Von den kubischen Resten und Nichtresten.

Ist eine Zahl a in der Differenz der Zahlen b und c *ohne Rest* enthalten, so werden die beiden letzteren Zahlen b und c *congruent in Bezug auf die erste Zahl* a genannt; a selbst heißt der *Modulus* der Congruenz, jede der beiden Zahlen b und c ein *Rest* der anderen. — Ist dagegen die Zahl a in der Differenz der Zahlen b und c *nicht ohne Rest* enthalten, so sind b und c *nicht congruent in Bezug auf* a, und jede von ihnen heißt ein *Nichtrest* der anderen.

Diese Bezeichnungen gelten von allen ganzen, sowohl positiven, als negativen Zahlen; nur der Modulus ist offenbar immer absolut, d. h. ohne Vorzeichen zu nehmen. — So sind z. B. $+3$ und $+11$ congruent (oder $+3$ Rest von $+11$, und $+11$ Rest von $+3$) in Bezug auf den Modulus 4, weil ihre Differenz durch 4 ohne Rest theilbar ist. Ebenso sind -3 und -11 congruent (oder -3 Rest von -11, und umgekehrt) in Bezug auf den Modulus 4; ferner $+3$ und -11, desgleichen -3 und $+11$ congruent in Bezug auf den Modulus 7. Dagegen sind $+3$ und $+11$ nicht congruent (oder $+3$ Nichtrest von $+11$, und $+11$ Nichtrest von $+3$) in Bezug auf den Modulus 5, weil ihre Differenz durch 5 nicht ohne Rest theilbar ist.

Die Congruenz der Zahlen soll (nach Gauß) durch das Zeichen $\equiv$ bezeichnet werden. Also: $+3 \equiv +11 \pmod 4$; $-3 \equiv +11 \pmod 7$.

Ist eine von den beiden congruenten Zahlen b und c eine Kubikzahl, so heißt die andere ein *kubischer Rest* in Bezug auf den Modulus a, die Congruenz eine (reine) *kubische* und die Grundzahl des Kubus eine *Wurzel* der kubischen Congruenz. So ist $+4 \equiv +5^3 \pmod{11}$, $-7 \equiv +5^3 \pmod{11}$, $-4 \equiv -5^3 \pmod{11}$, $+7 \equiv -5^3 \pmod{11}$; d. h. $+4$, -7, -4, $+7$ sind kubische Reste von 11.

Ist dagegen eine Zahl b keiner Kubikzahl in Bezug auf den Modulus a congruent, so heißt b ein *kubischer Nichtrest von* a. So sind z. B. die Zahlen 2, 3, 4, 5, sowohl positiv, als negativ genommen, kubische Nichtreste von 7, weil sie keiner Kubikzahl in Bezug auf den Modulus 7 congruent sind.

Im Folgenden soll nun hauptsächlich untersucht werden: 1. welche Eigenschaften die (reinen) kubischen Congruenzen haben; 2. welche Zahlen kubische Reste oder Nichtreste einer gegebenen Zahl sind; 3. welche Beziehungen zwischen den kubischen Resten und Nichtresten einer gegebenen Zahl stattfinden; 4. welcher

Kubikzahl ein bestimmter kubischer Rest einer gegebenen Zahl congruent ist. — Diese Untersuchungen sollen zunächst in Bezug auf eine Primzahl, dann in Bezug auf eine zusammengesetzte Zahl als Modulus angestellt werden.

I. Der Modulus sei eine Primzahl (p).

1. Ist $a^3 \equiv b \pmod{p}$, so sind a und b entweder beide durch p theilbar, oder beide nicht durch p theilbar. — Denn da $a^3 \equiv b$ durch p ohne Rest theilbar ist, so muß, wenn eine von den Zahlen a^3 und b durch p theilbar ist, auch die andere durch p theilbar sein. Ist a durch p theilbar, so ist es auch a^3, mithin auch b; ist b durch p theilbar, so ist es auch a^3, mithin auch a. — Ist dagegen a nicht durch p theilbar, so ist es auch a^3 nicht, und dann kann auch b nicht durch p theilbar sein; ist b nicht durch p theilbar, so kann auch a^3 nicht durch p theilbar sein, mithin auch a nicht.

Ist $b = o$, so ist a entweder auch $= o$, oder eine durch p theilbare Zahl.

Im Folgenden soll nur von solchen congruenten Zahlen die Rede sein, die nicht durch den Modulus p theilbar sind.

2. Ist $a^3 \equiv b \pmod{p}$, so ist auch $a^3 \equiv b \pm np \pmod{p}$. — Denn ist $a^3 - b$ durch p theilbar, also etwa $= fp$, so ist $a^3 - b \pm np = fp \pm np = (f \pm n)\, p$, also $a^3 - b \pm np$ auch durch p theilbar, d. h. $a^3 \equiv b \pm np \pmod{p}$.

Ist also eine Zahl b kubischer Rest von p, so ist es auch jede andere Zahl c, die von b um ein Vielfaches von p verschieden ist.

3. Ist $a^3 \equiv b \pmod{p}$, so ist auch $(a \pm np)^3 \equiv b \pmod{p}$. — Denn $(a \pm np)^3$ ist

$$= a^3 \pm 3a^2np + 3a\,(np)^2 \pm (np)^3$$
$$= a^3 + p\,(\pm 3a^2n + 3an^2p \pm n^3p^2)$$

Da nun $a^3 \equiv b \pmod{p}$, d. h. $a^3 - b = fp$, also $a^3 = b + fp$ ist, so ist

$$(a \pm np)^3 = b + p\,(f \pm 3a^2n + 3an^2p \pm n^3p^2)$$

oder $(a \pm np)^3 - b$ durch p theilbar,

d. h. $(a \pm np)^3 \equiv b \pmod{p}$.

Ist also eine Zahl a Wurzel der Congruenz $x^3 \equiv b \pmod{p}$, so ist es auch jede andere Zahl, die von a um ein Vielfaches von p verschieden ist.

4. Ist $a^3 \equiv b \pmod{p}$, so ist $-a^3 \equiv -b$ und $(np - a)^3 \equiv -b \pmod{p}$. — Denn da $a^3 - b$ durch p theilbar ist, so ist es auch $-(a^3 - b)$ oder $-a^3 + b$, d. h. $-a^3 \equiv -b \pmod{p}$. Da ferner $np - a$ von $-a$ um ein Vielfaches von p verschieden ist, so ist auch $(np - a)^3 \equiv -b \pmod{p}$.

Ist also eine Zahl b kubischer Rest von p, so ist es auch $-b$, insbesondere die Zahl, welche b zum Modulus p ergänzt, also $p - b$, wenn b positiv und kleiner als p ist.

5. Ist $a^3 \equiv b$ und $c^3 \equiv d \pmod{p}$, so ist $(ac)^3 \equiv bd \pmod{p}$. — Denn wenn $a^3 = b + fp$ und $c^3 = d + gp$ ist, so ist a^3c^3 oder $(ac)^3 = bd + p\,(bg + df + fgp)$, d. h. $(ac)^3 \equiv bd \pmod{p}$. Das Produkt zweier (also auch mehrerer) kubischen Reste einer Primzahl p ist mithin ebenfalls ein kubischer Rest von p.

Hieraus folgt auch, daß jede Potenz eines kubischen Restes von p ebenfalls ein kubischer Rest von p ist. Denn setzt man $c = a$, und $d = b$, so ist $(a^2)^3 \equiv b^2 \pmod{p}$. Ebenso ergiebt sich, daß $(a^3)^3 \equiv b^3 \pmod{p}$, $(a^4)^3 \equiv b^4 \pmod{p}$ u. s. w. ist.

6. Ist $a^3 \equiv b$ und $c^3 \equiv d$ (mod. p), so ist $(a:c)^3 \equiv (b:d)$ und $(c:a)^3 \equiv (d:b)$ (mod. p).

Ist a : c eine ganze Zahl, etwa q, also $a = c \cdot q$, so ist $c^3 \cdot q^3 \equiv b$ (mod. p). Nun sei $q^3 \equiv r$ (mod. p); dann ist, weil $c^3 \equiv d$ (mod. p), (nach 5) $c^3 q^3 \equiv dr$ (mod. p), mithin $b \equiv dr$, oder $(b:d) \equiv r$ (mod. p), folglich $(a:c)^3 \equiv (b:d) \equiv r$ (mod p).

Ist a : c keine ganze Zahl, so läßt sich immer eine ganze Zahl m von der Beschaffenheit finden, daß $a \pm mp$ durch c ohne Rest theilbar, also $(a \pm mp) : c$ eine ganze Zahl, etwa q ist. Dann ist (nach 3) auch $(a \pm mp)^3 \equiv b$ (mod. p); also, weil $a \pm mp = cq$, ebenfalls $c^3 q^3 \equiv b$ (mod. p). Ist nun $q^3 \equiv r$ (mod. p), so ist $c^3 q^3 \equiv dr$ (mod. p), mithin $b \equiv dr$ oder $(b:d) \equiv r$ (mod. p), folglich q^3, d. i. $\left[(a \pm mp) : c\right]^3 \equiv (b:d)$ (mod. p), und da $a \pm mp \equiv a$ (mod. p) ist, auch $(a:c)^3 \equiv (b:d) \equiv r$ (mod. p).

Ebenso ergiebt sich, daß $(c:a)^3 \equiv (d:b)$ (mod. p) ist.

Beispiel: Es ist $\left.\begin{aligned} 69^3 &\equiv (69-65)^3 \equiv 4^3 \equiv 12 \\ \text{und } 32^3 &\equiv (32-26)^3 \equiv 6^3 \equiv 8 \end{aligned}\right\}$ (mod. 13).

Hier ist $69 + 7 \cdot 13 = 5 \cdot 32$ und $5^3 \equiv 8$ (mod. 13), also $69^3 \equiv (69 + 7 \cdot 13)^3 \equiv 5^3 \cdot 32^3 \equiv 8 \cdot 8$, folglich $12 \equiv 8 \cdot 8$ und $(12:8) \equiv 8$ (mod. 13). Demnach ist $(69:32)^3 \equiv 8$ (mod. 13). — Andrerseits ist $32 + 40 \cdot 13 = 8 \cdot 69$ und $8^3 \equiv 5$ (mod. 13), also $32^3 \equiv (32 + 40 \cdot 13)^3 \equiv 8^3 \cdot 69^3 \equiv 5 \cdot 12$; folglich $8 \equiv 5 \cdot 12$ und $(8:12) \equiv 5$ (mod. 13). Demnach ist $(32:69)^3 \equiv 5$ (mod. 13).

Der Quotient zweier kubischen Reste einer Primzahl p ist demnach ebenfalls ein kubischer Rest von p oder einem kubischen Reste von p congruent. — Hieraus ergiebt sich auch, daß, wenn eine Quadratzahl kubischer Rest von p ist, auch die Quadratwurzel kubischer Rest von p ist. Denn ist $b^2 \equiv a^3$ (mod. p), so ist (nach 5) b^4 oder $b^3 \cdot b \equiv (a^2)^3$, mithin $b \equiv (a^2 : b)^3$ (mod. p).

7. Die Anzahl der positiven Wurzeln der Congruenz $x^3 \equiv b\ (b > 1)$ (mod. p), welche kleiner als der Modulus p sind, ist gleich der Anzahl der positiven Wurzeln ($< p$) der Congruenz $x^3 \equiv +1$ (mod. p).

Ist $a^3 \equiv b$ und $c^3 \equiv +1$ (mod. p), wo a und c positiv und $< p$ sind, so ist (nach 5) $(ac)^3 \equiv b$ (mod. p), also, wenn c von $+1$ verschieden ist, ac ebenfalls eine Wurzel der Congruenz $x^3 \equiv b$ (mod. p). Nun ist ac entweder $< p$ oder $> p$, nie $= p$ oder einem Vielfachen von p, weil p eine Primzahl ist.

Ist $ac > p$, etwa $= mp + d$, wo d positiv und $< p$ ist, so ist (nach 3) auch $d^3 \equiv b$ (mod. p). Giebt es nun außer $+1$ und c noch andere positive Zahlen $< p$, deren Kuben $\equiv +1$ (mod. p) sind, so giebt es demgemäß auch noch andere positive Zahlen $< p$, und zwar ebenso viel, deren Kuben $\equiv b$ (mod. p) sind. Denn, wenn auch $e^3 \equiv +1$ (mod. p) ist, so ist auch $(a \cdot e)^3 \equiv b$ (mod. p), und wenn $a \cdot e = np + f$, wo f positiv und $< p$ ist, so ist auch $f^3 \equiv b$ (mod. p). Die Zahlen a, d, f sind aber von einander verschieden, wenn c und e von einander und von $+1$ verschieden sind. Daß d und f von a verschieden sind, geht daraus hervor, daß $d = ac - mp$ und $f = a \cdot e - np$ ist. Wären nämlich d und $f = a$, so müßte einerseits $mp = a(c-1)$, andrerseits $np = a(e-1)$ sein, was nicht möglich ist, da a, c und e positiv und $< p$, c und e von $+1$ verschieden, und p eine Primzahl ist. Aber auch d und f sind von einander verschieden, wenn c und e von einander verschieden sind. Denn wäre $d = f$, also $ac - mp = ae - np$, so müßte $a(c-e) = p(m-n)$ sein, was aus den obigen Gründen ebenfalls nicht möglich ist.

8. Die Congruenz $x^3 \equiv +1$ (mod. p) hat eine einzige positive Wurzel $< p$, nämlich $+1$, wenn $p = 3$ oder eine Primzahl von der Form $3n - 1$ ist, und drei verschiedene positive Wurzeln $< p$, wenn p eine Primzahl von der Form $3n + 1$ ist.

$x^3 \equiv +1 \pmod{p}$ bedeutet, daß $x^3 - 1$ durch p ohne Rest theilbar ist, oder daß $x^3 - 1$ ein Vielfaches von p, etwa $= fp$ ist, wo f auch 0 oder 1 sein kann. Nun ist $x^3 - 1 = (x-1)(x^2+x+1)$. Daher ist $x^3 - 1$ zunächst und immer durch p theilbar, wenn $x - 1 = fp$ ist. Da es sich hier aber nur um positive Zahlen $< p$ handelt, so kann x nur den Werth $+1$ haben. Demnach ist $+1$ in allen Fällen eine Wurzel der Congruenz $x^3 \equiv +1 \pmod{p}$.

Ferner ist $x^3 - 1$ durch p theilbar, wenn $x^2 + x + 1$ durch p theilbar, d. h. $= fp$ ist. Multiplicirt man alle Glieder der Gleichung $x^2 + x + 1 = fp$ mit 4, so erhält man $4x^2 + 4x + 4 = 4fp$ oder $(2x+1)^2 + 3 = fp$. Diese Gleichung ist gleichbedeutend mit der Congruenz $(2x+1)^2 \equiv -3 \pmod{p}$, welche, wie aus der Lehre von den quadratischen Resten sich ergiebt, lösbar ist, wenn p eine Primzahl von der Form $3n+1$ ist, dann aber auch immer lösbar ist und stets zwei von $+1$ verschiedene positive Wurzeln $< p$ hat. Ist $p = 3$, so ist diese Congruenz zwar auch lösbar, aber nur durch $x = +1$.

Die Congruenz $x^3 \equiv +1 \pmod{p}$ hat demnach nur die positive Wurzel $x = +1$, wenn $p = 3$ oder eine Primzahl von der Form $3n - 1$ ist; wenn aber p eine Primzahl von der Form $3n + 1$ ist, so giebt es stets drei verschiedene positive Zahlen $< p$, darunter immer $+1$, welche der Congruenz genügen.

Es hat daher (nach 7) auch die Congruenz $x^3 \equiv b \pmod{p}$, wo b von $+1$ verschieden ist, nur eine positive Wurzel $< p$, wenn $p = 3$ oder von der Form $3n-1$ ist, dagegen drei verschiedene positive Wurzeln $< p$, wenn p von der Form $3n+1$ ist.

9. Die Congruenz $(2x+1)^2 \equiv -3 \pmod{p}$, deren Wurzeln, wenn p von der Form $3n+1$ ist, zugleich Wurzeln der Congruenz $x^3 \equiv +1 \pmod{p}$ sind, läßt sich einfach auf folgende Weise auflösen.

Jede Primzahl von der Form $3n+1$ läßt sich, wie sich aus der Lehre von den quadratischen Resten ergiebt, stets unter der Form $u^2 + 3v^2$ darstellen, d. h. es ist $u^2 \equiv -3v^2 \pmod{p}$, mithin $(u^2 : v^2)$ oder $(u : v)^2 \equiv -3 \pmod{p}$. Es ist daher $2x + 1 \equiv \pm (u : v)$, oder $(2x+1)\,v \equiv \pm u \pmod{p}$, und diese Congruenz, die in Bezug auf die unbekannte Größe x vom 1. Grade ist, giebt immer (wenn man nämlich u einmal positiv, dann negativ annimmt) zwei und nicht mehr positive Werthe $< p$ für x.

Beispiele: $p = 67$ ist $= 8^2 + 3$, also $8^2 \equiv -3 \pmod{67}$; mithin $2x + 1 \equiv \pm 8$, also $2x \equiv -1 \pm 8 \pmod{67}$.

Daher ist einmal $2x \equiv +7 \equiv +74$, folglich $x_1 \equiv +37$,

und dann $2x \equiv -9 \equiv +58$, folglich $x_2 \equiv +29$.

37^3 ist $= 50653 = 756 \cdot 67 + 1$, also $37^3 \equiv +1 \pmod{67}$,

29^3 ist $= 24389 = 364 \cdot 67 + 1$, also $29^3 \equiv +1 \pmod{67}$.

$p = 37$ ist $= 5^2 + 3 \cdot 2^2$, also $5^2 \equiv -3 \cdot 2^2$ und $(5:2)^2 \equiv -3 \pmod{37}$. Mithin ist $2x+1 \equiv \pm (5:2)$ oder $2(2x+1) \equiv \pm 5 \pmod{37}$. Dann ist einmal $2(2x+1) \equiv +5 \equiv +42$, also $2x + 1 \equiv +21$, $2x \equiv +20$, folglich $x_1 \equiv +10$. Ferner ist $2(2x+1) \equiv -5 \equiv -42$, also $2x + 1 \equiv -21$, $2x \equiv -22$, folglich $x_2 \equiv -11 \equiv +26 \pmod{37}$.

10^3 ist $= 1000 = 27 \cdot 37 + 1$, also $10^3 \equiv +1 \pmod{37}$.

26^3 ist $= 17576 = 475 \cdot 37 + 1$, also $26^3 \equiv +1 \pmod{37}$.

Die 3 Wurzeln der Congruenz $x^3 \equiv +1 \pmod{p = 3n+1}$, welche positiv und $< p$ sind, sollen im Folgenden die kubischen Wurzeln der Einheit genannt, und die beiden, welche > 1 sind, mit α und β bezeichnet werden.

10. Ist $\gamma\ (< p)$ eine Wurzel der Congruenz $x^3 \equiv b \pmod{p = 3n+1}$, also $\gamma^3 \equiv b \pmod{p}$ so sind die beiden andern (wie γ positiv und $< p$), die im Folgenden mit δ und ε bezeichnet werden sollen,

den Producten aus dieser Wurzel γ und den beiden kubischen Wurzeln der Einheit, welche > 1 sind, congruent; also $\delta \equiv \gamma\alpha$ und $\varepsilon \equiv \gamma\beta$ (mod. p).

Da einerseits $\gamma^3 \equiv b$ sein soll, andrerseits $\alpha^3 \equiv +1$ und $\beta^3 \equiv +1$ (mod. p) ist, so ist (nach 7) sowohl $\gamma^3\alpha^3$ oder $(\gamma\alpha)^3 \equiv b$, als auch $\gamma^3\beta^3$ oder $(\gamma\beta)^3 \equiv b$ (mod. p).

Beispiel: Es ist $8^3 \equiv 31$ (mod. 37), weil $8^3 = 512 = 13 \cdot 37 + 31$ ist, also $\gamma \equiv 8$. Da nun, wie in 9 gefunden, $\alpha \equiv 10$ und $\beta \equiv 26$ ist, so ist $\delta \equiv 8 \cdot 10 \equiv 6$ und $\varepsilon \equiv 8 \cdot 26 \equiv 23$ (mod. 37).

6^3 ist $= 216 = 5 \cdot 37 + 31$, also $6^3 \equiv 31$ (mod. 37).

23^3 ist $= 12167 = 328 \cdot 37 + 31$, also $23^3 \equiv 31$ (mod. 37).

11. Die Summe der drei positiven Wurzeln einer reinen kubischen Congruenz, deren Modulus eine Primzahl p von der Form $3n+1$ ist, ist durch den Modulus theilbar und zwar entweder $= p$ oder $= 2p$.

Nach 8 ist, wenn α und β die beiden Wurzeln der Congruenz $x^3 \equiv +1$ (mod. p) sind,

sowohl $\alpha^2 + \alpha + 1$, als auch $\beta^2 + \beta + 1$

durch p ohne Rest theilbar, mithin auch

$$(\alpha^2 + \alpha + 1) - (\beta^2 + \beta + 1) \text{ oder } \alpha^2 - \beta^2 + \alpha - \beta$$

oder

$$(\alpha - \beta)(\alpha + \beta + 1).$$

Da nun α und β beide positiv und $< p$ sind, so kann $\alpha - \beta$ nicht durch p theilbar sein; mithin ist $\alpha + \beta + 1$, d. h. die Summe der kubischen Wurzeln der Einheit durch p theilbar.

Ferner ist sowohl α, als auch $\beta < p-1$; denn $p-1$ ist keine Wurzel der Congruenz $x^3 \equiv +1$ (mod. p), weil $(p-1)^3 = p^3 - 3p^2 + 3p - 1 = -1 + p(p^2 - 3p + 3)$, also $(p-1)^3 \equiv -1$ (mod. p) ist. Daher ist $\alpha + \beta < 2p - 2$ und

$$\alpha + \beta + 1 < 2p - 1;$$

mithin ist $\alpha + \beta + 1$, da diese Summe $< 2p$, aber durch p theilbar ist, $= p$.

Von den 3 positiven Wurzeln der Congruenz $x^3 \equiv b$ (mod. $p = 3n+1$), welche $< p$ sind, d. h. von γ, δ, ε ist $\delta \equiv \gamma\alpha$ und $\varepsilon \equiv \gamma\beta$ (nach 10); mithin ist

$$\gamma + \delta + \varepsilon \equiv \gamma(1 + \alpha + \beta) \text{ (mod. p)},$$

folglich, weil $1 + \alpha + \beta$ durch p theilbar ist, auch

$$\gamma + \delta + \varepsilon \text{ durch p theilbar.}$$

Da nun jede der 3 Zahlen γ, δ, $\varepsilon < p$ ist, so ist ihre Summe $< 3p$, mithin, da $\gamma + \delta + \varepsilon$ durch p theilbar ist,

$$\gamma + \delta + \varepsilon = p \text{ oder } = 2p.$$

Hieraus folgt weiter noch Folgendes:

(1) Ist eine der beiden kubischen Wurzeln der Einheit, die > 1 sind, bekannt, so ist es auch die andere, und zwar ergänzt diese die um 1 vermehrte erste zum Modulus, d. h. β ist $= p - (\alpha + 1)$ und $\alpha = p - (\beta + 1)$.

Denn β^3 ist $= p^3 - 3p^2(\alpha + 1) + 3p(\alpha + 1)^2 - (\alpha + 1)^3$, also

$$\left.\begin{aligned} &\equiv -(\alpha + 1)^3 \equiv -\alpha^3 - 3\alpha^2 - 3\alpha - 1 \\ &\equiv -(\alpha^2 + \alpha + 1)(\alpha + 1) - (\alpha^2 + \alpha) \end{aligned}\right\} \text{ (mod. p)}$$

und da $\alpha^2 + \alpha + 1$ durch p theilbar ist (nach 8), so ist $\beta^3 \equiv -(\alpha^2 + \alpha)$ und $\alpha^2 + \alpha \equiv -1$ (mod. p), mithin $\beta^3 \equiv +1$ (mod. p), d. h. β eine kubische Wurzel der Einheit.

(2) Sind von den drei positiven Wurzeln ($< p$) der Congruenz $x^3 \equiv b$ (mod. p) zwei bekannt, so ist es auch die dritte, und zwar ergänzt diese die Summe der beiden ersten zu p oder $2p$, je nachdem diese Summe $<$ oder $> p$ ist.

Ist $\gamma^3 \equiv b$ und $\delta^3 \equiv b \pmod{p}$, ferner $\gamma + \delta = p - \varepsilon$, so ist $\varepsilon = p - (\gamma + \delta)$, also $\varepsilon^3 \equiv -(\gamma+\delta)^3 \equiv -(\gamma^3 + 3\gamma^2\delta + 3\gamma\delta^2 + \delta^3) \equiv -2b - 3\gamma\delta(\gamma+\delta) \pmod{p}$. Es sei nun $\delta \equiv \gamma\alpha \pmod{p}$. Dann ist $\varepsilon^3 \equiv -2b - 3\gamma^3\alpha(1+\alpha)$, also, da $\gamma^3 \equiv b$ und $\alpha(1+\alpha) \equiv -1 \pmod{p}$ ist, $\varepsilon^3 \equiv -2b + 3b \equiv b \pmod{p}$, folglich ε eine Wurzel der Congruenz $x^3 \equiv b \pmod{p}$. Dasselbe ergiebt sich, wenn $\delta \equiv \gamma\beta$, oder $\gamma \equiv \delta\alpha$, oder $\gamma \equiv \delta\beta \pmod{p}$ angenommen wird.

Ist $\gamma + \delta > p$, also $\gamma + \delta = 2p - \varepsilon$, mithin $\varepsilon = 2p - (\gamma+\delta)$, so ist ε^3 ebenfalls $\equiv -(\gamma+\delta)^3$, mithin ε^3 auch $\equiv b \pmod{p}$.

12. Das Produkt zweier positiven Wurzeln einer reinen kubischen Congruenz, deren Modulus $p = 3n+1$ ist, ist dem Quadrate der dritten Wurzel congruent.

Da die Summe der drei kubischen Wurzeln der Einheit, d. h. $1+\alpha+\beta = p$ ist, so ist $\alpha(1+\alpha+\beta) = \alpha p$, oder $\alpha\beta \equiv -\alpha(1+\alpha) \pmod{p}$, also, weil $\alpha(1+\alpha) \equiv -1 \pmod{p}$, $\alpha\beta \equiv +1 \equiv 1^2 \pmod{p}$. Hieraus folgt ferner $\alpha\beta^3 \equiv \beta^2$, also, da $\beta^3 \equiv +1$, $\alpha \equiv \beta^2 \pmod{p}$. Endlich ist, weil $\alpha\beta \equiv +1$, $\alpha^3\beta \equiv \alpha^2$, folglich, weil $\alpha^3 \equiv +1$, $\beta \equiv \alpha^2 \pmod{p}$.

Sind γ, δ, ε die positiven Wurzeln der Congruenz $x^3 \equiv b \pmod{p}$ und $\delta \equiv \gamma\alpha$, $\varepsilon \equiv \gamma\beta$, so ist

$$\left.\begin{array}{lll} \gamma\delta \equiv \gamma^2\alpha & \equiv \gamma^2\beta^2 \equiv (\gamma\beta)^2 & \equiv \varepsilon^2 \\ \gamma\varepsilon \equiv \gamma^2\beta & \equiv \gamma^2\alpha^2 \equiv (\gamma\alpha)^2 & \equiv \delta^2 \\ \delta\varepsilon \equiv \gamma^2\alpha\beta & \equiv \gamma^2 & \end{array}\right\} \pmod{p}.$$

13. Das Produkt der drei positiven Wurzeln einer reinen kubischen Congruenz, deren Modulus $p = 3n+1$ ist, ist dem Kubus einer jeden congruent.

Denn $\gamma\delta\varepsilon$ ist $\equiv \gamma \cdot \gamma\alpha \cdot \gamma\beta \equiv \gamma^3 \cdot \alpha\beta \equiv \gamma^3$, also, weil $\gamma^3 \equiv b$, $\delta^3 \equiv b$, $\varepsilon^3 \equiv b$ ist, $\gamma\delta\varepsilon$ auch $\equiv \delta^3 \equiv \varepsilon^3 \pmod{p}$.

14. Der Quotient zweier positiven Wurzeln einer reinen kubischen Congruenz, deren Modulus $p = 3n+1$ ist, ist einer der beiden kubischen Wurzeln der Einheit, welche > 1 sind, und dem Quadrate der andern dieser beiden Wurzeln congruent.

Nach 12 ist $\alpha\beta \equiv +1$, ferner $\alpha^2 \equiv \beta$ und $\beta^2 \equiv \alpha \pmod{p}$. Daher ist

$$\left.\begin{array}{ll} \frac{1}{\alpha} \equiv \beta \equiv \alpha^2; & \frac{1}{\beta} \equiv \alpha \equiv \beta^2 \\ \frac{\alpha}{\beta} \equiv \beta \equiv \alpha^2; & \frac{\beta}{\alpha} \equiv \alpha \equiv \beta^2 \end{array}\right\} \pmod{p}.$$

Ferner ist $\delta \equiv \gamma\alpha$ und $\varepsilon \equiv \gamma\beta \pmod{p}$; mithin ist

$$\left.\begin{array}{lll} \frac{\gamma}{\delta} \equiv \frac{1}{\alpha} \equiv \beta \equiv \alpha^2; & \frac{\gamma}{\varepsilon} \equiv \frac{1}{\beta} \equiv \alpha \equiv \beta^2 \\ \frac{\delta}{\gamma} \equiv \alpha \equiv \beta^2; & \frac{\delta}{\varepsilon} \equiv \frac{\alpha}{\beta} \equiv \beta \equiv \alpha^2 \\ \frac{\varepsilon}{\gamma} \equiv \beta \equiv \alpha^2; & \frac{\varepsilon}{\delta} \equiv \frac{\beta}{\alpha} \equiv \alpha \equiv \beta^2 \end{array}\right\} \pmod{p}.$$

15. Die Summe der Quadrate der drei positiven Wurzeln einer reinen kubischen Congruenz, deren Modulus $p = 3n+1$ ist, ist durch den Modulus ohne Rest theilbar.

Zunächst ist $(+1)^2 + \alpha^2 + \beta^2 \equiv 1 + \alpha^2 + \alpha$ (weil $\beta^2 \equiv \alpha$), und da $1 + \alpha^2 + \alpha$ oder $1 + \alpha + \alpha^2$ (nach 8) durch p theilbar ist, so ist es auch $(+1)^2 + \alpha^2 + \beta^2$.

Ferner ist $\gamma^2 + \delta^2 + \varepsilon^2 \equiv \gamma^2 + \gamma^2\alpha^2 + \gamma^2\beta^2 \equiv \gamma^2(1 + \alpha^2 + \beta^2)$, also, da $1 + \alpha^2 + \beta^2$ durch p theilbar ist, auch $\gamma^2 + \delta^2 + \varepsilon^2$.

16. Die Summe der Produkte je zweier positiven Wurzeln ($< p$) ist durch den Modulus ohne Rest theilbar.

$1 . \alpha + 1 . \beta + \alpha\beta$ ist $\equiv \alpha + \beta + 1$ (mod. p), also durch p theilbar.

$\gamma\delta + \gamma\varepsilon + \delta\varepsilon$ ist (nach 12) $\equiv \varepsilon^2 + \delta^2 + \gamma^2$ (mod. p), also (nach 15) durch p theilbar.

17. Ist sowohl die Summe dreier positiven Zahlen, die kleiner als eine Primzahl p von der Form $3n + 1$ sind, als auch die Summe ihrer Quadrate durch diese Primzahl ohne Rest theilbar, so sind diese drei Zahlen die Wurzeln einer reinen kubischen Congruenz, deren Modulus jene Primzahl ist.

Es seien γ, δ, ε positive Zahlen $< p\,(= 3n + 1)$, ferner sei sowohl $\gamma + \delta + \varepsilon$, als $\gamma^2 + \delta^2 + \varepsilon^2$ durch p ohne Rest theilbar.

Ferner sei $\left.\begin{array}{l} \delta : \gamma \equiv \alpha \text{ und } \varepsilon : \gamma \equiv \beta \\ \text{oder } \delta \equiv \gamma\alpha \quad \text{und } \varepsilon \equiv \gamma\beta \end{array}\right\}$ (mod. p),

wo α und $\beta < p$ sind, was immer möglich ist. Denn da γ durch p nicht theilbar ist, so kann auch keins der Produkte dieser Zahl mit allen Zahlen von 1 bis $p-1$ durch p theilbar sein, d. h. alle diese Produkte, deren Anzahl $p-1$ ist, geben, durch p dividirt, Reste. Diese Reste sind sämmtlich von einander verschieden (denn zwei Produkte $k\gamma$ und $h\gamma$, die, durch p dividirt, denselben Rest gäben, müßten congruent, ihre Differenz also durch p theilbar sein, was nicht möglich ist) und den Zahlen von 1 bis $p-1$ gleich; mithin gibt es immer zwei Produkte $\gamma\alpha$ und $\gamma\beta$, die, durch p dividirt, δ und ε als Reste haben, d. h. die δ unnd ε congruent ist.

Dann ist einerseits $\left.\begin{array}{l} \gamma + \delta + \varepsilon \equiv \gamma\,(1 + \alpha + \beta) \\ \text{andrerseits } \gamma^2 + \delta^2 + \varepsilon^2 \equiv \gamma^2\,(1 + \alpha^2 + \beta^2) \end{array}\right\}$ (mod. p)

und da sowohl $\gamma + \delta + \varepsilon$, als $\gamma^2 + \delta^2 + \varepsilon^2$ durch p theilbar sind, γ aber nicht, so muß auch einerseits $1 + \alpha + \beta$, andrerseits $1 + \alpha^2 + \beta^2$ durch p theilbar sein. Nun kann $1 + \alpha + \beta$, weil α und $\beta < p$ sind, durch p nur dann theilbar sein, wenn $1 + \alpha + \beta = p$ oder $1 + \alpha = p - \beta$ ist. Dann ist $(1+\alpha)^2 = p^2 - 2p\beta + \beta^2$, also $(1 + \alpha)^2 \equiv \beta^2$ (mod. p).

Da ferner auch $1 + \alpha^2 + \beta^2$ durch p theilbar, d. h. $\beta^2 \equiv -(1 + \alpha^2)$ (mod. p) ist, so ist demnach $(1 + \alpha)^2 \equiv -(1 + \alpha^2)$, oder $(1 + \alpha)^2 + (1 + \alpha^2)$, d. i. $2(1 + \alpha + \alpha^2)$ durch p theilbar, mithin auch $1 + \alpha + \alpha^2$, ferner auch $\alpha(1 + \alpha + \alpha^2)$ oder $\alpha + \alpha^2 + \alpha^3$, d. h. $\alpha^3 \equiv -(\alpha + \alpha^2)$ (mod. p), und da $\alpha + \alpha^2 \equiv -1$ (mod. p) ist, so ist $\alpha^3 \equiv +1$ (mod. p), also α eine kubische Wurzel der Einheit. Da ferner $\beta = p - (\alpha + 1)$ ist, so ist (nach 11) auch β eine kubische Wurzel der Einheit.

Ist nun $\gamma^3 \equiv b$ (mod. p), so ist $\left.\begin{array}{l} \delta^3 \equiv \gamma^3\alpha^3 \equiv \gamma^3 \equiv b \\ \text{und } \varepsilon^3 \equiv \gamma^3\beta^3 \equiv \gamma^3 \equiv b \end{array}\right\}$ (mod. p),

also γ, δ, ε die positiven Wurzeln der Congruenz

$$x^3 \equiv b \text{ (mod. p)}.$$

18. Ist $p = 3$ oder eine Primzahl von der Form $3n - 1$, so sind alle ganzen Zahlen kubische Reste von p.

Nach 8 hat jede reine kubische Congruenz, wenn der Modulus $p = 3$ oder eine Primzahl von der Form $3n - 1$ ist, nur eine einzige positive Wurzel $< p$; mithin ist jede positive ganze Zahl einem Kubus congruent, also (nach 2) überhaupt jede ganze Zahl.

19. Die Wurzel der Congruenz $x^3 \equiv a$ in Bezug auf den Modulus $p = 3$ ist congruent a.

Nach dem Fermat'schen Satze ist, wenn p eine Primzahl ist, die $(p-1)$te Potenz jeder ganzen Zahl $\equiv +1$ (mod. p). Mithin ist, wenn $p = 3$ ist, x^{3-1} oder $x^2 \equiv +1$ (mod. 3), folglich $x^3 \equiv x$, und, weil $x^3 \equiv a$ (mod. 3) sein soll, $x \equiv a$ (mod. 3).

Alle ganzen Zahlen sind entweder durch 3 theilbar, also Vielfache von 3 (3 mit einbegriffen), oder von der Form $3n \pm 1$. Ist a durch 3 theilbar, etwa $= 3n$, so muß x auch durch 3 theilbar, also $\equiv a \pmod 3$ sein; denn der Kubus jeder durch 3 theilbaren Zahl ist ebenfalls durch 3 theilbar; dagegen ist der Kubus jeder nicht durch 3 theilbaren Zahl auch nicht durch 3 theilbar. — Ist $a = 3n + 1$, so muß $x^3 \equiv +1 \pmod 3$ sein, also (nach 8) $x \equiv +1$, d. h. x muß ebenfalls von der Form $3n + 1$, oder $\equiv a \pmod 3$ sein.

Ist $a = 3n - 1$, so muß $x^3 \equiv -1 \pmod 3$ oder $(-x)^3 \equiv +1 \pmod 3$ sein. Da nun $(+1)^3 \equiv +1 \pmod 3$ ist, so muß $-x \equiv +1$, oder $x \equiv -1 \pmod 3$ sein, d. h. x von der Form $3n - 1$ oder $\equiv a \pmod 3$.

20. Die Wurzel der Congruenz $x^3 \equiv a \pmod p$, wo $a < p$ und p von der Form $3n - 1$ ist, ist congruent b^{n-1}, wo $ab \equiv +1 \pmod p$ ist.

Nach dem Fermat'schen Satze ist $x^{p-1} \equiv +1 \pmod p$, also, wenn $p = 3n - 1$ ist, $x^{3n-2} \equiv +1 \pmod p$. Da nun $x^3 \equiv a \pmod p$ sein soll, so muß (nach 5) auch $(x^{n-1})^3$ oder $x^{3n-3} \equiv a^{n-1}$, also $x^{3n-2} \equiv a^{n-1} \cdot x$, mithin $a^{n-1} \cdot x \equiv +1 \pmod p$ sein. Ist nun $ab \equiv +1 \pmod p$, was (nach 17) immer möglich ist, so ist auch $a^{n-1} \cdot b^{n-1} \equiv +1$, mithin $a^{n-1} \cdot x \equiv a^{n-1} \cdot b^{n-1}$, folglich $x \equiv b^{n-1} \pmod p$. — Setzt man diesen Werth für x in $x^3 \equiv a$ ein, so erhält man $b^{3n-3} \equiv a$, und wenn man auf beiden Seiten mit b multiplicirt, $b^{3n-2} \equiv ab$, und da einerseits $b^{3n-2} \equiv +1$ ist (nach dem Fermat'schen Satze), andrerseits $ab \equiv +1$ sein soll, so ist in der That $b^{3n-2} \equiv ab \pmod p$.

Zu demselben Resultate gelangt man auch auf folgende Weise. Nach dem Fermat'schen Satze ist $a^{3n-2} \equiv +1$, oder $a \cdot (a^{n-1})^3 \equiv +1 \pmod p$. Ist nun $ab \equiv +1$, also auch $(a^{n-1})^3 (b^{n-1})^3 \equiv +1$, so ist, wenn man x für b^{n-1} setzt, $(a^{n-1})^3 x^3 \equiv +1$, folglich $x^3 \equiv a \pmod p$.

Es kann jedoch auch schon eine niedrigere Potenz von a, als die $(p-1)$te, $\equiv +1 \pmod p$ sein. In diesem Falle ist der Exponent ein genauer Theil von $p - 1$, und da $p = 3n - 1$, also $p - 1 = 3n - 2$, mithin nicht durch 3 theilbar ist, so kann auch der Exponent der niedrigeren Potenz von a, welche $\equiv +1 \pmod p$ ist, nicht durch 3 theilbar sein; er ist daher entweder von der Form $3m + 1$ oder $3m - 1$. — Ist a^{3m+1} oder $a^{3m} \cdot a \equiv +1 \pmod p$, ferner $ab \equiv +1$, mithin auch $a^{3m} \cdot b^{3m} \equiv +1 \pmod p$, so ist $a \equiv b^{3m}$, also $x \equiv b^m \pmod p$. Ist dagegen $a^{3m-1} \equiv +1$, also $a^{3m} \equiv a \pmod p$, so ist $x \equiv a^m \pmod p$.

Beispiele: Soll $x^3 \equiv 7 \pmod{17}$ sein, so ist, weil $17 = 3 \cdot 6 - 1$ und $7 \cdot 5 \equiv +1 \pmod{17}$ ist, $x \equiv 5^5 \pmod{17}$, d. i. $x \equiv 14$. (14^3 ist $= 161 \cdot 17 + 7$, folglich $14^3 \equiv 7 \pmod{17}$).

Soll $x^3 \equiv 9 \pmod{17}$ sein, so ist, weil $9 \cdot 2 \equiv +1 \pmod{17}$ ist, $x \equiv 2^5 \equiv 15$. (15^3 ist $= 198 \cdot 17 + 9$, folglich $15^3 \equiv 9 \pmod{17}$). Es ist aber auch $9^8 \equiv +1 \pmod{17}$, also, da $8 = 3 \cdot 3 - 1$, $x \equiv 9^3 \equiv 15$.

Soll $x^3 \equiv 4 \pmod{17}$ sein, so ist, weil $4 \cdot 13 \equiv +1 \pmod{17}$ ist, $x \equiv 13^5 \equiv 13$. (13^3 ist $\equiv 129 \cdot 17 + 4$, folglich $13^3 \equiv 4 \pmod{17}$).

Es ist aber auch $4^4 \equiv +1 \pmod{17}$, also, da $4 = 1 \cdot 3 + 1$ und $4 \cdot 13 \equiv +1 \pmod{17}$ ist, $x \equiv 13^1$ oder 13.

21. Ist p eine Primzahl von der Form $3n + 1$, so ist die Anzahl der (positiven) kubischen Reste von p, welche kleiner als p sind, $= \frac{p-1}{3}$, d. h. $= n$, und die Anzahl der kubischen Nichtreste $(< p) = 2n$.

Da (nach 8) jede reine kubische Congruenz, deren Modulus eine Primzahl p von der Form $3n + 1$ ist, drei verschiedene positive Wurzeln $< p$ hat, d. h. jeder kubische Rest einer solchen Primzahl den Kuben

dreier verschiedenen positiven Zahlen $< p$ congruent ist, so können von den Zahlen von 1 bis $p-1$ nur $\frac{p-1}{3} = n$ kubische Reste von p sein; die übrigen 2n sind daher kubische Nichtreste von p.

Beispiel: Von den Zahlen, die < 19 sind, sind folgende 6: 1, 7, 8, 11, 12, 18 kubische Reste von 19; denn

$$\left.\begin{array}{rl} 1 \text{ ist } \equiv & 1^3 \equiv 7^3 \equiv 11^3; \quad 7 \equiv 4^3 \equiv 6^3 \equiv 9^3; \\ 8 \equiv & 2^3 \equiv 3^3 \equiv 14^3; \quad 11 \equiv 5^3 \equiv 16^3 \equiv 17^3; \\ 12 \equiv & 10^3 \equiv 13^3 \equiv 15^3; \quad 18 \equiv 8^3 \equiv 12^3 \equiv 18^3; \end{array}\right\} \text{(mod. 19).}$$

Die übrigen 12 Zahlen, die < 19 sind, nämlich:

2, 3, 4, 5, 6, 9, 10, 13, 14, 15, 16, 17,

sind keinem Kubus in Bezug auf den Modulus 19 congruent, also kubische Nichtreste von 19.

22. Eine Zahl a ist kubischer Rest einer Primzahl $p = 3n+1$, wenn der Exponent der niedrigsten Potenz von a, welche $\equiv +1$ (mod. p) ist, $= \frac{p-1}{3}$, d. i. n oder ein Faktor von n ist; andernfalls ist a kubischer Nichtrest von p.

Soll $a \equiv x^3$ (mod. $p = 3n+1$) sein, so muß, da nach dem Fermat'schen Satze x^{p-1}, hier also x^{3n} oder $(x^3)^n \equiv +1$ (mod. p) ist, $a^n \equiv +1$ (mod. p) sein.

Ist schon eine niedrigere Potenz von a, als die nte, etwa $a^m \equiv +1$ (mod. p) und m ein Faktor von n, also n etwa $= tm$, so ist $(a^m)^t$ oder a^{tm}, d. i. a^n ebenfalls $\equiv +1$ (mod. p), also a kubischer Rest von p.

Ist dagegen a^n nicht $\equiv +1$ (mod. p), oder ist der Exponent m der niedrigsten Potenz von a, welche $\equiv +1$ (mod. p) ist, kein Faktor von n, so ist a kein kubischer Rest von p.

Denn ist $a^n \equiv b$ (mod. p) und b von $+1$ verschieden, so müßte, wenn $a \equiv x^3$ (mod. p), also $a^n \equiv x^{3n}$ wäre, $x^{3n} \equiv b$ (mod. p) sein, was dem Fermat'schen Satze widerspräche. Ist $m < n$ und kein Faktor von n, also etwa $n = tm + u$, wo $u < m$ ist, so ist $a^n = a^{tm+u} = (a^m)^t . a^u$. Ist nun $a^m \equiv +1$ (mod. p), so ist auch $(a^m)^t \equiv +1$, mithin $a^n \equiv a^u$. Da nun a^m die niedrigste Potenz von a sein soll, welche $\equiv +1$ (mod. p), ist, so ist a^u nicht $\equiv +1$, mithin auch a^n nicht $\equiv +1$ (mod. p), also a kein kubischer Rest von p.

Beispiele: 7 ist kubischer Rest von 19, weil $7^3 \equiv +1$ (mod. 19) und 3 ein Faktor von 6 ist. Setzt man $7 \equiv x^3$, so ist $x^9 \equiv +1$, mithin auch $x^{18} \equiv +1$ (mod. 19), was dem Fermat'schen Satze entspricht. — 12 ist kubischer Rest von 19, weil $12^6 \equiv +1$ ist. Setzt man $12 \equiv x^3$, so ist $x^{18} \equiv +1$ (mod. 19).

Dagegen ist 2 kein kubischer Rest von 19, weil erst $2^{18} \equiv +1$ (mod. 19) ist. 2^6 ist $\equiv 7$ (mod. 19). Setzt man $2 \equiv x^3$, so müßte $x^{18} \equiv 7$ (mod. 19) sein, was nicht möglich ist, weil nach dem Fermat'schen Satze $x^{18} \equiv +1$ (mod. 19) ist. — Ebenso ist 4 kubischer Nichtrest von 19, weil erst $4^9 \equiv +1$ (mod. 19) ist. 4^6 ist $\equiv 11$ (mod. 19). Wäre nun $4 \equiv x^3$, so müßte $x^{18} \equiv 11$ (mod. 19) sein, während nach dem Fermat'schen Satze $x^{18} \equiv +1$ (mod. 19) ist.

23. Das Produkt aus einem kubischen Reste und einem kubischen Nichtreste einer Primzahl $p = 3n+1$ ist einem anderen kubischen Nichtreste derselben Primzahl congruent.

Ist a ein kubischer Rest von p, also $a^n \equiv +1$ (mod. p), und b ein kubischer Nichtrest von p, also b^n nicht $\equiv +1$ (mod. p), sondern etwa $b^n \equiv c$ (mod. p), so ist $a^n . b^n$ oder $(ab)^n \equiv c$ (mod. p) also nicht $\equiv +1$ (mod. p), folglich ab kein kubischer Rest von p.

24. Der Quotient eines kubischen Restes und eines kubischen Nichtrestes einer Primzahl $p = 3n+1$ ist einem anderen kubischen Nichtreste derselben Primzahl congruent.

Ist $a^n \equiv +1$ und $b^n \equiv c \pmod{p}$, so ist $a^n : b^n$ oder $(a:b)^n \equiv (+1:c) \pmod{p}$. Da nun $+1:c$ nicht $\equiv +1 \pmod{p}$ sein kann, wenn c von $+1$ verschieden ist, so kann auch $a:b$ kein kubischer Rest von p sein. — Dasselbe gilt von $b:a$. Denn $b^n : a^n$ oder $(b:a)^n$ ist $\equiv c \pmod{p}$, mithin ist $b:a$ kein kubischer Rest von p.

25. Von den drei Wurzeln einer reinen kubischen Congruenz, deren Modulus eine Primzahl $p = 3n+1$ ist, ist die eine ein kubischer Rest, die beiden andern aber kubische Nichtreste von p, wenn n nicht durch 3 theilbar ist; dagegen sind alle drei Wurzeln kubische Reste oder Nichtreste von p, wenn n durch 3 theilbar ist.

Von den drei kubischen Wurzeln der Einheit $+1$, α, β ist $+1$ immer zugleich kubischer Rest des Modulus; dagegen sind α und β, weil $\alpha^3 \equiv +1$ und $\beta^3 \equiv +1 \pmod{p}$, kubische Nichtreste von p, wenn 3 kein Faktor von n ist, da dann α^n und β^n nicht $\equiv +1$ sind; ist aber 3 ein Faktor von n, so sind auch α^n und $\beta^n \equiv +1 \pmod{p}$, also α und β ebenfalls kubische Reste von p.

Da von den drei Wurzeln γ, δ, ε der Congruenz $x^3 \equiv b \pmod{p = 3n+1}$ $\delta \equiv \gamma\alpha$ und $\varepsilon \equiv \gamma\beta$ ist, so sind, wenn n durch 3 theilbar ist, also α und β kubische Reste von p sind, entweder alle drei Wurzeln kubische Reste von p, wenn γ kubischer Rest von p ist (denn δ und ε sind dann den Produkten kubischer Reste congruent, also (nach 7) ebenfalls kubische Reste), oder alle drei Wurzeln kubische Nichtreste von p, wenn γ kubischer Nichtrest von p ist (denn δ und ε sind dann den Produkten aus einem Reste und einem Nichtreste, also (nach 23) ebenfalls Nichtresten congruent).

Ist n nicht durch 3 theilbar, also α und β Nichtreste von p, so sind δ und γ, wenn γ kubischer Rest von p ist, nach 23 kubische Nichtreste von p. Ist aber γ kubischer Nichtrest von p, so sind δ und γ den Produkten zweier Nichtreste congruent. Da γ kubischer Nichtrest von p ist, so kann γ^n nicht $\equiv +1 \pmod{p}$ sein; andrerseits ist aber γ^{3n} immer $\equiv +1 \pmod{p}$ (nach dem Fermat'schen Satze); also muß $\gamma^n \equiv \alpha$ oder $\equiv \beta \pmod{p}$ sein, denn dann ist $\gamma^{3n} \equiv +1 \pmod{p}$. Ist $\gamma^n \equiv \alpha$, so ist $\delta^n \equiv \gamma^n\alpha^n \equiv \alpha^{n+1}$ und $\varepsilon^n \equiv \gamma^n\beta^n \equiv \alpha\beta^n$; wenn aber $\gamma^n \equiv \beta$ ist, so ist $\delta \equiv \alpha^n\beta$ und $\varepsilon \equiv \beta^{n+1} \pmod{p}$.

Ist nun $n = 3m+1$, so ist im ersten Falle $\delta^n \equiv \alpha^{3m+2} \equiv (\alpha^3)^m . \alpha^2 \equiv \alpha^2 \equiv \beta \pmod{p}$ (nach 12) und $\varepsilon^n \equiv \alpha\beta^{3m+1} \equiv \alpha\beta . (\beta^3)^m \equiv \alpha\beta \equiv +1 \pmod{p}$, d. h. δ ist kubischer Nichtrest, ε dagegen kubischer Rest von p; im zweiten Falle ist $\delta^n \equiv \alpha^{3m+1} . \beta \equiv (\alpha^3)^m . \alpha\beta \equiv +1 \pmod{p}$ (nach 12)

und $\varepsilon^n \equiv \beta^{3m+2} \equiv (\beta^3)^m . \beta^2 \equiv \beta^2 \equiv \alpha \pmod{p}$,

d. h. δ ist kubischer Rest, ε dagegen kubischer Nichtrest von p.

Ist aber $n = 3m-1$, so ist im ersten Falle $\delta^n \equiv \alpha^{3m} \equiv +1 \pmod{p}$ und $\varepsilon^n \equiv \alpha\beta^{3m-1} \equiv \frac{\alpha}{\beta} . (\beta^3)^m \equiv \frac{\alpha}{\beta} \equiv \beta \pmod{p}$ (nach 14), d. h. δ ist kubischer Rest, ε kubischer Nichtrest von p; im zweiten Falle ist $\delta^n \equiv \alpha^{3m-1} . \beta \equiv (\alpha^3)^m . \frac{\beta}{\alpha} \equiv \frac{\beta}{\alpha} \equiv \alpha \pmod{p}$, und $\varepsilon^n \equiv \beta^{3m} \equiv +1 \pmod{p}$, also δ kubischer Nichtrest, ε kubischer Rest von p.

Mithin ist in allen Fällen eine Wurzel der Congruenz $x^3 \equiv b \pmod{p = 3n+1}$, wo n nicht durch 3 theilbar ist, ein kubischer Rest, die beiden andern aber kubische Nichtreste von p.

26. Das Produkt zweier kubischen Nichtreste von $p = 3n+1$ ist ebenfalls ein kubischer Nichtrest, wenn ihre nten Potenzen zugleich $\equiv \alpha$ oder $\beta \pmod{p}$ sind, dagegen ein kubischer Rest, wenn die nte Potenz des einen $\equiv \alpha$, die nte Potenz des andern $\equiv \beta$ ist.

Denn sind a und b kubische Nichtreste von p, so sind (wie oben gezeigt worden ist) ihre nten Potenzen entweder $\equiv \alpha$ oder $\equiv \beta$ (mod. p). Ist sowohl a^n, als auch $b^n \equiv \alpha$ (oder $\equiv \beta$), so ist $(ab)^n \equiv \alpha^2$ (oder $\equiv \beta^2$) $\equiv \beta$ (oder $\equiv \alpha$), also ab ein kubischer Nichtrest von p. — Ist dagegen $a^n \equiv \alpha$ und $b^n \equiv \beta$, so ist $(ab)^n \equiv \alpha\beta \equiv +1$ (mod. p), folglich ab ein kubischer Rest von p.

27 Der Quotient zweier kubischen Nichtreste von $p = 3n + 1$ ist einem kubischen Reste oder einem andern kubischen Nichtreste von p congruent, je nachdem ihre nten Potenzen zugleich $\equiv \alpha$ oder β, oder die eine $\equiv \alpha$, die andere $\equiv \beta$ ist.

Denn, wenn a^n und b^n zugleich $\equiv \alpha$ (oder $\equiv \beta$) sind, so ist sowohl $(a:b)^n$, als auch $(b:a)^n \equiv +1$ (mod. p), mithin sowohl a : b, als auch b : a einem kubischen Reste congruent. — Ist dagegen $a^n \equiv \alpha$ und $b^n \equiv \beta$, so ist $(a:b)^n \equiv (\alpha:\beta) \equiv \beta$ und $(b:a)^n \equiv (\beta:\alpha) \equiv \alpha$ (nach 14), mithin sowohl a : b, als b : a einem kubischen Nichtreste von p congruent.

28. Sämmtliche positive Zahlen $< p$ $(= 3n + 1)$ lassen sich in drei Gruppen von je n Zahlen bringen, nämlich:

1) diejenigen Zahlen, deren nte Potenzen $\equiv +1$ (mod. p) sind;
2) diejenigen Zahlen, deren nte Potenz n $\equiv \alpha$ (mod. p) sind;
3) diejenigen Zahlen, deren nte Potenzen $\equiv \beta$ (mod. p) sind.

Die erste Gruppe enthält die kubischen Reste, die beiden anderen die kubischen Nichtreste von p. Die Nichtreste einer Gruppe sollen im Folgenden gleichartige, die Nichtreste verschiedener Gruppen ungleichartige Nichtreste genannt werden.

Daß diejenigen Zahlen, deren nte Potenzen $\equiv +1$ (mod. p) sind, kubische Reste, diejenigen Zahlen, deren nte Potenzen nicht $\equiv +1$ sind, kubische Nichtreste von p sind, ist schon unter 22 nachgewiesen. Ferner ist unter 21 nachgewiesen, daß die Anzahl sämmtlicher positiven kubischen Reste von p, die kleiner als p sind, $= n$, die Anzahl sämmtlicher Nichtreste $= 2n$ ist. Endlich ist unter 25 nachgewiesen, daß die nten Potenzen der kubischen Nichtreste entweder $\equiv \alpha$, oder $\equiv \beta$ (mod. p) sind. — Daß nun auch die Anzahl der Nichtreste jeder der beiden Gruppen $= n$ ist, d. h. daß es n verschiedene Nichtreste, deren nte Potenzen $\equiv \alpha$, und n verschiedene Nichtreste, deren nte Potenzen $\equiv \beta$ sind, giebt, läßt sich folgendermaßen nachweisen.

Es giebt immer solche Zahlen $< p$, deren $(p-1)$te Potenz erst $\equiv +1$ (mod. p) ist (oder die zum Exponenten $p-1$ gehören). Solche Zahlen heißen primitive Wurzeln der Primzahl p. Denkt man sich sämmtliche Potenzen einer solchen primitiven Wurzel von der ersten bis zur $(p-1)$ten gebildet, so sind dieselben den positiven Zahlen von 1 bis $p-1$ in Bezug auf p congruent. Denn wären, wenn g eine solche primitive Wurzel von p bedeutet, irgend zwei Potenzen derselben, etwa g^k und g^m, wo k und m verschiedene ganze positive Zahlen $< p-1$ sind, derselben Zahl h congruent, so müßte auch $g^k \equiv g^m$ (mod. p) sein, also, wenn $k > m$ ist, $g^{k-m} \equiv +1$ (mod. p), was nicht möglich ist, weil $k - m < p - 1$ und erst $g^{p-1} \equiv +1$ (mod. p) ist.

Von diesen $p-1$ Potenzen der primitiven Wurzel g haben, wenn $p = 3n+1$, also $p-1 = 3n$ ist, n durch 3 theilbare Exponenten, nämlich: $g^3, g^6, g^9, \ldots, g^{3n}$; eine zweite Gruppe von Potenzen von g, deren Anzahl ebenfalls $= n$ ist, nämlich: $g^1, g^4, g^7, \ldots, g^{3n-2}$ hat Exponenten von der Form $3m+1$; die übrigen n Potenzen von g endlich, nämlich: $g^2, g^5, g^8, \ldots, g^{3n-1}$, haben Exponenten von der Form $3m-1$. — Ist nun die Zahl a einer der Potenzen der ersten Gruppe congruent, also $a \equiv g^{3m}$, so ist, weil $g^{3m} \equiv (g^m)^3$, a ein kubischer Rest von p Dies gilt natürlich von allen Zahlen, die den Potenzen der ersten Gruppe congruent sind. — Ist ferner die Zahl b einer der Potenzen der zweiten

Gruppe congruent, also $b \equiv g^{3m+1}$, so ist $b^n \equiv g^{3mn} . g^n \equiv (g^{3n})^m . g^n \equiv g^n$. Da nun erst $g^{3n} \equiv +1$ (mod. p) ist, so ist g^n, mithin auch b einer der beiden kubischen Wurzeln der Einheit α oder β congruent. — Ist endlich c einer der Potenzen der dritten Gruppe congruent, also $c \equiv g^{3m-1}$, so ist

$$c^n \equiv g^{3mn} : g^n \equiv +1 : g^n, \text{ also, wenn } g^n \equiv \alpha \text{ ist,}$$

$$c^n \equiv \frac{1}{\alpha} \equiv \beta \text{ (mod. p), und wenn } g^n \equiv \beta \text{ ist,}$$

$$c^n \equiv \frac{1}{\beta} \equiv \alpha \text{ (mod. p).}$$

Demnach sind die Zahlen, die den Potenzen der primitiven Wurzel mit Exponenten von der Form $3m+1$ congruent sind, kubische Nichtreste der einen Gruppe, und die Zahlen, die den Potenzen der primitiven Wurzel mit Exponenten von der Form $3m-1$ congruent sind, kubische Nichtreste der andern Gruppe. Da nun die Anzahl der Potenzen jeder der beiden Gruppen $= n$ ist, so ist auch die Anzahl der Nichtreste jeder Gruppe $= n$.

29. Ist eine Zahl a ($< p$) kubischer Rest oder Nichtrest einer Primzahl $p = 3n+1$, so ist auch $p - a$, d. h. die Zahl, welche a zu p ergänzt, mithin auch $-a$ kubischer Rest oder Nichtrest von p, und zwar im letztern Falle Nichtrest derselben Gruppe, zu der a gehört.

Daß $p - a$ und $-a$ ebenfalls kubische Reste von p sind, wenn a kubischer Rest von p ist, ist schon unter 4 nachgewiesen.

Ist a kubischer Nichtrest von p, so ist (nach 28) a^n entweder $\equiv \alpha$ oder $\equiv \beta$ (mod. p). Ist $a^n \equiv \alpha$, so ist $(p-a)^n \equiv (-a)^n$ (mod. p); denn alle Glieder des Polynoms, das $= (p-a)^n$ ist, sind bis auf das letzte, $(-a)^n$, durch p theilbar. Da nun n, weil p eine Primzahl, also $p-1$ oder $3n$ eine gerade Zahl ist, stets eine gerade Zahl ist, so ist $(-a)^n = a^n$; folglich ist $(p-a)^n \equiv a^n \equiv \alpha$, d. h. $p-a$ und $-a$ kubische Nichtreste derselben Gruppe, zu der a gehört. — Ist $a^n \equiv \beta$, so ist $(p-a)^n \equiv (-a)^n \equiv a^n \equiv \beta$ (mod. p); folglich $p-a$ und $-a$ ebenfalls Nichtreste derselben Gruppe, zu der a gehört.

30. Die Summe sämmtlicher positiven kubischen Reste einer Primzahl $p = 3n+1$, welche $< p$ sind, und die Summe sämmtlicher positiven kubischen Nichtreste einer Gruppe, welche $< p$ sind, ist durch p theilbar, nämlich $\equiv \left(\frac{p-1}{6}\right) . p$.

Sämmtliche positiven kubischen Reste $< p$, deren Anzahl $= n$ ist, lassen sich (nach 29) paarweise so ordnen, daß die Reste, die ein Paar bilden, einander zu p ergänzen, d. h. daß die Summe der Reste jedes Paares $= p$ ist. Die Anzahl dieser Paare ist $= \frac{n}{2}$, also die Summe sämmtlicher positiven Reste $(< p) = \frac{n}{2} . p = \left(\frac{p-1}{6}\right) . p$. — Dasselbe läßt sich auf dieselbe Weise von der Summe sämmtlicher positiven kubischen Nichtreste ($< p$) jeder Gruppe nachweisen.

Beispiel: Sämmtliche positiven kubischen Reste von 19, welche < 19 sind, sind (wie unter 21 angegeben) paarweise geordnet: 1 und 18, 7 und 12, 8 und 11; ihre Summe ist $= 3.19 = \left(\frac{19-1}{6}\right) . 19$. — Die positiven kubischen Nichtreste von 19, welche < 19 sind, sind paarweise geordnet:

1. Gruppe: 2 und 17, 3 und 16, 5 und 14 (denn $2^6 \equiv 17^6 \equiv 3^6 \equiv 16^6 \equiv 5^6 \equiv 14^6 \equiv 7$); ihre Summe $= 3.19$.
2. Gruppe: 4 und 15, 6 und 13, 9 und 10 (denn $4^6 \equiv 15^6 \equiv 6^6 \equiv 13^6 \equiv 9^6 \equiv 10^6 \equiv 11$); ihre Summe $= 3.19$.

31. Das Produkt aus einem kubischen Reste und einem kubischen Nichtreste einer Primzahl $p = 3n + 1$ ist einem gleichartigen Nichtreste congruent.

Ist r ein kubischer Rest und a ein kubischer Nichtrest von p, so ist $r^n \equiv +1$ und $a^n \equiv \alpha$ (oder β) (mod. p), mithin $(r.a)^n \equiv \alpha$ (oder β) (mod. p), also r.a ein Nichtrest derselben Gruppe, zu der a gehört.

Demnach lassen sich, wenn sämmtliche positiven kubischen Reste $< p$ und ein positiver Nichtrest $< p$ bekannt sind, die übrigen positiven Nichtreste derselben Gruppe durch Multiplikation sämmtlicher Reste mit jenem Nichtreste finden.

Beispiel: Die positiven kubischen Reste von 19 sind: 1, 7, 8, 11, 12, 18. Da sich unter diesen die Zahl 2 nicht vorfindet, so ist 2 ein Nichtrest. Dann sind die übrigen Nichtreste derselben Gruppe: $2.7 = 14$, $2.8 = 16$, $2.11 \equiv 3$, $2.12 \equiv 5$, $2.18 \equiv 17$. — Unter diesen letzteren findet sich die Zahl 4 nicht vor; daher ist 4 ein Nichtrest der anderen Gruppe. Die übrigen Nichtreste dieser Gruppe sind: $4.7 \equiv 9$, $4.8 \equiv 13$, $4.11 \equiv 6$, $4.12 \equiv 10$, $4.18 \equiv 15$.

32. Der Quotient eines kubischen Nichtrestes durch einen kubischen Rest ist einem gleichartigen Nichtreste congruent.

Denn, wenn $a^n \equiv \alpha$ (oder β) und $r^n \equiv +1$ (mod. p) ist, so ist auch $(a:r)^n \equiv \alpha$ (oder β) (mod. p).

33. Der Quotient eines kubischen Restes durch einen kubischen Nichtrest ist einem ungleichartigen Nichtreste congruent.

Denn, wenn $r^n \equiv +1$ und $a^n \equiv \alpha$ (oder β) (mod. p) ist, so ist $(r:a)^n \equiv \frac{1}{\alpha}\left(\text{oder } \frac{1}{\beta}\right) \equiv \beta$ (oder α), d. h. r:a ist einem Nichtreste congruent, der nicht zu derselben Gruppe gehört, zu welcher a gehört.

34. Das Product zweier gleichartigen Nichtreste ist einem ungleichartigen Nichtreste congruent.

Sind a und b gleichartige Nichtreste, also a^n und $b^n \equiv \alpha$ (oder β), so ist $(ab)^n \equiv \alpha^2$ (oder β^2) $\equiv \beta$ (oder α); d. h. ab ist a und b nicht gleichartig.

Mithin ist auch das Quadrat eines Nichtrestes einem ungleichartigen Nichtreste congruent, und die Quadratwurzel aus einem Nichtreste ein ungleichartiger Nichtrest.

35. Das Produkt zweier ungleichartigen Nichtreste ist einem Reste congruent.

Sind a und b ungleichartige Nichtreste, d. h. $a^n \equiv \alpha$ und $b^n \equiv \beta$, so ist $(ab)^n \equiv \alpha\beta \equiv +1$, mithin ab einem Reste congruent.

36. Der Quotient zweier gleichartigen Nichtreste ist einem Reste congruent.

Ist $a^n \equiv \alpha$ (oder β) und $b^n \equiv \alpha$ (oder β), so ist sowohl $(a:b)^n$, als auch $(b:a)^n \equiv +1$.

37. Der Quotient zweier ungleichartigen Nichtreste ist einem Nichtreste congruent, der dem Divisor gleichartig ist.

Ist $a^n \equiv \alpha$ und $b^n \equiv \beta$, so ist $(a:b)^n \equiv \alpha:\beta \equiv \beta$ und $(b:a)^n \equiv \beta:\alpha \equiv \alpha$.

38. Die Summe der Quadrate sowohl aller positiven Reste einer Primzahl $p = 3n + 1$, als auch aller positiven Nichtreste einer Gruppe, welche $< p$ sind, ist durch p ohne Rest theilbar, außer, wenn $p = 7$ ist.

Die kubischen Reste sind (nach 28) denjenigen Potenzen einer primitiven Wurzel g von p, deren Exponenten durch 3 theilbar sind, congruent. Mithin ist die Summe der Quadrate aller kubischen Reste $< p$

$$\equiv g^6 + g^{12} + g^{18} + \ldots + g^{6n} \equiv \frac{g^6(g^{6n} - 1)}{g^6 - 1} \text{ (mod. p).}$$

Da nun $g^{6n} \equiv +1$ ist, weil $g^{3n} \equiv +1$ ist, so ist $g^{6n} - 1$ durch p theilbar, mithin, da

$\frac{g^6(g^{6n}-1)}{g^6-1}$ immer eine ganze Zahl, und g^6-1 durch p nicht theilbar ist (außer, wenn $p=7$ ist), ist $\frac{g^6(g^{6n-1})}{g^6-1}$ durch p theilbar.

Die Summe der Quadrate aller kubischen Nichtreste $<p$ der einen Gruppe ist $\equiv g^2+g^8+g^{14}+\ldots+g^{6n-4} \equiv \frac{g^2(g^{6n}-1)}{g^6-1}$ (mod. p), mithin, aus den vorher angegebenen Gründen, durch p theilbar (außer, wenn $p=7$ ist).

Die Summe der Quadrate aller kubischen Nichtreste $<p$ der andern Gruppe ist $\equiv g^4+g^{10}+g^{16}+\ldots+g^{6n-2} \equiv \frac{g^4(g^{6n}-1)}{g^6-1}$ (mod. p), mithin durch p theilbar (außer, wenn $p=7$ ist).

Ist $p=7$, so ist die Summe der Quadrate der Reste $(<7) \equiv 2$, die der Nichtreste der einen Gruppe $\equiv 1$ und die der Nichtreste der andern Gruppe $\equiv 4$ (mod. 7).

Denn, da $7=2\,.\,3+1$ ist, so ist die Summe der Quadrate der Reste $\equiv \frac{g^6(g^{12}-1)}{g^6-1} \equiv g^6(g^6+1)$, die Summe der Quadrate der Nichtreste der einen Gruppe $\equiv g^2(g^6+1)$ und die Summe der Quadrate der Nichtreste der andern Gruppe $\equiv g^4(g^6+1)$. Da nun $g^6 \equiv +1$ (mod. 7) ist, so ist g^2 der einen, g^4 der andern kubischen Wurzel der Einheit in Bezug auf 7 congruent. Diese sind 2 und 4. — Die kubischen Reste von 7 sind: 1 und 6, und die Summe ihrer Quadrate ist $\equiv 2$ (mod. 7). Die Nichtreste der einen Gruppe sind: 2 und 5, und die Summe ihrer Quadrate ist $\equiv 4.2 \equiv 1$ (mod. 7). Die Nichtreste der andern Gruppe sind: 3 und 4, und die Summe ihrer Quadrate ist $\equiv 4$ (mod. 7).

39. Die Summe der Produkte sowohl je zweier kubischen Reste einer Primzahl $p \equiv 3n+1$, als auch je zweier Nichtreste einer Gruppe, welche $<p$ sind, ist durch p ohne Rest theilbar, außer, wenn $p=7$ ist.

Nach 30 ist die Summe sämmtlicher positiven Reste $<p$ durch p theilbar, mithin auch das Quadrat dieser Summe. Da dieses nun gleich der Summe der Quadrate der Reste und der doppelten Produkte je zweier von ihnen, und (nach 38) die Summe der Quadrate sämmtlicher Reste durch p theilbar ist (außer wenn $p=7$ ist), so muß auch die Summe der doppelten Produkte je zweier Reste, mithin auch die Summe der Produkte je zweier Reste durch p theilbar sein. — Ebenso wird bewiesen, daß die Summe der Produkte je zweier Nichtreste einer Gruppe durch p (außer, wenn $p=7$ ist) theilbar ist.

Ist $p=7$, so sind nur zwei positive Reste <7 und zwei Paar positive Nichtreste <7 vorhanden. Dieser Fall findet deshalb im Folgenden seine Erledigung.

40. Das Produkt sämmtlicher (positiven) kubischen Reste einer Primzahl $p=3n+1$, welche $<p$ sind, ist $\equiv -1$ (mod. p), das sämmtlicher Nichtreste $(<p) \equiv +1$ (mod. p).

Das Produkt sämmtlicher Reste $<p$ ist (nach 28) $\equiv g^3 \,.\, g^6 \,.\, g^9 \ldots . g^{3n} \equiv g^{3+6+9+\ldots+3n} \equiv g^{3(1+2+3+\ldots+n)} \equiv g^{\frac{3n}{2}\cdot(n+1)} \equiv \left(g^{\frac{3n}{2}}\right)^{n+1}$. Da nun erst $g^{3n} \equiv +1$ (mod. p) ist, so muß $g^{\frac{3n}{2}} \equiv -1$ (mod. p) sein, mithin, da $n+1$ ungerade ist, auch $\left(g^{\frac{3n}{2}}\right)^{n+1} \equiv -1$ (mod. p).

Das Produkt sämmtlicher Nichtreste $<p$ ist (nach 28) $\equiv (g^1 \,.\, g^4 \,.\, g^7 \ldots . g^{3n-2}) \,.\, (g^2 \,.\, g^5 \,.\, g^8 \ldots . g^{3n-1}) \equiv g^{(1+4+7+\ldots+3n-2)+(2+5+8+\ldots+3n-1)} \equiv g^{\frac{n(3n-1)}{2}+\frac{n(3n+1)}{2}} \equiv (g^{3n})^n \equiv +1$ (mod. p).

Das Produkt sämmtlicher Nichtreste der einen Gruppe ist $\equiv g^{\frac{n(3n-1)}{2}}$, oder, da $\frac{n(3n-1)}{2} = n + \frac{3n(n-1)}{2}$ ist, $\equiv g^n \cdot g^{\frac{3n(n-1)}{2}}$, mithin, da $g^{\frac{3n(n-1)}{2}}$ ebenso, wie $g^{\frac{3n(n+1)}{2}} \equiv -1 \pmod{p}$ ist, (weil auch $n-1$ eine ungerade Zahl ist) $\equiv -g^n$, also, da $g^n \equiv \alpha$ oder β ist, $\equiv -\alpha$ oder $-\beta$.

Das Produkt sämmtlicher Nichtreste der anderen Gruppe ist $\equiv g^{\frac{n(3n+1)}{2}}$, oder, da $\frac{n(3n+1)}{2} = 2n + \frac{3n(n-1)}{2}$ ist, $\equiv g^{2n} \cdot g^{\frac{3n(n-1)}{2}} \equiv -g^{2n} \equiv -\alpha^2$ oder $-\beta^3 \equiv -\beta$ oder $-\alpha$.

Hieraus ergiebt sich auch, daß sowohl das Produkt sämmtlicher kubischen Reste $< p$, als auch das Produkt sämmtlicher kubischen Nichtreste $< p$ stets einem kubischen Reste congruent ist. Dagegen ist das Produkt sämmtlicher Nichtreste einer Gruppe nur dann einem kubischen Reste congruent, wenn n durch 3 theilbar ist, weil dann α und β, mithin auch $-\alpha$ und $-\beta$ (nach 25) kubische Reste von p sind.

Ist aber n nicht durch 3 theilbar, so sind α und β, mithin auch $-\alpha$ und $-\beta$ (nach 25) kubische Nichtreste von p, und zwar (nach 35) ungleichartige, weil ihr Produkt $\equiv +1 \pmod{p}$, d. h. einem kubischen Reste congruent ist.

In diesem Falle ist daher das Produkt sämmtlicher Nichtreste einer Gruppe einem ungleichartigen Nichtreste congruent.

41. Die Aufgabe, sämmtliche positiven kubischen Reste und Nichtreste einer Primzahl $p = 3n+1$, welche kleiner als p sind, zu finden, läßt sich mit Hülfe der meisten der bisher gefundenen Sätze leicht lösen.

Zunächst sind immer einige kubische Reste von vornherein bekannt, nämlich die ersten natürlichen Kubikzahlen: 8, 27, 64, 125 u. s. w., oder die Zahlen, die diesen in Bezug auf den Modulus p congruent sind, ferner die Zahlen, die diese zu p ergänzen, und, wenn n durch 3 theilbar ist, die kubischen Wurzeln der Einheit und deren Ergänzungen zu p. Die andern Reste ergeben sich aus diesen durch Multiplikation, Potenzirung und Division. Die Nichtreste erhält man durch Multiplikation sämmtlicher Reste mit einer Zahl $< p$, die nicht unter den Resten vorkommt, und mit dem Quadrate derselben oder der Zahl $< p$, die demselben in Bezug auf p congruent ist. Ist n nicht durch 3 theilbar, so sind die beiden kubischen Wurzeln der Einheit α und β die ersten ungleichartigen Nichtreste.

Beispiele: Ist $p = 31$, so sind die kubischen Wurzeln der Einheit: 1, 5 u. 25. Von diesen sind, weil $n = 10$, also nicht durch 3 theilbar ist, 5 und 25 ungleichartige Nichtreste. — Die zehn kubischen Reste sind: 1 und 30, 8 und 23, 27 und 4, 2 und 29, 16 und 15. Die zehn kubischen Nichtreste der einen Gruppe erhält man durch Multiplikation der zehn Reste mit 5; sie sind: 5 und 26, 9 und 22, 11 und 20, 10 und 21, 18 und 13. Die zehn kubischen Nichtreste der andern Gruppe erhält man durch Multiplikation der zehn Reste mit 25 oder 6 (oder durch Multiplikation der Nichtreste der ersten Gruppe mit 5); sie sind: 25 und 6, 14 und 17, 24 und 7, 19 und 12, 28 und 3.

Ist $p = 37$, so sind die kubischen Wurzeln der Einheit: 1, 10, 26 und die Zahlen, welche dieselben zu 37 ergänzen: 36, 27, 11, zugleich kubische Reste von 37, weil $n = 12$ durch 3 theilbar ist. Die übrigen sechs Reste findet man durch Multiplikation der bereits bekannten mit 6 (denn da $36 = 6^2$ ein kubischer Rest von 37 ist, so ist es auch 6); sie sind: 6, 23, 8 und 31, 14, 29. — Da sich unter diesen zwölf Resten die Zahl 2 nicht vorfindet, so ist 2 ein Nichtrest von 37; die Nichtreste der einen Gruppe sind daher: 2, 20, 15, 35, 17, 22, 12, 9, 16, 25, 28, 21. — Die Nichtreste der zweiten Gruppe erhält man,

wenn man die Reste mit 4 oder die Nichtreste der ersten Gruppe mit 2 multiplicirt; dann erhält man: 4, 3, 30, 33, 34, 7, 24, 18, 32, 13, 19, 5.

42. Eine der drei Wurzeln der Congruenz $x^3 \equiv a \pmod{p = 3n+1}$, wo n nicht durch 3 und a nicht durch p theilbar ist, ist $\equiv a^t$ oder $\equiv b^t$, wo b durch die Congruenz $ab \equiv +1 \pmod{p}$ bestimmt ist, je nachdem $n = 3t-1$ oder $= 3t+1$ ist.

Die Congruenz $x^3 \equiv a \pmod{p = 3n+1}$ ist nur dann lösbar, wenn a ein kubischer Rest von p, also $a^n \equiv +1 \pmod{p}$ ist (nach 22). Ist dies der Fall und $n = 3t-1$, so ist a^{3t-1} oder $a^{3t} : a \equiv +1$, mithin $a^{3t} \equiv a$, also a^{3t} oder $(a^t)^3 \equiv x^3 \pmod{p}$. Dieser Congruenz genügt offenbar $x \equiv a^t \pmod{p}$.

Ist $n = 3t+1$, so ist a^{3t+1} oder $a^{3t} . a \equiv +1 \pmod{p}$. Ist nun $ab \equiv +1$, also auch $a^{3t} . b^{3t} \equiv +1 \pmod{p}$, so ist $a^{3t} . a$ oder $a^{3t} . x^3 \equiv a^{3t} . b^{3t}$, mithin $x^3 \equiv b^{3t}$. Dieser Congruenz genügt offenbar $x \equiv b^t \pmod{p}$.

Ist schon $a^m \equiv +1 \pmod{p}$, wo m ein Faktor von n ist (nach 22), so ist, je nachdem $m = 3t-1$ oder $= 3t+1$ ist, ebenfalls $x \equiv a^t$ oder $\equiv b^t \pmod{p}$.

Die beiden andern Wurzeln der Congruenz $x^3 \equiv a \pmod{p}$ sind (nach 10) $\equiv a^t . \alpha$ und $a^t . \beta$ in dem einen Falle, im andern Falle $\equiv b^t . \alpha$ und $b^t . \beta \pmod{p}$.

Beispiele: 2 ist ein kubischer Rest von 43, weil $2^{14} \equiv +1 \pmod{43}$ ist. Da nun $14 = 3.5-1$ ist, so ist $x \equiv 2^5 \equiv 32$.

Die beiden andern Wurzeln sind, da $\alpha = 6$ und $\beta = 36$ ist, $\equiv 6 . 32$ und $\equiv 36 . 22$, oder $\equiv 20$ und $\equiv 34$.

(32^3 ist $= 32768 = 762 . 43 + 2$, also $32^3 \equiv 2 \pmod{43}$;
20^3 ist $= 8000 = 186 . 43 + 2$, also $20^3 \equiv 2 \pmod{43}$;
34^3 ist $= 39304 = 914 . 43 + 2$, also $34^3 \equiv 2 \pmod{43}$). —

4 ist ein kubischer Rest von 43, weil $4^7 \equiv +1 \pmod{43}$ ist. Da nun $7 = 3.2+1$ und $4 . 11 \equiv +1 \pmod{43}$ ist, so ist $x \equiv 11^2 \equiv 35$. Die beiden andern Wurzeln sind $\equiv 6 . 35$ und $\equiv 36 . 35$, oder $\equiv 38$ und $\equiv 13$. — (35^3 ist $= 42875 = 997 . 43 + 4$; $38^3 = 54872 = 1276 . 43 + 4$; $13^3 = 2197 = 51 . 43 + 4$).

43. Wenn der Modulus p einer kubischen Congruenz $x^3 \equiv a \pmod{p}$ von der Form $3n+1$ und n durch 3 oder durch eine Potenz von 3 theilbar ist, so läßt sich p, da n immer eine gerade Zahl ist, unter der Form $2k . 3^m + 1$, wo k nicht durch 3 theilbar ist, darstellen. Dann ist $n = 2k . 3^{m-1}$; also ist, da a ein kubischer Rest von p ist, $a^{2k . 3^{m-1}} \equiv +1 \pmod{p}$. Dies ist der Fall, wenn $a^{2k . 3^{m-2}}$ entweder $\equiv 1$ oder $\equiv \alpha$ oder $\equiv \beta$ ist. Der erste dieser 3 Fälle tritt ein, wenn $a^{2k . 3^{m-3}}$ entweder $\equiv 1$ oder $\equiv \alpha$ oder $\equiv \beta$ ist. Setzt man diese Betrachtung fort, so gelangt man dahin, daß

entweder $a^{2k} \equiv 1$ oder $\equiv \alpha$ oder $\equiv \beta$,

oder $a^{2k . 3^r} \equiv \alpha$ oder $\equiv \beta \pmod{p}$,

wo r eine positive ganze Zahl $< m-1$, ist.

I. Ist $a^{2k} \equiv 1 \pmod{p}$, so ist (wie in 42) $x \equiv a^t$ oder $\equiv b^t$, wo b durch die Congruenz $ab \equiv +1 \pmod{p}$ bestimmt ist, je nachdem 2k (oder, wenn schon $a^s \equiv +1 \pmod{p}$ ist, s) $= 3t-1$ oder $= 3t+1$ ist.

Beispiel: Es ist $33^4 \equiv +1 \pmod{109}$, also, da $4 = 3 . 1 + 1$ und $33 . 76 \equiv +1 \pmod{109}$ ist, $33 \equiv 76^3 \pmod{109}$. ($76^3$ ist $= 438976 = 4027 . 109 + 33$). Die andern Wurzeln sind, da $\alpha = 45$, $\beta = 63$ ist: 41 und 101.

II. Ist $a^{2k} \equiv \alpha$ oder $\beta \pmod{p}$, so sei b ein Nichtrest, also (nach 28) b^n, d. i. $b^{2k \cdot 3^{m-1}} \equiv \alpha$ oder $\beta \pmod{p}$.

In dem Falle, daß a^{2k} und b^n zugleich $\equiv \alpha$ (oder β) sind, ist also $a^{2k} \equiv b^{2k \cdot 3^{m-1}}$ oder $\equiv \left(b^{2k \cdot 3^{m-2}}\right)^3$. Ist nun 2k (oder, wenn schon $a^s \equiv \alpha$ ist, s) $= 3t+1$, so ist a^{3t+1} oder $a^{3t} \cdot a \equiv \left(b^{2k \cdot 3^{m-2}}\right)^3$, also $a \equiv \left(b^{2k \cdot 3^{m-2}} : a^t\right)^3$; mithin $x \equiv \left(b^{2k \cdot 3^{m-2}} : a^t\right) \pmod{p}$. — Ist aber 2k (oder s) $= 3t-1$, so ist $a^{3t-1} \equiv \left(b^{2k \cdot 3^{m-2}}\right)^3$, also $a^{3t} \equiv a \cdot \left(b^{2k \cdot 3^{m-2}}\right)^3$; mithin $x \equiv \left(a^t : b^{2k \cdot 3^{m-2}}\right) \pmod{p}$.

In dem Falle, daß a^{2k} (oder a^s) $\equiv \alpha$ (oder β), dagegen $b^n \equiv \beta$ (oder α) ist, ist $a^{2k} \equiv \beta^2$ (oder α^2), d. h. $a^{2k} \equiv b^{2n} \equiv \left(b^{4k \cdot 3^{m-2}}\right)^3$.

Dann ist, wenn 2k (oder s) $= 3t+1$ ist, $x \equiv \left(b^{4k \cdot 3^{m-2}} : a^t\right)$,

und, wenn 2k (oder s) $= 3t-1$ ist, $x \equiv \left(a^t : b^{4k \cdot 3^{m-2}}\right) \pmod{p}$.

Ist schon eine niedrigere Potenz, als die nte, von b, etwa $b^{3q} \equiv \alpha$ oder β, so ist x

im ersten Falle entweder $\equiv (b^q : a^t)$ oder $\equiv (a^t : b^q)$,

im zweiten Falle entweder $\equiv (b^{2q} : a^t)$ oder $\equiv (a^t : b^{2q})$.

Beispiele: Die kubischen Wurzeln der Einheit in Bezug auf 109 sind: 1, 45, 63; also 46 ein kubischer Rest von 109, da $46 = 109 - 63$ ist — Ferner ist $3^9 \equiv 63$, und $3^{18} \equiv 45$, mithin $3^{27} \equiv +1 \pmod{109}$, also, da 27 kein Faktor von $\frac{109-1}{3} = 36$ ist, 3 ein Nichtrest von 109. — Nun ist $46^4 \equiv 63$, also $46^4 \equiv 3^9 \equiv (3^3)^3$. Da nun $4 = 3 \cdot 1 + 1$ ist, so ist $x \equiv (3^3 : 46) \equiv 93$. — $(93^3 = 804357 = 7379 \cdot 109 + 46$; mithin $93^3 \equiv 46 \pmod{109}$. Die andern Wurzeln sind 43 $(\equiv 93 \cdot 45)$ und 82 $(\equiv 93 \cdot 63)$. — Ferner ist $64^4 \equiv 45$, also $64^4 \equiv 3^{18} \equiv (3^6)^3$; mithin ist $x \equiv (3^6 : 64) \equiv 71$. $(71^3 = 357911 = 3283 \cdot 109 + 64$; mithin ist $71^3 \equiv 64 \pmod{109}$. Die andern Wurzeln sind 34 $(\equiv 71 \cdot 45)$ und 4 $(\equiv 71 \cdot 63)$.

III. Ist $a^{2k \cdot 3^r} \equiv \alpha$ und $\alpha \equiv b^{2k \cdot 3^{m-1}}$, wo b ein Nichtrest ist, so ist $a^{2k \cdot 3^r} \equiv b^{2k \cdot 3^{m-1}}$. Setzt man nun $a^{2k} \equiv b^{3y} \pmod{p}$, so ist $b^{3^{r+1} \cdot y} \equiv b^{2k \cdot 3^{m-1}}$, also $b^{3^{r+1} \cdot y - 2k \cdot 3^{m-1}}$, d. i. $b^{3^{r+1} \cdot (y - 2k \cdot 3^{m-r-2})} \equiv +1$, also, da $b^{2k \cdot 3^m} \equiv +1 \pmod{p}$ ist, $3^{r+1} \cdot (y - 2k \cdot 3^{m-r-2}) = 2k \cdot 3^m$ oder einem Vielfachen davon. Es sei daher $3^{r+1} \cdot (y - 2k \cdot 3^{m-r-2}) = 2k \cdot 3^m \cdot z$. Dann ist, weil $r < m-1$, also $r+1 < m$ ist, $y - 2k \cdot 3^{m-r-2} = 2k \cdot 3^{m-r-1} \cdot z$, also $y = 2k \cdot 3^{m-r-1} \cdot z + 2k \cdot 3^{m-r-2} = 2k \cdot 3^{m-r-2} \cdot (3z+1)$. Der Werth von z ist durch die Congruenz $a^{2k} \equiv b^{3y} \equiv b^{2k \cdot 3^{m-r-1}(3z+1)} \pmod{p}$ bestimmt.

Somit ist der Fall, daß $a^{2k \cdot 3^r} \equiv \alpha$ ist, zurückgeführt auf den unter II. angegebenen Fall, und diesem analog weiter zu behandeln.

Ist $a^{2k \cdot 3^r} \equiv \beta$ und $\alpha \equiv b^{2k \cdot 3^{m-1}}$, wo b ein Nichtrest ist, so ist, weil $\beta \equiv \alpha^2$, $a^{2k \cdot 3^r} \equiv b^{4k \cdot 3^{m-1}}$, und man gelangt durch die eben angestellte Betrachtung zu der Congruenz $a^{2k} \equiv b^{4k \cdot 3^{m-r-1}(3z+1)} \pmod{p}$, die dann, wie unter II. angegeben, weiter zu behandeln ist.

Beispiel: Es ist $2^{12} \equiv 63 \pmod{109}$, also, da $63 \equiv 3^9 \pmod{109}$ ist, $2^{12} \equiv 3^9 \pmod{109}$. Setzt man nun $2^4 \equiv 3^{3y}$, so ist $2^{12} \equiv 3^{9y}$, also $3^{9y} \equiv 3^9$ oder $3^{9(y-1)} \equiv +1 \pmod{109}$. Da nun

$3^{27} \equiv +1$ (mod. 109) ist, so ist $9(y-1) = 27z$ oder $y-1 = 3z$, also $y = 3z+1$. Mithin ist $2^4 \equiv 3^{3(3z+1)}$ oder $(3^9)^z . 3^3$, also, weil $3^9 \equiv 63 \equiv 2^{12}$ ist, $2^4 \equiv 2^{12z} . 3^3$. Nun ist 2^4 oder $16 \equiv 3^3 . 45$, also, da $45 \equiv 63^2 \equiv 2^{24}$ ist, $2^4 \equiv 2^{24} . 3^3$, und deshalb $2^{12z} . 3^3 \equiv 2^{24} . 3^3$, woraus sich für z der Werth 2 ergiebt. Demnach ist $2^4 \equiv 3^{3.7} \equiv (3^7)^3$ oder $2^3 . 2 \equiv (3^7)^3$, woraus $2 \equiv (3^7:2)^3$ folgt. Nun ist $3^7 \equiv 7$, also $3^7:2 \equiv 7:2$ d. i. $\equiv 58$. Mithin ist $2 \equiv 58^3$ (mod. 109). ($58^3 = 195112 = 179.109+2$). Die beiden andern Wurzeln der Congruenz $x^3 \equiv 2$ (mod. 109) sind: 103 ($\equiv 58.45$) und 57 ($\equiv 58.63$).

II. Der Modulus sei eine zusammengesetzte Zahl.

44. Die Congruenz $x^3 \equiv a$ (mod. p^n), wo p eine Primzahl ist, läßt sich nur auflösen, wenn $x^3 \equiv a$ (mod. p) lösbar ist.

Denn die Congruenz $x^3 \equiv a$ (mod. p^n) ist gleichbedeutend mit der Gleichung $x^3 - a = m . p^n$. Diese Gleichung läßt sich aber auch schreiben: $x^3 - a = (m . p^{n-1}) . p$, und diese ist gleichbedeutend mit $x^3 \equiv a$ (mod. p). Ist $x^3 - a$ nicht durch p theilbar, d. h. x^3 nicht $\equiv a$ (mod. p), so kann natürlich $x^3 - a$ auch nicht durch p^n theilbar, d. h. x^3 nicht $\equiv a$ (mod. p^n) sein.

Eine Zahl kann demnach nur dann kubischer Rest einer Potenz einer Primzahl sein, wenn sie kubischer Rest der Primzahl selbst ist.

45. Die Wurzel der Congruenz $x^3 \equiv a$ (mod. p^n) ist eine durch p theilbare Zahl, wenn a ebenfalls durch p oder eine Potenz von p theilbar ist; ist dagegen a nicht durch p theilbar, so ist es auch x nicht.

Ist $a = b . p^m$, wo b eine ganze, von o verschiedene und nicht durch p theilbare Zahl bedeutet, so ist die Congruenz $x^3 \equiv b . p^m$ (mod. p^n) nur lösbar, wenn x auch durch p theilbar ist. Denn da diese Congruenz gleichbedeutend mit der Gleichung $x^3 = b . p^m + f . p^n$ ist, so leuchtet sofort ein, daß x durch p theilbar sein muß.

Es sei nun zunächst $m < n$, also $x^3 = p^m . (b + f . p^{n-m})$. Dann muß offenbar m durch 3 theilbar sein. Ist daher $m = 3k$, so ist $x^3 = p^{3k} . (b + f . p^{n-3k})$. Setzt man nun $x = p^k . z$, wo z nicht durch p theilbar sein soll, so ist $p^{3k} . z^3 = p^{3k} . (b + f . p^{n-3k})$ oder $z^3 = b + f . p^{n-3k}$, d. h. $z^3 \equiv b$ (mod. p^{n-3k}). Ist diese Congruenz lösbar, so ist es auch die gegebene.

Ist ferner $m = n$, so ist $x^3 = p^n . (b + f)$. Dies ist möglich, wenn $x = p^t$ ist, wo t so beschaffen ist, daß $3t =$ oder $> n$ ist. Denn die Gleichung $p^{3t} = p^n . (b + f)$ oder $p^{3t-n} = b + f$ ist unter der angegebenen Bedingung immer lösbar, da f eine beliebige ganze Zahl ist.

Ist endlich $m > n$, also $x^3 = p^n . (b . p^{m-n} + f)$, so ist dies ebenfalls möglich, wenn $x = p^t$ und $3t =$ oder $> n$ ist. Denn dann ist $p^{3t} = p^n . (b . p^{m-n} + f)$ oder $p^{3t-n} = b . p^{m-n} + f$, was aus dem vorher angegebenen Grunde immer möglich ist.

46. Die Wurzel der Congruenz $x^3 \equiv a$ (mod. p^2) (wo a eine ganze, von o verschiedene, nicht durch p theilbare Zahl, und p nicht $= 3$ sein soll) ist $= y + zp$, wo y Wurzel der Congruenz $y^3 \equiv a$ (mod. p), und z durch die Congruenz $3zy^2 + f \equiv o$ (mod. p), in welcher $f = \frac{y^3 - a}{p}$ ist, bestimmt ist.

Die Congruenz $x^3 \equiv a \pmod{p^2}$ ist (nach 44) nur lösbar, wenn a kubischer Rest von p, also $a \equiv y^3 \pmod{p}$, oder $y^3 = a + fp$ ist. Setzt man nun $x^3 = a + vp^2$, so ist $x^3 - y^3$ oder $(x-y)(x^2 + xy + y^2) = p(vp - f)$.

Dieser Gleichung wird genügt, wenn $x - y = zp$ oder $x = y + zp$ ist. Durch Substitution dieses Werthes für x geht sie über in $z(3y^2 + 3zyp + z^2p^2) = vp - f$ oder $3zy^2 + f = p(v - 3z^2y + z^3p)$. Diese Gleichung ist gleichbedeutend mit der Congruenz $3zy^2 + f \equiv o \pmod{p}$. Aus dieser läßt sich, da y und f durch $y^3 = a + fp$ bestimmt sind, z, und dann auch x bestimmen.

Substituirt man in der gegebenen Congruenz $x^3 \equiv a \pmod{p^2}$ den Werth $y + zp$ für x, so geht sie über in: $y^3 + 3y^2zp + 3yz^2p^2 + z^3p^3 \equiv a \pmod{p^2}$, d. h. da die beiden letzten Glieder auf der linken Seite durch p^2 theilbar sind, $y^3 + 3y^2zp$ oder $y^2(y + 3zp) \equiv a \pmod{p^2}$. Auch aus dieser Congruenz läßt sich z bestimmen.

Setzt man in dieser letzten Congruenz $x - y$ für zp, so erhält man: $y^2(3x - 2y) \equiv a \pmod{p^2}$, woraus sich x unmittelbar bestimmen läßt.

Beispiele: Um die Congruenz $x^3 \equiv 12 \pmod{5^2}$ aufzulösen, muß man zuerst die Congruenz $y^3 \equiv 12 \pmod{5}$ auflösen. Da $12 \equiv 2 \pmod{5}$ ist, so ist auch $y^3 \equiv 2 \pmod{5}$. Da der Modulus 5 eine Primzahl von der Form $3n - 1$ ist, so ist (nach 20), da $2 \cdot 3 \equiv +1 \pmod{5}$ ist, $y \equiv 3$ (da $5 = 3 \cdot 2 - 1$, also $n = 2$ und $n - 1 = 1$ ist). Nun ist $3^3 = 12 + 3 \cdot 5$, also $f = 3$. Jetzt ist noch die Congruenz $3 \cdot 3^2z + 3 \equiv o \pmod{5}$ zu lösen. Diese geht durch Division mit 3 über in $9z + 1 \equiv o \pmod{5}$, woraus sich $z = 1$ ergiebt. Mithin ist $x = 3 + 5 = 8$. ($8^3 = 512 = 20 \cdot 25 + 12$, also $8^3 \equiv 12 \pmod{5^2}$).

Um z aus der Congruenz $3^2(3 + 15z) \equiv 12 \pmod{5^2}$ zu bestimmen, dividire man dieselbe erst wieder durch 3. Dadurch erhält man $3(3 + 15z) \equiv 4$ oder $9 + 45z \equiv 4$ oder $5 + 45z \equiv o \pmod{5^2}$, woraus sich ebenfalls $z = 1$ ergiebt.

Unmittelbar läßt sich x bestimmen aus der Congruenz: $3^2(3x - 2 \cdot 3) \equiv 12 \pmod{5^2}$. Durch Division mit 3 erhält man $9x - 18 \equiv 4$ oder $9x \equiv 22 \pmod{5^2}$, woraus sich $x = 8$ ergiebt.

Um die Congruenz $x^3 \equiv 15 \pmod{7^2}$ aufzulösen, muß man erst die Congruenz $y^3 \equiv 15$ oder $y^3 \equiv 1 \pmod{7}$ auflösen. Nach 8 und 9 hat diese Congruenz, da ihr Modulus eine Primzahl von der Form $3n + 1$ ist, drei Wurzeln. Diese sind 1, 2, 4. Dann ist zunächst, wenn $y = 1$ gesetzt wird, $3x - 2 \equiv 15$ oder $3x \equiv 17 \pmod{7^2}$, woraus sich $x = 22$ ergiebt. — Setzt man ferner $y = 2$, so ist $4(3x - 4) \equiv 15$ oder $12x - 16 \equiv 15$ oder $12x \equiv 31 \pmod{7^2}$, woraus sich $x = 23$ ergiebt. — Setzt man endlich $y = 4$, so ist $16(3x - 8) \equiv 15$ oder $48x - 128 \equiv 15$ oder $48x \equiv 143 \pmod{7^2}$, woraus sich $x = 4$ ergiebt. — Es ist also $22^3 \equiv 15 \pmod{7^2}$ ($22^3 = 10648 = 217 \cdot 7^2 + 15$), ferner $23^3 \equiv 15 \pmod{7^2}$ ($23^3 = 12167 = 248 \cdot 7^2 + 15$) und $4^3 \equiv 15 \pmod{7^2}$ ($4^3 = 64 = 7^2 + 15$).

47. Eine besondere Betrachtung erfordert die Auflösung der Congruenz $x^3 \equiv a \pmod{3^2}$. Diese setzt zunächst wieder die Auflösung der Congruenzen $y^3 \equiv a \pmod{3}$ und $3z \cdot y^2 + f \equiv o \pmod{3}$ voraus. Die letztere aber ist, weil das erste Glied durch 3 theilbar ist, nur dann lösbar, wenn auch f durch 3 theilbar ist. Da nun $f = \frac{y^3 - a}{3}$ ist, so muß $y^3 - a$ nicht blos durch 3, sondern auch durch 9 oder 3^2 theilbar sein. Wenn a, wie dies nothwendig ist, kubischer Rest von 3 und nicht durch 3 theilbar sein soll, so muß a entweder die Form $3n + 1$ oder $3n - 1$ haben. Ist $a = 3n + 1$, so ist $f = \frac{y^3 - 1 - 3n}{3}$.

Dieser Gleichung wird genügt durch $y = 1$; denn dann ist $f = \frac{1-1-3n}{3} = -n$. Da nun f durch 3 theilbar sein muß, so muß es auch n sein; d. h. a ist in diesem Falle von der Form $9n+1$. — Ist $a = 3n-1$, so ist $f = \frac{y^3+1-3n}{3}$, und wenn man $y = -1$ setzt, $f = -n$. Da nun f, also auch n durch 3 theilbar sein muß, so ist in diesem Falle a von der Form $9n-1$. — Die Congruenz $x^3 \equiv a \pmod{3^2}$ ist demnach nur lösbar, wenn a von der Form $9n+1$ oder $9n-1$ ist.

Da nun f in diesen Fällen durch 3 theilbar ist, so ergiebt sich aus der Congruenz $3z.y^2+f \equiv o \pmod 3$ kein bestimmter Werth für z; denn derselben wird durch jeden ganzzahligen (positiven oder negativen) Werth für z genügt. Mithin ist jede Wurzel der Congruenz $x^3 \equiv a \pmod{3^2}$, wo a den oben angegebenen Bedingungen genügt, in $y+3z$ enthalten, also, da y in dem einen Falle $= +1$, in dem andern $= -1$ ist, in $\pm 1 + 3z$. Hieraus ergiebt sich nun, daß die Congruenz $x^3 \equiv a \pmod{3^2}$ drei verschiedene positive Wurzeln $< 3^2$ hat, nämlich: ± 1, $\pm 1+3$, $\pm 1+6$, oder in dem einen Falle, wenn $a = 9n+1$ ist, die Wurzeln $+1$, $+4$, $+7$, im andern Falle, wenn $a = 9n-1$ ist, die Wurzeln $+8$ ($\equiv -1$), $+2$, $+5$. ($1^3 = 1$, $4^3 = 64 = 7.9+1$, $7^3 = 343 = 38.9+1$; $8^3 = 512 = 57.9-1$, $2^3 = 8 = 9-1$, $5^3 = 125 = 14.9-1$).

48. Die Wurzel der Congruenz $x^3 \equiv a \pmod{p^{2n}}$ (wo a eine ganze, von o verschiedene und durch p nicht theilbare Zahl und p nicht $= 3$ ist) ist $= y + z.p^n$, wo y durch die Congruenz $y^3 \equiv a \pmod{p^n}$, und z durch die Congruenz $3y^2.z+f \equiv o \pmod{p^n}$, in welcher $f = \frac{y^3-a}{p^n}$ ist, bestimmt ist.

Dieser Satz, der nur eine Verallgemeinerung des Satzes unter 46 ist, wird auch ganz ebenso, wie jener, bewiesen.

Der Werth von z läßt sich (wie in 46) auch aus der Congruenz $y^2(y+3zp^n) = a \pmod{p^{2n}}$, und der Werth von x unmittelbar aus der Congruenz $y^2(3x-2y) \equiv a \pmod{p^{2n}}$ bestimmen.

Beispiel: Um der Congruenz $x^3 \equiv 187 \pmod{5^4}$ aufzulösen, hat man erst die Congruenz $y^3 \equiv 187 \pmod{5^2}$ oder $y^3 \equiv 12 \pmod{5^2}$ aufzulösen. Diese Congruenz hat (wie schon unter 46 gefunden) die Wurzel $y = 8$. Dann läßt sich x unmittelbar bestimmen aus der Congruenz: $8^2(3x-16) \equiv 187 \pmod{5^4}$. Nun ist $187 = 11.17 \equiv (-614)(-608) \equiv 614.608 \equiv 8^2.307.19 \equiv 8^2.208 \pmod{5^4}$, also $3x-16 \equiv 208$ oder $3x \equiv 224 \pmod{5^4}$, woraus $x = 283$ folgt. ($283^3 = 22665187 = 36264.5^4+187$; also $283^3 \equiv 187 \pmod{5^4}$).

49. Die Wurzel der Congruenz $x^3 \equiv a \pmod{p^{2n-1}}$, wo p nicht $= 3$ ist, ist $= y + z.p^n$, wo y durch die Congruenz $y^3 \equiv a \pmod{p^n}$ und z durch die Congruenz $3y^2z+f \equiv o \pmod{p^{n-1}}$, in welcher $f = \frac{y^3-a}{p^n}$ ist, bestimmt ist.

Die Congruenz $x^3 \equiv a \pmod{p^{2n-1}}$ ist gleichbedeutend mit der Gleichung $x^3 = a + m.p^{2n-1}$ Es sei nun $y^3 \equiv a \pmod{p^t}$ oder $y^3 = a + f.p^t$, wo $t < 2n-1$ sein soll. Dann ist x^3-y^3 oder $(x-y)(x^2+xy+y^2) = p^t(m.p^{2n-1-t}+f)$. Es kann daher $x-y$ durch p^t theilbar sein. Setzt man nun $x-y = z.p^t$, also $x = y+z.p^t$, so ist $x^3 = y^3+3y^2.zp^t+3y.z^2.p^{2t}+z^3.p^{3t} = a + m.p^{2n-1}$, also, da $y^3 = a+f.p^t$ ist, $fp^t+3y^2.zp^t+3yz^2p^{2t}+z^3p^{3t} = m.p^{2n-1}$, oder, wenn man durch p^t dividirt, $f+3y^2z+3yz^2p^t+z^3p^{2t} = m.p^{2n-1-t}$.

Der Exponent t läßt sich nun so wählen, daß $t =$ oder $> 2n-1-t$, also $2t =$ oder $> 2n-1$ ist. Dies ist der Fall, wenn $t = n$ genommen wird, was der obigen Bedingung, daß $t < 2n-1$ sein soll,

nicht widerspricht. Setzt man also $t = n$, so geht die letzte Gleichung über in: $f + 3y^2z + 3yz^2p^n + z^3p^{2n} = m \cdot p^{n-1}$, d. h. $f + 3y^2z \equiv o \pmod{p^{n-1}}$. Hieraus läßt sich z bestimmen, und x ist dann $= y + z \cdot p^n$, wenn $y^3 \equiv a \pmod{p^n}$ ist.

Substituirt man für x den Werth $y + z \cdot p^n$ in der gegebenen Congruenz $x^3 \equiv a \pmod{p^{2n-1}}$, so erhält man: $y^3 + 3y^2 \cdot zp^n + 3y \cdot z^2p^{2n} + z^3p^{3n} \equiv a \pmod{p^{2n-1}}$, oder, da die beiden letzten Glieder auf der linken Seite durch p^{2n-1} theilbar sind, $y^3 + 3y^2 \cdot zp^n \equiv a \pmod{p^{2n-1}}$, und, wenn man $x - y$ für zp^n setzt, $y^3 + 3y^2(x - y)$, d. ist $y^2(3x - 2y) \equiv a \pmod{p^{2n-1}}$. Aus dieser Congruenz läßt sich x unmittelbar bestimmen.

Beispiele: Soll $x^3 \equiv 37 \pmod{5^3}$ sein, so muß $y^3 \equiv 37 \pmod{5^2}$ oder $y^3 \equiv 12 \pmod{5^2}$ sein. Wie in 46 gefunden, ist $y = 8$. Es ist daher $8^2(3x - 16) \equiv 37 \pmod{5^3}$, oder, da $37 \equiv -88 \pmod{5^3}$ ist, $24x - 128 \equiv -11$, oder $24x \equiv 117$, oder $8x \equiv 39$, oder $8x \equiv 164$, oder $2x \equiv 41 \pmod{5^3}$, woraus sich $x = 83$ ergiebt. $(83^3 = 571787 = 4574 \cdot 5^3 + 37)$.

Soll $x^3 \equiv 37 \pmod{5^5}$ sein, so muß $y^3 \equiv 37 \pmod{5^3}$ sein. Nun ist soeben gefunden worden, daß 83 Wurzel dieser Congruenz ist. Mithin ist $83^2(3x - 166) \equiv 37 \pmod{5^5}$. Hieraus ergiebt sich $x = 458$. $(458^3 = 96071912 = 30743 \cdot 5^5 + 37$; also $458^3 \equiv 37 \pmod{5^5})$.

50. Ist $p = 3$, so erleiden die beiden Sätze unter 48 und 49 einige Abänderungen. Die Wurzel der Congruenz $x^3 \equiv a$ sowohl in Bezug auf den Modulus 3^{2n}, als in Bezug auf den Modulus 3^{2n-1} ist ebenfalls $= y + z \cdot 3^n$; y aber ist Wurzel der Congruenz $y^3 \equiv a \pmod{3^{n+1}}$ und z ist bestimmt in dem ersten Falle durch die Congruenz $y^2z + f \equiv o \pmod{3^{n-1}}$, im andern Falle durch die Congruenz $y^2z + f \equiv o \pmod{3^{n-2}}$, wo $f = \frac{y^3 - a}{3^{n+1}}$ ist.

Setzt man nämlich $x = y + z \cdot 3^n$, so ist $x^3 = y^3 + 3y^2 \cdot z \cdot 3^n + 3y \cdot z^2 \cdot 3^{2n} + z^3 \cdot 3^{3n}$, also $y^3 + y^2z \cdot 3^{n+1} \equiv a$, oder $y^3 - a \equiv -y^2z \cdot 3^{n+1}$, sowohl mod. 3^{2n}, als mod. 3^{2n-1}. Es muß daher, da $y^2z \cdot 3^{n+1}$ den Faktor 3^{n+1} hat, auch $y^3 - a$ durch 3^{n+1} theilbar, d. h. $y^3 \equiv a \pmod{3^{n+1}}$ sein. Ist nun $y^3 - a = f \cdot 3^{n+1}$, so ist $f \cdot 3^{n+1} \equiv -y^2z \cdot 3^{n+1}$, d. h. $3^{n+1}(y^2z + f)$ in dem ersten Falle durch 3^{2n}, im andern durch 3^{2n-1}, also $y^2z + f$ im ersten Falle durch 3^{n-1}, im andern Falle durch 3^{n-2} theilbar.

Beispiel: Wenn $x^3 \equiv 62 \pmod{3^4}$ sein soll, so muß $y^3 \equiv 62 \pmod{3^3}$, also $y^3 \equiv 8 \pmod{3^3}$ sein. Dieser Congruenz genügen die Werthe $y = 2$, 11, 20, und diesen Werthen von y entsprechen die Werthe $f = -2$, 47, 294, woraus sich für z die Werthe 2, 4, 6 und für x die Werthe 20 $(= 2 + 2 \cdot 3^2)$, 47 $(= 11 + 4 \cdot 3^2)$, 74 $(= 20 + 6 \cdot 9^2)$ ergeben. $(20^3 = 8000 = 98 \cdot 3^4 + 62$, $47^3 = 103823 = 1281 \cdot 3^4 + 62$, $74^3 = 405224 = 5002 \cdot 3^4 + 62)$.

51. Die Anzahl der positiven Wurzeln der Congruenz $x^3 \equiv a \pmod{p^n}$, welche $< p^n$ sind, ist gleich der Anzahl der positiven Wurzeln $< p$ derselben Congruenz in Bezug auf den Modulus p, außer wenn $p = 3$ ist; dann hat die Congruenz $x^3 \equiv a \pmod{3^n}$ $(n > 1)$ immer drei positive Wurzeln $< 3^n$.

Da die Congruenz $x^3 \equiv a \pmod{p^n}$ (nach 44) nur lösbar ist, wenn die Congruenz $y^3 \equiv a \pmod{p}$ lösbar ist, so läßt sich auch jede Wurzel der ersteren Congruenz durch eine Wurzel der letzteren darstellen, und zwar ist immer $x = y + z \cdot p$, wo $y < p$ und $z < p^{n-1}$ ist, da andernfalls $x > p^n$ wäre. Es sei nun $x = y + vp$ eine andere Wurzel der Congruenz $x^3 \equiv a \pmod{p^n}$. Dann ist

einerseits $y^3 + 3y^2zp + 3y \cdot z^2p^2 + z^3p^3 \equiv a \pmod{p^n}$

andrerseits $y^3 + 3y^2vp + 3y \cdot v^2p^2 + v^3p^3 \equiv a \pmod{p^n}$,

mithin $3y^2(z - v)p + 3y(z^2 - v^2)p^2 + (z^3 - v^3)p^3 \equiv o \pmod{p^n}$

oder $(z - v)p\left|3y^2 + 3y(z + v)p + (z^2 + zv + v^2)p^2\right| \equiv o \pmod{p^n}$

Da nun $z - v$ nicht durch p^{n-1} theilbar ist, weil sonst z oder $v > p^{n-1}$, also $x > p^n$ wäre, so müßte, wenn $z - v$ nicht $= o$ wäre, $3y^2 + 3y(z + v)p + (z^2 + zv + v^2)p^2$ durch p^{n-1}, also zunächst y durch p theilbar, d. h. $y > p$ sein. Da aber $y < p$ sein soll, so kann y nicht durch p theilbar sein, und die letzte Congruenz kann dann nur stattfinden, wenn $z - v = o$, also $z = v$ ist; dann ist aber $y + zp$ nicht von $y + vp$ verschieden. Einem bestimmten Werthe von y entspricht also nur ein einziger Werth von x, d. h. die Congruenz $x^3 \equiv a \pmod{p^n}$ hat ebenso viel positive Wurzeln $< p^n$, als die Congruenz $y^3 \equiv a \pmod{p}$ positive Wurzeln $< p$ hat. Die Anzahl dieser ist unter 8 angegeben.

Anders verhält es sich, wenn $p = 3$ ist. Denn in diesem Falle muß (nach 47) $y^3 - a$ nicht blos durch 3, sondern auch durch 3^2 theilbar, d. h. $y^3 \equiv a \pmod{3^2}$ sein, und da diese Congruenz drei positive Wurzeln $< 3^2$ hat, so hat auch die Congruenz $x^3 \equiv a \pmod{3^n}$ drei positive Wurzeln $< 3^n$.

Demnach hat die Congruenz $x^3 \equiv a \pmod{p^n}$ nur eine positive Wurzel $< p^n$, wenn p eine Primzahl von der Form $3n - 1$ ist, dagegen drei positive Wurzeln $< p^n$, wenn $p = 3$ oder eine Primzahl von der Form $3n + 1$ ist.

52. Die Congruenz $x^3 \equiv a \pmod{pq}$, wo p und q verschiedene Primzahlen sind, ist nur lösbar, wenn a kubischer Rest sowohl von p, als von q ist.

Denn die Congruenz $x^3 \equiv a \pmod{pq}$ ist gleichbedeutend mit der Gleichung $x^3 - a = fpq$; es muß also $x^3 - a$ sowohl durch p, als durch q theilbar, d. h. a kubischer Rest sowohl von p, als von q sein.

Dieser Beweis gilt offenbar auch, wenn der Modulus aus mehr als zwei verschiedenen Primzahlen zusammengesetzt ist.

53. Der Congruenz $x^3 \equiv a \pmod{pq}$ wird genügt durch $x = y + mp = z + nq$, wenn y und z den Congruenzen $y^3 \equiv a \pmod{p}$ und $z^3 \equiv a \pmod{q}$ genügen.

Nach 52 ist die Congruenz $x^3 \equiv a \pmod{pq}$ nur lösbar, wenn sowohl $x^3 \equiv a \pmod{p}$, als auch $x^3 \equiv a \pmod{q}$ ist. Es sei nun $y^3 \equiv a \pmod{p}$ und $z^3 \equiv a \pmod{q}$. Wenn nun $x^3 \equiv a \pmod{pq}$ und $y^3 \equiv a \pmod{p}$ oder $x^3 = a + fpq$ und $y^3 = a + gp$ ist, so ist $x^3 - y^3$ oder $(x - y)(x^2 + xy + y^2) = p(fq - g)$. Dies ist der Fall, wenn $x - y$ durch p theilbar, d. h. $x = y + mp$ ist. Ebenso ergiebt sich $x = z + nq$. Mithin ist $y + mp = z + nq$, woraus sich m und n bestimmen lassen.

54. Die Anzahl der positiven Wurzeln der Congruenz $x^3 \equiv a \pmod{pq}$, welche $< pq$ sind, ist gleich dem Produkt aus der Anzahl der positiven Wurzeln $< p$ der Congruenz $x^3 \equiv a \pmod{p}$ und der Anzahl der positiven Wurzeln $< q$ der Congruenz $x^3 \equiv a \pmod{q}$.

Nach 53 ist $x = y + mp = z + nq$, also $y - z = nq - mp$. Hieraus ergeben sich immer positive ganzzahlige Werthe für m und n, und zwar ist der kleinste Werth von m stets $< q$ und der kleinste Werth von n stets $< p$. Demnach ist, wenn man für m und n ihre kleinsten Werthe setzt, da auch $y < p$ und $z < q$ ist, x stets $< pq$. Ist nun die Anzahl der verschiedenen positiven Werthe von y, welche $< p$ sind, $= u$, und die Anzahl der verschiedenen positiven Werthe von z, welche $< q$ sind, $= v$, so ergeben sich aus der Combination jedes der u Werthe von y mit jedem der v Werthe von z offenbar $u \cdot v$ verschiedene positive Werthe für x, die $< pq$ sind. Denn ist

$$x = y + mp = z + nq \quad \text{und} \quad x' = y' + m'p = z' + n'q,$$

so müßte, wenn $x' = x$ wäre,

$$\text{einerseits } y' + m'p = y + mp \quad \text{oder } y' - y = (m - m')p,$$
$$\text{andrerseits } z' + n'q = z + nq \quad \text{oder } z' - z = (n - n')q$$

sein.

Das ist nicht möglich, da p und q Primzahlen, y und $y' < p$, z und $z' < q$, y' von y und z' von z verschieden sind.

55. Die Congruenz $x^3 \equiv a \pmod{z}$, wo $z = p^m \cdot q^n \cdot r^t \ldots$ und p, q, r .... verschiedene Primzahlen sind, ist nur lösbar, wenn a kubischer Rest jeder der Primzahlen p, q, r .... ist. Sie wird gelöst, indem man sie zunächst in Bezug auf p^m, q^n, r^t, ... auflöst und dann, wie in 54 angegeben ist, weiter verfährt.