Ueber

relative Prim- und correspondirende Zahlen, primitive und sekundäre Wurzeln und periodische Decimalbrüche.

---

§. 1.

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

Es ist klar, dass die Summe jeder zwei von beiden Endpunkten dieser Reihe gleich weit entfernten Zahlen $= c$, und dass, wenn z. B. $c = 15$, also $c - 1$ grade ist, ein Dreifaches in beliebiger Entfernung vom ersten Endpunkte einem Dreifachen in derselben Entfernung vom zweiten entspricht. Dasselbe ist mit den Fünffachen der Fall. Ist z. B. $c = 30$, also $c - 1$ ungrade, so gilt das eben Bemerkte auch für die Primfaktoren 2, 3, 5, und so fort. Die zwischen und neben den Primfaktoren von c und ihren Vielfachen stehenden Zahlen sind die relativen Primzahlen gegen c, die kleiner als c. In welcher Entfernung daher auch eine derselben vom ersten Endpunkte vorkommen mag, in derselben Entfernung vom zweiten muss wieder eine stehen. Demgemäss folgt:

1. Sämmtliche relative Primzahlen gegen eine Zahl c (ausser 2), die kleiner als c, kommen paarweise vor.

2. Je 2 relative Primzahlen, die einander entsprechen, bilden die Summe c (Summen-Paar).

3. Die Summe aller relativen Primzahlen gegen eine Zahl c, die kleiner als c, ist theilbar durch c.

4. Ist z. B. $c = 105 = 3 \,.\, 5 \,.\, 7$, so sind alle Dreifachen von 1 bis 105, der Anzahl nach $= \frac{105}{3}$, bleiben ohne Dreifache: $105 - \frac{105}{3} = \frac{105 \,.\, 2}{3}$ Zahlen; alle Fünffachen $= \frac{105}{5}$, ohne Dreifache $= \frac{105 \,.\, 2}{5 \,.\, 3}$, bleiben ohne Drei- und Fünffache: $\frac{105 \,.\, 2}{3} - \frac{105 \,.\, 2}{5 \,.\, 3} = \frac{105 \,.\, 2 \,.\, 4}{3 \,.\, 5}$ Zahlen; alle Siebenfachen $= \frac{105}{7}$, ohne Drei- und Fünffache $= \frac{105 \,.\, 2 \,.\, 4}{7 \,.\, 3 \,.\, 5}$, bleiben ohne Drei-, Fünf-, Siebenfache, d. h. alle relativen Primzahlen gegen 105: $\frac{105 \,.\, 2 \,.\, 4}{3 \,.\, 5} - \frac{105 \,.\, 2 \,.\, 4}{7 \,.\, 3 \,.\, 5} = \frac{105 \,.\, 2 \,.\, 4 \,.\, 6}{3 \,.\, 5 \,.\, 7} = 48$. Man erhält daher die Anzahl aller relativen Primzahlen gegen eine Zahl c, die kleiner sind als c, wenn man c mit dem Produkte ihrer verschiedenen Primfaktoren dividirt, und mit demselben, nachdem von jedem 1 subtrahirt worden, den Quotienten multiplicirt.

5. Sämmtliche Faktoren der $105 = 1, 3, 5, 7, 15, 21, 35, 105$; folglich:

Alle	1 Fachen	=	105,	ohne	3, 5, 7 Fache	=	d. Anz. d. rel. Pz. g.	105,	=	$\frac{105 \,.\, 2 \,.\, 4 \,.\, 6}{3 \,.\, 5 \,.\, 7}$	=	48.
„	3 „	=	35,	„	5, 7 „	=	„ „ „ „ „ „	35,	=	$\frac{35 \,.\, 4 \,.\, 6}{5 \,.\, 7}$	=	24.
„	5 „	=	21,	„	3, 7 „	=	„ „ „ „ „ „	21,	=	$\frac{21 \,.\, 2 \,.\, 6}{3 \,.\, 7}$	=	12.
„	7 „	=	15,	„	3, 5 „	=	„ „ „ „ „ „	15,	=	$\frac{15 \,.\, 2 \,.\, 4}{3 \,.\, 5}$	=	8.
„	15 „	=	7,	„	7 „	=	„ „ „ „ „ „	7,	=	$\frac{7 \,.\, 6}{7}$	=	6.
„	21 „	=	5,	„	5 „	=	„ „ „ „ „ „	5,	=	$\frac{5 \,.\, 4}{5}$	=	4.
„	35 „	=	3,	„	3 „	=	„ „ „ „ „ „	3,	=	$\frac{3 \,.\, 2}{3}$	=	1.
„	105 „	=	1,								=	1.

Universitäts- und
Landesbibliothek Düsseldorf

Die Summe der Zahlen in der letzten Colonne ist die gegebene Zahl 105; da sie alle relativen Primzahlen gegen den Faktor 105, so wie alle Ein- und Vielfachen der anderen Faktoren, jedes einmal, in sich fasst. „Jedes einmal" wird aber durch die Anzahl der relativen Primzahlen gegen jeden einzelnen Faktor bestimmt. Folglich ist die Anzahl der relativen Primzahlen gegen sämmtliche Faktoren einer Zahl c, $= c$.

§. 2.

$$1a,\ 2a,\ 3a,\ 4a,\ \ldots\ldots (c-1)\,a.$$

1. Ist c eine Primzahl, a relative Primzahl gegen c, und dividirt man jedes dieser Produkte mit c; so entsteht überall ein Rest; denn c relative Primzahl gegen jeden der beiden Faktoren.

2. Jeder Rest ist wieder relative Primzahl gegen c; denn er ist kleiner als c und c eine Primzahl.

3. Sämmtliche Reste sind unter einander verschieden; denn $ab = cy + r$*) und $ad = cy + r$ gäbe: $a\,(b-d) = cy$, also $a\,(b-d)$ theilbar durch c, was nicht der Fall; da a relative Primzahl gegen c, und $(b-d) < c$. Sämmtliche Reste fallen daher mit allen relativen Primzahlen gegen c, die kleiner als c, in irgend einer Ordnung zusammen.

4. Diese drei Sätze bleiben wahr, wenn auch c keine Primzahl, dagegen die Faktoren neben a die sämmtlichen relativen Primzahlen gegen c sind, die kleiner als c, und a seine Bedeutung behält.

5. Ist c eine Primzahl, $a < c$ aber > 1; so kann, wenn man jedes Glied der Reihe mit c dividirt, das letzte der ersten Hälfte, nämlich $\frac{c-1}{2}\,a$, nie den Rest $\frac{c-1}{2}$ liefern. Denn $\frac{c-1}{2}\,a = cy + \frac{c-1}{2}$ gäbe: $(c-1)\,a = cy + c - 1$, also $(c-1)\,(a-1) = cy$, theilbar durch c, was nicht möglich, da $c-1$ und $a-1$ kleiner als c und c eine Primzahl **). Wäre nun in der ersten Hälfte der Reihe jeder Rest $< \frac{c}{2}$, also der grösste ihres letzten Gliedes $= \frac{c-1}{2} - 1$, der kleinste $= 1$, so würde folgen, da jeder Rest der ersten Hälfte $+$ Rest ihres letzten Gliedes $=$ einem Reste der zweiten: $1 + \frac{c-1}{2} - 1 = \frac{c-1}{2} =$ Rest der zweiten, und $< \frac{c}{2}$, gegen die Annahme. Es kann daher in keiner der beiden Reihen-Hälften jeder Rest kleiner sein als $\frac{c}{2}$.

6. Bezeichnet man die Reste der ersten Hälfte, welche kleiner als $\frac{c}{2}$, mit $r_1, r_2, r_3, \ldots$, die, welche grösser, mit $\rho_1, \rho_2, \rho_3, \ldots$; so ist jede der Differenzen: $c - \rho_1, c - \rho_2, c - \rho_3, \ldots$, $< \frac{c}{2}$, aber keine $=$ einem der Reste: $r_1, r_2, r_3, \ldots$; denn $c - \rho = r$ gäbe: $c = r + \rho$, und $ma = cy + r$, $na = cy + \rho$: $(m+n)\,a = cy + r + \rho = cy$, also theilbar durch c, was nicht der Fall, da $a < c$, $(m+n) < c$ und c eine Primzahl. Die Zahlen $r_1, r_2, r_3, \ldots c - \rho_1$, $c - \rho_2, c - \rho_3, \ldots$ fallen daher mit den Zahlen $1, 2, 3, \ldots \frac{c-1}{2}$ in irgend einer Ordnung zusammen.

7. $a^{\frac{c-1}{2}} = cy \pm 1$, je nachdem die Anzahl der x Reste in der ersten Hälfte der Reihe, welche $> \frac{c}{2}$, grade oder ungrade. Denn $1a.\ 2a.\ 3a \ldots \frac{c-1}{2}\,a = 1.\ 2.\ 3 \ldots \frac{c-1}{2}.\ a^{\frac{c-1}{2}} = (cy + r_1)\,(cy + r_2) \ldots (cy + \rho_1)\,(cy + \rho_2) \ldots (cy + \rho_x) = cy + r_1, r_2 \ldots \rho_1, \rho_2 \ldots \rho_x$. Da aber $na = cy + \rho = cy + c - \rho = cy - \rho$; so wird, wenn man die negativen Reste setzt,

---

*) Der Kürze wegen bezeichne y jeden Quotienten, jeden einfachen oder zusammengesetzten Ausdruck in ganzen Zahlen.

**) $a > c$, aber nicht theilbar durch c, und nicht $= nc + 1$, wo n jede ganze Zahl, giebt dasselbe Resultat.

Universitäts- und
Landesbibliothek Düsseldorf

$1.\,2.\,3 \ldots . \frac{c-1}{2}\, a^{\frac{c-1}{2}} = cy + r_1, r_2 \ldots . \rho_1 . \rho_2 \ldots . \rho_x . (-1)^x$, daher $1.\,2.\,3 \ldots . \frac{c-1}{2}$ $(a^{\frac{c-1}{2}} - (-1)^x) = cy$, (No. 6); folglich theilbar durch c, und, weil es keiner der Faktoren von 1 bis $\frac{c-1}{2}$ ist, und c eine Primzahl, $a^{\frac{c-1}{2}} - (-1)^x) = cy$, also $a^{\frac{c-1}{2}} = cy + (-1)^x$, w. z. b. w.

Es folgt sogleich, x mag grade oder ungrade sein, $a^{c-1} = cy + (-1)^{2x} = cy + 1$, wenn c eine Primzahl und $a < c$.

8. Ist c eine Primzahl, so sind $2, 3, 4, \ldots . c-2$ correspondirende Zahlen, d. h. für jede Zahl a derselben giebt es unter ihnen eine andere Zahl b, dass $ab = cy + 1$. Fügt man nämlich 1 und $c-1$ dieser Reihe hinzu, so hat man sämmtliche relativen Primzahlen gegen c, die als Reste wieder erscheinen, wenn man jede mit a multiplicirt und mit c dividirt, also auch der Rest 1. Nun giebt aber weder $a\,.\,1$, noch $a\,(c-1)$, noch a^2 den Rest 1; folglich muss es ab sein. In der That würde $a^2 = cy + 1$, also $a^2 - 1 = (a+1)\,(a-1) = cy$ etwas Unmögliches enthalten; da a höchstens $= c-2$ und c eine Primzahl.

9. Wenn c keine Primzahl, so kann sehr wohl $(a+1)\,(a-1) = cy$, oder $a^2 = cy + 1$ sein, z. B. wenn $c = 15$, $a = 4$ oder 11; also kann es auch unter den relativen Primzahlen gegen c, von der ersten nach 1 bis nächsten vor $c-1$, Zahlen geben, die nicht anders correspondirend sind, als mit sich selber. Ist dann a eine solche, so muss es auch $c-a$ sein; denn auch $(c-a)^2 = cy + a^2 = cy + 1$. Das Produkt zweier nicht correspondirenden Zahlen $= cy - 1$; da $a\,(c-a) = ac - a^2 = ac - (cy+1) = cy - 1$. Da $1^2 = cy + 1$, $(c-1)^2 = cy + 1$ und $1.\,(c-1) = cy - 1$, so ist $1, c-1$ das allgemeine nicht-correspondirende Zahlen-Paar.

10. Ist c eine beliebige Zahl, z. B. $c = 15$, also p die Anzahl der relativen Primzahlen gegen 15, $= \frac{15\,.\,2\,.\,4}{3\,.\,5} = 8$, und sucht man zu jeder, von der nach 1 bis zu der vor $c-1$, ihre correspondirende oder nicht-correspondirende Zahl; so wird: 2.8, 4.11, 7.13, 8.2, 11.4, 13.7, $= 15\,y \pm 1$, je nachdem das correspondirende oder nichtcorrespondirende Paar gemeint ist. Jedes muss zweimal vorkommen, also alle Paare die $p-2$ relativen Primzahlen von 2 bis 13 auch zweimal enthalten. Nimmt man daher von jedem Doppelpaar ein Paar und multiplicirt diese $\frac{p-2}{2}$ Paare mit einander; so wird: $2\,.\,4\,.\,7\,.\,8\,.\,11\,.\,13 = 15\,y - 1$; folglich $1\,.\,2\,.\,4\,.\,7\,.\,8\,.\,11\,.\,13\,.\,14 = (15\,y - 1)\,(15 - 1) = 15\,y + 1$, und daher das Product aller relativen Primzahlen gegen eine Zahl c, die kleiner als c, $= cy \pm 1$, je nachdem unter den relativen Primzahlen von der ersten nach 1 bis ersten vor $c-1$ ein nicht-correspondirendes Zahlen-Paar vorhanden ist oder nicht. Für $c = 18$ ist: $1\,.\,5\,.\,7\,.\,11\,.\,13\,.\,17 = 18y - 1$, und für jede Primzahl c: $1\,.\,2\,.\,3\,.\,4 \ldots . (c-1) = cy - 1$.

11. Ist c eine Primzahl, $an = cy + 1$, $bm = cy + 1$ und $a + b = c$; so folgt: $am = cy - 1$, $bn = cy - 1$ und $n + m = c$. Denn $am + bm = am + cy + 1 = cm$, also $am = cy - 1$; eben so $bn = cy - 1$; daher $an + am = a(n+m) = cy$, also theilbar durch c, und, da es a nicht ist, $n + m = cy$; aber $n < c$, $m < c$; folglich $n + m = c$. Ist $ab = cy + 1$, $a + b = c$; so folgt eben so: $a^2 = cy - 1$, $b^2 = cy - 1$. Für welche Primzahl c aber auch zwei relative Primzahlen a, b vorkommen, dass $ab = cy + 1$, $a + b = c$, für dieselbe giebt es nur ein solches Zahlen-Paar (singuläres). Denn wäre auch $pq = cy + 1$, $p + q = c$; so entstände: $a^2 - p^2 = (a+p)\,(a-p) = cy$, also theilbar durch c, was nur möglich, wenn $p = b$, so dass p und q nicht von b und a unterschieden sind. Ist daher die Primzahl c von der Form $4\,m + 3$, und bildet man alle $\frac{c-3}{2} = 2\,m$ Summen-Paare der $c-3$ Zahlen: $2, 3, 4, \ldots . c-2$; so hat jedes ein correspondirendes Summen-Paar unter den $2\,m$ Paaren; weil sonst, da $2\,m$ grade, und zu jeder

Universitäts- und
Landesbibliothek Düsseldorf

dieser Zahlen eine correspondirende unter ihnen vorhanden, Summen-Paare in grader Anzahl übrig blieben, wovon jedes singulär, was nicht möglich. Also kann keine Primzahl c, von der Form $4m+3$ ein singuläres Zahlen-Paar haben. Ist dagegen die Primzahl c von der Form $4m+1$, folglich $\frac{c-3}{2}=2m-1$, also ungrade; so kann es nicht für jedes der $2m-1$ Summen-Paare ein anderes unter ihnen geben, das mit ihm correspondirt, eins wird immer übrig bleiben. Jede dieser Zahlen hat aber unter ihnen eine correspondirende; folglich müssen die Summanden des übrig bleibenden Summen-Paares correspondirend, und beide daher ein singuläres Zahlen-Paar sein. Es folgt, dass es nur für Primzahlen von der Form $4m+1$ ein singuläres Zahlen-Paar geben kann, und für jede derselben ein solches geben muss. Für $c=11=4.2+3$ bilden die Zahlen von 2 bis 9 folgende $2.2=4$ Summen-Paare: $2+9$, $3+8$, $4+7$, $5+6$; mit dem ersten correspondirt: $6+5$, mit dem zweiten: $4+7$, mit dem dritten: $3+8$, mit dem vierten: $9+2$. Für $c=13=4.3+1$ geben die Zahlen von 2 bis 11 folgende $2.3-1=5$ Summen-Paare: $2+11$, $3+10$, $4+9$, $5+8$, $6+7$; mit dem ersten correspondirt: $7+6$, mit dem zweiten: $9+4$, mit dem dritten: $10+3$, mit dem fünften: $11+2$, nur mit dem vierten das vierte selber als $8+5$. — Ist daher $a<c$, und soll a^2+1 theilbar sein durch eine Primzahl c; so muss c von der Form $4m+1$, und a eine der beiden singulären Zahlen sein, z. B. 8^2+1 und 5^2+1 theilbar durch $13,=4.3+1$; und, wenn c keine Primzahl: 7^2+1 und 18^2+1 theilbar durch $25=4.6+1$; da $p=\frac{25.4}{5}=20$, also $\frac{p-2}{2}=9$ ungrade.*)

12. Ist c eine beliebige Zahl, a relative Primzahl gegen c, und die Anzahl aller relativen Primzahlen gegen c, die kleiner als c, $=p$; so hat man stets $a^p=cy+1$. Multiplicirt man nämlich jede dieser relativen Primzahlen mit a, so entstehen p Producte, jedes $=cy+r$, wo r jeden der p Reste repräsentirt, die zusammen wieder die p relativen Primzahlen sind, welche mit a multiplicirt worden, (No. 3 u. 4). Werden daher auch alle jene p Produkte mit einander multiplicirt, so wie die ihnen gleichen Summen: $cy+r$; so entsteht: $(cy\pm1).a^p=cy+(cy\pm1)$, (No. 10); folglich $(cy\pm1).(a^p-1)=cy$, also theilbar durch c; da es nun $cy\pm1$ nicht ist, so muss es a^p-1, folglich $a^p=cy+1$ sein. Ist z. B. $c=14$, $a=3$, also $p=\frac{14.1.6}{2.7}=6$; so muss $3^6=14y+1$, oder 3^6-1 theilbar sein durch 14.

13. Ist $c=14$, also $p=6$, und a relative Primzahl gegen 14, ausser 1; so ist, weil $a^6=14y+1$, unmöglich $a^5=14y+1$, da sogleich folgen würde: $a^6=14y+a$. Eben so wenig ist $a^4=14y+1$, weil dies gäbe: $a^6=14y+a^2$. Allein möglich ist: $a^3=14y+1$, $a^2=14y+1$; da hierneben ohne Widerspruch: $a^6=14y+1$. Man sieht, dass, wenn allgemein $a^e=cy+1$, wo $e<p$, und kleinster Exponent zu a für den Rest 1, p allemal durch e theilbar sein, und dass, wenn $d<e$, und $a^d=cy+1$, $a^e=cy+1$, und d kleinster Exponent, d und e in p, als auch d in e aufgehen muss.

Wenn c eine Primzahl, also $p=c-1$, so ist $a^{c-1}=cy+1$, und ist zugleich $c-1$ der kleinste Exponent zu a für den Rest 1, und $a<c$; so ist a primitive Wurzel von c. Ist c eine Primzahl, $c-1$ theilbar durch e, so ist, wenn $a<c$, und in $a^e=cy+1$, e kleinster Exponent zu a für den Rest 1, a sekundäre Wurzel von c zu e. Es ist z. B. 3 primitive Wurzel von 7, da erst $3^6=7y+1$; dagegen 2 secundäre Wurzel von 7 zu 3, weil schon $2^3=7y+1$.

14. Es folgt: jede Zahl a, die kleiner als c, ist entweder primitive oder sekundäre Wurzel von c. Zu keiner solchen Zahl a können verschiedene Exponenten für den Rest 1

*) Hat die Zahl a eine correspondirende Zahl x, so ergiebt sich dieselbe aus der Gleichung: $ax=cy+1$; von den nicht-correspondirenden Zahlen die eine am schnellsten durch Quadriren der relativen Primzahlen gegen c, innerhalb der ersten Hälfte ihrer Reihe, denn $a^2=cy+1$, die zweite durch Subtraction von c; eben so die singulären Zahlen, denn $a^2=cy-1$.

Universitäts- und
Landesbibliothek Düsseldorf

kleinste zugleich sein; daher sind die primitiven und sekundären Wurzeln von c sämmtlich unter einander verschieden, und werden gebildet von sämmtlichen relativen Primzahlen gegen c, die kleiner als c; folglich ist ihre Anzahl $= c-1$, ihre Summe theilbar durch c, ihr Produkt $= cy-1$.

15. Ist a primitive Wurzel von c, so sind alle $c-1$ Reste, wenn man $a^1, a^2, a^3 \ldots a^{c-1}$ mit c dividirt, unter einander verschieden. Denn ist z. B. $c=41$, und es wäre etwa $a^{10} = 41y+r$ und auch $a^{18} = 41y+r$; so entstände: $a^{18} - a^{10} = a^{10}(a^8-1) = 41y$, also theilbar durch 41, a^{10} ist es nicht, also müsste es a^8-1, folglich $a^8 = 41y+1$ sein, was nicht der Fall, da erst $a^{40} = 41y+1$. — Ist a sekundäre Wurzel von c zu e, so gilt dasselbe für die e Reste von $a^1, a^2, a^3 \ldots a^e$.

16. Eine primitive Wurzel von c giebt alle von c, und eine sekundäre Wurzel von c zu e alle von c zu e. Ist z. B. a primitive Wurzel von 41, so sind sämmtliche primitive Wurzeln von 41 die Reste von $a^1, a^3, a^7 \ldots a^{39}$, wo die Exponenten sämmtliche 16 relative Primzahlen gegen 40; und ist b sekundäre Wurzel von 41 zu 10, so sind sämmtliche sekundäre Wurzeln von 41 zu 10 die 4 Reste von: b^1, b^3, b^7, b^9. Denn aus $a^{40} = 41y+1$ folgt: $(a^{40})^3 = (a^3)^{10} = 41y+1$, und, ist $a^3 = 41y+h$, h primitive Wurzel von 41. In der That, wäre etwa schon $h^8 = 41y+1$, so entstände $a^{3\cdot 8} = 41y+1$, was unmöglich, da $3 \,.\, 8 < 40$ und a primitive Wurzel von 41; wäre $h^{20} = 41y+1$, so entstände: $a^{3\cdot 20} = 41y+1$, was wieder unmöglich, da 40 in $3 \,.\, 20$ aufgehen müsste, was wegen der relativen Primzahl 3 nicht der Fall; daher erst $h^{40} = 41y+1$. Ist $a^7 = 41y+k$, so ist k primitive Wurzel von 41, und, wegen No. 15, h nicht $= k$, u. s. w.

Giebt es daher eine primitive Wurzel a von 41, so existiren deren $16 = \frac{40 \,.\, 1 \,.\, 4}{2 \,.\, 5}$ und nicht mehr. Denn wäre r nicht einer jener 16 Reste, also etwa a^4 oder $a^{15} = 41y+r$ (No. 15); so entstände: $a^{4\cdot 10} = 41y+r^{10} = 41y+1$, oder $a^{15\cdot 8} = 41y+r^8 = 41y+1$; folglich r nicht primitive Wurzel. Giebt es eine sekundäre Wurzel b von 41 zu 10; so existiren $4 = \frac{10 \,.\, 1 \,.\, 4}{2 \,.\, 5}$ und nicht mehr. Denn wäre r nicht einer jener 4 Reste, also etwa b^5 oder $b^8 = 41y+r$ (No. 15); so entstände: $b^{5\cdot 2} = 41y+r^2 = 41y+1$, oder $b^{8\cdot 5} = 41y+r^5 = 41y+1$; folglich r nicht sekundäre Wurzel von 41 zu 10. Daher: so viele relative Primzahlen gegen $c-1$, eben so viele primitive Wurzeln von c, und so viele relative Primzahlen gegen e, eben so viele secundäre Wurzeln von c zu e. Hieraus lässt sich, mit Hinblick auf No. 14, die Existenz primitiver Wurzeln von jeder Primzahl c, so wie die der sekundären Wurzeln von c zu jedem Exponenten e, der Faktor von $c-1$, leicht nachweisen. Es folgt nun ferner, dass die primitiven Wurzeln stets paarweise vorkommen, einzeln nur die von $c=2$ und 3, die $=1$ und 2; eben so die sekundären Wurzeln, einzeln nur die von c zu 1 und 2, die $=1$ und $c-1$; endlich, dass die Anzahl aller Wurzeln von c zu allen Exponenten, die Factoren von e, $= e$, es mag $e = c-1$ oder irgend ein anderer Faktor von $c-1$ sein. (§. 1, No. 5.)

17. Eine primitive Wurzel von c giebt alle sekundären Wurzeln von c, und eine sekundäre Wurzel von c zu e die von c zu $\frac{e}{n}$, wenn e theilbar durch n. Denn aus $a^{40} = 41y+1$ folgt: $a^{4\cdot 10}, a^{5\cdot 8}, a^{2\cdot 20} = 41y+1$. Ist nun z. B. $a^4 = 41y+h$, so ist h secundäre Wurzel von 41 zu 10; da z. B. $h^5 = 41y+1$ geben würde: $a^{4\cdot 5} = 41y+1$, was nicht möglich, da a primitive Wurzel von 41, u. s. w., No. 16 giebt dann die übrigen secundären Wurzeln von 41 zu 10. Wie mit den Exponenten 40 und 10, eben so ist es mit den Exponenten e und $\frac{e}{n}$.

18. Die Produkte jeder zwei sekundären Wurzeln von c zu verschiedenen Exponenten geben primitive oder bestimmte sekundäre Wurzeln von c. Ist z. B. a sekundäre Wurzel von 41 zu 8, b zu 5; so ist ab, oder wenn $ab = 41y+h$, h primitive Wurzel von 41; denn z. B. $h^{20} = 41y$

Universitäts- und
Landesbibliothek Düsseldorf

$+1$ gäbe: $a^{20} . b^{20} = 41y+1$, was nicht möglich, da wol $b^{20} = 41y+1$, aber nicht, wie erforderlich, auch $a^{20} = 41y+1$, u. s. w.; a sekundäre Wurzel zu 4, b zu 5, giebt h sekundäre Wurzel zu 20; a zu 8, b zu 10 giebt h zu 40 oder primitive Wurzel; a zu 2, b zu 10 giebt h zu 5; denn $a = c-1$, und sowol $(c-1)^5$ als b^5, $= 41y-1$; daher schon $(ab)^5 = 41y + h^5 = 41y+1$, u. s. w.

19. Alle primitiven Wurzeln von c, so wie alle sekundären Wurzeln von c zu e sind correspondirende Zahlen, ausser, wenn $e=1$ oder 2. Denn ist z. B. a sekundäre Wurzel von 41 zu 20, so sind alle sekundären Wurzeln von 41 zu 20 die Reste von a^1, a^3, a^7, a^9, a^{11}, a^{13}, a^{17}, a^{19}; daher $a^{19} . a^1 = a^{20} = 41y+1$, $a^{17} . a^3 = a^{20} = 41y+1$, u. s. w.; folglich auch die Produkte der Reste dieser mit einander multiplicirten Potenzen $= 41y+1$, w. z. b. w. Es folgt, dass das Produkt aller Wurzeln zu jedem Exponenten e, $= cy+1$, nur wenn $e=2$ ist die Wurzel: -1 oder $c-1$; und dass daher das sämmtlicher Wurzeln von c zu allen Exponenten, die Faktoren von e, $= cy \mp 1$, je nachdem unter diesen Exponenten die 2 vorkommt oder nicht, z. B. das aller sekundären Wurzeln von 41 zu 1, 2, 4, 8, $= 41y-1$; das aller von 41 zu 1, 5. $= 41y+1$; das aller von 73 zu 1, 3, 9, $= 73y+1$.

20. Die Summe aller Wurzeln von c zu allen Exponenten, die Faktoren vom Exponenten e, ist theilbar durch c. Für $e = c-1$ erhellet die Wahrheit aus No. 14. Für $c=41$, $e=8$ ist die Summe der Wurzeln zu allen Exponenten, die Faktoren der 8, die zu 1, 2. 4, 8, also ihre Anzahl $= 8$. Ist nun a primitive Wurzel von 41, b irgend eine der 8 Wurzeln; so giebt es ein x, dass $a^x = 41y+b$; folglich $a^{x \cdot 8} = 41y+b^8 = 41y+1$; also hat x die 8 Werthe: 0, 5, 10, 15, 20, 25, 30, 35, und die Reste von a^0, a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35} sind die 8 Wurzeln. Die Summe dieser Potenzen aber $= \frac{a^{40}-1}{a^5-1}$, wo a^5-1 relative Primzahl gegen c; denn a^5-1 theilbar durch c gäbe: $a^5 = 41y+1$, was unmöglich, da a primitive Wurzel von c. Also $a^{40}-1$ theilbar durch 41 (a^5-1); folglich die Summe der Potenzen durch 41, also auch die der zugehörigen 8 Reste oder Wurzeln. Für $e=10$ ist die Anzahl der Wurzeln zu allen Exponenten, die Faktoren der 10, also zu 1, 2, 5, 10, $= 10$, und $a^{x \cdot 10} = 41y+b^{10} = 41y+1$; folglich hat x die 10 Werthe: 0, 4, 8, 12, 16, 20, 24, 28, 32, 36. Die Summe der Potenzen $= \frac{a^{40}-1}{a^4-1}$ also die Summe der 10 Wurzeln wieder theilbar durch c, u. s. w.

Da die Summe der Wurzeln zu den Exponenten 1, 2, 4, 8 theilbar durch 41, eben so die zu 1, 2, 4; so ist es die zu 8 allein; da es die zu 1, 2, 5, 10, und die zu 1, 5; so muss es die zu 2, 10 allein sein; der Rest der Wurzel zu 2, $= -1$; also der von der Summe der Wurzel zu 10, $= +1$, so dass

$$\text{für } c=41: \begin{array}{cccccccc} 1 & 1 & 2 & 4 & 4 & 4 & 8 & 16 \\ 1, & 2, & 4, & 5, & 8, & 10, & 20, & 40; \\ +1 & -1 & 0 & -1 & 0 & +1 & 0 & 0 \end{array}$$

$$\text{für } c=67: \begin{array}{cccccccc} 1 & 1 & 2 & 2 & 10 & 10 & 20 & 20 \\ 1, & 2, & 3, & 6, & 11, & 22, & 33, & 66; \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{array}$$

$$\text{für } c=73: \begin{array}{ccccccccccccc} 1 & 1 & 2 & 2 & 2 & 4 & 6 & 4 & 6 & 8 & 12 & 24 \\ 1, & 2, & 3, & 4, & 6, & 8, & 9, & 12, & 18, & 24, & 36, & 72. \\ +1 & -1 & -1 & 0 & +1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \qquad \text{U. s. w.}$$

wo der Rest, welchen die Summe der Wurzeln zu jedem Exponenten giebt, unter demselben steht, darüber die Anzahl der dem Exponenten angehörigen Wurzeln.

Ist $c = 4m+1$, so ist 4 Faktor von $c-1$, und das singuläre Zahlen-Paar bildet allemal die beiden sekundären Wurzeln von c zu 4; eben weil ihre Summe theilbar durch c, und beide correspondirend sind (No. 11.).

21. Wenn $c = 4m+3$, also $\frac{c-1}{2} = 2m+1$; so ergänzen die sekundären Wurzeln von c zu $\frac{c-1}{2}$ und die primitiven Wurzeln von c einander zu c. Denn ist z. B. a primitive Wurzel von

Universitäts- und
Landesbibliothek Düsseldorf

$67 = 4m + 3$, so folgt: $a^{\frac{67-1}{2}} = 67y - 1$; daher, weil $\frac{67-1}{2} = 33$, ungrade: $(-a)^{33} = 67y + 1$, und 33 kleinster Exponent; denn z. B. $(-a)^{11} = (-1)^{11} a^{11} = -a^{11} = 67y + 1$ würde geben: $a^{11} = 67y - 1$, $a^{22} = 67y + 1$, was unmöglich, da a primitive Wurzel von 67; folglich $-a$ oder $c - a$ sekundäre Wurzel zu $\frac{c-1}{2}$, und $a + (c - a) = c$. Dasselbe findet statt für die sekundären Wurzeln zu e und $\frac{e}{2}$, wenn $\frac{e}{2}$ eine ganze Zahl und ungrade, es mag $c = 4m + 3$ oder $4m + 1$ sein, z. B. für die sekundären Wurzeln von 67 zu 22 und 11, von 41 zu 10 und 5, von 73 zu 18 und 9. Für diese Fälle ergeben sich die Wurzeln zu dem einen Exponenten aus denen zu dem anderen durch Subtraktion von c.

22. Wenn $c = 4m + 1$, also $\frac{c-1}{2} = 2m$; so ergänzen die primitiven Wurzeln von c einander zu c. Denn ist z. B. a primitive Wurzel von 73, so ist $a^{\frac{73-1}{2}} = 73y - 1$, folglich, da $\frac{73-1}{2}$ grade, auch $(-a)^{\frac{73-1}{2}} = 73y - 1$; also $(-a)^{73-1} = 73y + 1$, und $73 - 1$ kleinster Exponent; denn z. B. $(-a)^{24} = 73y + 1$ gäbe: $a^{24} = 73y + 1$, was unmöglich; $(-a)^{9} = 73y + 1$ gäbe: $a^{9} = 73y - 1$, $a^{18} = 73y + 1$, was wieder unmöglich; daher sind a und $c - a$ primitive Wurzeln, und $a + (c - a) = c$. Dasselbe findet statt für die sekundären Wurzeln zu e, wenn $\frac{e}{2}$ eine ganze Zahl und grade, z. B. für die von 41 zu 20, 8, 4; für die von 73 zu 36, 24, 12, 8, 4. Für diese Fälle ergiebt sich die eine Hälfte der Wurzeln zu einem Exponenten aus der anderen zu demselben Exponenten durch Subtraktion von c. Für $c = 4m + 3$ findet weder das Eine noch das Andere statt. Denn ist a primitive Wurzel von c, so ist zwar auch $(-a)^{\frac{c-1}{2}} = cy + 1$, aber $c - 1$ nicht kleinster Exponent; da sonst $(-a)^{\frac{a-1}{2}} = cy - 1$, also, da $\frac{c-1}{2}$ ungrade, $a^{\frac{c-1}{2}} = cy + 1$, und daher a nicht primitive Wurzel wäre. Eben so giebt es für $c = 4m + 3$ keine Zahl $\frac{e}{2}$, die grade; weil es keine Zahl $e = 4n$ giebt, die in $c - 1 = 4m + 2$ aufgeht.

23. Um nun alle primitiven und sekundären Wurzeln von einer gegebenen Primzahl c, z. B. von $41 = 4m + 1$, möglichst schnell zu erhalten, potenzire man die 2. Es wird $2^{10} = 41y - 1$, folglich 2 sekundäre Wurzel von 41 zu **20**, sämmtliche: 2, 5, 8, 20, (No 16), und 21, 33, 36, 39 (No. 22). — Es ist $(2^2)^{10} = 4^{10} = 41y + 1$, also 4 sekundäre Wurzel zu **10** (No. 17), sämmtliche: 4, 23, 25, 31 (No. 16). — Zu **5**: 10, 16, 18, 37 (No. 21). — Unter allen diesen Wurzeln ist z. B. nicht die 3; $3^4 = 41y - 1$, folglich 3 sekundäre Wurzel zu **8**, sämmtliche: 3, 27 (No. 16), und 38, 14 (No. 22). — Es ist $(3^2)^4 = 9^4 = 41y + 1$, also 9 sekundäre Wurzel zu **4** (No. 17), sämmtliche: 9, 32 (No. 20 oder 22). — Zu **1** und **2**: 1, 40. — Diese 24 Wurzeln aus der Zahlenreihe von 1 bis 40 genommen, giebt die 16 primitiven Wurzeln: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

Ist $c = 67 = 4m + 3$, so wird, wenn man die 2 potenzirt, $2^{33} = 67y - 1$, also 2 primitive Wurzel, sämmtliche: 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63 (No. 16). — Zu **33**: 4, 6, 10, 16, 17, 19, 21, 23, 26, 33, 35, 36, 39, 47, 49, 54, 55, 56, 60, 65 (No. 21). — $(2^3)^{22} = 8^{22} = 67y + 1$, also 8 sekundäre Wurzel zu **22** (No. 17), sämmtliche: 3, 5, 8, 27, 42, 43, 45, 52, 53, 58 (No. 16). — Zu **11**: 9, 14, 15, 22, 24, 25, 40, 59, 62, 64 (No. 21). — $(2^{11})^6 = 38^6 = 67y + 1$, also 38 sekundäre Wurzel zu **6** (No. 17), sämmtliche: 30, 38 (No. 16). — Zu **3**: 29, 37 (No. 21). — Zu **1** und **2**: 1, 66.

Ist $c = 73 = 4m + 1$, so wird, wenn man die 2 potenzirt, $2^9 = 73y + 1$, also 2 sekundäre Wurzel zu **9**, sämmtliche: 2, 4, 16, 32, 37, 55 (No. 16). — Zu **18**: 18, 36, 41, 57, 69,

Universitäts- und
Landesbibliothek Düsseldorf

71 (No. 21). — $(2^3)^3 = 8^3 = 73y+1$, also 8 sekundäre Wurzel zu **3** (No. 17), 64 die zweite (No. 16). — Zu **6**: 9, 65 (No. 21). — Unter allen diesen Wurzeln ist z. B. nicht die 10; $10^4 = 73y-1$, also 10 sekundäre Wurzel zu **8**, sämmtliche: 10, 51 (No. 16), und 22, 63 (No. 22). — 10 sekundäre Wurzel zu 8, 2 zu 9 giebt 10. 2 = 20 primitive Wurzel (No. 18), sämmtliche: 20, 45, 42, 58, 59, 5, 29, 47, 39, 33, 60. 62 (No. 16 oder 18), und 53, 28, 31, 15, 14, 68, 44, 26, 34, 40, 13, 11 (No. 22). — $(10^2)^4 = 27^4 = 73y+1$, also 27 sekundäre Wurzel zu **4** (No. 17), 46 die zweite (No. 20). — Zu **36**: 6, 12, 19, 23, 25, 35, 38, 48, 50, 54, 61, 67 (theils durch No. 18, theils durch No.22). — Zu **24**: 7, 17, 21, 30; 43, 52, 56, 66 (No. 18 und 22). — Zu **12**: 3, 24, 49, 70 (No. 18 u. 22). — Zu **1** u. **2**: 1, 72.

24. Ist a primitive Wurzel von c, so ist die Anzahl der Reste, die entstehen, wenn jedes der Produkte $1a$, $2a$, $3a$, ... $\frac{c-1}{2}a$ mit c dividirt wird, welche $> \frac{c}{2}$, stets ungerade, denn $a^{\frac{c-1}{2}} = cy-1$ (§. 2, No. 7), z. B. wenn $a=11$, $c=41$, 67, 73. — Ist a sekundäre Wurzel von c zu $\frac{c-1}{2}$, so ist die Anzahl dieser Reste stets gerade; denn $a^{\frac{c-1}{2}} = cy+1$ (§. 2, No. 7), z. B. wenn $a=2$ und $c=41$, $a=4$ und $c=67$, $a=6$ und $c=73$. — Ferner: 2 sekundäre Wurzel von 73 zu 9, also $2^{36} = 73y+1$; folglich die Anzahl der Reste für $a=2$ und $c=73$, welche $> \frac{73}{2}$, grade. — 10 sekundäre Wurzel von 73 zu 8, also $10^4 = 73y-1$; $10^{36} = 73y-1$; folglich die Anzahl der Reste für $a=10$, $c=73$, welche $> \frac{73}{2}$, ungrade. — 10 sekundäre Wurzel von 41 zu 5, also $10^{20} = 41y+1$; daher die Anzahl der Reste für $a=10$, $c=41$, welche $> \frac{41}{2}$, grade, u. s. w.

25. Primitive oder sekundäre Wurzeln von 2 verschiedenen Primzahlen geben eine Wurzel von dem Produkte derselben. Da z. B. 3 primitive Wurzel von 5 und 7, also $3^4 = 5y+1$, $3^6 = 7y+1$; so ist $3^{12} = 5.7y+1$, und 12 kleinster Exponent; denn gäbe es einen kleineren, so könnte es, da $p = \frac{35.4.6}{5.7} = 24$, nur eine der Zahlen 2, 3, 4, 6, 8 sein; aber keine Potenz der 3 mit diesen Exponenten giebt, mit 5 und 7 dividirt zugleich den Rest 1. — 2 sekundäre Wurzel von 7 zu 3 und primitive Wurzel von 11; folglich $2^{3\cdot 10} = 7.11y+1$. — 4 sekundäre Wurzel von 19 zu 9 und von 23 zu 11; folglich $4^{9\cdot 11} = 19.23y+1$. — 2 primitive Wurzel von 5, und $p = \frac{5^2.4}{5} = 4.5$; folglich $2^{4\cdot 5} = 5^2y+1$, und 20 kleinster Exponent; denn wäre z. B. schon $2^4 = 5^2y+1$, so müsste 5 in 2^4-1 und in dem Quotienten aufgehen, was nicht der Fall. Eben so folgt aus $2^4 = 5y+1$, dass nicht 2^5 oder $2^{10} = 5y+1$, um so weniger also $= 5^2y+1$ sein kann. — 3 sekundäre Wurzel von 11 zu 5, also $3^5 = 11y+1$; daher $3^{5\cdot 11} = 11^2y+1$; denn $11y = x$ gesetzt, giebt: $(x+1)^{11} = 11_{11}.x^{11} + 11_{10}.x^{10} + \ldots + 11_1 x^1 + 1$ (Binomischer Lehrsatz). Da jedoch 11 in 3^5-1 und in dem Quotienten aufgeht, so ist 5, und nicht 5.11 kleinster Exponent, u. s. w.

§. 3.

$1^n, 2^n, 3^n, 4^n, \ldots (c-1)^n$.

1. Ist z. B. $c=41$, $n=40$, und dividirt man jedes Glied dieser Reihe mit 41; so entsteht überall der Rest 1; dagegen für $n=5$ nur bei den 5 Reihen-Zahlen, welche sekundäre Wurzeln zu 1, 5; für $n=8$ bei den 8 Reihen-Zahlen, welche sekundäre Wurzeln zu 1, 2, 4, 8, u. s. w. Für $n=5$ können nur Reste sein die sekundären Wurzeln zu 1, 2, 4, 8; denn ist $a^5 = 41y+r$, so folgt: $a^{5\cdot 8} = 41y+r^8 = 41y+1$; für $n=8$ die sekundären Wurzeln zu 1, 5; für $n=4$ die zu 1, 2, 5, 10; für $n=20$ die zu 1, 2, u. s. w. Allgemein: Ist n Faktor von $c-1$ und $a^n = cy+r$, so ist $a^{\frac{n(c-1)}{n}} = cy + r^{\frac{c-1}{n}} = cy+1$; folglich r Rest der Reihe, wenn $r^{\frac{c-1}{n}} = cy+1$.

Universitäts- und
Landesbibliothek Düsseldorf

2. Jeder andere Rest, ausser dem Reste 1, muss eben so oft erscheinen als dieser. Ist z. B. $n = 5$, so entsteht der Rest 1 bei der sekundären Wurzel zu 1 und jeder der 4 sekundären Wurzeln zu 5. Die übrigen Reste sind die eine sekundäre Wurzel zu 2, die 2 sekundären Wurzeln zu 4, und die 4 sekundären Wurzeln zu 8. Ist nun $a^5 = 41y + 1$, $b^5 = 41y + 1$, $d^5 = 41y +$ s. W. z. 2; so folgt $(ad)^5$, oder, wenn $ad = 41y + h$, $h^5 = 41y +$ s. W. z. 2; eben so $(bd)^5$, oder, wenn $bd = 41y + k$, auch $k^5 = 41y +$ s. W. zu 2, und h nicht $= k$; denn $h = k$ gäbe: $ad - bd = d(a - b) = 41y$, also $d(a - b)$ theilbar durch 41, was nicht der Fall. Multiplicirt man daher eine der Reihen-Zahlen, welche bei dem Exponenten n irgend einen Rest r geben, wo r nicht $= 1$, mit allen, bei welchen der Rest 1 erscheint, und dividirt mit c, so erhält man alle Reihen-Zahlen, welche den Rest r geben.

3. Für $c = 41$, $n = 2$ erscheinen 20 verschiedene Reste. Es sind die sekundären Wurzeln zu 1, 2, 4, 5, 10, 20; da für jede: $r^{20} = 41y + 1$. Für jede der 20 fehlenden Zahlen ρ ist $\rho^{20} = 41y - 1$ (No. 1 und 2). Daher ist r quadratischer Rest von c, wenn $r^{\frac{c-1}{2}} = cy + 1$, und ρ quadratischer Nichtrest von c, wenn $\rho^{\frac{c-1}{2}} = cy - 1$. Die sekundären Wurzeln von c zu allen Exponenten, die Faktoren von $\frac{c-1}{2}$, sind quadratische Reste von c; daher ist, weil in $\frac{c-1}{2}$, wenn $c = 4m + 1$, die 2 immer aufgeht, -1, oder die sekundäre Wurzel zu 2, quadratischer Rest von jeder Primzahl $4m + 1$. Die primitiven Wurzeln, und die sekund. Wurzeln von c zu den Exponenten, welche nicht in $\frac{c-1}{2}$ aufgehen, sind quadratische Nichtreste von c; daher ist, weil in $\frac{c-1}{2}$, wenn $c = 4m + 3$, die 2 nie aufgeht, -1 quadratischer Nichtrest von jeder Primzahl $4m + 3$. Zugleich sieht man, dass jeder quadratische Rest r von c, die Eigenschaft hat, dass, wenn man die Produkte $1r, 2r, 3r \ldots \frac{c-1}{2} r$ mit c dividirt, die Anzahl Reste, welche $> \frac{c}{2}$, stets grade; jeder quadratische Nichtrest ρ die, dass in $1\rho, 2\rho, 3\rho, \ldots \frac{c-1}{2}\rho$ die Anzahl solcher Reste stets ungrade (§. 2, No. 7), und umgekehrt: Ist die Anzahl dieser Reste grade, so ist r quadratischer Rest von c; ist sie ungrade: ρ quadratischer Nichtrest von c. — Ist $c = 4m + 1$, so giebt die Division von $\left(\frac{c-1}{2}\right)^2 = (2m)^2$ durch c den Rest $-m$ oder: $3m + 1$, als quadratischen Rest von $c = 4m + 1$. Ist $c = 4m + 3$, so giebt die Division von $\left(\frac{c-1}{2}\right)^2 = (2m + 1)^2$ durch c den Rest $m + 1$, als quadratischen Rest von $c = 4 + 3$. Es ist aber $4(3m + 1) = (4m + 1)y + 1$, und $4(m + 1) = (4m + 3)y + 1$; folglich sind 4 und $3m + 1$, wie 4 und $m + 1$ correspondirende Zahlen, und daher 4 und $3m + 1$ sekundäre Wurzeln von $c = 4m + 1$ zu demselben Exponenten; eben so 4 und $m + 1$ von $c = 4m + 3$.

4. Ist n relative Primzahl gegen $c - 1$, so kann nur bei dem ersten Gliede der Reihe der Rest 1 entstehen, alle $c - 1$ Reste sind unter einander verschieden. Denn wären auch nur 2 Reste gleich, und etwa $b^n = cy + r$, $d^n = cy + r$, und a primitive Wurzel von c; so gäbe es ein x, dass $a^x = cy + b$, und ein v, dass $a^v = cy + d$; folglich $a^{nx} = cy + b^n = cy + r$, $a^{nv} = cy + d^n = cy + r$; daher $a^{nx} - a^{nv} = a^{nv}(a^{n(x-v)} - 1) = cy$, also theilbar durch c; folglich $a^{n(x-v)} = cy + 1$, was nur möglich, wenn, da sowol x als v kleiner als c, und n relative Primzahl gegen $c - 1$, $x - v = o$, also $x = v$; folglich $b = d$. Also sind, wenn n relative Primzahl gegen $c - 1$, nicht 2 verschiedene Glieder mit demselben Reste möglich.

5. Haben n und $c - 1$ einen gemeinschaftlichen Faktor, und ist v der grösste; so ist es wie bei $n = v$; nur erscheinen die Reste in anderer Ordnung. Da z. B. 6 primitive Wurzel von 41, so ist $6^5 = 41y +$ s. W. z. $8 = 41y + 27$, $6^{15} = 41y + 27^3 = 41y +$ s. W. z. $8 = 41y + 3$. Oder: $6^3 = 41y +$ primitive Wurzel $= 41y + 11$, $6^{15} = 41y + 11^5 = 41y +$ s. W. z. $8 = 41y + 3$. Also ist sowol für $n = 5$, als für $n = 15$ bei derselben Reihen-Zahl 6, der Rest eine sekundäre Wurzel zu 8, uur kann es nicht dieselbe sein; denn $27^2 = 41y + 27$ gäbe: $27(27^2 - 1)$

Universitäts- und
Landesbibliothek Düsseldorf

$= 41y$, was nicht möglich. — 2 sekundäre Wurzel von 41 zu 20, also $2^8 = 41y +$ s. W. z. 5 $= 41y + 10$, $2^{16} = 41y + 10^2 = 41y +$ s. W. z. 5 $= 41y + 18$. Oder: $2^2 = 41y +$ s. W. z. 10 $= 41y + 4$, $2^{16} = 41y + 4^8 = 41y +$ s. W. z. 5 $= 41y + 18$, u. s. w.

6. Die Summe der Reihen-Zahlen, welche bei irgend einem Exponenten n denselben Rest r haben, wo r nicht $= 1$, ist theilbar durch c; ihr Produkt $= cy \mp r$, je nachdem unter den Faktoren von n die Zahl 2 vorkommt oder nicht. Ist z. B. $a^8 = 41y + 1$, $\alpha^8 = 41y + r$, und multiplicirt man jede der 8 Reihen-Zahlen, welche bei $n = 8$ den Rest 1 geben, mit α; so entstehen die 8 Produkte, welche, mit 41 dividirt, die 8 Reihen-Zahlen zu Resten haben, die bei $n = 8$ den Rest r liefern (No. 2). Addirt man daher die 8 Produkte und die ihnen gleichen Summen; so wird $\alpha S_1 = 41y + S_r$, wo S_1 die Summe der Zahlen mit dem Reste 1, S_r die mit dem Reste r. Nun ist S_1 theilbar durch 41 (§ 2, No. 20); folglich S_r, wodurch der erste Theil des Satzes erwiesen. — Für $n = 8$ geben die 8 Reihen-Zahlen, welche sekundäre Wurzeln zu 1, 2, 4, 8, den Rest 1, nämlich 1, 40, 9, 32, 3, 14, 27, 38; die übrigen Reste sind die sekundären Wurzeln zu 5: 10, 16, 18, 37, jede 8mal. Nun ist z. B. $2^8 = 41y + 10$; folglich sind die Reihen-Zahlen, welche bei $n = 8$ den Rest 10 geben, die Reste von: 2.1, 2.40, 2.9, 2.32, 2.3, 2.14, 2.27, 2.38, nämlich: 2, 39, 18, 23, 6, 28, 13, 35; ihre Summe $= 164$, theilbar durch 41. Multiplicirt man die 8 Produkte mit einander, so entsteht: $2^8.1.40.9.32.3.14.27.38$ (A). Das Produkt neben 2^8 ist aber das aller Wurzeln zu sämmtlichen Exponenten, die Faktoren von 8, also $= 41y - 1$ (§ 2, No. 19); folgl. $A = 2^8(42y - 1) = 41y - 2^8 = 41y - 10$, wodurch der zweite Theil des Satzes erwiesen. — $2^2 = 41y + 4$, $39^2 = 41y + 4$; folglich $2.39 = 41y - 4$, u. s. w.

7. Die Summe der Reihe, n mag eine ganze Zahl sein, welche man will, ist theilbar durch c, wenn c eine Primzahl. Für $n = 1$ wird sie theilbar durch c schon wegen § 1, No. 3. Für $n = 10$, $c = 41$ hat die Reihe 4 verschiedene Reste, jeden 10mal, nämlich die 4 sekundären Wurzeln zu 1, 2, 4. Die Summe derselben aber theilbar durch 41; folglich die 10fache Summe, und somit die der Reihe. — Das Produkt $= 1^n.2^n.3^n \ldots (c-1)^n = (1.2.3 \ldots (c-1))^n = (cy - 1)^n = cy \mp 1$ (§ 2, No. 10), je nachdem n ungrade oder grade.

8. Die Betrachtung der Reihe führt unmittelbar zur Lösung der Gleichung: $x^n = cy + r$ in ganzen Zahlen, wo also c eine Primzahl $r < c$, n eine ganze Zahl, und nur erforderlich, dass $r^{\frac{c-1}{n}} = cy + 1$. — Ist $c = 41$, $n = 40$, $r^1 = 41y + 1$ also $r = 1$; so ist jede Zahl von 1 bis 40 ein Werth von x, und zwar jede der 16 primitiven Wurzeln ausschliesslich. — Ist $n = 20$, $r^2 = 41y + 1$, also r sekundäre Wurzel zu 1, 2; so ist für $r = 1$ jede der sekundären Wurzeln zu 1, 2, 4, 5, 10, 20 ein Werth von x; für $r =$ s. W. z. 2, oder $r = -1$, jede sekundäre Wurzel zu 8 und jede primitive Wurzel. — Ist $n = 10$, $r^4 = 41y + 1$, also r sekundäre Wurzel zu 1, 2, 4; so ist für $r = 1$ jede der 10 sekundären Wurzeln zu 1, 2, 5, 10 ein Werth von x; für $r =$ s. W. zu 2 jede s. W. z. 4 und 20; für $r =$ s. W. z. 4 die zu 8 und die primitiven Wurzeln. Denn $(\text{s. W. z. } 4)^{10} = (\text{s. W. z. } 4)^8.(\text{s. W. z. } 4)^2 = 41y - 1 = 41y +$ s. W. z. 2; $(\text{s. W. z. } 8)^{10.4} = 41y + (\text{s. W. z. } 4)^4 = 41y + 1$, und $(\text{s. W. z. } 8)^{10.2} = (\text{s. W. z. } 8)^{4.5} = 41y + (\text{s. W. z. } 4)^2 = 41y - 1$; $(\text{p. W.})^{10.4} = 41y + (\text{s. W. z. } 4)^4 = 41y + 1$ und $(\text{p. W.})^{10.2} = 41y + (\text{s. W. z. } 4)^2 = 41y - 1$. Man erhält für jedes r alle 10 Werthe von x, wenn man einen kennt und die 10 von x für den Rest 1. Die Summe jeder 10 dieser Werthe ist theilbar durch 41, ihr Produkt $= 41y - r$. — Ist $n = 8$, $r^5 = 41y + 1$; also r sekundäre Wurzel zu 1, 5; so ist für $r = 1$ jede sekundäre Wurzel zu 1, 2, 4, 8 ein Werth von x; für $r =$ s. W. z. 5 die zu 5, 10, 20 und die primitiven Wurzeln. — Ist $n = 5$, $r^8 = 41y + 1$, also r sekundäre Wurzel zu 1, 2, 4, 8; so ist für $r = 1$ jede sekundäre Wurzel zu 1, 5 ein Werth von x; für $r =$ s. W. z. 2 die zu 10 und 2; für $r =$ s. W. z. 4 die zu 4, 20; für $r =$ s. W. z. 8 die zu 8 und die primitiven Wurzeln. Die Summe jeder 5 zusammen-

Universitäts- und
Landesbibliothek Düsseldorf

gehörigen Werthe ist wieder theilbar durch 41, ihr Produkt $=41y+r$. — Ist $n=4$, $r^{10}=41y+1$, also r sekundäre Wurzel zu 1, 2, 5, 10; so ist für $r=1$ jede sekundäre Wurzel zu 1, 2, 4 ein Werth von x; für $r=$ s. W. z. 2 die zu 8; für $r=$ s. W. z. 5 die zu 5, 10, 20; für $r=$ s. W. z. 10 die primitiven Wurzeln. — Ist $n=2$, $r^{20}=41y+1$, also r sekundäre Wurzel zu 1, 2, 4, 5, 10, 20; so ist für $r=1$ die sekundäre Wurzel zu 1, 2 ein Werth von x; für $r=$ s. W. z. 2 die zu 4; für $r=$ s. W. z. 4 die zu 8; für $r=$ s. W. z. 5 die zu 5, 10; für $r=$ s. W. z. 10 die zu 20; für $r=$ s. W. z. 20 die primitiven Wurzeln. — Haben n und 40 einen gemeinschaftlichen Faktor, ist z. B. $n=15$, $r^{\frac{40}{5}}=41y+1$; $n=24$, $r^{\frac{40}{8}}=41y+1$; $n=28$, $r^{\frac{40}{4}}=41y+1$, u. s. w.; so ergeben sich die Werthe von x, wie vorhin, wo $n=5, 8, 4$. — Ist n relative Primzahl gegen 40, so kann r jede Zahl von 1 bis 40 sein, aber x für jedes r nur einen Werth haben; z. B. für $n=9$, $r=\pm 1$ wird unmittelbar $x=\pm 1$. Für $r=32=$ s. W. z. 4 wird aus $x^9=41y+32$: $(32x)^9=41y+32^{10}=41y+32^2=41y-1$, $32x=41y-1$, $x=32$. Für $r=10=$ s. W. z. 5 wird $(10x)^9=41y+10^{10}=41y+1$, also $10x=41y+1$, $x=37$. Für $r=3=$ s. W. z. 8 wird $(3x)^9=41y+3^{10}=41y+3^2$, und, $9z=8y+2$ gesetzt, $z=2$, also $x=3^1$. Für $r=4=$ s. W. z. 10 wird $(4x)^9=41y+4^{10}=41y+1$, also $4x=41y+1$, $x=31$. Für $r=2=$ s. W. z. 20 wird $(2x)^9=41y+2^{10}=41y-1$, also $2x=41y-1$, $x=20$. Für $r=6=$primitive Wurzel wird $(6x)^9=41y+6^{10}$, und, $9z=40y+10$ gesetzt, $z=10$, also $x=6^9$, oder, da $6^9=41y+19$, $x=19$, u. s. w. — Ist $n>40$, z. B. $n=85=2.40+5$, so ist es wie bei $n=5$.

9. Bedeutende Modificationen treten ein, wenn c keine Primzahl ist, und ein nicht-correspondirendes Zahlen-Paar hat, z. B. wenn $c=35$, wo $p=\frac{35.4.6}{5.7}=24$, und die nicht-correspondirenden Zahlen : 6, 29. Jede der 24 relativen Primzahlen : 1, 2, 3, 4, 6, 8, 9, ... 33, 34 ist mit dem Exponent n behaftet. Bei $n=2$ muss 4 mal der Rest 1 entstehen, nämlich bei: 1, 6, 29, 34; und eben so oft jeder der 5 anderen Reste : a, b, c, d, e, welche 10 Paaren correspondirenden Zahlen angehören, so dass 4 Paaren die Reste a, b; 4 Paaren die Reste c, d und 2 Paaren die 4 Reste e zukommen. Da nun die Produkte der Reste von den Quadraten jeder 2 correspondirenden Zahlen ebenfalls den Rest 1 liefern; so ist $e^2=35y+1$, folglich e eine der Zahlen: 6, 29, 34, und da singuläre Zahlen nicht vorhanden, $e=6$, 29, nämlich 29; ferner erscheinen bei 2 correspondirenden Zahlen dieselben Zahlen als Reste, es ist nämlich: $11^2=25y+16$ und $16^2=35y+11$; daher $11^3=35y+1$, $16^3=35y+1$; $11^4=35y+11$, $16^4 35y+16$. Es folgt, dass bei $n=4$, 8 mal der Rest 1 und 8 mal der Rest 16 und 11; bei $n=8$, 8 mal der Rest 1, und umgekehrt der Rest 11 und 16; bei $n=12$ aber 24 mal der Rest 1 erscheinen muss. Bei $n=3$ entsteht 3 mal der Rest 1, und eben so oft jeder der übrigen, worunter : 6, 29, 34; denn für jede dieser Zahlen ist $a^3=35y+a$; folglich entsteht bei $n=6$, 12 mal der Rest 1, und eben so oft der Rest 29; da aus $a^2=25y+29$ folgt: $a^{2.3}=35y+29^3=35y+29$. Daher folgt wieder : bei $n=12$, 24 mal der Rest 1. — Demgemäss hat in der Gleichung: $x^{24}=35y+1$ die Unbekannte 24 Werthe, keinen jedoch ausschliesslich; in $x^{12}=35y+1$ deren ebenfalls 24, 8 derselben ausschliesslich; in $x^8=35y+1$ deren 8, keinen ausschliesslich, sowie 8 in $x^8=35y+11$, 16; in $x^6=35y+1$ deren 12, 6 derselben ausschliesslich, so wie 12 in $x^6=35y+29$; in $x^4=35y+1$ deren 8, 4 derselben ausschliesslich, ferner 8 in $x^4=35y+16$, 11; in $x^3=35y+1$ deren 3, 2 davon ausschliesslich, ferner 3 in $x^3=35y+8$, 27, 29, 6, 22, 13, 34; in $x^2=35y+1$ deren 4, 3 davon ausschliesslich, ferner 4 in $x^2=35y+4$, 9, 16, 29, 11. — In $x^{13}=35y+4$, wo 13 relative Primzahl gegen 24, ist, da $4^6=35y+1$, $x=4$. In $x^{13}=35y+11$, wo $11^3=35y+1$, $x=11$. In $x^5=35y+3$, wo erst $3^{12}=35y+1$, ist $(3x)^5=35y+3^6$, und, $5z=12y+6$ gesetzt, $z=6$, also $x=3^5$, oder, da $3^5=$

Universitäts- und
Landesbibliothek Düsseldorf

$35y+33$, $x=33$. In $x^5=35y+9$, wo $9^6=35y+1$, ist $(9x)^5=35y+9^6$, $5z=6y+6=6y$ gesetzt, $z=6$, $x=9^5$, oder, da $9^5=35y+4$, $x=4$, u. s. w.

§ 4.

$$a^1, a^2, a^3, a^4 \ldots\ldots a^{c-1}.$$

1. Ist a primitive Wurzel von c, und dividirt man jedes Glied dieser Reihe mit c; so bilden die $c-1$ relativen Primzahlen gegen c, die kleiner als c, sämmtliche Reste (§ 2, No. 15), die, wenn man die Reihe fortsetzt, in derselben Ordnung wiederkehren, also eine Periode bilden. Die Summe dieser $c-1$ Reste ist daher theilbar durch c, und ihr Produkt $=cy-1$.

2. Ist $c=41$, also $a^{20}=41y-1$, so folgt: $a^1+a^{21}=41y$, $a^2+a^{22}=41y$, $a^3+a^{23}=41y$, u. s. w.; also ist die Summe des ersten Gliedes dieser Reihe und des ersten ihrer zweiten Hälfte, des zweiten und zweiten, des dritten und dritten, u. s. w., so wie die der dazu gehörigen Reste, theilbar durch c.— Es ist $a^1.a^{39}=a^{40}$, $=41y+1$, $a^2.a^{38}=a^{40}=41y+1$, u. s. w.; also sind das erste Glied und das erste vor dem letzten, das zweite und zweite, u. s. w.; folglich auch die dazu gehörigen Reste, correspondirende Zahlen, nur $a^{\frac{c-1}{2}}$ hier a^{20}, giebt mit sich selber multiplicirt, $41y+1$. — Es ist $a^1.a^{40}=a^{41}=41y+a$, $a^2.a^{39}=a^{41}=41y+a$, u. s. w.; also geben die Produkte des ersten und letzten, des zweiten und vorletzten Gliedes, u. s. w., wenn man jedes mit c dividirt, den Rest a.

3. Ist a sekundäre Wurzel von 41 zu 2, also $=40$ oder $=-1$; so sind die Reste der Reihe abwechselnd: -1, $+1$.— Ist a sekundäre Wurzel zu 4, so hat das erste Glied den Rest a, das zweite die sekundäre Wurzel zu 2, das dritte die zweite sekundäre Wurzel zu 4, das vierte den Rest 1. In dieser Ordnung wiederholen sich die Reste, und bilden daher eine Periode. — Ist a sekundäre Wurzel zu 10, so erscheint erst bei dem zehnten Gliede der Rest 1; die Resten-Periode hat daher 10 Stellen, und zwar ist der erste Rest sekundäre Wurzel zu 10, der zweite zu 5, der dritte zu 10, der vierte zu 5, der fünfte zu 2, der sechste zu 5, der siebente zu 10, der achte zu 5, der neunte zu 10, der zehnte zu 1. — Die Reste, welche eine Periode bilden, sind unter einander verschieden (§ 2, No. 15). — Die Summe der Potenzen, die zu einer Resten-Periode gehören, also auch die der Reste, ist theilbar durch c. Denn hat die Periode e Reste, so ist $1+a^1+a^2+a^3+\ldots a^{e-1}=\frac{a^c-1}{a^1-1}$, also theilbar durch c und $a-1$, die relative Primzahlen, folglich die Potenzen-Summe durch c, und somit die der Reste. — Das Produkt dieser Potenzen, also auch das der dazu gehörigen Reste, $=cy-1$, wenn e grade, und $=cy+1$, wenn e ungrade. Im ersten Falle ist nämlich $e-1$ ungrade, und $a^{e-1}.a^1=a^e=cy+1$, $a^{e-2}.a^2=a^e=cy+1$, und so für jede 2 Glieder, die von a^{e-1} und a^1 gleich weit entfernt sind; nur das Mittelglied $a^{\frac{e}{2}}$ hat den Rest $c-1$ oder -1; also ist das Produkt $=(cy+1)(c-1)=cy-1$. Ist e ungrade, also $e-1$ grade, so ist kein einzelnes Mittelglied vorhanden, daher das Produkt $=cy+1$.— Ist e grade, so gelten auch für die e Reste der Periode die Sätze in No. 2; die 2 letzten, wenn e ungrade; dagegen ist in diesem Falle der Rest von dem Quadrate des Gliedes vor dem mittelsten = dem Reste des vorletzten; denn $(a^{\frac{e-1}{2}})^2=a^{e-1}$.

4. Ist c keine Primzahl, z. B. $c=35$; also $p=\frac{35.4.6}{5.7}=24$, a relative Primzahl gegen c, und z. B. $a^{12}=35y+1$, wo 12 kleinster Exponent; so entsteht ebenfalls eine Resten-Periode von 12 Stellen. Die Summe der Potenzen, welche zu dieser gehört, also auch die der Reste ist theilbar durch 35, wenn 35 und $a-1$ relative Primzahlen; haben beide einen gemeinschaftlichen Faktor, so ist die Summe der Potenzen, also auch die der Reste durch den nicht gemeinschaftlichen

Universitäts- und
Landesbibliothek Düsseldorf

Faktor in c theilbar. — Das Produkt aller Reste der Periode, also auch das der zugehörigen Potenzen, ist, wenn e grade, theils $cy+n$, wo n nicht-correspond. Zahl, z. B. $3^1 . 3^2 . 3^3 \ldots . 3^{12} = 35y+29$; theils $cy-1$, z. B. $8^1 . 8^2 . 8^3 \ldots . 8^6 = 27y-1$, und nur wenn e ungrade, immer $= cy+1$, z. B. $4^1 . 4^2 . 4^3 \ldots . 4^9 = 27y+1$.

5. Wird jedes Glied der Reihe mit einer Zahl b, welche relative Primzahl gegen c, multiplicirt, so bleiben sämmtliche $c-1$ Reste verschieden, wenn auch in anderer Ordnung; also bleibt die Summe der Reste theilbar durch c, und, weil $b^{c-1} = cy+1$, auch ihre Produkt $= cy-1$. Der Rest von ba^{c-1} wird $+b$, von $ba^{\frac{c-1}{2}}$: $-b$; daher bleibt die Summe des ersten Gliedes und ersten der zweiten Hälfte, des zweiten und zweiten, u. s. w., so wie die der dazugehörigen Reste, theilbar durch c. Das Produkt des ersten Gliedes und ersten vor dem letzten, zweiten und zweiten, u. s. w. ist nicht $cy+1$, sondern $cy+b^2$. Das Produkt des ersten und letzten Gliedes, des zweiten und vorletzten, u. s. w. ist $b^2 a$, oder $= k$, wenn c wegdividirt wird. — Ist a primitive Wurzel oder sekundäre Wurzel zu e, so ergeben sich die Reste bei dem Faktor b, wenn man jeden der Reste bei $b=1$ mit b multiplicirt. — Für die Summe der e Reste der Periode ist es wie in No. 3; das Produkt derselben $= cy-b^e$, wenn e grade, und $= cy+b^e$, wenn e ungrade, u. s. w.

6. Ist $a=10$, und relative Primzahl gegen c, und dividirt man jedes Glied der Reihe mit c, darauf den Quotienten mit dem Divident; so hat man überall den Bruch $\frac{1}{c}$ in einen Decimalbruch verwandelt; eben so den Bruch $\frac{b}{c}$, wenn man $b . 10^n$ mit c, und den Quotienten mit 10^n dividirt. Dieser Exponent n des Divisors 10^n liefert dem Decimalbruche seine Stellen-Anzahl (nach dem Komma), nämlich n. Nun lässt das bekannte Divisions-Verfahren bei Potenzen, wenn man den Bruch $\frac{1}{c}$ in einen Decimalbruch verwandelt, bei jeder der Potenzen: $10^1, 10^2, 10^3, \ldots . 10^n$, und ist es der Bruch $\frac{b}{c}$, bei jedem der Produkte: $b . 10^1, b . 10^2, b . 10^3, \ldots . b . 10^n$, den zugehörigen Rest, also überhaupt n Reste, erscheinen. Daher hat jeder Decimalbruch eben so viele Stellen, als Reste bei der Verwandlung seines gemeinen Bruches entstanden sind. — Ist c keine Primzahl, und jeder Primfaktor von c ein Faktor von 10, so hat der Decimalbruch von $\frac{1}{c}$ oder $\frac{b}{c}$, wo $b < c$ und relative Primzahl gegen c, so viele Stellen als der grösste Exponent der gemeinschaftlichen Primfaktoren Einheiten, z. B. $\frac{10^2}{5^2} = 2^2$, also $\frac{1}{25} = 0{,}04$; $\frac{10^3}{2^3} = 5^3$, also $\frac{1}{8} = 0{,}125$; $\frac{10^4}{5^3\, 2^4} = 5$, also $\frac{1}{2000} = 0{,}0005$. Ist nicht jeder Primfaktor von c ein Faktor von 10, z. B. wenn $c = 5^3 . 2^4 . p$, wo $\frac{1}{p}$ oder $\frac{x}{p}$ allein n Stellen haben mag; so hat der Decimalbruch von $\frac{1}{5^3 . 2^4 . p}$ oder $\frac{b}{5^3 . 2^4 . p}$, $(n+4)$ Stellen; denn $\frac{b . 10^{n+4}}{5^3 . 2^4 . p} = \frac{b . 10^n . 5}{p}$, wo nachher der Quotient mit 10^{n+4} zu dividiren.

§. 5.

Periodische Decimalbrüche.

1. Ist 10 primitive Wurzel von c, und verwandelt man den Bruch $\frac{1}{c}$ in einen Decimalbruch; so folgt unmittelbar aus den abgehandelten Sätzen: Jede auf einander folgenden $c-1$ Reste sind unter einander verschieden und bilden eine Periode. Der $c-1$te Rest $= +1$, der $\frac{c-1}{2}$te $= -1$. Die Summe jeder aufeinander folgenden $c-1$ Reste ist theilbar durch c, ihr Produkt $= cy-1$. Von den ersten $c-1$ Resten und jeden $c-1$ darauf folgenden ist die Summe des ersten und ersten der zweiten Hälfte, des zweiten und zweiten, u. s. w. theilbar durch c, und, da jeder $< c$, $= c$. Das Produkt des ersten und letzten, des zweiten und vorletzten, u. s. w. giebt den Rest 10, wenn $c > 10$; bei $\frac{1}{7}$ den Rest 3, weil 3 primitive Wurzel von 7, und $7+3=10$, also auch $(7+3)^6 = 7y+1$. Der erste und erste vor dem letzten, der zweite und zweite, u. s. w. sind

Universitäts- und
Landesbibliothek Düsseldorf

correspondirende Zahlen, und auch das Quadrat des letzten der ersten Hälfte $= cy + 1$. Jede aufeinander folgenden $c-1$ Stellen des Decimalbruches bilden eine Periode. Da z. B. 10 primitive Wurzel von 17, 19, 23, 29, 47, 59, 61, 97; so hat die Periode von $\frac{1}{17}$ 16, von $\frac{1}{19}$ 18, von $\frac{1}{23}$ 22, von $\frac{1}{29}$ 28, von $\frac{1}{47}$ 46, von $\frac{1}{59}$ 58, von $\frac{1}{61}$ 60, von $\frac{1}{97}$ 96 Stellen. Bei der Verwandlung des Bruches $\frac{b}{c}$, wo $b < c$ und relative Primzahl gegen c, ist Alles wie bei der von $\frac{1}{c}$; nur ist der $c-1$te Rest $= +b$, der $\frac{c-1}{2}$te $= -b$; das Produkt des ersten und letzten, des zweiten und vorletzten, u. s. w. $= cy + b^2 . 10$, oder es hat, wenn $b^2 . 10 = cy + h$, den constanten Rest h; eben so ist das des ersten und ersten vor dem letzten, des zweiten und zweiten, u. s. w., $= cy + b^2$, oder es hat, wenn $b^2 = cy + k$, den constanten Rest k. Durch Multiplikation der Reste und des Decimalbruches von $\frac{1}{c}$ mit b erhält man Reste und Decimalbruch für $\frac{b}{c}$.

2. Ist 10 sekundäre Wurzel von c zu e, und man verwandelt den Bruch $\frac{1}{c}$ in einen Decimalbruch; so folgt unmittelbar aus den abgehandelten Sätzen: Jede auf einander folgenden e Reste sind unter einander verschieden und bilden eine Periode. Immer ist $c-1$ theilbar durch e. Der $e$te Rest $= +1$, der $\frac{e}{2}$te $= -1$, wenn e grade; der $e-1$te $=$ dem von r^2, wenn der $\frac{e-1}{2}$te $= r$ und e ungrade. Die Summe jeder auf einander folgenden e Reste ist theilbar durch c, ihr Produkt $= cy - 1$, wenn e grade, und $= cy + 1$, wenn e ungrade. Von den ersten e Resten, und jeden e darauf folgenden, ist, wenn e grade, die Summe des ersten und ersten der zweiten Hälfte, zweiten und zweiten, u. s. w. theilbar durch c, und, da jeder $< c$, $= c$. Das Produkt des ersten und letzten, des zweiten und vorletzten, u. s. w., mit c dividirt, giebt den Rest 10, und, wenn e ungrade, auch das Quadrat des Mittelgliedes. Der erste und erste vor dem letzten Reste, der zweite und zweite, u. s. w. sind correspondirende Zahlen, und, wenn e grade, auch das Quadrat des letzten Gliedes der ersten Hälfte $= cy + 1$. Jede auf einander folgenden e Stellen des Decimalbruches bilden eine Periode. Da z. B. 10 sekundäre Wurzel von 11 zu 2, von 13 zu 6, von 31 zu 15, von 37 zu 3, von 41 zu 5, von 43 zu 21, von 53 zu 13, von 67 zu 33, von 71 zu 35, von 73 zu 8, von 79 zu 13, von 83 zu 41, von 89 zu 44, von 101 zu 4; so hat die Periode von $\frac{1}{11}$ 2, von $\frac{1}{13}$ 6, von $\frac{1}{31}$ 15, von $\frac{1}{37}$ 3, von $\frac{1}{41}$ 5, von $\frac{1}{43}$ 21, von $\frac{1}{53}$ 13, von $\frac{1}{67}$ 33, von $\frac{1}{71}$ 35, von $\frac{1}{73}$ 8, von $\frac{1}{79}$ 13, von $\frac{1}{83}$ 41, von $\frac{1}{89}$ 44, von $\frac{1}{101}$ 4 Stellen, und, da 1 sekundäre Wurzel von 3 zu 1, also auch $(3 . 3 + 1)^1 = 10^1 = 3y + 1$, die von $\frac{1}{3}$ 1 Stelle. Verwandelt man den Bruch $\frac{b}{c}$, so ist es wie in No. 1, und nur wenn e ungrade, im Einzelnen abweichend. Durch Multiplikation der Reste und des Decimalbruches von $\frac{1}{c}$ mit b erhält man Reste und Decimalbruch für $\frac{b}{c}$.

3. Hat die Periode von $\frac{1}{c}$ $c-1$ Stellen, so hat man in den aufeinander folgenden $c-1$ Resten sämmtliche primitive und sekundäre Wurzeln von c; hat sie e Stellen, in den aufeinander folgenden e Resten bestimmte sekundäre Wurzeln. Die Periode von $\frac{1}{17}$ hat 16 Stellen; also sind der 1te, 3, 5, 7, 9, 11, 13, 15te Rest die 8 primitiven Wurzeln von 17; der 2te, 6, 10, 14te die 4 sekundären Wurzeln zu 8; der 4te und 12te die 2 sekundären Wurzeln zu 4; der 8te die zu 2; der 16te zu 1. — Die Periode von $\frac{1}{13}$ hat 6 Stellen; also sind der 1te und 5te Rest sekundäre Wurzeln von 13 zu 6; der 2te und 4te zu 3; der 3te zu 2; der 6te zu 1. — $\frac{1}{41}$ hat 5 Stellen; also sind die ersten 4 Reste sekundäre Wurzeln von 41 zu 5; der 5te zu 1, u. s. w. — Umgekehrt, da z. B. bei $\frac{1}{17}$ der 3te Rest primitive Wurzel von 17; so muss 10 primitive Wurzel von 17 und die Periode 16stellig sein. Bei $\frac{1}{31}$ ist der 7te Rest sekundäre Wurzel von 31 zu 15; also muss 10 sekundäre Wurzel von 31 zu 15 und die Periode 15stellig sein. Man sieht, dass im 1ten Beispiel die 3, im 2ten die 7 relative Primzahl gegen $c-1$. Dagegen lässt es z. B. der 2te Rest

Universitäts- und
Landesbibliothek Düsseldorf

bei $\frac{1}{19}$, der sekundäre Wurzel von 19 zu 9, zweifelhaft, ob 10 primitive Wurzel oder sekundäre Wurzel von 19 zu 9; denn $10^{2\cdot 9} = 19y + (\text{s. W. z. } 9)^9 = 19y + 1$, aber auch: $10^{9\cdot 2} = (19y+1)^2 = 19y + 1$; erst mit dem 3ten Reste, der sekundären Wurzel von 19 zu 6, tritt die Entscheidung ein; denn $10^3 = 19y + \text{s. W. z. } 6$ giebt: $10^9 = 19y + (\text{s. W. z. } 6)^3 = 19y - 1$; folglich 10 pr. W. von 19, und die Periode von $\frac{1}{19}$ 18stellig. — Der zweite Rest bei $\frac{1}{31}$ ist sekundäre Wurzel von 31 zu 15, der dritte zu 5; folglich 10 sek. Wurzel von 31 zu 15, nicht, weil $10^2 = 31y + \text{s. W. z. } 15$, daher: $10^{2\cdot 15} = 31y + (\text{s. W. z. } 15)^{15} = 31y + 1$; sondern, weil $10^{2\cdot 5} = 31y + (\text{s. W. z. } 5)^5 = 31y + 1$.

4. Auch aus § 2, No. 21 und 22 lässt sich beurtheilen, was für eine Wurzel $+10$ von c, also die Anzahl-Stellen der Periode von $\frac{1}{c}$, wenn die Wurzel -10 oder $c-10$ bekannt ist. Da z. B., wenn $c = 11$, -10 oder $11 - 10 = 1 =$ sekund. 1; so ist $+10$ sekundäre Wurzel von 11 zu 2, und die Periode von $\frac{1}{11}$ 2stellig. — Da -10 oder $19 - 10 = 9 =$ s. W. z. 9; so ist $+10$ primitive Wurzel, und $\frac{1}{19}$ 18stellig. — Da -10 oder $31 - 10 = 21 =$ prim. Wurzel; so ist $+10$ sekundäre Wurzel von 31 zu 15, und $\frac{1}{31}$ 15stellig. — Da -10 oder $13 - 10 = 3 =$ s. W. z. 3; so ist $+10$ sekundäre Wurzel von 13 zu 6, und $\frac{1}{13}$ 6stellig (§ 2, No. 21). — Da -10 oder $17 - 10 = 7 =$ primitive Wurzel; so ist auch $+10$ primitive Wurzel, und $\frac{1}{17}$ 16 stellig. — Da -10 oder $73 - 10 = 63 =$ s. W. z. 8; so ist auch $+10$ sekundäre Wurzel zu 8, und $\frac{1}{73}$ 8stellig. — Da -10 oder $101 - 10 = 91 =$ s. W. z. 4; so ist auch $+10$ sekundäre Wurzel von 101 zu 4, und $\frac{1}{101}$ 4 stellig (§ 2, No. 22).

5. Ist $c = 4m + 1$, und bei der Verwandlung von $\frac{1}{c}$ in einen Decimalbruch der $n$te Rest zuerst eine der beiden singulären Zahlen; so hat die Periode $4n$ Stellen; denn ist $10^n = cy + r$, r singuläre Zahl, so ist $10^{4n} = cy + r^4 = cy + 1$, und $4n$ kleinster Exponent (§ 2, No. 20). Erscheint die zweite singuläre Zahl nach der $p$ten Division als Rest; so ist p ein Vielfaches von n; denn $10^{4n} = cy + 1$, und $10^{4p} = cy + (c-r)^4 = cy + 1$, und $n < p$ (§ 2, No. 13). Es ist z. B. bei $\frac{1}{29}$ der 7te Rest die singuläre Zahl 17; also hat die Periode $4 . 7 = 28$ Stellen. Der $7 . 3 =$ 21te Rest ist die zweite singuläre Zahl $29 - 17 = 12$. Bei $\frac{1}{73}$ ist der zweite Rest die singuläre Zahl 27; also hat die Periode $4 . 2 = 8$ Stellen. Der $2 . 3 =$ 6te Rest ist die zweite singuläre Zahl $73 - 27 = 46$. Bei $\frac{1}{101}$ ist der erste Rest die singuläre Zahl 10, also hat die Periode $4 . 1 =$ 4 Stellen. Der $1 . 3 =$ 3te Rest ist die zweite singuläre Zahl 91. — Ist umgekehrt 10 primitive Wurzel, oder sekundäre Wurzel zu n; so ist, wenn n durch 4 theilbar, da es $c - 1 = 4m$ allemal, der Rest nach der $\frac{c-1}{4}$ oder $\frac{n}{4}$ Division, singuläre Zahl. Es ist z. B. 10 primitive Wurzel von 61; folglich der Rest nach der $\frac{61-1}{4} =$ 15ten Division singuläre Zahl, nämlich 50; die 2te $= 61 - 50 = 11$ muss nach der 45ten Division erscheinen. 10 sekundäre Wurzel von 89 zu 44; folglich ist der Rest nach der $\frac{44}{4} =$ 11ten Division singuläre Zahl, nämlich 55; die 2te $= 89 - 55 = 34$ muss nach der 33ten Division erscheinen, u. s. w.

6. Hat die Periode eines Decimalbruches e Stellen, so ist $10^e = cy + 1$, oder $b . 10^e = cy + b$, e kleinster Exponent, und die Primzahl c Nenner des verwandelten Bruches $\frac{1}{c}$ oder $\frac{b}{c}$; folglich $10^e - 1$, oder $b\,(10^e - 1) = cy$. Es ist aber $10^e - 1$ eine Zahl, die mit e Neunen geschrieben wird, welche also die 9 und die Zahl zu Faktoren hat, deren Ziffer aus e Einsen besteht. Es folgt, dass, wenn für $\frac{1}{c}$ oder $\frac{b}{c}$ der Decimalbruch e Stellen hat, die Zahl, deren Ziffer aus e Neunen oder e Einsen besteht, allemal theilbar sein muss durch c, (für $c = 3$ gilt natürlich nur die 9). Es hat z. B. $\frac{1}{7}$ 6 Stellen; also ist 999999 oder 111111 theilbar durch 7. — $\frac{1}{37}$ hat 3 Stellen; folglich 111 theilbar durch 37. — $\frac{8}{101}$ hat 4 Stellen; folglich 1111 theilbar durch 101. — $\frac{7}{41}$ hat 5 Stellen; folglich 11111 theilbar durch 41, u. s. w. — Um daher alle Primzahlen c zu

Universitäts- und
Landesbibliothek Düsseldorf

erfahren, für welche die Periode von $\frac{1}{c}$ oder $\frac{b}{c}$ 6 Stellen hat, ist nur erforderlich die Zahl 111111 in ihre Primfaktoren zu zerlegen. Es ist $111111 = 3 . 7 . 11 . 13 . 37$; aber die Divisoren 3, 11, 37 geben schon vor der letzten 1 den Rest 0; folglich sind es nur die Brüche mit den Nennern 7, 13, welche 6stellige Perioden liefern. — $111 = 3 . 37$; folglich liefern nur Brüche mit dem Nenner 37 eine 3stellige Periode. — $1111 = 11 . 101$; daher geben nur Brüche mit dem Nenner 101 eine 4stellige Periode. — $11111 = 41 . 271$; folglich liefern nur Brüche mit den Nennern 41, 271 eine 5stellige Periode. — Soll ermittelt werden, für welche Primzahlen c die Periode z. B. 7stellig werde; so hat man natürlich nur solche Primzahlen c zu Divisoren der 1111111 zu wählen, bei welchen 7 in $c-1$ aufgeht. Man findet, dass nur Brüche mit den Primzahlen 239, 4649 zu Nennern 7stellige Perioden liefern.

7. Ist c ein Produkt von Primfaktoren (2, 5 ausgenommen); so erhält man die Anzahl Stellen der Periode von $\frac{1}{c}$, wenn man die kleinste Zahl sucht, welche durch die Anzahl Stellen der Perioden aller einzelnen Faktoren theilbar ist. Da z. B. $\frac{1}{11}$ 2, $\frac{1}{41}$, 5 Stellen hat; so ist die Periode von $\frac{1}{11 . 41}$ $2 . 5 = 10$ stellig. Denn in $10^{2 . 5} - 1$ geht sowohl 11 als 41, also, da 11 und 41 relative Primzahlen, $11 . 41$ auf, folglich $10^{2 . 5} = 11 . 41\, y + 1$ und $2 . 5$ kleinster Exponent. — $\frac{1}{3}$ hat 1, $\frac{1}{7}$ 6; also $\frac{1}{3 . 7}$ $1 . 6 = 6$ Stellen. — $\frac{1}{37}$ 3, $\frac{1}{7}$ 6; also $\frac{1}{37 . 7}$ $1 . 6 = 6$ Stellen. — $\frac{1}{73}$ 8, $\frac{1}{13}$ 6, also $\frac{1}{73 . 13}$ $8 . 3 = 24$ Stellen. — $\frac{1}{7}$ 6, $\frac{1}{11}$ 2, $\frac{1}{101}$ 4, also $\frac{1}{7 . 11 . 101}$ $6 . 2 = 12$ Stellen. — Alle diese Exponenten der 10 müssen natürlich in p aufgehen, z. B. der letzte, die 12 in $\frac{7 . 11 . 101 . 6 . 10 . 100}{7 . 11 . 101} = 6000$. — Ist 10 primitive Wurzel von c; so hat die Periode von $\frac{1}{c^2}$, wo $p = \frac{c^2 . (c-1)}{c} = c(c-1)$, p Stellen, wenn der Quotient $\frac{10^c - 1}{c}$, wo p theilbar durch e, nicht theilbar durch c. Es hat z. B. die Periode von $\frac{1}{7^2}$ $7 . 6 = 42$ Stellen; da 7 nicht in $\frac{10^6 - 1}{7}$ aufgeht. Da ferner $10^6 = 7\, y + 1$, wo 6 kleinster Exponent, so kann nicht sein 10^7, 10^{14}, $10^{21} = 7\, y + 1$, also um so weniger $= 7^2 y + 1$; folglich ist in $10^{42} = 7^2\, y + 1$, 42 kleinster Exponent. — Ist 10 sekundäre Wurzel von c zu e, so hat die Periode von $\frac{1}{c_2}$ ec Stellen, wenn der Quotient $\frac{10^n - 1}{c}$, wo e theilbar durch n, nicht theilbar durch c. Denn aus $10^e = cy + 1$ folgt: $10^{ec} = (cy + 1)^c = c^2 y + 1$ (Binomischer Lehrsatz). Da z. B. 10 sekundäre Wurzel von 11 zu 2; so hat die Periode von $\frac{1}{11^2}$ $2 . 11 = 22$ Stellen, da weder $\frac{10^2 - 1}{11}$ noch $\frac{10^{11} - 1}{11}$ durch 11 theilbar, also $2 . 11$ in $10^{2 . 11} = 11^2 y + 1$ kleinster Exponent ist. — $\frac{1}{3^2}$ hat nicht $1 . 3$ Stellen; sondern, weil der Quotient $\frac{10^3 - 3}{3}$ durch 3 theilbar, 1 Stelle. — $10^1 = 3^2 y + 1$, also $10^{1 . 3} = 3 . 3^2\, y + 1$ (Binomischer Lehrsatz); folglich die Periode von $\frac{1}{3^3}$ 3 stellig, u. s. w.

8. Aus §. 4, No. 6, und §. 5, No. 1, 2, 7, folgt sogleich, dass z. B. die Periode von $\frac{1}{5^3 . 11}$ 2 stellig, und nach der 3ten Stelle; die von $\frac{1}{2^4 . 73}$ 8 stellig, und nach der 4ten Stelle; die von $\frac{1}{2^5 . 5^3 . 21}$ 6 stellig, und nach der 5ten Stelle hinter dem Komma erscheint, u. s. w.

9. Ist $\frac{b}{c} = o, |324|$, wo 324 die Periode, so ist

$$\frac{b}{c} = 0{,}324 + \frac{b}{c . 10^3}, \text{ (§. 4, Nr. 1), folglich}$$

$$10^3 . \frac{b}{c} = 324 = \frac{b}{c} \quad ,,$$

$$(10^3 - 1)\frac{b}{c} = 324, \quad ,,$$

$$\frac{b}{c} = \frac{324}{10^3 - 1} = \frac{324}{999} = \frac{12}{37}.$$

Ist $\frac{b}{c} = 0, 18\,|324|$; so ist

$$10^2 . \frac{b}{c} = 18, |324| = 18 + \frac{324}{10^3 - 1}, \text{ folglich}$$

$$\frac{b}{c} = \frac{18 + \frac{324}{10^3 - 1}}{10^2} = \frac{18306}{99900} = \frac{339}{1850} = \frac{339}{37 . 5^2 . 2^1}.$$

Fr. Heime.

Universitäts- und
Landesbibliothek Düsseldorf