= 1, 2, \ldots . mp;$$

daher findet man

$$(41)\qquad \mathfrak{Q}^{d}_{mp} = \mathfrak{q}\frac{\mathfrak{Q}^{d}_{m}}{p},$$

$$(42)\qquad \mathfrak{R}^{d}_{mp} = m\, \mathfrak{r}\frac{\mathfrak{Q}^{d}_{m}}{p} + \mathfrak{R}^{d}_{m}.$$

Auch hier ist die Verwechslung der Factoren oder der Theiler gestattet.

XIV.

Quoti von Summen und Unterschieden.

Seien a, b, c, d, ... absolute Zahlen, theils zu einer Zahl u zu addiren, theils abzuziehen, oder theils positiv, theils negativ zusammenzufassen, der

dadurch erhaltene zusammengesezte Ausdruck durch die Zahl t zu theilen und der Quotus zu suchen.

1. Vermöge Gleichung (4) ist

$$a = t\,\mathfrak{q}\tfrac{a}{t} + \mathfrak{r}\tfrac{a}{t},$$
$$b = t\,\mathfrak{q}\tfrac{b}{t} + \mathfrak{r}\tfrac{b}{t},$$
$$c = t\,\mathfrak{q}\tfrac{c}{t} + \mathfrak{r}\tfrac{c}{t},$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

daher, wenn man noch eine beliebige Zahl u in der Rechnung unverändert mitführen will,

$$u \pm a \pm b \pm c \ldots = t\left(\pm\mathfrak{q}\tfrac{a}{t} \pm \mathfrak{q}\tfrac{b}{t} \pm \mathfrak{q}\tfrac{c}{t} \ldots\right) + u \pm \mathfrak{r}\tfrac{a}{t} \pm \mathfrak{r}\tfrac{b}{t} \pm \mathfrak{r}\tfrac{c}{t} \ldots$$

Aus demselben Grunde ist

$$u \pm \mathfrak{r}\tfrac{a}{t} \pm \mathfrak{r}\tfrac{b}{t} \pm \mathfrak{r}\tfrac{c}{t} \ldots = t\,\mathfrak{q}\frac{u \pm \mathfrak{r}\frac{a}{t} \pm \mathfrak{r}\frac{b}{t} \pm \mathfrak{r}\frac{c}{t} \ldots}{t} + \mathfrak{r}\frac{u \pm \mathfrak{r}\frac{a}{t} \pm \mathfrak{r}\frac{b}{t} \pm \mathfrak{r}\frac{c}{t} \ldots}{t}$$

und vermöge XI, 3

$$\mathfrak{r}\frac{u \pm \mathfrak{r}\frac{a}{t} \pm \mathfrak{r}\frac{b}{t} \pm \mathfrak{r}\frac{c}{t} \ldots}{t} = \mathfrak{r}\frac{u \pm a \pm b \pm c \ldots}{t},$$

folglich, wenn man diese Ausdrücke substituirt,

$$u \pm a \pm b \pm c \ldots = t\left(\pm\mathfrak{q}\tfrac{a}{t} \pm \mathfrak{q}\tfrac{b}{t} \pm \mathfrak{q}\tfrac{c}{t} \ldots + \mathfrak{q}\frac{u \pm \mathfrak{r}\frac{a}{t} \pm \mathfrak{r}\frac{b}{t} \pm \mathfrak{r}\frac{c}{t} \ldots}{t}\right) + \mathfrak{r}\frac{u \pm a \pm b \pm c \ldots}{t}.$$

Die gewöhnliche Theilung gibt demnach

$$(43)\quad \mathfrak{q}\frac{u \pm a \pm b \pm c \ldots}{t} = \pm\mathfrak{q}\tfrac{a}{t} \pm \mathfrak{q}\tfrac{b}{t} \pm \mathfrak{q}\tfrac{c}{t} \ldots + \mathfrak{q}\frac{u \pm \mathfrak{r}\frac{a}{t} \pm \mathfrak{r}\frac{b}{t} \pm \mathfrak{r}\frac{c}{t} \ldots}{t}.$$

2. Will man auch negative Dividende in der Rechnung behalten, so hat man nach Gleichung (4)

$$\pm a = t\,\mathfrak{q}\tfrac{\pm a}{t} + \mathfrak{r}\tfrac{\pm a}{t},$$
$$\pm b = t\,\mathfrak{q}\tfrac{\pm b}{t} + \mathfrak{r}\tfrac{\pm b}{t},$$
$$\pm c = t\,\mathfrak{q}\tfrac{\pm b}{t} + \mathfrak{r}\tfrac{\pm c}{t},$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

also

$$u \pm a \pm b \pm c \ldots = t\left(\mathfrak{q}\tfrac{\pm a}{t} + \mathfrak{q}\tfrac{\pm b}{t} + \mathfrak{q}\tfrac{\pm c}{t} \ldots\right) + u + \mathfrak{r}\tfrac{\pm a}{t} + \mathfrak{r}\tfrac{\pm b}{t} + \mathfrak{r}\tfrac{\pm c}{t} \ldots$$

Weil ferner aus gleichem Grunde

$$u + \mathfrak{r}\tfrac{\pm a}{t} + \mathfrak{r}\tfrac{\pm b}{t} + \mathfrak{r}\tfrac{\pm c}{t} \ldots = t\,\mathfrak{q}\frac{u + \mathfrak{r}\frac{\pm a}{t} + \mathfrak{r}\frac{\pm b}{t} + \mathfrak{r}\frac{\pm c}{t} \ldots}{t} + \mathfrak{r}\frac{u + \mathfrak{r}\frac{\pm a}{t} + \mathfrak{r}\frac{\pm b}{t} + \mathfrak{r}\frac{\pm c}{t} \ldots}{t}$$

und vermöge XI, 3

$$\mathfrak{r}\frac{u + \mathfrak{r}\frac{\pm a}{t} + \mathfrak{r}\frac{\pm b}{t} + \mathfrak{r}\frac{\pm c}{t} \ldots}{t} = \mathfrak{r}\frac{u \pm a \pm b \pm c \ldots}{t}$$

ist, so findet man

$$u \pm a \pm b \pm c \ldots = t\left(\mathfrak{q}\tfrac{\pm a}{t} + \mathfrak{q}\tfrac{\pm b}{t} + \mathfrak{q}\tfrac{\pm c}{t} \ldots + \mathfrak{q}\frac{u + \mathfrak{r}\frac{\pm a}{t} + \mathfrak{r}\frac{\pm b}{t} + \mathfrak{r}\frac{\pm c}{t} \ldots}{t}\right) + \mathfrak{r}\frac{u \pm a \pm b \pm c \ldots}{t}.$$

Darnach gibt die gewöhnliche Theilung

$$(44)\quad \mathfrak{q}\frac{u \pm a \pm b \pm c \ldots}{t} = \mathfrak{q}\tfrac{\pm a}{t} + \mathfrak{q}\tfrac{\pm b}{t} + \mathfrak{q}\tfrac{\pm c}{t} \ldots + \mathfrak{q}\frac{u + \mathfrak{r}\frac{\pm a}{t} + \mathfrak{r}\frac{\pm b}{t} + \mathfrak{r}\frac{\pm c}{t} \ldots}{t}.$$

3. Ist ein Glied des zusammengesezten Ausdruckes durch den Theiler theilbar, oder ein Vielfaches des Theilers, z. B. $a = \alpha t$, so ist

$$\mathfrak{q}\tfrac{a}{t} = \alpha, \quad \mathfrak{r}\tfrac{a}{t} = 0, \quad \mathfrak{q}\tfrac{-a}{t} = -\alpha, \quad \mathfrak{r}\tfrac{-a}{t} = 0,$$

daher nach Gleichung (43) und (44)

$$(45)\quad \mathfrak{q}\frac{u \pm \alpha t \pm b \pm c \ldots}{t} = \pm\alpha \pm \mathfrak{q}\tfrac{b}{t} \pm \mathfrak{q}\tfrac{c}{t} \ldots + \mathfrak{q}\frac{u \pm \mathfrak{r}\frac{b}{t} \pm \mathfrak{r}\frac{c}{t} \ldots}{t} = \pm\alpha + \mathfrak{q}\tfrac{\pm b}{t} + \mathfrak{q}\tfrac{\pm c}{t} \ldots + \mathfrak{q}\frac{u + \mathfrak{r}\frac{\pm b}{t} + \mathfrak{r}\frac{\pm c}{t} \ldots}{t}.$$

Anmerkung. In diesen Gleichungen kann überall statt der gewöhnlichen Theilung auch die außerordentliche gesezt werden.

4. **Besondere Fälle.** Sind die Zahlen a, b, c, ... sämmtlich zu addiren, oder stellt man sich unter den Buchstaben a, b, c, ... eben sowohl negative als positive Zahlen vor, so geben die Gleichungen (43) und (44)

$$(46)\quad \mathfrak{q}\frac{u + a + b + c + \ldots}{t} = \mathfrak{q}\tfrac{a}{t} + \mathfrak{q}\tfrac{b}{t} + \mathfrak{q}\tfrac{c}{t} + \ldots + \mathfrak{q}\frac{u + \mathfrak{r}\frac{a}{t} + \mathfrak{r}\frac{b}{t} + \mathfrak{r}\frac{c}{t} + \ldots}{t}$$

Eben so findet man nach Gleichung (43)

$$(47)\qquad \mathfrak{q}\frac{u+a\pm b}{t}=\mathfrak{q}\frac{a}{t}\pm\mathfrak{q}\frac{b}{t}+\mathfrak{q}\frac{u+\mathfrak{r}\frac{a}{t}\pm\mathfrak{r}\frac{b}{t}}{t},$$

und wenn man erst $a=0$ und dann a statt u setzt.

$$(48)\qquad \mathfrak{q}\frac{a\pm b}{t}=\pm\mathfrak{q}\frac{b}{t}+\mathfrak{q}\frac{a\pm\mathfrak{r}\frac{b}{t}}{t}.$$

Läßt man hierin b in $b-1$ und a in $a\pm 1$ übergehen, so erhält man

$$(49)\qquad \mathfrak{q}\frac{a\pm b}{t}=\pm\mathfrak{q}\frac{b-1}{t}+\mathfrak{q}\frac{a\pm\left(1+\mathfrak{r}\frac{b-1}{t}\right)}{t},\text{ oder nach Gleich. (8)}$$

$$=\pm\mathfrak{q}\frac{b-1}{t}+\mathfrak{q}\frac{a\pm\mathfrak{R}\frac{b}{t}}{t};$$

oder es ist

$$(50)\qquad \mathfrak{q}\frac{a\pm b}{t}=\mathfrak{q}\frac{a\pm t\mathfrak{Q}\frac{b}{t}\pm\mathfrak{R}\frac{b}{t}}{t}=\pm\mathfrak{Q}\frac{b}{t}+\mathfrak{q}\frac{a\pm\mathfrak{R}\frac{b}{t}}{t}.$$

5. Kommen unter den theils zu addirenden, theils abzuziehenden Zahlen (den Gliedern des zu theilenden zusammengesetzten Ausdruckes), selbst wieder Divisionsreste vor; so geben dafür die Gleichungen (43) bis (49) folgende Rechnungsweisen an die Hand.

$$(51)\qquad \mathfrak{q}\frac{u\pm\mathfrak{r}\frac{a}{t}\pm\mathfrak{r}\frac{b}{t}\pm\mathfrak{r}\frac{c}{t}\cdots}{t}=\mathfrak{q}\frac{u\pm a\pm b\pm c\ldots.}{t}\mp\mathfrak{q}\frac{a}{t}\mp\mathfrak{q}\frac{b}{t}\mp\mathfrak{q}\frac{c}{t}\cdots$$

$$(52)\qquad \mathfrak{q}\frac{u+\mathfrak{r}\frac{\pm a}{t}+\mathfrak{r}\frac{\pm b}{t}+\mathfrak{r}\frac{\pm c}{t}\cdots}{t}=\mathfrak{q}\frac{u\pm a\pm b\pm c\ldots.}{t}-\mathfrak{q}\frac{\pm a}{t}-\mathfrak{q}\frac{\pm b}{t}-\mathfrak{q}\frac{\pm c}{t}\cdots$$

$$(53)\qquad \mathfrak{q}\frac{u+\mathfrak{r}\frac{a}{t}+\mathfrak{r}\frac{b}{t}+\mathfrak{r}\frac{c}{t}\cdots}{t}=\mathfrak{q}\frac{u+a+b+c\ldots.}{t}-\mathfrak{q}\frac{a}{t}-\mathfrak{q}\frac{b}{t}-\mathfrak{q}\frac{c}{t}\cdots$$

$$(54)\qquad \mathfrak{q}\frac{u+\mathfrak{r}\frac{a}{t}\pm\mathfrak{r}\frac{b}{t}}{t}=\mathfrak{q}\frac{u+a\pm b}{t}-\mathfrak{q}\frac{a}{t}\mp\mathfrak{q}\frac{b}{t},$$

$$(55)\qquad \mathfrak{q}\frac{a\mp\mathfrak{r}\frac{b}{t}}{t}=\mathfrak{q}\frac{a\mp b}{t}\mp\mathfrak{q}\frac{b}{t}=\mp\mathfrak{q}\frac{b}{t}-\mathfrak{q}\frac{-a\pm b-1}{t}-1,$$

$$(56)\qquad \mathfrak{q}\frac{a\pm\mathfrak{R}\frac{b}{t}}{t}=\mathfrak{q}\frac{a\mp b}{t}\mp\mathfrak{q}\frac{b-1}{t}=\mp\mathfrak{q}\frac{b-1}{t}-\mathfrak{q}\frac{-a\pm b-1}{t}-1.$$

XV.

Addition und Subtraction der Quoti und Reste.

1. Für das Addiren und Abziehen der Quoti liefern die Gleichungen (43), (44) und (19) folgende Vorschriften:

(57) $\pm a \pm \mathfrak{q}\frac{b}{t} \pm \mathfrak{q}\frac{c}{t} \ldots = \mathfrak{q}\frac{u \pm at \pm b \pm c \ldots .}{t} - \mathfrak{q}\frac{u \pm \mathfrak{r}\frac{b}{t} \pm \mathfrak{r}\frac{c}{t} \ldots .}{t},$

(58) $a + \mathfrak{q}\frac{b}{t} = \mathfrak{q}\frac{at+b}{t},$

(59) $a - \mathfrak{q}\frac{b}{t} = a + \mathfrak{Q}\frac{-b}{t} + 1 = \mathfrak{Q}\frac{(a+1)t-b}{t} = \mathfrak{q}\frac{(a+1)t-(b+1)}{t}.$

Sezt man in den Gleichungen (48) und (55) $a \mp b$ für a, so übergehen sie in

(60) $\mathfrak{q}\frac{a}{t} \pm \mathfrak{q}\frac{b}{t} = \mathfrak{q}\frac{a \pm b \mp \mathfrak{r}\frac{b}{t}}{t},$

oder wenn man die Gleichung (10) beachtet, in

(61) $\mathfrak{q}\frac{a}{t} \pm \mathfrak{q}\frac{b}{t} = \mathfrak{q}\frac{a \pm (b+1) \mp \mathfrak{R}\frac{b+1}{t}}{t}.$

Eben so findet man, wenn man auf die Gleichung (19) Rücksicht nimmt,

$$\mathfrak{q}\frac{a}{t} - \mathfrak{q}\frac{b}{t} = \mathfrak{q}\frac{-b-1}{t} + 1 + \mathfrak{q}\frac{a}{t},$$

also nach der Gleichung (58)

$$= \mathfrak{q}\frac{t-b-1}{t} + \mathfrak{q}\frac{a}{t},$$

daher nach den Gleichungen (60) und (61)

(62) $$\mathfrak{q}\frac{a}{t} - \mathfrak{q}\frac{b}{t} = \mathfrak{q}\frac{a - b + t - 1 - \mathfrak{r}\frac{a}{t}}{t}$$
$$= \mathfrak{q}\frac{a - b + t - \mathfrak{R}\frac{a+1}{t}}{t} = \mathfrak{q}\frac{a - b + \mathfrak{r}\frac{-a-1}{t}}{t}.$$

Bei jedem solchen Unterschiede von Quotis kann man auch beide Dividende um ein beliebiges Vielfaches des gemeinsamen Theilers vermehren oder vermindern; denn es ist

$$\mathfrak{q}\frac{a}{t} - \mathfrak{q}\frac{b}{t} = \mathfrak{q}\frac{a}{t} \pm n - \left(\mathfrak{q}\frac{b}{t} \pm n\right) = \mathfrak{q}\frac{a \pm nt}{t} - \mathfrak{q}\frac{b \pm nt}{t}.$$

2. Sollten die Quoti verschiedene Theiler besizen, so bringt man sie, nach (35) oder (37), wie Quotienten oder Brüche vorerst auf einerlei Theiler und hält sich dann an die eben ertheilten Vorschriften.

So ist z. B.

$$a - \mathfrak{q}\frac{b}{m} - \mathfrak{q}\frac{c}{p} = a - \mathfrak{q}\frac{bp}{mp} - \mathfrak{q}\frac{cm}{mp}; \text{ nach (59)}$$
$$= \mathfrak{q}\frac{(a+1)\,mp - (bp+1)}{mp} - \mathfrak{q}\frac{cm}{mp}; \text{ nach (60)}$$
$$= \mathfrak{q}\frac{mpa - pb - mc + mp - 1 + \mathfrak{r}\frac{mc}{mp}}{mp}; \text{ endlich nach (36)}$$

$$a - \mathfrak{q}\frac{b}{m} - \mathfrak{q}\frac{c}{p} = \mathfrak{q}\frac{mpa - pb - mc + mp - 1 + m\,\mathfrak{r}\frac{c}{p}}{mp}.$$

3. Sucht man die Summe oder den Unterschied der Reste $r\frac{a}{t}$ und $r\frac{b}{t}$, so findet man

$$r\tfrac{a}{t} \pm r\tfrac{b}{t} = a - t\,q\tfrac{a}{t} \pm b \mp t\,q\tfrac{b}{t}$$
$$= a \pm b - t\cdot\left(q\tfrac{a}{t} \pm q\tfrac{b}{t}\right),$$

folglich vermöge Gleichung (60)

$$(63)\qquad r\tfrac{a}{t} \pm r\tfrac{b}{t} = a \pm b - t\,q\frac{a \pm b \mp r\frac{b}{t}}{t}.$$

In gleicher Weise ergibt sich

$$(64)\qquad R\tfrac{a}{t} \pm R\tfrac{b}{t} = a \pm b - t\,Q\frac{a \pm b \mp R\frac{b}{t}}{t}.$$

XVI.

Differenzen der Functionen.

Jede allgemeine Zahl, welche in einerlei Untersuchung verschiedene besondere Zahlen vorzustellen vermag, wird **veränderlich**, und falls sie in einer Untersuchung stets dieselbe Zahl vorstellen sollte, **beständig** genannt

Sehr oft stehen allgemeine Zahlen mit einander in einem solchen Zusammenhange, daß, während einige völlig beliebige Werthe annehmen, die übrigen nur gewisse Werthe erhalten können; sie heißen dann **gleichzeitig veränderliche**, und insbesondere die ersteren **frei**, die letzteren **abhängig veränderliche Zahlen**, oder erstere die **Gründveränderlichen** und letztere ihre **Functionen**. So ist jeder allgemeine Rechnungsausdruck eine Function aller in ihm vorkommenden allgemeinen Zahlen.

Von den mancherlei Eigenschaften der Veränderlichen und ihrer Functionen interessiren am meisten die **Differenzen** (Unterschiede) oder **Aenderungen** derselben, nemlich die Unterschiede ihrer Werthe, wenn man eine, einige oder alle Veränderlichen um Gegebenes ändert, und von jedem solchen **späteren** Werthe den **früheren** oder ursprünglichen abzieht. Eine solche Differenz einer Veränderlichen oder Function heißt eine **Zunahme** oder ein **Wachsthum** (incrementum), wenn sie positiv, dagegen eine **Abnahme** (decrementum), wenn sie negativ ausfällt. Auch nennt man sie im algebraischen Sinne durchgehends eine Zunahme, wofern man negative Zunahmen für eigentliche Abnahmen ansieht.

Die Aenderung einer allgemeinen Zahl bezeichnet man, indem man ihrem Zeichen den Buchstaben Δ vorschreibt; z. B. durch Δx die Aenderung oder Differenz der Zahl x.

Aendert ſich oder wächſt demnach eine Zahl x um ihre Differenz Δx, ſo iſt ihr nachfolgender oder ſpäterer Werth $x + \Delta x$.

Aus den Lehren über die Aenderungen der veränderlichen Zahlen, Rechnungsausdrücke oder Functionen heben wir nur die folgenden heraus.

1. Bleiben ſich zwei veränderliche Zahlen ſtets gleich, ſo ſind auch ihre Aenderungen gleich.

Denn ſind die veränderlichen Zahlen u und v, wie ſie ſich auch immer ändern mögen, ſtets gleich; ſo müſſen ſie auch noch einander gleich ſein, wenn ſie ſich um Δu und Δv in die Werthe $u + \Delta u$ und $v + \Delta v$ abändern. Man hat demnach nicht nur $u = v$, ſondern auch $u + \Delta u = v + \Delta v$, folglich auch $\Delta u = \Delta v$.

2. Bleiben zwei veränderliche Zahlen einander ſtets congruent nach einem Modul, ſo ſind auch ihre Aenderungen nach dieſem Modul congruent.

Denn ſind die veränderlichen Zahlen u und v, wie ſie ſich auch ändern mögen, immer nach demſelben Modul m congruent, ſo müſſen ſie auch noch, wenn ſie ſich um Δu und Δv in $u + \Delta u$ und $v + \Delta v$ verändern, congruent ſein. Man hat demnach nicht nur $u \equiv v$, mod m, ſondern auch $u + \Delta u \equiv v + \Delta v$, mod m; daher auch noch $\Delta u \equiv \Delta v$, mod m.

3. Die Aenderung einer algebraiſchen Summe iſt die algebraiſche Summe der Aenderungen ihrer einzelnen Summanden.

Seien nemlich u, v, w, ... theils poſitive, theils negative veränderliche Zahlen, und ihre algebraiſche Summe $u + v + w + \ldots$. Wachſen jene um die, theils poſitiven, theils negativen Differenzen $\Delta u, \Delta v, \Delta w, \ldots$ zu den Werthen $u + \Delta u$, $v + \Delta v$, $w + \Delta w, \ldots$ an; ſo übergeht jene Summe in $u + \Delta u + v + \Delta v + w + \Delta w + \ldots$; mithin beträgt die Aenderung dieſer Summe

$$\begin{aligned}\Delta(u + v + w + \ldots) &= (u + \Delta u + v + \Delta v + w + \Delta w + \ldots) \\ &\quad - (u + v + w + \ldots) \\ &= \Delta u + \Delta v + \Delta w + \ldots\end{aligned}$$

4. Die Aenderung einer beſtändigen Zahl iſt Null.

Denn iſt a eine beſtändige, u eine veränderliche Zahl, die Summe beider $u + a$, und ändert ſich u um Δu in $u + \Delta u$, alſo die Summe in $u + \Delta u + a$ ab; ſo iſt die Aenderung derſelben Summe

$$\Delta(u + a) = u + \Delta u + a - (u + a) = \Delta u.$$

Die nemliche Aenderung betrüge aber nach dem vorhergehenden Saze

$$\Delta(u + a) = \Delta u + \Delta a;$$

mithin muß man $\Delta a = 0$ erachten.

5. Die Aenderung des Productes einer beständigen Zahl in eine veränderliche ist das Product des beständigen Factors in die Aenderung des veränderlichen.

Denn unter den eben gemachten Voraussezungen ändert sich das Product au in $a(u+\Delta u)$ ab, daher beträgt seine Aenderung

$$\Delta(au) = a(u+\Delta u) - au = a\Delta u.$$

6. Aendert sich in einem gewöhnlichen Quotus $\text{q}\frac{u}{m}$ blos der Dividend u in $u+\Delta u$, also der Quotus selbst in $\text{q}\frac{u+\Delta u}{m}$ ab, so beträgt die Aenderung des gewöhnlichen Quotus

$$\Delta\,\text{q}\tfrac{u}{m} = \text{q}\tfrac{u+\Delta u}{m} - \text{q}\tfrac{u}{m},$$

folglich nach Gleichung (48) oder (60)

$$(65)\qquad \Delta\,\text{q}\tfrac{u}{m} = \text{q}\frac{\Delta u + \text{r}\frac{u}{m}}{m}$$

oder vermöge Gleichung (43)

$$(66)\qquad \Delta\,\text{q}\tfrac{u}{m} = \text{q}\tfrac{\Delta u}{m} + \text{q}\frac{\text{r}\frac{u}{m} + \text{r}\frac{\Delta u}{m}}{m}.$$

Nun ist aber $\text{r}\frac{u}{m} + \text{r}\frac{\Delta u}{m} = (0, 1, \ldots m-1) + (0, 1, \ldots m-1)$

$$= 0, 1, \ldots 2m-2,$$

folglich $\text{q}\frac{\text{r}\frac{u}{m} + \text{r}\frac{\Delta u}{m}}{m} = 0, 1;$

daher

$$(67)\qquad \Delta\,\text{q}\tfrac{u}{m} = \text{q}\tfrac{\Delta u}{m} \text{ oder } = \text{q}\tfrac{\Delta u}{m} + 1.$$

Z. B. Es ist $\text{q}\frac{538}{4} = 134$, $\text{r}\frac{538}{4} = 2$; wächst nun $u = 538$ um $217 = \Delta u$, so wächst der Quotus um $\Delta\,\text{q}\frac{538}{4} = \text{q}\frac{217+2}{4} = \text{q}\frac{219}{4} = 54$. In der That ist $\text{q}\frac{538+217}{4} = \text{q}\frac{755}{4} = 188 = 134 + 54$.

Auf dieselbe Weise findet man die Aenderung des außerordentlichen Quotus

$$(68)\qquad \Delta\,\text{Q}\tfrac{u}{m} = \text{Q}\frac{\Delta u + \text{R}\frac{u}{m}}{m} = \text{Q}\tfrac{\Delta u}{m} + \text{Q}\frac{\text{R}\frac{n}{m} + \text{R}\frac{\Delta u}{m}}{m}$$

$$= \text{Q}\tfrac{\Delta u}{m} \text{ oder } \text{Q}\tfrac{\Delta u}{m} + 1.$$

7. Aendert sich in einem gewöhnlichen Divisionsreste $\text{r}\frac{u}{m}$ blos der Dividend u in $u+\Delta u$, also der Rest selbst in $\text{r}\frac{u+\Delta u}{m}$ ab; so ist die Aenderung des gewöhnlichen Restes

$$\Delta \mathfrak{r}\tfrac{u}{m} = \mathfrak{r}\tfrac{u+\Delta u}{m} - \mathfrak{r}\tfrac{u}{m},$$

daher eben so wie jeder der beiden Reste kleiner als der Theiler. Da nun nach dieser Gleichung, vermöge III, 1,

$$\Delta \mathfrak{r}\tfrac{u}{m} \equiv u + \Delta u - u \equiv \Delta u, \text{ mod } m,$$

so muß, vermöge Gleichung (32), $\Delta \mathfrak{r}\frac{u}{m}$ entweder der kleinste positive oder der kleinste negative Rest von Δu nach dem Theiler m, mithin

(69) $\Delta \mathfrak{r}\frac{u}{m} \equiv \Delta u, \text{ mod } m = \pm \mathfrak{r}\frac{\pm \Delta u}{m}$, nemlich entweder $= \mathfrak{r}\frac{\Delta u}{m}$

$$\text{oder} = -\mathfrak{r}\tfrac{-\Delta u}{m} = -\left(m - \mathfrak{R}\tfrac{\Delta u}{m}\right)$$

sein.

Noch deutlicher ersieht man dies daraus, daß in der allgemeinsten Form, vermöge Gleichung (3) und (65),

$$\Delta \mathfrak{r}\tfrac{u}{m} = \Delta u - m\,\mathfrak{q}\frac{\Delta u + \mathfrak{r}\frac{u}{m}}{m} = \Delta u \pm pm - m\,\mathfrak{q}\frac{\Delta u \pm pm + \mathfrak{r}\frac{u}{m}}{m}$$

$$= \pm \mathfrak{r}\tfrac{\pm \Delta u}{m} - m\,\mathfrak{q}\frac{\pm \mathfrak{r}\frac{\pm \Delta u}{m} + \mathfrak{r}\frac{u}{m}}{m}$$

sein muß; indem man Δu um ein beliebiges Vielfaches von dem Theiler m vermehren, oder Δu durch einen beliebigen seiner Reste nach demselben Theiler ersezen darf. (XI, 3 und XV, 1.).

Ist $\mathfrak{r}\frac{\Delta u}{m} = 0$, d. h. der Zuwachs Δu durch m theilbar, so ist auch $\mathfrak{r}\frac{-\Delta u}{m} = 0$, also ebenfalls $\Delta \mathfrak{r}\frac{u}{m} = 0$, übereinstimmend mit XI, 3.

Auf gleiche Weise findet man die Aenderung eines außerordentlichen Restes

(70) $\Delta \mathfrak{R}\frac{u}{m} \equiv \Delta u, \text{ mod } m = \pm \mathfrak{R}\frac{\pm \Delta u}{m}$, nemlich entweder $= \mathfrak{R}\frac{\Delta u}{m}$

oder $= -\mathfrak{R}\tfrac{-\Delta u}{m} = -\left(m - \mathfrak{r}\tfrac{\Delta u}{m}\right)$, oder $\Delta \mathfrak{R}\tfrac{u}{m} = \Delta u - m\,\mathfrak{Q}\frac{\Delta u + \mathfrak{R}\frac{u}{m}}{m}$.

Die Aenderungen der Reste richten sich demnach blos nach den Resten der Aenderungen der Dividende; weil man (vermöge XI, 3) Δu durch einen ihrer Reste ersezen kann. Läßt man also den Dividend u nach der natürlichen Reihe der Zahlen wachsen, so müssen seine Reste wenigstens nach je m Gliedern in der nemlichen Ordnung wiederkehren.

8. Erforscht man die gleichzeitigen Aenderungen des Quotus und Restes, wenn der Dividend u um Δu sich verändert; so hat man, wegen der Gleichung

$$u = m\,\mathfrak{q}\tfrac{u}{m} + \mathfrak{r}\tfrac{u}{m} = m\,\mathfrak{Q}\tfrac{u}{m} + \mathfrak{R}\tfrac{u}{m}$$

(nach dem 1. und 3. Satze) die Aenderung

$$\Delta u = m\,\Delta\mathfrak{q}\tfrac{u}{m} + \Delta\mathfrak{r}\tfrac{u}{m} = m\,\Delta\mathfrak{Q}\tfrac{u}{m} + \Delta\mathfrak{R}\tfrac{u}{m}.$$

Vermöge VI, Anmerkung 2 sind die gewöhnlichen und außerordentlichen Theilungsergebnisse, also auch ihre Aenderungen, gleich, wenn weder u noch Δu durch m theilbar sind, und die Aenderungen sind allein gleich, wenn Δu durch m theilbar ist. Nur wenn u theilbar und Δu untheilbar ist, hat man

$$\Delta\mathfrak{r}\tfrac{u}{m} = \mathfrak{r}\tfrac{u+\Delta u}{m} - \mathfrak{r}\tfrac{u}{m} = \mathfrak{r}\tfrac{\Delta u}{m}, \text{ dagegen}$$

$$\Delta\mathfrak{R}\tfrac{u}{m} = \mathfrak{R}\tfrac{u+\Delta u}{m} - \mathfrak{R}\tfrac{u}{m} = \mathfrak{R}\tfrac{\Delta u}{m} - m = -\mathfrak{r}\tfrac{-\Delta u}{m},$$

$$\text{also } \Delta\mathfrak{R}\tfrac{u}{m} = \Delta\mathfrak{r}\tfrac{u}{m} - m, \text{ und } \Delta\mathfrak{Q}\tfrac{u}{m} = \Delta\mathfrak{q}\tfrac{u}{m} + 1.$$

Somit genügt es, nur die Gleichung

$$\Delta u = m\,\Delta\mathfrak{q}\tfrac{u}{m} + \Delta\mathfrak{r}\tfrac{u}{m}$$

zu untersuchen.

Aus ihr findet man sogleich vermöge Gleichung (23)

$$(71)\qquad \Delta\mathfrak{q}\tfrac{u}{m} = \pm\mathfrak{q}\tfrac{\pm\Delta u}{m}, \qquad \Delta\mathfrak{r}\tfrac{u}{m} = \pm\mathfrak{r}\tfrac{\pm\Delta u}{m},$$

also, wenn der Rest wachsen soll,

$$(72)\qquad \Delta\mathfrak{q}\tfrac{u}{m} = \mathfrak{q}\tfrac{\Delta u}{m} = -\left(\mathfrak{Q}\tfrac{-\Delta u}{m} + 1\right), \qquad \Delta\mathfrak{r}\tfrac{u}{m} = \mathfrak{r}\tfrac{\Delta u}{m},$$

dagegen, wenn der Rest abnehmen soll,

$$(73)\qquad \Delta\mathfrak{q}\tfrac{u}{m} = -\mathfrak{q}\tfrac{-\Delta u}{m} = \mathfrak{Q}\tfrac{\Delta u}{m} + 1, \qquad \Delta\mathfrak{r}\tfrac{u}{m} = -\mathfrak{r}\tfrac{-\Delta u}{m}.$$

XVII.

Verschiedentliches Zählen der Glieder einer Reihe.

1. Fortlaufendes Zählen. Die Glieder einer Reihe zählt man gewöhnlich von einem gewissen, gewählten oder sonst wie festgesetzten Gliede ausgehend, in einer bestimmten Richtung nach der natürlichen Reihe der Ordnungszahlen fortschreitend oder fortlaufend, indem man, wie sonst üblich, jenes Glied das erste, das folgende das zweite, und die weiteren der Ordnung nach das dritte, vierte, u. s. f. nennt. Die bei einer fortlaufenden Zählung auf ein Glied treffende Ordnungszahl pflegt man im gewöhnlichen Sprachgebrauche die Nummer oder Zahl, in der Combinationslehre den Stellenzeiger (index) des Gliedes zu nennen.

Man ist jedoch auch sehr oft veranlaßt, die vor jenem hervorgehobenen ersten Gliede befindlichen Glieder der Reihe nach entgegengesetzter Richtung, also nicht mehr wie früher, fortschreitend, sondern rückschreitend zu zählen. Dann zählt man diese vorausgehenden Glieder gewöhnlich eben-

falls nach der natürlichen Reihe der Ordnungszahlen fortlaufend als das erste, zweite, dritte, vierte, u. s. f. vor jenem ausgezeichneten. Allein, wollte man hier die Stellenzeiger der vorausgehenden Glieder, wegen des Gegensazes der Richtung des Zählens, jenen ursprünglich angenommenen, positiven Stellenzeigern der nachfolgenden Glieder entgegensezen, folglich negativ in Rechnung bringen; so würden sämmtliche Stellenzeiger die Reihe

$$\ldots . -4, -3, -2, -1; +1, +2, +3, +4, \ldots .$$

bilden; in welcher jedoch bei den beiden benachbarten Gliedern -1 und $+1$, bei dem Uebergange vom Negativen zum Positiven, das sonst überall in der Reihe herrschende Gesez, »daß jedes folgende Glied aus dem vorhergehenden erhalten wird, indem man diesem $+1$ zugibt,« unterbrochen wird, und welchem Gesezе gemäß zwischen jenen zwei Gliedern die Null fehlt.

2. Algebraisches Zählen. Demnach erheischt die Lehre von dem algebraischen Gegensaze der Größen, daß man bei dem vor- und rückschreitenden algebraischen Zählen der Glieder einer Reihe irgend ein Glied, als das Ausgangs- oder Anfangsglied, sowohl von den nachfolgenden, als von den vorausgehenden Gliedern unterscheide, und ihm die Nummer 0 beilege, — weßwegen man es auch das nullte nennen mag —; dann den ihm folgenden Gliedern der Ordnung nach die positiven Nummern 1, 2, 3, 4, ... den vor ihm hergehenden Gliedern dagegen die negativen Nummern $-1, -2, -3, -4, \ldots .$ zuweise; so daß sämmtliche Nummern in der stetigen natürlichen Reihe der positiven und negativen Zahlen

$$\ldots . -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots .$$

auf einander folgen.

Vergleicht man obiges gewöhnliche und dieses algebraische rückschreitende Zählen der Glieder vor dem hervorgehobenen ersten Gliede; so ersieht man, daß das 1^{ste}, 2^{te}, 3^{te}, ... n^{te}, $n+1^{\text{te}}$, ... Glied vor jenem ausgezeichneten ersten Gliede,
das 0^{te}, -1^{te}, -2^{te}, ... $-(n-1)^{\text{te}}$, $-n^{\text{te}}$, ... Glied
der Reihe ist; wornach man also hier immer um eins weniger als dort zählt.

Bei der algebraischen Zählung der Glieder einer Reihe gibt der Zahlwerth der Nummer jedes Gliedes zu erkennen, wie weit dieses Glied von dem Anfangsgliede (dem nullten) absteht; ihr Vorzeichen, + und —, aber, ob dasselbe dem Anfangsgliede nachfolgt oder vorgeht; mithin die algebraische Nummer selbst, das wie vielte jenes Glied nach oder vor dem Anfangsgliede in der Reihe ist.

Ueberhaupt, wenn man von dem Stellenzeiger n eines Gliedes A einer Reihe den Stellenzeiger p eines anderen Gliedes B abzieht; so gibt der Unterschied der Stellenzeiger $n - p$ den Abstand des ersteren Gliedes A hinter

dem lezteren **B**, oder er läßt erkennen, das wie vielte jenes Glied **A** hinter dieſem **B** iſt, nemlich wenn der Unterſchied poſitiv ausfällt, daß jenes wirklich hinter, dagegen wenn er negativ ausfällt, daß es nicht hinter, ſondern im Gegentheil vor dem anderen ſtehe. So iſt z. B. das $60^{ſte}$ Glied einer Reihe nach dem 17^{ten} das $60 - 17 = 43^{ſte}$, und hinter dem -17^{ten} das $60 - (-17) = 60 + 17 = 77^{ſte}$; dagegen iſt es hinter dem $80^{ſten}$ das $60 - 80 = -20^{ſte}$, d. h. es iſt das $20^{ſte}$ vor dem $80^{ſten}$.

3. Vergleichung fortlaufender Zählweiſen. Sehr oft zählt man die Glieder derſelben Reihe zwar nach einerlei Richtung und algebraiſch, aber von verſchiedenen Anfangsgliedern ausgehend; ſo daß ein und dasſelbe Glied **A** der Reihe nach der einen Zählung das n^{te} und nach der andern das ν^{te} wird. Soll nun ein anderes Glied **B** dieſer Reihe nach der erſteren Art zu zählen das p^{te}, und nach der zweiten das π^{te} ſein; ſo iſt jenes Glied **A** hinter dieſem **B** das $n - p^{te}$ vermöge der erſten, und

das $\nu - \pi^{te}$ vermöge der zweiten Zählweiſe;

folglich, da der Abſtand derſelben zwei Glieder bei jeglicher Zählung ſich gleich bleibt,

$$n - p = \nu - \pi, \tag{74}$$

oder, in wie fern die Nummern der erſten Zählung jenen der zweiten Zählung bei allen Gliedern der Reihe um gleich viel voreilen,

$$n - \nu = p - \pi. \tag{75}$$

Dieſe einander gleichgeltenden Gleichungen bahnen den Uebergang von der einen Zählweiſe zur anderen, da nach ihnen

$$n = \nu + p - \pi \text{ iſt.} \tag{76}$$

XVIII.

Fortſezung.

4. Periodiſches Zählen. Zuweilen zählt man die Glieder einer Reihe nicht in einem Zuge fort, ſondern nachdem man von 1 bis zu einer gewiſſen Zahl t gezählt hat, wieder von vorn, folglich immer nur in ſolchen Abſäzen von 1 bis t. In ſo fern man bei dieſer Zählung die Glieder der Reihe in Abtheilungen, Gruppen oder Partien von gleich vielen, nemlich t, Gliedern abſondert, nennt man eine ſolche Abtheilung eine Periode, und daher das Zählen ſelbſt periodiſch oder wiederkehrend. Dieſes Zählen gebraucht man vorzüglich da, wo den gleichvielten Gliedern der Perioden gemeinſchaftliche Eigenſchaften zukommen, wie bei der Abtheilung der Ziffern einer Zahl in Claſſen, bei den periodiſchen Decimal- und Kettenbrüchen, bei den Quadranten in der Geometrie, bei den Stunden des Tages u. dergl.

5. Vergleichung der wiederkehrenden und fortlaufenden Zählung. Bei dem wiederkehrenden Zählen hat man demnach, zur Feststellung jedes Gliedes in der Reihe, nicht blos die Glieder in jeder einzelnen Periode, sondern auch diese Perioden selbst der Ordnung nach zu zählen, und daher bei der Angabe der Stelle eines Gliedes anzuführen, in der wie vielten Periode, und das wie vielte Glied in dieser — laufenden — Periode es sei. Ist es nun das p^{te} Glied in der π^{ten} Periode, so sind vor dieser Periode $\pi - 1$ andere Perioden, also weil jede Periode t Glieder enthält, $\pi - 1$ Mal $t = (\pi - 1)\,t$ Glieder; daher ist es in der Reihe selbst das

$$n = (\pi - 1)\,t + p^{te} \text{ Glied.} \tag{77}$$

Aus dieser Gleichung findet man umgekehrt, weil p die Nummer eines Gliedes in einer Periode vorstellt, daher nie Null, sondern nur 1, 2, 3, ... t sein kann, durch die außerordentliche Theilung

$$\pi - 1 = \mathfrak{Q}\tfrac{n}{t} = \mathfrak{q}\tfrac{n-1}{t} \tag{78}$$

$$\pi = \mathfrak{Q}\tfrac{n}{t} + 1 = -\mathfrak{q}\tfrac{-n}{t} \tag{79}$$

$$p = \mathfrak{R}\tfrac{n}{t}; \tag{80}$$

nemlich, wenn man nicht fortlaufend, sondern nach tgliedrigen Perioden zählen will, so ist das n^{te} Glied der Reihe das $p = \mathfrak{R}\tfrac{n}{t}^{te}$ Glied hinter der $\pi - 1 = \mathfrak{Q}\tfrac{n}{t}^{ten}$ Periode oder in der $\pi = \mathfrak{Q}\tfrac{n}{t} + 1^{ten}$ Periode.

Sehr oft wird aber auch von den Gliedern einer Reihe nur angegeben, die wie vielten Glieder sie in derlei Perioden sind, ohne Rücksicht, in der wie vielten Periode sie stehen. Dann genügt zur Vergleichung der fortlaufenden Zählung mit der periodischen schon allein die Gleichung

$$p = \mathfrak{R}\tfrac{n}{t} \tag{80}$$

oder die aus ihr, so wie auch aus der Gleichung (77) folgende Congruenz

$$p \equiv n, \bmod t, \tag{81}$$

der zu Folge das n^{te} Glied der Reihe mit dem p^{ten} Gliede einer der tgliedrigen Perioden übereinkommt.

Ist nun noch bekannt, daß bei derselben fortlaufenden Zählweise das N^{te} Glied der Reihe mit dem P^{ten} Gliede einer eben solchen tgliedrigen Periode zusammenfällt, so hat man auch

$$P \equiv N, \bmod t,$$

daher, wenn man diese Congruenz von der vorhergehenden abzieht,

$$p - P \equiv n - N, \bmod t. \tag{82}$$

Von der Giltigkeit dieser Congruenz kann man sich auch durch folgende Betrachtung überzeugen. Treffen bei fortlaufender Zählung das n^{te} und N^{te}

Glied der Reihe auf das p^{te} und P^{te} Glied von tgliedrigen Perioden; so muß sowohl bei dem $n - p^{ten}$, als bei dem $N - P^{ten}$ Gliede der Reihe eine derartige Periode zu Ende laufen, folglich zwischen beiden Gliedern eine Anzahl voller tgliedrigen Perioden stehen. Der Abstand dieser zwei Glieder von einander, das ist der Unterschied ihrer Stellenzeiger $n - p$ und $N - P$, muß demnach ein Vielfaches von der Anzahl t der Glieder einer jeden Periode, daher nach der Erklärung der congruenten Zahlen in Art. II,

(83) $N - P \equiv n - p, \mod t$

sein, woraus man sogleich die vorhergehende Congruenz erhält.

Aus diesen beiden gleichgeltenden Congruenzen läßt sich leicht finden, das wie vielte (p^{te}) Glied in einer tgliedrigen Periode das n^{te} Glied der Reihe ist; wenn bekannt ist, daß das N^{te} Glied der Reihe mit dem P^{ten} einer solchen Periode zusammentrifft. Denn man erhält

(84) $p \equiv P + n - N, \mod t,$

folglich, weil p von 1 bis t reicht,

(85) $p = \mathfrak{R}\frac{P+n-N}{t}.$

Schließt sich mit dem N^{ten} Gliede der Reihe eine Periode, so ist $P = t$, daher (86) $p \equiv n - N, \mod t$

(87) $p = \mathfrak{R}\frac{n-N}{t}.$

Dabei ist nicht einmal die Kenntniß der Nummern n und N der einzelnen Glieder der Reihe selbst erforderlich, da es schon hinreicht, nur ihren Abstand $n - N$ von einander zu kennen.

Hebt eine Periode mit dem ersten Gliede der Reihe an, so ist $P = N = 1$, daher wie oben (80) $p = \mathfrak{R}\frac{n}{t}.$

XIX.

Auflösung von Congruenzen des ersten Grades.

Die Congruenzen des ersten Grades mit einer unbekannten Zahl sind in der allgemeinen Form

(88) $kx \equiv a, \mod m$

begriffen, wenn x die zu suchende Zahl vorstellt. Soll man diese unbekannte Zahl x bestimmen, und dadurch die Congruenz auflösen; so bemerke man, daß der Unterschied der zwei congruenten Zahlen kx und a ein Vielfaches, etwa das yfache, des Moduls, also

(89) $kx + my = a$

sein muß, wofern auch die Zahl y noch unbestimmt oder unbekannt ist. Diese unbestimmte Gleichung mit zwei Unbekannten x und y gibt auch noch die Congruenz

(90) $my \equiv a, \mod k.$

Wir werden daher beide Congruenzen (88) und (90) mit einem Male auflösen, sobald wir nur die Gleichung (89) auflösen.

Zu diesem Zwecke theilen wir diese Gleichung durch m und x, wodurch wir

$$\frac{kx+my}{mx} = \frac{k}{m} + \frac{y}{x} = \frac{a}{mx}$$

erhalten. Zugleich bemerken wir, erstens: »daß der Unterschied zweier nach einander folgenden Näherungsbrüche eines Kettenbruches gleich ist ± 1, getheilt durch das Product ihrer Nenner,« und zweitens: »daß die unbestimmte Gleichung des ersten Grades (89) nur dann in ganzen Zahlen auflösbar ist, wenn die Coefficienten, k und m, der Unbekannten, x und y, keinen gemeinschaftlichen Theiler besizen, durch den nicht auch das bekannte Glied a theilbar ist.« (III, 11.)

Sei nun der Bruch $\frac{k}{m}$ echt, also $k < m$, wohin wir es in der gegebenen Congruenz (88), vermöge XI, 3, immer leicht bringen können, wenn wir von dem Coefficienten der Unbekannten x den Modul m, so oft als es angeht, weg werfen; dieser Bruch $\frac{k}{m}$ habe, wenn er in einen Kettenbruch verwandelt wird, keinen dem Zähler k und Nenner m gemeinschaftlichen Theiler, der nicht auch dem bekannten Gliede a zukäme, ferner besize er n Theilnenner vor dem lezten, also n Näherungswerthe, und sein n^{ter} Näherungswerth sei der Bruch $\frac{\varkappa}{\mu}$. Dann übersteigt der gegebene Bruch $\frac{k}{m}$ seinen lezten Näherungsbruch $\frac{\varkappa}{\mu}$ um den Unterschied

$$\frac{k}{m} - \frac{\varkappa}{\mu} = \frac{k\mu - m\varkappa}{m\mu} = \frac{(-1)^n}{m\mu},$$

welcher positiv oder negativ ausfällt, je nachdem n eine gerade oder ungerade Anzahl ist.

Theilen wir jezt durch diese Gleichung die vorhergehende, so erhalten wir

$$\frac{kx+my}{k\mu - m\varkappa} = (-1)^n a,$$

daraus ferner $k(x-(-1)^n\mu a) = m(-y-(-1)^n\varkappa a)$

und $$\frac{x-(-1)^n\mu a}{-y-(-1)^n\varkappa a} = \frac{m}{k}.$$

Sollen aber diese zwei gewöhnlichen Brüche einander gleich sein, so müssen der Zähler und Nenner des einen Gleichvielfache vom Zähler und Nenner des anderen sein; also wenn z den willkürlichen Multiplicator vorstellt,

$$x - (-1)^n\mu a = mz$$
$$-y-(-1)^n\varkappa a = kz;$$

und sofort ergeben sich für die unbestimmte Gleichung (89) oder für die ihr gleichgeltenden Congruenzen (88) und (90) die Auflösungen

$$(91) \qquad x = (-1)^n\mu a + mz$$
$$y = (-1)^{n-1}\varkappa a - kz,$$

oder auch (92) $x \equiv (-1)^n \mu a \pmod m$

$$y \equiv (-1)^{n-1} \varkappa a \pmod k.$$

Nehmen wir an, daß in dem besonderen Falle, wo $a = 1$ ist, die Zahlen x und y in ξ und η übergehen, so daß wir eigentlich die Gleichung

(93) $k\xi + m\eta = 1$

oder die Congruenzen

(94) $k\xi \equiv 1 \pmod m$

$$m\eta \equiv 1 \pmod k$$

aufzulösen haben, so finden wir dafür die Auflösungen

(95) $\xi \equiv (-1)^n \mu \pmod m$

$$\eta \equiv (-1)^{n-1} \varkappa \pmod k.$$

Multipliciren wir diese mit a, so erhalten wir

$$a\xi \equiv (-1)^n \mu a \pmod m$$

$$a\eta \equiv (-1)^{n-1} \varkappa a \pmod k;$$

daher wegen der Congruenzen (92), vermöge III, 2, die Auflösungen

(96) $x \equiv a\xi \pmod m$

$$y \equiv a\eta \pmod k,$$

oder, zu Folge der Gleichungen (91),

(97) $x = a\xi + mz$

$$y = a\eta - kz,$$

indem man von den Gleichvielfachen der beiden Coefficienten der Unbekannten das eine addirt, das andere abzieht.

Soll demnach eine Congruenz von der Form

(88) $kx \equiv a \pmod m$

aufgelöst werden, so wird man vorerst an die Stelle des Coefficienten der Unbekannten und anstatt des bekannten Gliedes einen Rest nach dem Modul, am besten den möglich kleinsten, sezen, und durch die etwa erforderliche Zeichenänderung den Coefficienten der Unbekannten wieder positiv herstellen. Ferner sieht man nach, ob der nunmehrige Coefficient und der Modul einen größten gemeinschaftlichen Theiler besizen. Ist dies, und kommt dieser Theiler nicht auch noch dem bekannten Gliede zu, so ist die Congruenz unmöglich; kommt er aber auch diesem zu, so wird man alle drei bekannten Zahlen durch ihren größten gemeinschaftlichen Theiler dividiren. Man wird es demnach nur immer mit Congruenzen von der Form (88) zu thun haben, in denen der Coefficient k positiv, kleiner als der Modul und gegen diesen relativ prim ist. Dann wird man zuvörderst die einfachere Congruenz

(98) $k\xi \equiv 1 \pmod m$ auflösen.

Zu dieſem Zwecke theilt man m durch k auf dieſelbe Weiſe, als wollte man den echten Bruch $\frac{k}{m}$ in einen Kettenbruch verwandeln, und ſucht deſſen lezten Näherungsbruch $\frac{x}{\mu}$. Man ſchreibt nemlich, indem man die gefundenen Quoti oder Theilnenner in umgekehrter Ordnung auffaßt, unter den lezten 1, unter den vorlezten ihn ſelbſt. Aus dieſen zwei Zahlen, und ſo auch aus jeden zwei vor einander hergehenden bereits berechneten, findet man die nächſt voran zu ſtellende, indem man mit dem unmittelbar vorhergehenden Quotus die lezt angeſchriebene (vorderſte) Zahl multiplicirt und die vorlezt geſchriebene hinzu addirt, bis auch der erſte Quotus in Rechnung gebracht worden. Dann iſt die lezte auf dieſe Weiſe berechnete Zahl der Nenner μ, die vorlezt berechnete der Zähler x des geſuchten lezten Näherungsbruches.*) Schreibt man nun unter die dem lezten Quotus untergeſezte Zahl 1 das Zeichen +, von da vorwärts ſchreitend unter die Zahlen der zulezt berechneten Reihe abwechſelnd die Zeichen — und +, ſo erhält man auch noch das angemeſſene Zeichen oder den Factor $(-1)^n$ für die vorderſte Zahl μ, wodurch ſie vollſtändig die geforderte Zahl

(99) $\xi \equiv (-1)^n \mu$, mod m wird.

Multiplicirt man endlich dieſe noch mit dem bekannten Gliede a, ſo erhält man die gewünſchte Auflöſung

(100) $x \equiv a\xi$, mod m

oder (101) $x = a\xi + mz$.

Da man gleichzeitig für den Zähler x das entgegengeſezte Zeichen des Nenners μ oder den Factor $(-1)^{n-1}$ erhält, ſo löſt man durch das beſchriebene Verfahren eigentlich mit Einem Schlage beide Congruenzen (94) auf, indem man dafür die Auflöſungen (95) erhält; und darnach ergeben ſich für die allgemeineren Congruenzen (88) und (90) die Auflöſungen (96) oder (97).

1. Beiſpiel. Seien die Congruenzen

$$19\xi \equiv 1, \text{ mod } 28$$

und $$28\eta \equiv 1, \text{ mod } 19$$

aufzulöſen. Hier iſt

1	2	9
28 : 19 : 9 : 1		
3	2	1
+	—	+
ξ	η	

nemlich $1 \cdot 2 + 1 = 3$

daher $\xi \equiv 3$, mod 28

$\eta \equiv -2$, mod 19.

*) Vergleiche Knar, Anfangsgründe der Arithmetik, §. 231; Vega, Vorleſ. über Mathematik, 6. Auflage, herausgegeben von Matzka, §. 108, I.

Daraus folgt für $19x \equiv a$, mod 28

und $28y \equiv a_{,}$, mod 19

$x \equiv 3a$, mod 28 $= 3a + 28z$

$y \equiv -2a$, mod 19 $= -2a - 19z$.

2. Beispiel. Ist die Congruenz

$$268\xi \equiv 1, \text{ mod } 601$$

aufzulösen, so hat man

	2	4	8	8		nemlich
601 :	268 :	65 :	8 :	1	4.	$8 + 1 = 33$
	74	33	8	1	2.	$33 + 8 = 74$
	—	+	—	+		

folglich $\xi = -74$.

XX.

Berechnung der Zahlen aus ihren Resten nach angegebenen Theilern.

Die Congruenzen des ersten Grades vermitteln die Lösung folgender wichtigen Aufgabe:

Man soll alle diejenigen Zahlen bestimmen, welche, durch gegebene Zahlen getheilt, gewisse angewiesene Reste lassen;

Oder: Aus den Resten einer Zahl nach angegebenen Theilern soll man ihren Rest nach dem kleinsten gemeinschaftlichen Vielfachen der Theiler bestimmen.

Hier muß sogleich vor Allem bemerkt werden, daß, falls nach mehreren Theilern derselbe Rest von einer Zahl bleiben sollte, eben dieser Rest auch, vermöge III, 14, nach dem kleinsten gemeinschaftlichen Vielfachen der Theiler entfallen muß; mithin alle jene Theiler sogleich durch ihr kleinstes gemeinschaftliche Vielfache zu ersezen kommen. Suchen wir nun

1. eine Zahl x, welche durch eine Zahl M, oder durch mehrere andere, deren kleinstes gemeinschaftliche Vielfache M ist, (ohne Rest) theilbar ist, und durch eine zweite Zahl m, welche gegen die erstere M relativ prim ist, getheilt einen Rest r gibt.

Nach der ersten Bedingung muß $x \equiv 0$, mod M, also x irgend ein Vielfaches, etwa das ufache, von M, daher $x = Mu$, und nach der anderen $x \equiv r$, mod m sein. Beiden Bedingungen wird entsprochen, wenn $Mu \equiv r$, mod m ist.

Man wird daher, nach Art. XIX, die kleinste Zahl ξ suchen, für welche

(102) $M\xi \equiv 1$, mod m ist, und

$$u \equiv \xi r, \mod m \quad \text{oder} \quad u = \xi r + mz$$

ſezen, wo z ein willkürlicher Multiplicator iſt. Dann hat man die geforderte Zahl x

$$x = M\xi r + Mm.z \tag{103}$$

oder

$$x \equiv M\xi r, \mod Mm, \tag{104}$$

$$\equiv \mp\frac{M\xi r}{Mm} \equiv M \mp \frac{\xi r}{m}$$

und die kleinſte poſitive ſolche Zahl

$$x = \mp\frac{M\xi r}{Mm} = M \mp \frac{\xi r}{m}. \tag{105}$$

Z. B. Man beſtimme jene Zahlen, die durch 3, 4, 5, 7, oder durch 15 und 28, oder durch 15. 28 = 420 = M theilbar ſind, und durch 19 = m getheilt den Reſt a = r geben.

Hiefür hat man $420\xi \equiv 1, \mod 19$ oder $2\xi \equiv 1, \mod 19$,

daher

$$\begin{array}{rrrr} & 9 & 2 & \\ 19 & : & 2 & : 1 \\ & 9 & 1 & \\ & - & + & \end{array}$$

und $\xi \equiv -9 \equiv 10, \mod 19.$

Daraus folgt demnach $x \equiv 420 \mp\frac{-9a}{19} \equiv 420 \mp\frac{10a}{19}, \mod 7980.$

Insbeſondere wird für

den Reſt	a =	1,	2,	3, ...
die Zahl	x ≡	4200,	420,	4620, ..., mod 7980.

Betrachten wir ferner

2. den Fall, wo jene Zahlen x zu beſtimmen ſind, welche durch die Theiler oder Moduln m, m′, m″, ..., deren jede zwei unter ſich Primzahlen ſind, getheilt, die Reſte r, r′, r″, ... laſſen.

Da läßt ſich leicht erkennen, daß die geforderte Zahl x enthalten müſſe: erſtlich ein Glied, welches durch alle Theiler m, m′, m″, ... folglich auch, weil ſie paarweiſe relativ prim ſind, d. h. weil keine zwei einen von 1 verſchiedenen gemeinſchaftlichen Theiler beſizen, durch ihr Product mm′m″. . . = μ theilbar iſt, alſo durch μw ausgedrückt werden kann, wenn w einen willkürlichen Multiplicator vorſtellt;

und dann noch ſo viele und ſolche Glieder u, u′, u″,...., als wie viel Theiler angegeben ſind, und von denen jedes nur durch den gleichvielten Theiler getheilt, den dieſem Theiler entſprechenden Reſt der Zahl x gibt, durch alle übrigen Theiler aber, alſo auch durch ihr Product, untheilbar iſt.

Man kann demnach ſezen

$$x = \mu w + u + u' + u'' + \ldots. \tag{106}$$

und die Producte der Theiler m, m′, m″, ..., wenn man einen nach dem andern ausläßt, am einfachſten durch die ganzzahligen Quotienten

$$\frac{\mu}{m}, \frac{\mu}{m'}, \frac{\mu}{m''}, \ldots.$$

darſtellen. Dann wird man die Glieder u, u′, u″, ... gemäß der über ſie ausgeſprochenen Bedingungen,

$$u \equiv o, \mod \frac{\mu}{m}; \quad u \equiv r, \mod m$$

$$u' \equiv o, \mod \frac{\mu}{m'}; \quad u' \equiv r', \mod m'$$

$$u'' \equiv o, \mod \frac{\mu}{m''}; \quad u'' \equiv r'', \mod m''$$

. . . . . .

beſtimmen, indem man vorerſt die kleinſten möglichen Zahlen $\xi, \xi', \xi'', \ldots.$ ſucht, welche den Congruenzen

$$\frac{\mu}{m} \xi \equiv 1, \mod m \tag{107}$$

$$\frac{\mu}{m'} \xi' \equiv 1, \mod m'$$

$$\frac{\mu}{m''} \xi'' \equiv 1, \mod m''$$

. . . . . .

genügen, und nachher dieſe Glieder u, u′, u″, ... ſelbſt, als die kleinſten Zahlen, welche die Congruenzen

$$u \equiv \frac{\mu}{m} \xi\, r, \mod \mu \equiv \frac{\mu}{m} \mp \frac{\xi r}{m} \tag{108}$$

$$u' \equiv \frac{\mu}{m'} \xi'\, r', \mod \mu \equiv \frac{\mu}{m'} \mp \frac{\xi' r'}{m'}$$

$$u'' \equiv \frac{\mu}{m''} \xi''\, r'', \mod \mu \equiv \frac{\mu}{m''} \mp \frac{\xi'' r''}{m''}$$

. . . . . .

befriedigen.

Sofort iſt eine ſolche Zahl, wie man fordert,

$$x = \mu w + u + u' + u'' + \ldots \quad \text{oder} \tag{106}$$

$$x \equiv u + u' + u'' + \ldots, \mod \mu$$

$$\equiv \mp \frac{u + u' + u'' + \ldots}{\mu}, \mod \mu.$$

Beiſpiel. Man ſuche den allgemeinen Ausdruck der Zahlen, welche der Ordnung nach durch 28, 19, 15 getheilt, die Reſte r, r′, r″ laſſen.

Hier iſt $m = 28, \; m' = 19, \; m'' = 15$

$\mu = 28 . 19 . 15 = 7980,$

$\frac{\mu}{m} = 19.\ 15 = 285$, $\frac{\mu}{m'} = 15.\ 28 = 420$, $\frac{\mu}{m''} = 28.\ 19 = 532$.

daher
$$1 \equiv 285\,\xi, \bmod 28 \equiv 5\,\xi \quad \Big| \quad \xi \equiv -11$$
$$1 \equiv 420\,\xi', \bmod 19 \equiv 2\,\xi' \quad \Big| \quad \xi' \equiv -9$$
$$1 \equiv 532\,\xi'', \bmod 15 \equiv 7\,\xi'' \quad \Big| \quad \xi'' \equiv -2$$

und (109) $x \equiv 285\, r\frac{-11r}{28} + 420\, r\frac{-9r'}{19} + 532\, r\frac{-2r''}{15}$, mod 7980

oder
$$x \equiv -(3135\,r + 3780\,r' + 1064\,r'')$$
$$\equiv 4845\,r + 4200\,r' + 6916\,r'', \bmod 7980.$$

Insbesondere erhält man für die Reste

$$r = 10,\ r' = 2,\ r'' = 4$$

die Zahl $x \equiv 285 \cdot r\frac{-110}{28} + 420\, r\frac{-18}{19} + 532\, r\frac{-8}{15}$, mod 7980

$$\equiv 285 \cdot 2 + 420 \cdot 1 + 532 \cdot 7$$
$$\equiv 570 + 420 + 3724, \text{ oder}$$

(110) $x \equiv 4714$, mod 7980.

Höchst beachtenswerth ist der **besondere Fall**, wo nur nach zwei Theilern m und m', welche Primzahlen unter sich sind, die Reste r und r' angegeben werden. Da ist $\mu = mm'$, $\frac{\mu}{m} = m'$, $\frac{\mu}{m'} = m$; daher hat man die beiden Congruenzen

(111)
$$m'\xi \equiv 1, \bmod m$$
$$m\xi' \equiv 1, \bmod m'$$

aufzulösen, wobei man das im Art. XIX. (98) bis (101) erörterte Verfahren in Anwendung bringt. Dann findet man

$$u \equiv m'\xi r, \bmod mm' \equiv m'\, r\frac{\xi r}{m}$$

$$u' \equiv m\xi' r', \bmod mm' \equiv m\, r\frac{\xi' r'}{m'},$$

und sofort die verlangte Zahl

(112)
$$x \equiv m'\xi r + m\xi' r', \bmod mm'$$
$$\equiv m'\, r\frac{\xi r}{m} + m\, r\frac{\xi' r'}{m'}, \bmod mm'.$$

Z. B. Der allgemeine Ausdruck der Zahlen, welche durch 28 und 19 getheilt, die Reste r und r' geben, ist aufzustellen. Hier ist $m = 28$, $m' = 19$, $mm' = 532$.

Sucht man nun ξ und ξ' aus $19\,\xi \equiv 1$, mod 28
und $28\,\xi' \equiv 1$, mod 19, so erhält man, nach XIX. Beisp. 1, $\xi \equiv 3$, $\xi' \equiv -2$, daher wird der geforderte Ausdruck

(113) $x \equiv 19\, r\frac{3r}{28} + 28\, r\frac{-2r'}{19} \equiv 57r - 56r'$, mod 532.

Mittels dieſes einfachen Verfahrens kann man die Zahlen, welche die nach mehreren Theilern angegebenen Reſte laſſen, beſtimmen, oder aus den Reſten einer Zahl nach mehreren Theilern ihren Reſt nach dem kleinſten gemeinſchaftlichen Vielfachen der Theiler ſuchen; indem man zuerſt zwei Theiler in Rechnung bringt, dann ihr Product und einen dritten Theiler, hierauf wieder das Product dieſer und einen vierten Theiler, u. ſ. f., bis alle Theiler der Rechnung beigezogen worden ſind. Dieſer Vorgang iſt hauptſächlich dazumal vortheilhaft, wenn die Reſte und Theiler in beſonderen Zahlen angewieſen werden. Hiebei kürzt man die Rechnung zuweilen namhaft ab, wenn man die Theiler vom größten bis zum kleinſten abwärts vornimmt.

Der allgemeinſte Fall endlich iſt der, wo manche Theiler oder Moduln gemeinſchaftliche Theiler beſizen. Er läßt ſich durch folgende Betrachtung auf den vorhergehenden Fall zurückführen.

Nach Art. III, 13 und XI, 4 geben zwei congruente Zahlen auch nach jedem Factor des Moduls gleiche Reſte. Iſt demnach der Reſt der zu ſuchenden Zahl für einen zuſammengeſezten Theiler angegeben, ſo kann man ihren Reſt für einen Factor des Theilers beſtimmen, indem man von jenem Reſte den kleinſten poſitiven oder negativen Reſt nach dieſem Factor nimmt. Zerfällt man nun je den Modul, welcher mit einem anderen einen Theiler gemeinſchaftlich hat, in lauter paarweiſe relativ prime Factoren, (am einfachſten in Potenzen von durchgängig verſchiedenen Primzahlen, indem man ihn in lauter einfache oder Primfactoren zerlegt und die gleichen Factoren in eine Potenz zuſammenfaßt), und beſtimmt man die nach den einzelnen Factoren entfallenden Reſte der zu ſuchenden Zahl: ſo können, vermöge des zweiten Falles, jene Factoren die gegebenen Moduln und dieſe Reſte die gegebenen Reſte erſezen.

Werden demnach auf die nemliche Weiſe alle zuſammengeſezten Moduln behandelt, welche mit anderen irgend welche Theiler gemeinſchaftlich beſizen; und ergeben ſich für jeden gemeinſchaftlichen Theiler einerlei Reſte — was jederzeit eintreten muß, wofern die Aufgabe nicht widerſinnig ſein ſoll —; ſo kann man jene Moduln durch ſolche erſezen, welche durchgängig paarweiſe Primzahlen unter ſich ſind. Am zweckmäßigſten vollbringt man dieſes Geſchäft, wenn man vorerſt jeden Modul, der ein Theiler eines größeren iſt, weg läßt; von den zurückbleibenden jeden, der mit einem oder einigen der übrigen einen Theiler gemein hat, als ein Product von Potenzen lauter verſchiedener Primzahlen darſtellt; dann aus allen ſolchen Moduln jede in ihnen als Factor vorfindige Primzahl, in ihrer höchſten Potenz, als Stellvertreter dieſer Moduln heraushebt, und dazu die entſprechenden Reſte der zu ſuchenden Zahl beſtimmt; endlich noch die übrigen Moduln, welche mit keinem anderen einen Theiler

gemeinſchaftlich beſizen, ſammt den angehörigen Reſten hinzunimmt. Zu dieſen neuen Reihen der Moduln und Reſte ſucht man ſofort, nach der im zweiten Falle ertheilten Anleitung, die geforderte Zahl.

Beiſpiel. Sucht man eine Zahl, welche

durch 4, 6, 8, 9, 10, 11, 13, 14, 15, 16, 18 getheilt,

die Reſte 1, 5, 5, 2, 3, 8, 4, 5, 3, 13, 11 gibt;

ſo kann man ſogleich die Theiler 4, 6, 8, 9 weg laſſen, weil ſie in den größeren 8, 18, 16, 18 genau enthalten ſind, und ihre Reſte aus den Reſten der lezteren richtig folgen. Von den übrigen werden 10, 14, 15, 16, 18 in Primfactoren aufgelöſt und geben $10=2.5$, $14=2.7$, $15=3.5$, $16=2^4$, $18=2.3^2$;

daher werden ſie durch $2^4=16$, $3^2=9$, 5, 7 erſezt,

und dazu gehören die Reſte 13, 2, 3, 5. Die Moduln 11 und 13 endlich werden, als Primzahlen, daher auch als relativ prim gegen jeden anderen, ganz unverändert beibehalten.

Somit ſtellt ſich die Aufgabe gegenwärtig ſo, als hätte man blos eine Zahl zu ſuchen, welche

zu den Theilern 5, 7, 9, 11, 13, 16

die Reſte 3, 5, 2, 8, 4, 13 liefert;

wobei demnach der zweite Fall eintritt. Zur leichteren Löſung dieſer Aufgabe wird man die möglich

kleinſten Reſte $-2, -2, 2, -3, 4, -3$ einführen:

weil man ſo, nach III, 14, die Theiler 5 und 7 durch ihr Product 35, dann 11 und 16 durch 176 erſezen kann. Man hat demnach zu

den Theilern 176, 35, 13, 9

die Reſte $-3, -2, 4, 2$.

Bezeichnet man nunmehr die zu ſuchende Zahl mit x, ſo muß ſein

$x \equiv -3$, mod 176 $\equiv -2$, mod 35 $\equiv 4$, mod 13 $\equiv 2$, mod 9.

Daraus folgt $x = 173 + 176u$,

ſonach

$$\begin{array}{l|l|l} 173 + 176u \equiv -2, \text{ mod } 35 & u \equiv 0, \text{ mod } 35 & u = 35.13.9w \\ \equiv 4, \text{ mod } 13 & \equiv 0, \text{ mod } 13 & \\ \equiv 2, \text{ mod } 9 & \equiv 0, \text{ mod } 9 & \end{array}$$

und daher $x = 173 + 720720w \equiv 173$, mod 720720.

Alle geforderten Zahlen bilden demnach eine arithmetiſche Progreſſion, deren kleinſtes poſitives Glied 173, und Unterſchied 720720 iſt.

XXI.

Untersuchung der Quoti und Reste lineärer Functionen oder arithmetischer Progressionen.

1. Höchst wichtig sind die Quoti und Reste solcher veränderlichen Rechnungsausdrücke oder Functionen y von einer Veränderlichen x und vom ersten Grade, welche in der allgemeinen Form

$$y = \eta x + \vartheta \qquad (114)$$

begriffen sind und gewöhnlich lineäre Functionen genannt werden. Theilt man diese Function durch die, so wie η und ϑ, beständige oder von x unabhängige, Zahl μ; so soll ihr, gleichfalls nach x veränderlicher, gewöhnlicher Quotus und Rest mit u und v bezeichnet, folglich

$$u = \text{Q}\frac{y}{\mu} = \text{Q}\frac{\eta x + \vartheta}{\mu} \qquad (115)$$

$$v = \text{R}\frac{y}{\mu} = \text{R}\frac{\eta x + \vartheta}{\mu} \qquad (116)$$

gesezt werden.

In Absicht auf die arithmetische Bedeutung der lineären Function (114) bemerken wir Folgendes. Läßt man die veränderliche Zahl x allmälig in sämmtliche algebraische Anzahlen, nach ihrer natürlichen Folge

$$\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots,$$

übergehen; so bilden die nach und nach hervortretenden Werthe ihrer Function y

$$\ldots, -3\eta + \vartheta, -2\eta + \vartheta, -\eta + \vartheta, \vartheta, \eta + \vartheta, 2\eta + \vartheta, 3\eta + \vartheta, \ldots$$

diejenige arithmetische Progression, deren Gliedern bei fortlaufender algebraischer Zählung die entsprechenden Werthe von x als Stellenzeiger zugehören, so daß ihr nulltes oder Anfangsglied ϑ und der beständige Unterschied η, ihr allgemeines Glied also die Function $y = \eta x + \vartheta$ ist. Demnach müssen die entfallenden Werthe des Quotus u und des Restes v ebenfalls Reihen bilden, deren Glieder auch gewonnen werden, wenn man jene der arithmetischen Progression durch den angenommenen Theiler μ dividirt.

2. Eröffnen wir nun unsere Untersuchungen mit der Betrachtung des Restes (116); so überzeugen wir uns leicht von der Giltigkeit folgenden Sazes:

Wenn τ den größten gemeinschaftlichen Theiler von η und μ vorstellt, so fallen für jede zwei Werthe der Veränderlichen x, welche um $\left\{\begin{matrix}\text{ein}\\\text{kein}\end{matrix}\right\}$ Vielfaches von $\mu:\tau$, also insbesondere $\left\{\begin{matrix}\text{selbst um}\\\text{um weniger als}\end{matrix}\right\}$ $\mu:\tau$, von einander sich unterscheiden, die Reste v $\left\{\begin{matrix}\text{gleich}\\\text{ungleich}\end{matrix}\right\}$ aus.

Denn läßt man x um Δx sich ändern, so ist die Aenderung des Dividendes y, vermöge XVI, 3, 4, 5,

$$(117) \qquad \Delta y = \eta \Delta x$$

daher die Aenderung des Restes v, vermöge (69),

$$(118) \qquad \Delta v \equiv \Delta y \equiv \eta \Delta x, \mod \mu.$$

Soll nun der Rest v für x und $x + \Delta x$ derselbe werden, folglich seine Differenz Δv keine oder 0 sein; so muß $\eta \Delta x \equiv 0$, mod μ, daher entweder $\eta \equiv 0$, mod μ d. h. η durch μ theilbar, oder wenn τ den größten gemeinschaftlichen Theiler von η und μ bezeichnet, vermöge III, 12, auch $(\mu:\tau)\,\Delta x \equiv 0$, mod $(\eta:\tau)$ sein. Da nun $\eta:\tau$ und $\mu:\tau$ Primzahlen unter sich sind, so hat man, vermöge III, 10, auch $\Delta x \equiv 0$, mod $(\mu:\tau)$; das heißt, der Unterschied Δx muß ein Vielfaches von $\mu:\tau$ sein.

Wäre demnach der Coefficient η ein Vielfaches des Theilers μ, so würde $\Delta v \equiv 0$, mod μ und $v = \mp\frac{\vartheta}{\mu}$ sein; nemlich alle Reste v wären gleich, und böten folglich nichts Bemerkenswerthes zu weiterer Forschung dar. Findet dies jedoch nicht Statt, so können nur solche Reste gleich ausfallen, bei denen der Unterschied Δx der sie bestimmenden Werthe ein Vielfaches von $\mu:\tau$, also wenigstens so groß als $\mu:\tau$, niemals aber kleiner als $\mu:\tau$ oder untheilbar dadurch ist. Sind die Zahlen η und μ Primzahlen unter sich, folglich $\tau = 1$, so werden die Reste nur dann gleich, wenn die Werthe der Veränderlichen um ein Vielfaches von μ sich unterscheiden.

Die Reste y der arithmetischen Progression wiederholen sich demnach periodisch nach je $\mu:\tau$-Gliedern, oder lassen sich auf $\mu:\tau$ Weisen in Perioden von je $\mu:\tau$ unter sich verschiedenen Gliedern abtheilen, deren gleichvielte Glieder gleich sind. Je τ solcher Perioden bilden wieder größere Perioden von je μ Resten. Ist insbesondere η durch μ theilbar, also $\tau = \mu$, so wird $\mu:\tau = 1$, also jeder Rest dem anderen gleich. Sind aber η und μ Primzahlen unter sich, ist also $\tau = 1$, so wird $\mu:\tau = \mu$; folglich wiederkehren die Reste erst nach je μ Gliedern.

3. Wenn die Werthe der Veränderlichen x um Δx sich unterscheiden, weichen nach dem obigen Ausdrucke und vermöge (69) die Reste v um

$$(119) \qquad \Delta v = \pm \mp\frac{\pm \eta \Delta x}{\mu} = \pm\, \tau \mp\frac{\pm(\eta:\tau)\Delta x}{\mu:\tau}$$

von einander ab. Läßt man insbesondere die Veränderliche x natürlich, d. i. stetig um $1 = \Delta x$, aufsteigen, so wird der Rest v um

$\Delta v = \pm \mp\frac{\pm\eta}{\mu} = \pm\, \tau \mp\frac{\pm(\eta:\tau)}{\mu:\tau}$ sich verändern, nemlich

entweder um $\mp\frac{\eta}{\mu} = \tau \mp\frac{\eta:\tau}{\mu:\tau}$ wachsen, oder um $\mp\frac{-\eta}{\mu} = \tau \mp\frac{-\eta:\tau}{\mu:\tau}$ ab-

nehmen. Zu Folge dieſes Satzes kann man die Reihe der Reſte v leicht fortſetzen, indem man entweder zu jedem ſchon berechneten Reſte $\mp\frac{\eta}{\mu} = \tau \mp\frac{\eta:\tau}{\mu:\tau}$ addirt, und davon, ſo oft es angeht, μ weg wirft, oder wenn man von jedem ſchon gefundenen, und falls er zu klein wäre, um μ vergrößerten Reſte $\mp\frac{-\eta}{\mu} = \tau \mp\frac{-\eta:\tau}{\mu:\tau}$ abzieht; noch leichter, wenn man entweder da $\mp\frac{\eta}{\mu}$ addirt, wo man zur Summe nicht mehr als $\mu-1$ erhält, oder da wo es angeht, $\mp\frac{-\eta}{\mu}$ abzieht.

Z. B. Der Reſt $v = \mp\frac{7x-6}{19}$, für welchen $\eta=7$, $\vartheta=-6$, $\mu=19$ iſt, wächſt entweder um 7 oder nimmt um $\mp\frac{-7}{19} = 12$ ab, und bietet ſonach folgende Werthe dar. mod. = 19

$x \equiv$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$v =$	13	1	8	15	3	10	17	5	12	0	7	14	2	9	16	4	11	18	6	13.

4. Umgekehrt laſſen ſich aus den Reſten v diejenigen Zahlen oder Stellenzeiger x beſtimmen, welche ſie hervorbringen. Denn aus der Gleichung (116) findet man

$$\eta x + \vartheta \equiv v, \text{ mod } \mu$$

folglich $$\eta x \equiv v - \vartheta, \text{ mod } \mu.$$

Haben η und μ zum größten gemeinſchaftlichen Theiler τ, ſo muß ηx, daher, vermöge III, 11, auch $v-\vartheta$ durch τ theilbar oder $v \equiv \vartheta$, mod τ ſein. Mithin erhält man, nach III, 12,

$$(120) \quad (\eta:\tau)\, x \equiv \frac{v-\vartheta}{\tau}, \text{ mod } (\mu:\tau) \text{ oder}$$

$$\equiv -\mp\frac{\vartheta}{\tau} + \frac{v - \mp\frac{\vartheta}{\tau}}{\tau}, \text{ mod } (\mu:\tau).$$

Sucht man demnach, weil $\eta:\tau$ und $\mu:\tau$ Primzahlen unter ſich ſind, nach Art. XIX. die möglich kleinſte Zahl χ, für welche

$$(121) \quad (\eta:\tau)\chi \equiv 1, \text{ mod } (\mu:\tau)$$

iſt, ſo erhält man die geforderten Zahlen

$$(122) \quad x \equiv \chi\frac{v-\vartheta}{\tau} \equiv -\chi\mp\frac{\vartheta}{\tau} + \chi\frac{v - \mp\frac{\vartheta}{\tau}}{\tau}, \text{ mod } (\mu:\tau)$$

von denen man gewöhnlich blos die $\mu:\tau$ kleinſten poſitiven, entweder von 0 bis $(\mu:\tau)-1$ oder von 1 bis $\mu:\tau$ nimmt.

Eben ſo findet man von der Congruenz (120) die Aenderung

$$(\eta:\tau)\,\Delta x \equiv \frac{\Delta v}{\tau}, \text{ mod } (\mu:\tau)$$

sogleich (123) $\Delta x \equiv \chi \frac{\Delta v}{\tau}$, mod $(\mu:\tau)$

$$= \pm \mp \frac{\pm\chi(\Delta v:\tau)}{\mu:\tau}.$$

Steigen demnach die Reste v in der natürlichen Folge um $\tau = \Delta v$, so ändern sich die Stellenzeiger x um $\Delta x = \pm \mp \frac{\pm\chi}{\mu:\tau}$; nemlich sie wachsen entweder um $\mp \frac{\chi}{\mu:\tau}$, oder sie nehmen um $\mp \frac{-\chi}{\mu:\tau}$ ab.

Z. B. Kehrt man die Aufgabe im vorigen Beispiele um, so findet man, wegen $\eta = 7$, $\vartheta = -6$, $\mu = 19$, $\tau = 1$, aus der Congruenz $7\chi \equiv 1$, mod 19 die Zahl $\chi = -8$, daher $x \equiv -8v - 48$, mod $19 \equiv -8v + 9$; $\Delta x \equiv 11$ oder -8.

Im Zusammenhange erhält man also, wenn man die Zahlen x entweder um 8 abnehmen oder um 11 wachsen läßt, zu den Resten v die Zahlen x wie folgt:

mod. = 19

v =	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x ≡	9	1	12	4	15	7	18	10	2	13	5	16	8	19	11	3	14	6	17.

5. Betrachten wir nunmehr den Quotus u, so finden wir, wenn die Veränderliche x um Δx sich ändert, die entsprechende Aenderung des Quotus u, vermöge (66)

$$\Delta u = \Delta \mp \frac{y}{\mu} = \mp \frac{\Delta y}{\mu} + \mp \frac{\mp \frac{\Delta y}{\mu} + \mp \frac{y}{\mu}}{\mu}$$

oder, wegen $\Delta y = \eta \Delta x$ und $\mp \frac{y}{\mu} = v$,

$$(124) \qquad \Delta u = \mp \frac{\eta \Delta x}{\mu} + \mp \frac{\mp \frac{\eta \Delta x}{\mu} + v}{\mu}$$

oder endlich, wenn wir abkürzend

$$(125) \qquad \mp \frac{\mp \frac{\eta \Delta x}{\mu} + v}{\mu} = w \qquad \text{setzen,}$$

$$(126) \qquad \Delta u = \mp \frac{\eta \Delta x}{\mu} + w.$$

Bezeichnet wieder τ den größten gemeinschaftlichen Theiler von η und μ, so ist, vermöge XII, (35),

$$\mp \frac{\eta \Delta x}{\mu} = \mp \frac{(\eta:\tau)\,\Delta x}{\mu:\tau}.$$

So oft demnach Δx ein Vielfaches von $\mu:\tau$ ist, wird

$$\mp \frac{\eta \Delta x}{\mu} = (\eta:\tau) \frac{\Delta x}{\mu:\tau},$$

zugleich aber auch $w = \mathfrak{f}\frac{v}{\mu} = 0$, weil $v < \mu$; daher ist

$$(127) \qquad \Delta u = (\eta : \tau)\frac{\Delta x}{\mu : \tau} \qquad \text{oder} \quad \frac{\Delta u}{\eta : \tau} = \frac{\Delta x}{\mu : \tau}.$$

Aendert sich demnach die Veränderliche x um ein Vielfaches von $\mu : \tau$; so ändert sich der Quotus u um das Ebensovielfache von $\eta : \tau$. Wäre η ein Vielfaches von μ, also $\tau = \mu$, so würde $\Delta u = (\eta : \mu)\,\Delta x$, daher änderte sich der Quotus u um das Ebensovielfache von Δx. In diesem Falle überginge dieser Quotus selbst in $u = (\eta : \mu)\,x + \mathfrak{f}\frac{\vartheta}{\mu}$, also in eine lineäre Function von x. Sind η und μ Primzahlen unter sich, so ist $\tau = 1$. Um ein Wievielfaches von μ sich demnach die Veränderliche x ändert, um das Ebensovielfache von η ändert sich der Quotus u.

Die der arithmetischen Progression der Dividende $y = \eta x + \vartheta$ zugehörige Reihe der Quoti $u = \mathfrak{f}\frac{y}{\mu}$ ändert sich daher nach je $\mu : \tau$ Gliedern um $\eta : \tau$. Sondert man demnach diese Quoti in Perioden von je $\mu : \tau$ Gliedern ab, so geht jede spätere Periode aus der nächst früheren hervor, wenn man zu allen ihren Gliedern $\eta : \tau$ addirt. Ist insbesondere der Coefficient η ein Vielfaches des Theilers μ, so bilden die Quoti eine arithmetische Progression, deren nulltes Glied $\mathfrak{f}\frac{\vartheta}{\mu}$ und Unterschied $\eta : \mu$ ist. Sind η und μ Primzahlen unter sich, so ändern sich die Quoti erst nach je μ Gliedern um η.

Daraus erhellet, daß es schon genüge, die Aenderung des Quotus u nur in dem Bereiche einer Periode von $\mu : \tau$ Gliedern oder bei $\mu : \tau$ nach einander folgenden Quotis zu erforschen, folglich $\Delta x < \mu : \tau$ anzunehmen.

Die Reste $\mathfrak{r}\frac{\eta \Delta x}{\mu}$ und v sind einzeln $< \mu$, also zusammen $< 2\mu$; daher ist, nach Gleichung (125), der Quotus w nur entweder 0 oder 1, folglich vermöge Gleichung (126) die Aenderung des Quotus u

$$(128) \qquad \Delta u = \mathfrak{f}\frac{\eta \Delta x}{\mu} \quad \text{oder} \quad = \mathfrak{f}\frac{\eta \Delta x}{\mu} + 1 = -\mathfrak{f}\frac{-\eta \Delta x}{\mu}.$$

Steigt die Veränderliche x nach der natürlichen Reihe der Zahlen, also stetig um $1 = \Delta x$, so beträgt die Aenderung des Quotus

$$(129) \qquad \Delta u = \mathfrak{f}\frac{\eta}{\mu} \quad \text{oder} \quad = \mathfrak{f}\frac{\eta}{\mu} + 1 = -\mathfrak{f}\frac{-\eta}{\mu}.$$

Ist überdies noch insbesondere η positiv und $< \mu$, so ist $\Delta u = 0$ oder 1; der Quotus u bleibt also entweder derselbe oder nimmt um 1 zu.

6. Besonders wichtig ist es, die Bedingungen kennen zu lernen, unter denen der Quotus w bald 0, bald 1 wird.

Damit überhaupt die Gleichung (125) beſtehe, alſo $\mathfrak{x}\frac{\eta\Delta x}{\mu} + v$ durch μ getheilt den Quotus w gebe, muß

$$\mu w \leqq \mathfrak{x}\frac{\eta\Delta x}{\mu} + v < \mu(w+1)$$

alſo $$\mu w - \mathfrak{x}\frac{\eta\Delta x}{\mu} \leqq v < \mu(w+1) - \mathfrak{x}\frac{\eta\Delta x}{\mu}$$

ſein. Hiemit bringen wir noch in Verbindung, daß der Annahme in (116) zu Folge auch ſtets

$$0 \leqq v < \mu$$

bleiben muß.

Somit kann der Quotus $w = \mathfrak{q}\frac{\mathfrak{x}\frac{\eta\Delta x}{\mu} + v}{\mu}$ nur dann 0 ſein, wenn

$$(130) \qquad 0 \leqq v < \mu - \mathfrak{x}\frac{\eta\Delta x}{\mu} = \mathfrak{R}\frac{-\eta\Delta x}{\mu}$$

daher
$$(131) \qquad v = \mathfrak{x}\frac{\eta x+\vartheta}{\mu} < \mu - \mathfrak{x}\frac{\eta\Delta x}{\mu} < \mathfrak{R}\frac{-\eta\Delta x}{\mu}$$

iſt; oder, wofern man die in (130) verglichenen Zahlen von μ abzieht, wenn

$$\mu \geqq \mu - v > \mathfrak{x}\frac{\eta\Delta x}{\mu}$$

alſo $$(132) \qquad \mu - v = \mu - \mathfrak{x}\frac{\eta x+\vartheta}{\mu} = \mathfrak{R}\frac{-(\eta x+\vartheta)}{\mu} > \mathfrak{x}\frac{\eta\Delta x}{\mu}$$ iſt.

Die Anzahl n der Werthe von x, bei denen dieſes, in einer $(\mu:\tau)$ gliedrigen Periode, für eine gegebene Aenderung Δx eintritt, beſtimmt ſich demnach daraus, daß einerſeits, nach Nr. 4, $v \equiv \vartheta$, mod τ, andererſeits, vermöge (131), $v < \mathfrak{R}\frac{-\eta\Delta x}{\mu}$ ſein muß; daher iſt

$$(n-1)\tau + \mathfrak{x}\frac{\vartheta}{\tau} < \mathfrak{R}\frac{-\eta\Delta x}{\mu}$$

$$n\tau < \tau\,\mathfrak{R}\frac{-(\eta:\tau)\Delta x}{\mu:\tau} + \tau - \mathfrak{x}\frac{\vartheta}{\tau}$$

alſo $$(133) \qquad n = \mathfrak{R}\frac{-(\eta:\tau)\Delta x}{\mu:\tau}.$$

Ueberdies findet man dieſe Werthe von x ſelbſt, mittels Nr. 4, wenn man

$$v \equiv \vartheta, \text{ mod } \tau \text{ aber } v < \mathfrak{R}\frac{-\eta\Delta x}{\mu},$$

mithin $$v = \mathfrak{x}\frac{\vartheta}{\tau} + \tau z$$

und darin $$z = 0, 1, 2, \ldots . n-1$$ ſezt.

Man erhält auf dieſe Weiſe

$$(134) \qquad x \equiv \chi\left(-\mathfrak{f}\frac{\vartheta}{\tau} + z\right), \mod (\mu:\tau)$$

ſo wie aus (121)

$$(135) \quad (\eta:\tau)\,x \equiv -\mathfrak{f}\frac{\vartheta}{\tau} + z, \mod (\mu:\tau).$$

Dagegen kann der Quotus $w = \mathfrak{f}\frac{\mathfrak{r}\frac{\eta\Delta x}{\mu} + v}{\mu}$ nur dann 1 werden,

wenn $(136) \qquad \mu - \mathfrak{r}\frac{\eta\Delta x}{\mu} = \mathfrak{R}\frac{-\eta\Delta x}{\mu} \leqq v < \mu$

daher $(137) \qquad v = \mathfrak{r}\frac{\eta x + \vartheta}{\mu} \geqq \mathfrak{R}\frac{-\eta\Delta x}{\mu}$

iſt; oder, wofern man die in (136) verglichenen Zahlen zu μ ergänzt, wenn

$$\mathfrak{r}\frac{\eta\Delta x}{\mu} \geqq \mu - v > 0$$

alſo $(138) \quad \mu - v = \mu - \mathfrak{r}\frac{\eta x + \vartheta}{\mu} = \mathfrak{R}\frac{-(\eta x + \vartheta)}{\mu} \leqq \mathfrak{r}\frac{\eta\Delta x}{\mu}$ iſt.

Die Anzahl n der Werthe von x, bei denen dieſes, in einer $(\mu:\tau)$ gliedrigen Periode, für eine gegebene Aenderung Δx eintritt, beſtimmt ſich demnach daraus, daß einerſeits, vermöge (138), $\mu - v \leqq \mathfrak{r}\frac{\eta\Delta x}{\mu}$, andererſeits, nach Nr. 4, $v \equiv \vartheta, \mod \tau$ alſo $\mu - v \equiv \mathfrak{R}\frac{-\vartheta}{\tau}, \mod \tau$ ſein muß; daher iſt

$$(n-1)\,\tau + \mathfrak{R}\frac{-\vartheta}{\tau} \leqq \mathfrak{r}\frac{\eta\Delta x}{\mu}$$

$$n\tau \leqq \tau\,\mathfrak{r}\frac{(\eta:\tau)\Delta x}{\mu:\tau} + \tau - \mathfrak{R}\frac{-\vartheta}{\tau}$$

alſo $(139) \qquad n = \mathfrak{r}\frac{(\eta:\tau)\,\Delta x}{\mu:\tau}.$

Ueberdies findet man dieſe Werthe von x ſelbſt, nach Nr. 4, wenn man

$$v \equiv \vartheta, \mod \tau \text{ und } v \geqq \mathfrak{R}\frac{-\eta\Delta x}{\mu}$$

oder $$\mu - v \equiv \mathfrak{R}\frac{-\vartheta}{\tau}, \mod \tau \text{ aber} \leqq \mathfrak{r}\frac{\eta\Delta x}{\mu},$$

mithin $$\mu - v = \mathfrak{R}\frac{-\vartheta}{\tau} + \tau z = \tau\,(z+1) - \mathfrak{r}\frac{\vartheta}{\tau}$$

und darin $$z = 0, 1, 2, \ldots . n - 1$$

ſezt. Man findet auf dieſem Wege

$$(140) \qquad x \equiv -\chi\left(\mathfrak{f}\frac{\vartheta}{\tau} + z + 1\right), \mod (\mu:\tau),$$

ſo wie aus (121)

$$(141) \quad (\eta:\tau)\,x \equiv -\mathfrak{f}\frac{\vartheta}{\tau} - (z+1), \mod (\mu:\tau).$$

Wächst die Veränderliche x nach der natürlichen Folge der Zahlen, also stetig um $1 = \Delta x$, so ist $w = 0$, so oft $v = \mathfrak{r}\frac{\eta x + \vartheta}{\mu} < \mathfrak{R}\frac{-\eta}{\mu}$, oder $< \mu - \mathfrak{r}\frac{\eta}{\mu}$; dagegen $w = 1$, wenn $v = \mathfrak{r}\frac{\eta x + \vartheta}{\mu} \geqq \mathfrak{R}\frac{-\eta}{\mu}$ oder $\geqq \mu - \mathfrak{r}\frac{\eta}{\mu}$.

7. Endlich findet man noch die gleichzeitigen Aenderungen des Quotus u und Restes v nach Art. XVI, 8 und XXI, 1, 2.

$$(142) \qquad \Delta u = \Delta\mathfrak{q}\frac{y}{\mu} = \pm\mathfrak{q}\frac{\pm\Delta y}{\mu} = \pm\mathfrak{q}\frac{\pm\eta\,\Delta x}{\mu} = \pm\mathfrak{q}\frac{\pm(\eta:\tau)\,\Delta x}{\mu:\tau}$$

$$\Delta v = \Delta\mathfrak{r}\frac{y}{\mu} = \pm\mathfrak{r}\frac{\pm\Delta y}{\mu} = \pm\mathfrak{r}\frac{\pm\eta\,\Delta x}{\mu} = \pm\tau\,\mathfrak{r}\frac{\pm(\eta:\tau)\,\Delta x}{\mu:\tau}$$

So oft demnach der Rest v um $\mathfrak{r}\frac{\eta\Delta x}{\mu} = \tau\,\mathfrak{r}\frac{(\eta:\tau)\Delta x}{\mu:\tau}$ wächst, muß der Quotus u um $\mathfrak{q}\frac{\eta\Delta x}{\mu} = \mathfrak{q}\frac{(\eta:\tau)\Delta x}{\mu:\tau}$, je nachdem dieser Werth positiv oder negativ ausfällt, wachsen oder abnehmen;

so oft dagegen der Rest v um $\mathfrak{r}\frac{-\eta\Delta x}{\mu} = \tau\,\mathfrak{r}\frac{(-\eta:\tau)\Delta x}{\mu:\tau}$ abnimmt, muß der Quotus u um $-\mathfrak{q}\frac{-\eta\Delta x}{\mu} = -\mathfrak{q}\frac{(-\eta:\tau)\Delta x}{\mu:\tau}$, je nachdem dieser Werth positiv oder negativ ausfällt, wachsen oder abnehmen.

Beispiel. 1. Wählt man die lineäre Function $y = 45x - 25$ und theilt sie durch 19, so hat man $\eta = 45$, $\vartheta = -25$, $\mu = 19$, $\tau = 1$, $\mathfrak{r}\frac{\eta}{\mu} = 7$, $-\mathfrak{r}\frac{-\eta}{\mu} = -12$, $\chi = -8$, $\mathfrak{q}\frac{\eta}{\mu} = 2$, $-\mathfrak{q}\frac{-\eta}{\mu} = 3$, $\mathfrak{R}\frac{-\eta}{\mu} = 12$; daher findet man folgende zusammen gehörige Werthe von x, y, u, Δu, v, Δv:

x =	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
y =	−25	−20	−6	5	110	155	200	245	290	335	380	425	470	515	560	605	650	695	740	785	830
u =	−2	−1	3	5	8	10	12	15	17	20	22	24	27	29	31	34	36	38	41	43
Δu =	3	2	2	3	2	2	3	2	3	2	2	3	2	2	3	2	2	3	2	
v =	13	1	8	15	3	10	17	5	12	0	7	14	2	9	16	4	11	18	6	13
Δv =	−12	7	7	−12	7	7	−12	7	−12	7	7	−12	7	7	−12	7	7	−12	7	

Die Anzahl der Reste $v < \mathfrak{R}\frac{-\eta}{\mu} = 12$ ist $= \mathfrak{R}\frac{-45}{19} = 12$, und die Anzahl der Reste $v \geqq \mathfrak{R}\frac{-\eta}{\mu} = 12$ ist $= \mathfrak{r}\frac{45}{19} = 7$.

Beispiel. 2. Theilt man die Function $y = 72x + 67$ durch 28, so ist $\eta = 72$, $\vartheta = 67$, $\mu = 28$, $\tau = 4$, $\mathfrak{r}\frac{\eta}{\mu} = 16$, $-\mathfrak{r}\frac{-\eta}{\mu} = -12$, $\mathfrak{R}\frac{-\eta}{\mu} = 12$, $\chi = 2$, $\mathfrak{q}\frac{\eta}{\mu} = 2$, $-\mathfrak{q}\frac{-\eta}{\mu} = 3$; daher ergeben sich folgende zusammen gehörige Werthe von x, y, u, Δu, v, Δv:

x =	0	1	2	3	4	5	6	7	8	9	10	11	12	13
y =	67	139	211	283	355	427	499	571	643	715	787	859	931	1003
u =	2	4	7	10	12	15	17	20	22	25	28	30	33	35
Δu =		2	3	3	2	3	2	3	2	3	3	2	3	2
v =	11	27	15	3	19	7	23	11	27	15	3	19	7	23
Δv =		16	−12	−12	16	−12	16	−12	16	−12	−12	16	−12	16

Die Anzahl der Reste $v < \mathfrak{R}\frac{-\eta}{\mu} = 12$ oder der Stellen, wo der Quotus w Null wird, ist $= \mathfrak{R}\frac{-18}{7} = 3$, namentlich ist $z = 0, 1, 2$, daher $v = 3 + 4z = 3, 7, 11$ und $x \equiv 2z + 3$, mod $7 \equiv 3, 5, 0$; dagegen die Anzahl der Reste $v \overline{>} \mathfrak{R}\frac{-\eta}{\mu} = 12$ ist $= \mathfrak{x}\frac{18}{7} = 4$, namentlich ist $z = 0, 1, 2, 3$, daher $\mu - v = 4z + 1 = 1, 5, 9, 13$, also $v = 27, 23, 19, 15$, und $x \equiv -2z + 1$, mod $7 \equiv 1, 6, 4, 2$.

XXII.

Aufstellung einiger Functionen einer Veränderlichen aus vorgezeichneten Eigenschaften.

Gestützt auf die Ergebnisse der so eben durchgeführten Untersuchung der Quoti und Reste lineärer Functionen einer Veränderlichen durch einen beständigen Theiler, sind wir nunmehr im Stande, einige Functionen — für unseren Bedarf eigentlich blos Quoti — dergestalt zu bestimmen, daß sie gewissen vorgeschriebenen Bedingungen genügen.

1. *Zuweilen verlangt man eine* Function *dermaßen aufzustellen, daß, während die Veränderliche von* 0 *oder* 1 *an bis zu einer gewissen Zahl* g *aufsteigt, die Function stets* 0 *bleibt, dagegen für die höheren Werthe der Veränderlichen bis zum Werthe* h *durchgängig* 1 *wird;*

Oder: Man fordert eine Reihe, deren Glieder vom 0^{ten} oder 1^{sten} bis zum g^{ten} Null, von da aber bis zum h^{ten} 1 sind.

Eine solche Function kann, vermöge XXI, 5, ein Quotus einer lineären Function $y = \eta x + \vartheta$, also

$$u = \mathfrak{q}\frac{\eta x + \vartheta}{\mu} \tag{115}$$

sein, in welchem die Constanten η, ϑ, μ den ausgesprochenen Bedingungen gemäß zu bestimmen sind.

Soll nun erstlich schon für $x = 0$, auch $u = 0$ sein, so hat man $\mathfrak{q}\frac{\vartheta}{\mu} = 0$, also $0 \overline{<} \vartheta < \mu$. Sollte aber erst von $x = 1$ an $u = 0$ werden, so ist $\mathfrak{q}\frac{\eta+\vartheta}{\mu} = 0$, also $0 \overline{<} \vartheta + \eta < \mu$.

Damit nun, so lange $x \gtreqless g$ ist, stets $u = 0$ bleibe, dagegen, sobald $x = g + 1$ wird, sogleich $u = 1$ ausfalle, muß

$$0 \gtreqless \eta + \vartheta < 2\eta + \vartheta < 3\eta + \vartheta < \ldots\ldots < g\eta + \vartheta < \mu \gtreqless (g+1)\eta + \vartheta$$

sein. Daraus folgt sogleich $\eta > 0$, nemlich der Coefficient η muß positiv angenommen werden; und man kann sezen

$$(143) \qquad \mu = g\eta + \vartheta + \varphi,$$

wofern $(144) \qquad \varphi = 1, 2, 3, \ldots . \eta$ gedacht wird.

Soll aber endlich selbst für $x = h > g$ der Quotus u noch immer 1 bleiben, also noch nicht 2 erreichen, so muß

$$h\eta + \vartheta < 2\mu$$

sein. Ersezt man in dieser Vergleichung μ durch obigen Ausdruck, so erhält man

$$\vartheta > (h - 2g)\,\eta - 2\varphi.$$

Man kann demnach, indem man $\omega \gtreqless 1$ voraussezt,

$$(145) \qquad \vartheta = (h - 2g)\,\eta - 2\varphi + \omega = h\eta + \omega - 2\,(g\eta + \varphi)$$

daher nach der Gleichung (143)

$$(146) \qquad \mu = (h - g)\,\eta - \varphi + \omega = h\eta + \omega - (g\eta + \varphi)$$

annehmen.

Am einfachsten ist es, für φ und ω Vielfache von η zu wählen, oder, weil dann der Factor η aus dem Dividend und Theiler weg fällt, blos $\eta = 1$ zu sezen. Dann muß auch $\varphi = 1$ sein, und man erhält

$$(147) \qquad u = \mathfrak{q}\frac{x+\vartheta}{\mu}$$

$$(148) \qquad \vartheta = h - 2g - 2 + \omega$$
$$\mu = h - g - 1 + \omega.$$

Z. B. Man soll die Function u so bestimmen, daß sie von $x = 0$ bis $x = 5$ Null bleibe, dagegen von da an bis $x = 13$ stets 1 werde.

Hier ist $g = 5$, $h = 13$, $h - g = 8$, $h - 2g = 3$.

Wählt man nun $\eta = 1$, d. i. so klein als möglich, so ist $\vartheta = 1 + \omega$ und $\mu = 7 + \omega$, daher $u = \mathfrak{q}\frac{x+1+\omega}{7+\omega}$. Nimmt man $\omega = 1$, auch so klein als möglich, so ist möglichst einfach $u = \mathfrak{q}\frac{x+2}{8}$.

Sezt man dagegen $\eta = 3$, so wird $\vartheta = 9 - 2\varphi + \omega$, $\mu = 24 - \varphi + \omega$; daher, für $\varphi = 2$ und $\omega = 1$, $\vartheta = 6$, $\mu = 23$ und $u = \mathfrak{q}\frac{3(x+2)}{23}$.

Ist h nicht festgesezt, darf aber die Veränderliche x einen gewissen unter $2(g + 1)$ liegenden Werth nicht übersteigen, so mag man

$$h = 2(g + 1) - 1 = 2g + 1$$

sezen; dann ergibt sich für $\eta = 1$, $\vartheta = \omega - 1$, $\mu = g + \omega$, und

$$(149) \qquad u = \text{Ⅎ}\frac{x+\omega-1}{g+\omega} = \text{Ⅎ}\frac{x+\vartheta}{g+1+\vartheta}$$

worin $\omega \gtreqless 1$ oder $\vartheta \gtreqless 0$ gedacht wird.

2. Man kann die Forderung dahin abändern, daß die zu bestimmende Function bei dem Werthe g der Veränderlichen bereits auf 1 sich erhebe, daher nur bis zum nächst vorhergehenden Werthe $g - 1$ Null bleibe.

Dann heißt $g - 1$ das, was früher g genannt wurde, folglich hat man in den Gleichungen (145), (146), (148) und (149) nur g in $g - 1$ zu verwandeln. Dadurch erhält man

$$(150) \qquad \begin{aligned} \vartheta &= (h - 2g + 2)\eta - 2\varphi + \omega \\ \mu &= (h - g + 1)\eta - \varphi + \omega \end{aligned}$$

und für $\eta = 1$, $\varphi = 1$

$$(151) \qquad \begin{aligned} \vartheta &= h - 2g + \omega \\ \mu &= h - g + \omega. \end{aligned}$$

Kann die Veränderliche x einen gewissen größten unter $2g$ liegenden Werth nicht übersteigen, so mag man

$$(152) \qquad h = 2g - 1$$

sezen, dann wird $\vartheta = \omega - 1$, $\mu = g + \omega - 1$ und

$$(153) \qquad u = \text{Ⅎ}\frac{x+\omega-1}{g+\omega-1} = \text{Ⅎ}\frac{x+\vartheta}{g+\vartheta},$$

wofern man $\omega \gtreqless 1$ oder $\vartheta \gtreqless 0$ annimmt. Am einfachsten nimmt man $\vartheta = 0$, daher

$$(154) \qquad u = \text{Ⅎ}\frac{x}{g}.$$

3. Sehr oft werden in den folgenden Untersuchungen Reihen nöthig werden, in denen das erste Glied 0 ist, deren spätere Glieder nur allmälig, nemlich an gewissen periodisch vertheilten Stellen, um 1 steigen, daher jede folgende Periode die nächst vorhergehende durchgängig um die Anzahl der in jeder Periode bestehenden Steigungen übertrifft, und deren allgemeines Glied sonach die Anzahl aller solchen ausnahmsweisen Steigungen angibt und daher die eigens aufzustellende Function des Stellenzeigers ist. Dabei muß zugleich die Aenderung dieser Function, bei dem natürlichen Steigen der Veränderlichen, als eine andere Function sich ergeben, die blos für gewisse Ausnahmswerthe der Veränderlichen gleich 1 wird, sonst immer 0 bleibt; und eigentlich das allgemeine Glied der Reihe der Unterschiede der vorigen Reihe ist, oder den Betrag der an jeder Stelle Statt findenden Steigung angibt.

Blicken wir zurück auf die Ergebnisse unserer Untersuchungen in XXI, 5, so überzeugen wir uns leicht, daß das allgemeine Glied der aufzustellenden Reihe oder die zu bestimmende nach dem Stellenzeiger x veränderliche Function u ein Quotus einer lineären Function von der Gestalt

$$(115) \qquad u = \mathfrak{q}\frac{\eta x + \vartheta}{\mu},$$

sein müsse, deren Constanten η, ϑ, μ den vorgezeichneten Bedingungen gemäß zu bestimmen sind.

Soll nach je ϖ Gliedern der Reihe die Folge der Steigungen regelmäßig wiederkehren und zwischen η und μ der größte gemeinschaftliche Theiler τ bestehen, so muß, vermöge XXI, 2, für den zu suchenden Theiler μ

$$(155) \qquad \mu : \tau = \varpi, \text{ also } \mu = \varpi\tau$$

sein. Sollen ferner bei je ϖ nach einander folgenden Gliedern der Reihe ε Steigungen oder Ausnahmen, mithin $\varpi - \varepsilon$ mal das Gleichbleiben oder die Regel eintreten, so muß, weil hier immer $\Delta x = 1$ vorausgesetzt wird, vermöge (133) und (139)

$$\varpi - \varepsilon = \mathfrak{R}\frac{-(\eta:\tau)}{\mu:\tau} = \varpi - \mathfrak{x}\frac{\eta:\tau}{\varpi}, \qquad \varepsilon = \mathfrak{x}\frac{\eta:\tau}{\mu:\tau} = \mathfrak{x}\frac{\eta:\tau}{\varpi}$$

also (156) $\eta : \tau \equiv \varepsilon, \bmod \varpi, \quad \eta : \tau = \varepsilon + \varpi z, \quad \eta = \varepsilon\tau + \mu z$

sein. Die Werthe des Quotus u sollen ferner der Reihe nach (d. i. für $\Delta x = 1$) nur um 0 oder 1 steigen, also soll vermöge XXI, 5, ihre Aenderung $\Delta u = \mathfrak{q}\frac{\eta}{\mu} + w = 0$ oder 1 werden; daher muß $\mathfrak{q}\frac{\eta}{\mu} = 0$ und vermöge (125)

$$(157) \qquad \Delta u = w = \mathfrak{q}\frac{\eta + v}{\mu} = 0, 1$$

sein, wenn, wie in XXI, der Rest

$$(116) \qquad \mathfrak{x}\frac{\eta x + \vartheta}{\mu} = v \text{ angedeutet wird.}$$

Weil nun nach den gestellten Bedingungen immer $\varepsilon < \varpi$, also $\varepsilon\tau < \varpi\tau = \mu$ sein muß, so ist $z = \mathfrak{q}\frac{\eta}{\mu}$ daher $z = 0$ und der zu suchende Coefficient

$$(158) \qquad \eta = \varepsilon\tau < \mu.$$

Zugleich sind $\varepsilon = \eta : \tau$ und $\varpi = \mu : \tau$ Primzahlen unter sich, weil τ den größten gemeinschaftlichen Theiler von η und μ vorstellt.

Kennzeichen, daß der Quotus u, von einer Stelle x zur nächst höheren $x + 1$, sich gleich bleibe, sind demnach, vermöge XXI, 6, entweder, daß die Aenderung desselben

$$(159) \qquad \Delta u = w = \mathfrak{q}\frac{\eta + v}{\mu} = \mathfrak{q}\frac{\eta + \mathfrak{x}\frac{\eta x + \vartheta}{\mu}}{\mu} = 0,$$

oder daß der Reſt

$$(160) \qquad v = \mathfrak{x}\frac{\eta x+\vartheta}{\mu} < \mu - \mathfrak{x}\frac{\eta}{\mu} \text{ oder } < \mathfrak{R}\frac{-\eta}{\mu}$$

oder daß der Reſt

$$(161) \qquad \mu - v = \mathfrak{R}\frac{-(\eta x+\vartheta)}{\mu} > \mathfrak{x}\frac{\eta}{\mu}$$

ſei; oder daß, wenn man den bald häufig vorkommenden Quotus $\mathfrak{q}\frac{\vartheta}{\tau}$ der Kürze halber durch δ bezeichnet, die Congruenz

$$(162) \qquad \varepsilon x + \delta \equiv z, \mod \varpi$$

Statt finde und darin

$$(163) \qquad z = 0, 1, 2, \ldots\ldots \varpi - \varepsilon - 1$$

ſei, oder daß, wofern χ aus

$$(164) \qquad \varepsilon\chi \equiv 1, \mod \varpi$$

beſtimmt wird, nemlich das χfache von ε, durch ϖ getheilt, 1 zum Reſte gibt, die Congruenz

$$(165) \qquad x \equiv \chi\,(-\delta + z), \mod \varpi \text{ beſtehe.}$$

Kennzeichen dagegen, daß der Quotus u, von einer Stelle x zur anderen x + 1, um 1 wachſe, ſind vermöge XXI, 6, entweder, daß die Aenderung desſelben

$$(166) \qquad \Delta u = w = \mathfrak{q}\frac{\eta+v}{\mu} = \mathfrak{q}\frac{\eta + \mathfrak{x}\frac{\eta x+\vartheta}{\mu}}{\mu} = 1,$$

oder daß der Reſt

$$(167) \qquad v = \mathfrak{x}\frac{\eta x+\vartheta}{\mu} \gtreqless \mu - \mathfrak{x}\frac{\eta}{\mu} \text{ oder } \gtreqless \mathfrak{R}\frac{-\eta}{\mu}$$

oder daß der Reſt

$$(168) \qquad \mu - v = \mathfrak{R}\frac{-(\eta x+\vartheta)}{\mu} \lesseqgtr \mathfrak{x}\frac{\eta}{\mu}$$

ſei; oder daß die Congruenz

$$(169) \qquad \varepsilon x + \delta \equiv -(z+1), \mod \varpi$$

Statt finde und darin

$$(170) \qquad z = 0, 1, 2, \ldots\ldots \varepsilon - 1$$

ſei, oder daß, wofern χ aus

$$(164) \qquad \varepsilon\chi \equiv 1, \mod \varpi$$

beſtimmt wird, die Congruenz

$$(171) \qquad x \equiv -\chi\,(\delta + z + 1), \mod \varpi \text{ beſtehe.}$$

Seien nun in jeder ϖſtelligen Periode die ausgezeichneten Stellenzeiger, oder die kleinſten poſitiven Reſte jener Stellenzeiger oder derjenigen Ausnahmswerthe der Veränderlichen x nach dem Theiler oder Modul ϖ, bei denen der Quotus u um 1 wächſt, gegeben. Man bezeichne ſie mit dem gemeinſchaftlichen

Zeichen ξ, denjenigen Stellenzeiger, welcher der in (169) vorkommenden durchlaufenden Zahl z entspricht, mit ξ_z, und so wie sie den in (170) angeführten Werthen dieser Zahl entsprechen, mit

$$(172) \qquad \xi_0, \xi_1, \xi_2, \ldots \xi_{\varepsilon-1}.$$

Sezt man demnach in der Congruenz (169), welche die Steigungen der Quoti charakterisirt, für z nach und nach ihre zulässigen Werthe aus (170), so gewinnt man folgende, die Bestimmung des Quotus $\Phi\frac{\vartheta}{\tau} = \delta$ vermittelnden, Congruenzen

$$(173) \qquad \begin{aligned} \delta + \varepsilon\xi_0 &\equiv -1, \mod \varpi \\ \delta + \varepsilon\xi_1 &\equiv -2 \\ \delta + \varepsilon\xi_2 &\equiv -3 \\ &\ldots\ldots\ldots \\ \delta + \varepsilon\xi_{\varepsilon-1} &\equiv -\varepsilon. \end{aligned}$$

In diesen Congruenzen sind aber die Stellenzeiger $\xi_0, \xi_1, \xi_2, \ldots \xi_{\varepsilon-1}$ keineswegs einzeln, sondern blos die ihnen insgesammt zukommenden Werthe bekannt; und es läßt sich also von ihnen lediglich nur ihre Summe, oder die Summe gleich hoher Potenzen derselben, oder ihr Product angeben. Um daher die Constante δ zu bestimmen, wird man am einfachsten diese ε Congruenzen addiren, dabei bemerken, daß bekanntlich die Summe

$$(174) \qquad 1 + 2 + 3 + \ldots + \varepsilon = \frac{\varepsilon(\varepsilon+1)}{2}$$

ist; und endlich wird man die Summe der ausgezeichneten Stellenzeiger ξ mittels des üblichen Summenzeichens Σ, nemlich

$$(175) \qquad \xi_0 + \xi_1 + \xi_2 \ldots + \xi_{\varepsilon-1} = \Sigma\xi$$

andeuten. Auf diesem Wege findet man

$$(176) \qquad \varepsilon\delta + \varepsilon\Sigma\xi \equiv -\frac{\varepsilon(\varepsilon+1)}{2} \mod \varpi.$$

Sei nun erstlich ε ungerad, also $\varepsilon + 1$ gerad, so darf man, vermöge III, 10, die beiden congruenten Zahlen durch ihren gemeinschaftlichen Theiler ε, der gegen den Modul ϖ relativ prim ist, theilen, und erhält

$$(177) \qquad \delta \equiv -\frac{\varepsilon+1}{2} - \Sigma\xi, \mod \varpi.$$

Ist aber zweitens ε gerad, so wird man χ aus

$$(164) \qquad \varepsilon\chi \equiv 1, \mod \varpi$$

bestimmen, und damit die Congruenz (176) multipliciren, wornach man

$$(178) \qquad \delta \equiv -\frac{\varepsilon}{2}(\chi + 1) - \Sigma\xi, \mod \varpi \text{ findet.}$$

Ueber die Einschränkungen der Werthe von δ beachte man jedoch Folgendes: Sollen die Steigungen der Quoti vom nullten Quotus, oder von $x = 0$, an gezählt werden, soll also $u = \text{Ⅎ}\frac{\vartheta}{\tau} = 0$ sein; so muß $0 \overline{\leqq} \vartheta < \mu$,

daher $0 \overline{\leqq} \tau \text{Ⅎ}\frac{\vartheta}{\tau} + \text{Ⅎ}\frac{\vartheta}{\tau} < \varpi\tau$ oder $-\text{Ⅎ}\frac{\vartheta}{\tau} \overline{\leqq} \tau\delta < (\varpi - 1)\tau + \tau - \text{Ⅎ}\frac{\vartheta}{\tau}$

also (179) $\quad -1 < \delta \overline{\leqq} \varpi - 1, \quad \delta = 0, 1, 2, \ldots \varpi - 1$

angenommen werden. Sind aber die Steigungen der Quoti vom ersten Quotus, oder von $x = 1$, an zu zählen, so daß $\text{Ⅎ}\frac{\eta + \vartheta}{\mu} = 0$ ausfällt, so muß

$$0 \overline{\leqq} \eta + \vartheta < \mu \text{ oder } 0 \overline{\leqq} \tau(\delta + \varepsilon) + \text{Ⅎ}\frac{\vartheta}{\tau} < \varpi\tau, \text{ also}$$

(180) $\quad -1 < \delta + \varepsilon \overline{\leqq} \varpi - 1, \quad \delta + \varepsilon = 0, 1, 2, \ldots \varpi - 1$

$\delta = -\varepsilon, -\varepsilon + 1, \ldots . 0, 1, \ldots . \varpi - \varepsilon - 1$ sein.

Allein auf obige Weise wird der Werth von δ nicht aus den einzelnen ausgezeichneten Stellenzeigern (172), sondern blos aus ihrer Summe (175) bestimmt; er ist folglich auch nur wahrscheinlich richtig, und daher noch weiter zu prüfen. Zu diesem Zwecke kann man die Congruenzen (173) zu gleich hohen Potenzen erheben und addiren. Wählt man, als die möglich niedrigste, die zweite Potenz, sezt man dabei nebst (175) auch noch die leicht zu bestimmende Summe

(181) $\quad \xi_0^2 + \xi_1^2 + \xi_2^2 + \ldots + \xi_{\varepsilon-1}^2 = \Sigma(\xi^2)$

und bemerkt man, daß nebst der Summe (174) auch die folgende

(182) $\quad 1^2 + 2^2 + 3^2 + \ldots + \varepsilon^2 = \frac{\varepsilon(\varepsilon+1)(2\varepsilon+1)}{1.2.3}$

gibt; so findet man

(183) $\quad \varepsilon\delta^2 + 2\varepsilon\Sigma\xi . \delta + \varepsilon^2\Sigma(\xi^2) \equiv \frac{\varepsilon(\varepsilon+1)(2\varepsilon+1)}{1.2.3}, \text{ mod } \varpi.$

Der oben gewonnene Werth von δ kann demnach geprüft werden, indem man ihn in diese neue Congruenz sezt und zusieht, ob er auch sie befriedige.

Ein anderer Weg zu gleichem Ziele öffnet sich, wenn man aus den Congruenzen (173) die Glieder $-\varepsilon\xi_0, -\varepsilon\xi_1, \ldots . -\varepsilon\xi_{\varepsilon-1}$ ausdrückt und sie mit einander multiplicirt. Hier findet man die Congruenz

(184) $(\delta+1)(\delta+2)(\delta+3)\ldots(\delta+\varepsilon) \equiv (-\varepsilon)^\varepsilon \xi_0 \xi_1 \xi_2 \ldots \xi_{\varepsilon-1}, \text{ mod } \varpi,$

in welcher das Product der ausgezeichneten Stellenzeiger leicht bekannt wird, und welche der gefundene Werth von δ ebenfalls befriedigen muß, wenn er der wahre sein soll.

Da ferner die Congruenzen (176), (183), (184) nur die eine Unbekannte δ enthalten, so müssen, wenn man diese aus ihnen eliminirt, die daraus entspringenden Congruenzen, weil sie diese Unbekannte nicht mehr enthalten,

die Bedingungen der gleichzeitigen Zulässigkeit der Rechnungsangaben (der Concordanz der Daten) oder der Möglichkeit der Aufgabe aussprechen. Am einfachsten ergibt sich eine solche Bedingungs-Congruenz, wenn man die Congruenz (176) zur zweiten Potenz erhebt, und von der mit ε multiplicirten Congruenz (183) abzieht, nemlich

$$(185) \qquad \varepsilon^2\,[\varepsilon\,\Sigma(\xi^2) - (\Sigma\xi)^2] \equiv \frac{\varepsilon^2(\varepsilon+1)(\varepsilon-1)}{2.\,2.\,3}, \mod \varpi.$$

Diese wird man demnach als vorläufiges Prüfungsmittel der Möglichkeit der gestellten Aufgabe verwenden; und erst, wenn sie zutrifft, wird man an die Bestimmung der Constanten δ gehen. Die einzig und völlig überzeugende Prüfung des mit Hilfe einer der Congruenzen (177) und (178) bestimmten Werthes von δ besteht jedoch darin, daß man ihn in die Congruenz (171) einführt, und nachher für z allmälig ihre Werthe aus (170) sezt, um zu erforschen, ob die für x sich ergebenden Werthe wirklich sämmtliche angewiesenen Ausnahmswerthe $\xi_0, \xi_1, \ldots \xi_{\varepsilon-1}$ sind.

Hat man auf diesen Wegen den Werth von $\delta = \mathfrak{f}\frac{\vartheta}{\tau}$ bestimmt und erprobt, so findet man, indem man den größten gemeinschaftlichen Theiler τ der Zahlen η und μ, so wie auch den Rest $\mathfrak{r}\frac{\vartheta}{\tau}$, nach Gefallen annimmt, die eigentlich zu bestimmende Constante ϑ aus

$$(186) \qquad \vartheta = \tau\delta + \mathfrak{r}\frac{\vartheta}{\tau}.$$

Da man nunmehr nach den Gleichungen (155), (158), (186) die Constanten μ, η, ϑ bestimmt hat; so gibt der Quotus (115) an, wie viele Steigungen oder Ausnahmen von dem nullten oder ersten Quotus an bis zu ihm dem x^{ten} Statt haben; seine Ergänzung zu x, vermöge (59)

$$(187) \qquad x - u = \mathfrak{f}\frac{(\mu-\eta)x + \mu - \vartheta - 1}{\mu},$$

an wie vielen Stellen der Quotus u in demselben Intervalle sich gleich verbleibt; die Vergleichungen des Restes (116), welche in (160), (161), (167), (168) aufgestellt wurden, ob an einer gewissen Stelle x eine Steigung eintrete oder nicht; die Congruenzen (165), (171), an welchen Stellen x der Quotus sich gleich bleibt oder um 1 sich erhebt; endlich der allgemeine Ausdruck (159), (166) der Aenderungen oder der Unterschiede der Quoti, wie viel die Steigung des Quotus überhaupt an jeder Stelle beträgt, folglich eine Function, die nur für gewisse Ausnahmswerthe (172) der Veränderlichen = 1, sonst immer = 0 ist.

Weil der Rest $\mathfrak{r}\frac{\vartheta}{\tau}$ beliebig gewählt werden darf, so ist es offenbar zur Vereinfachung der Rechnungsausdrücke am zuträglichsten, ihn gleich Null, also

$\mathfrak{S}$ durch τ theilbar oder $\mathfrak{S} = \tau\delta$ anzunehmen. Dann aber fällt der den Constanten μ, η, $\mathfrak{S}$ gemeinschaftliche Theiler τ, vermöge (35) aus dem Dividend und Theiler des Quotus u und seiner Aenderung Δu heraus; und es ist daher für diesen Quotus, den man doch eigentlich verlangte, da sein Rest v nur als sein unzertrennlicher Begleiter mit betrachtet werden mußte, dasselbe, als hätte man $\tau = 1$ gesezt, oder μ und η als Primzahlen unter sich angesehen, folglich geradehin

(188) $\mu = \varpi$, $\eta = \varepsilon$, $\mathfrak{S} = \delta$ genommen.

In dieser vereinfachten Darstellung verwandeln sich die Gleichungen (115), (187), (116), (157) in folgende

(189) $$u = \mathfrak{q}\frac{\varepsilon x + \delta}{\varpi}$$

(190) $$x - u = \mathfrak{q}\frac{(\varpi - \varepsilon)x + \varpi - \delta - 1}{\varpi}$$

(191) $$v = \mathfrak{r}\frac{\varepsilon x + \delta}{\varpi}$$

(192) $$\varpi - v = \mathfrak{R}\frac{-(\varepsilon x + \delta)}{\varpi}$$

(193) $$\Delta u = w = \mathfrak{q}\frac{\varepsilon + \mathfrak{r}\frac{\varepsilon x + \delta}{\varpi}}{\varpi} = \mathfrak{q}\frac{\varepsilon(x+1) + \delta}{\varpi} - \mathfrak{q}\frac{\varepsilon x + \delta}{\varpi},$$

die Bedingungen (160) und (161) für das Gleichbleiben der Quoti in

(194) $$\mathfrak{r}\frac{\varepsilon x + \delta}{\varpi} < \varpi - \mathfrak{r}\frac{\varepsilon}{\varpi} = \mathfrak{R}\frac{-\varepsilon}{\varpi}$$

(195) $$\varpi - v = \mathfrak{R}\frac{-(\varepsilon x + \delta)}{\varpi} > \mathfrak{r}\frac{\varepsilon}{\varpi},$$

und die Bedingungen (167), (168) für das Steigen der Quoti in

(196) $$\mathfrak{r}\frac{\varepsilon x + \delta}{\varpi} \geqq \varpi - \mathfrak{r}\frac{\varepsilon}{\varpi} = \mathfrak{R}\frac{-\varepsilon}{\varpi}$$

(197) $$\varpi - v = \mathfrak{R}\frac{-(\varepsilon x + \delta)}{\varpi} \leqq \mathfrak{r}\frac{\varepsilon}{\varpi}.$$

Noch mag bemerkt werden, daß für $\Delta x = 1$ und $\eta < \mu$ die Aenderung $\Delta u = w$ nach (149) oder (153) auch ganz allgemein durch

(198) $$\Delta u = \mathfrak{q}\frac{\eta + \psi + v}{\mu + \psi},\ \psi \geqq 0,\ \psi = 0, 1, 2, \ldots.$$

dargestellt werde, oder auch durch

(199) $$\Delta u = \mathfrak{q}\frac{\eta - \psi + v}{\mu - \psi},\ 0 \leqq \psi \leqq \mu - \eta,\ \psi = 0, 1, \ldots. \mu - \eta$$

weil für $v = \mu - 1$, $\eta - \psi + \mu - 1 \leqq 2(\mu - \psi) - 1$ bleiben muß. Denn sobald $\eta + v < \mu$, ist auch $\eta + v \pm \psi < \mu \pm \psi$, und ist $\eta + v \geqq \mu$, so ist auch $\eta + v \pm \psi \geqq \mu \pm \psi$. Man hat also nur darauf zu sehen, daß

weil $\eta + \nu < 2\mu$ bleiben soll, auch $\eta + \nu \pm \psi < 2(\mu \pm \psi)$ sei, was bei dem oberen Zeichen immer eintrifft.

4. Der wichtigste und zugleich einfachste Fall ist der, wo unter je ϖ Stellen nur an einer einzigen eine Steigung des Quotus oder unter je ϖ nach einander folgenden Werthen der Veränderlichen x blos ein Ausnahmswerth $\equiv \xi$, mod ϖ vorkommt, folglich $\varepsilon = 1$ ist. Da ist $\Sigma\xi = \xi$, $\Sigma(\xi^2) = \xi^2$, also die Congruenz (185) identisch. Ferner findet man vermöge (177)

(200) $\quad \delta \equiv -(\xi+1)$, mod ϖ,

folglich, die Perioden mögen bei dem nullten oder ersten Gliede, bei $x \equiv 0$ oder $x \equiv 1$, mod ϖ, anheben,

(201) $\quad \delta = \varpi - \xi - 1$.

Zur Prüfung dieses Ausdruckes hat man vermöge (164) die Hilfszahl $\chi = 1$, also nach (171) $x \equiv -1(-1-\xi+0+1) \equiv \xi$, mod ϖ; daher der Ausdruck richtig.

Dann ist die Anzahl der Ausnahmsfälle, von $x = 0$ oder 1 bis $x = x$, oder die Menge der Steigungen der Quoti vom nullten oder ersten bis zum x^{ten}

(202) $\quad u = \mathfrak{q}\frac{x+\varpi-\xi-1}{\varpi} = \mathfrak{q}\frac{x+\varpi-(\xi+1)}{\varpi}$,

die Anzahl der Gleichbleibungen der Quoti

(203) $\quad x-u = \mathfrak{q}\frac{(\varpi-1)x+\xi}{\varpi}$,

die Bedingung einer Steigung oder Ausnahme

(204) $\quad \nu = \mathfrak{r}\frac{x-\xi-1}{\varpi} = \varpi - 1$, oder $x \equiv \xi$, mod ϖ

und der Betrag der Steigung an einer angewiesenen Stelle x

(205) $\quad \Delta u = \mathfrak{q}\frac{x+\varpi-\xi}{\varpi} - \mathfrak{q}\frac{x+\varpi-\xi-1}{\varpi} = \mathfrak{q}\frac{1+\mathfrak{r}\frac{x-\xi-1}{\varpi}}{\varpi} = \mathfrak{q}\frac{\mathfrak{R}\frac{x-\xi}{\varpi}}{\varpi}$

Anwendungen in §§. 24. 52.