Über einige specielle zahlentheoretische Functionen.

Von R. Daublebsky von Sterneck in Wien.

Im Folgenden soll eine Classe ziemlich specieller zahlentheoretischer Functionen betrachtet werden; doch werden sich, wie sich zeigen wird, zwei von den Herren K. Zsigmondy¹⁾ und E. Lucas²⁾ unabhängig von einander gewonnene und scheinbar völlig verschiedene zahlentheoretische Resultate durch die folgenden Untersuchungen als Specialisierungen desselben allgemeinen Theoremes auffassen lassen.

§. 1.

Die zahlentheoretische Function $f(n)$ sei durch folgende vier Eigenschaften charakterisiert:

a) $f(1) = 1$.

b) Der größte gemeinsame Theiler von $f(m)$ und $f(n)$ sei $f(d)$, wenn d der größte gemeinsame Theiler von m und n ist; speciell also $f(m)$ durch $f(n)$ theilbar, wenn m durch n theilbar ist, und $f(m)$ zu $f(n)$ theilerfremd, wenn m zu n theilerfremd ist.

c) Für jede Primzahl p (mit Ausnahme einer oder mehrerer von vorneherein festgesetzter Primzahlen) soll eine der Zahlen $f(p-1)$ oder $f(p+1)$ durch p theilbar sein.

d) Der größte gemeinsame Theiler der Zahlen $\frac{f(pn)}{f(n)}$ und $f(n)$ soll ein Theiler von p sein.

Von diesen Functionen $f(n)$ lässt sich nun folgendes Theorem nachweisen:

Ist

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

und bildet man den Quotienten:

$$F(n) = \frac{f(n)f\left(\frac{n}{p_1 p_2}\right)f\left(\frac{n}{p_1 p_3}\right) \dots f\left(\frac{n}{p_1 p_2 p_3 p_4}\right) \dots}{f\left(\frac{n}{p_1}\right)f\left(\frac{n}{p_2}\right) \dots f\left(\frac{n}{p_1 p_2 p_3}\right)f\left(\frac{n}{p_1 p_2 p_4}\right) \dots},$$

¹⁾ Zur Theorie der Potenzreste. Monatsh. f. Math. u. Phys. Jhgg. III, 1892.

²⁾ Bullettino di bibliografia e di storia. Hsg. v. Boncampagni, Tomo X.

wobei im Zähler alle geradzahligen, im Nenner alle ungeradzahligen Combinationen ohne Wiederholung der in n aufgehenden Primzahlen $p_1, p_2, \dots, p_r$ zu setzen sind, so enthält $F(n)$ nur solche Primzahlen als Factoren, welche keine der Zahlen $f(1), f(2), \dots, f(n-1)$ theilen, sondern erst in $f(n)$ aufgehen; unter diesen Factoren kann sich höchstens der Factor p_1 vorfinden, wenn p_1 die größte der in n aufgehenden Primzahlen ist und schon in $f\left(\frac{n}{p_1^{\pi_1}}\right)$ aufgeht, hingegen in keinem der Functionswerte $f(v)$, wenn $v < \frac{n}{p_1^{\pi_1}}$ ist.

§. 2.

Den Beweis dieses Theoremes wollen wir auf folgenden Ausdruck für das kleinste gemeinsame Vielfache V der Zahlen $a_1, a_2, \dots, a_n$ stützen:

$$V = \frac{a_1 a_2 \dots a_n g(a_1 a_2 a_3) \dots g(a_1 a_2 a_4) \dots g(a_1 a_2 a_3 a_4 a_5) \dots}{g(a_1 a_2) g(a_1 a_3) \dots g(a_1 a_2 a_3 a_4) g(a_1 a_2 a_3 a_5) \dots},$$

wo die Function g den größten gemeinsamen Theiler ihrer Argumente bedeutet und im Zähler alle ungeradzahligen, im Nenner alle geradzahligen Combinationen ohne Wiederholung der Zahlen $a_1, a_2, \dots, a_n$ zu setzen sind.

Es bedeute nämlich p eine in allen oder einigen der Zahlen $a_1, a_2, \dots, a_n$ aufgehende Primzahl und $\pi_1, \pi_2, \dots, \pi_n$ die bezüglichen Potenzexponenten von p in $a_1, a_2, \dots, a_n$ (deren einige auch Null sein können). Nehmen wir ferner $\pi_1 \geq \pi_2 \geq \pi_3 \geq \dots \geq \pi_n$ an, was gestattet ist, da die Größe V von der Anordnung der Zahlen $a_1, a_2, \dots, a_n$ unabhängig ist. Es enthält dann $g(a_{i_1}, a_{i_2}, \dots, a_{i_\lambda})$ den Factor $p^{\pi_{i_\mu}}$, wenn i_μ der größte der Indices $i_1, i_2, \dots, i_\lambda$ ist. Das Product sämmtlicher $g(a_{i_1}, a_{i_2}, \dots, a_{i_\lambda})$ enthält daher p in der Potenz:

$$\pi_\lambda + \binom{\lambda}{\lambda-1} \pi_{\lambda+1} + \binom{\lambda+1}{\lambda-1} \pi_{\lambda+2} + \dots + \binom{\lambda-1}{\lambda-1} \pi_n$$

und somit geht p in dem Quotienten V in der Potenz

$$\sum_{\lambda=1}^{\lambda=n} (-1)^{\lambda-1} \left\{ \pi_\lambda + \binom{\lambda}{\lambda-1} \pi_{\lambda+1} + \binom{\lambda+1}{\lambda-1} \pi_{\lambda+2} + \dots + \binom{\lambda-1}{\lambda-1} \pi_n \right\} =$$

auf; da nun π_1 der größte Exponent war, so ist V in der That das kleinste gem. Vielfache der Zahlen $a_1, a_2, \dots, a_n$.

§. 3.

Wir suchen nun das kleinste gem. Vielfache der Zahlen $f\left(\frac{n}{p_1}\right), f\left(\frac{n}{p_2}\right), \dots, f\left(\frac{n}{p_r}\right)$, das wir mit $\Phi(n)$ bezeichnen wollen. Nach der Eigenschaft (b) der Function $f(n)$ ist der größte gemeinsame Theiler mehrerer solcher Functionswerte dem Functionswerte für den größten gem. Theiler der Argumente gleich; somit erhalten wir auf Grund obiger Formel für $\Phi(n)$ den Ausdruck:

$$\Phi(n) = \frac{f\left(\frac{n}{p_1}\right)f\left(\frac{n}{p_2}\right) \dots f\left(\frac{n}{p_r}\right)f\left(\frac{n}{p_1 p_2 p_3}\right)f\left(\frac{n}{p_1 p_2 p_4}\right) \dots}{f\left(\frac{n}{p_1 p_2}\right)f\left(\frac{n}{p_1 p_3}\right) \dots f\left(\frac{n}{p_1 p_2 p_3 p_4}\right)f\left(\frac{n}{p_1 p_2 p_3 p_5}\right) \dots}.$$

Das kleinste gem. Vielfache der Zahlen $f\left(\frac{n}{p_1}\right), f\left(\frac{n}{p_2}\right), \dots, f\left(\frac{n}{p_r}\right)$ ist aber zugleich das kleinste gem. Vielfache aller Functionswerte $f(d)$, wenn d alle Theiler von n durchläuft, nur n selbst nicht; denn jeder Theiler von n (mit Ausnahme von n selbst) muss Theiler einer der Zahlen $\frac{n}{p_1}, \frac{n}{p_2}, \dots, \frac{n}{p_r}$ sein.

Somit erhalten wir eine sehr einfache Bedeutung des Quotienten $F(n)$; es ist nämlich

$$F(n) = \frac{f(n)}{\Phi(n)},$$

wobei $\Phi(n)$ das kleinste gem. Vielfache der Functionswerte f für alle Theiler von n (nur n selbst nicht) bedeutet.

§. 4.

Nehmen wir nun an, $F(n)$ sei durch eine Primzahl p theilbar, welche schon in einer der Zahlen $f(1), f(2), \dots, f(n-1)$ aufgeht, etwa in $f(x)$; sie geht dann auch in dem größten gemeinsamen Theiler von $f(n)$ und $f(x)$, $f(d)$ auf, wenn d der größte gemeinsame Theiler von n und x ist, also gewiss auch in einer der Zahlen $f\left(\frac{n}{p_i}\right)$; nun ist aber:

$$\frac{f(n)}{f\left(\frac{n}{p_i}\right)} \equiv 0 \pmod{F(n)},$$

weil $F(n) = \frac{f(n)}{\Phi(n)}$ und $\Phi(n) \equiv 0 \pmod{f\left(\frac{n}{p_i}\right)}$ ist.

Es hätten also $\frac{f(n)}{f\left(\frac{n}{p_i}\right)}$ und $f\left(\frac{n}{p_i}\right)$ einen Theiler gemeinsam;

dies kann nach der Eigenschaft (d) der Functionen f nur die Zahl p_i selbst sein. Man sieht also, dass $F(n)$ mit den Zahlen $f(1)$, $f(2)$, $\dots$, $f(n-1)$ nur Primfactoren von n gemein haben kann.

Nehmen wir nun an, $F(n)$ (also umsomehr $f(n)$) enthalte den Factor p_1^{λ} ; da nach der Eigenschaft (c) eine der beiden Zahlen $f(p_1 \pm 1)$ durch p_1 theilbar sein muss, enthält sowohl $f(n)$ als auch $f(p_1 \pm 1)$ den Factor p_1 und es muss daher, wenn μ das kleinste Argument ist, für welches $f(\mu)$ durch p_1 theilbar ist, μ ein gemeinsamer Theiler von $p_1 \pm 1$ und n sein, d. h., n muss durch einen Theiler von $p_1 \pm 1$ theilbar sein.

Da nun n die Form $n = p_1^{\pi_1} p_2^{\pi_2} \dots p_r^{\pi_r}$ hat, so ist die Theilbarkeit $n \equiv 0 \pmod{\mu}$ nur erfüllbar, wenn

$$p_2^{\pi_2} \dots p_r^{\pi_r} \equiv 0 \pmod{\mu}$$

ist, da $p_1^{\pi_1}$ zu μ theilerfremd ist.

Es folgt also aus der Annahme, $F(n) \equiv 0 \pmod{p_1^{\lambda}}$ die Gleichung

$$p_2^{\pi_2} \dots p_r^{\pi_r} = s \cdot \mu.$$

Wir müssen nun zwei Fälle unterscheiden, je nachdem $s > 1$ oder $s = 1$ ist.

Ist $s > 1$, so kann es sich nur aus Potenzen der Primzahlen $p_2 \dots p_r$ zusammensetzen; nehmen wir etwa an, s enthielte den Factor p_2 . Dann können wir die Gleichung durch p_2 dividieren und erhalten:

$$p_2^{\pi_2-1} p_3^{\pi_3} \dots p_r^{\pi_r} \equiv 0 \pmod{\mu}$$

hieraus folgt auf Grund der Eigenschaft (b)

$$f(p_2^{\pi_2-1} p_3^{\pi_3} \dots p_r^{\pi_r}) \equiv 0 \pmod{f(\mu)},$$

also auch

$$f(p_2^{\pi_2-1} p_3^{\pi_3} \dots p_r^{\pi_r}) \equiv 0 \pmod{p_1}$$

und umsomehr:

$$f\left(\frac{p_1^{\pi_1} p_2^{\pi_2-1} p_3^{\pi_3} \dots p_r^{\pi_r}}{p_2}\right) = f\left(\frac{n}{p_2}\right) \equiv 0 \pmod{p_1};$$

$f\left(\frac{n}{p_2}\right)$ muss aber p_1 in derselben Potenz enthalten, wie $f(n)$; sonst hätten die beiden Zahlen $\frac{f(n)}{f\left(\frac{n}{p_2}\right)}$ und $f\left(\frac{n}{p_2}\right)$ den Factor p_1 gemein-

sam, während sie nach der Eigenschaft (d) höchstens den Factor p_2 gemein haben könnten.

Daraus folgt aber, dass $F(n)$ in diesem Falle den Factor p_1 nicht enthält, weil es aus $f(n)$ durch Division durch das kl. gem. Vielfache aller Functionswerte $f\left(\frac{n}{p_i}\right)$ hervorgeht.

Es sei zweitens $s=1$, d. h.

$$p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r} = \mu.$$

μ ist aber ein Theiler von $p_1 \pm 1$; dies ist offenbar nur möglich, wenn p_1 die größte der in n aufgehenden Primzahlen ist. Dann können wir die soeben durchgeführten Schlüsse nicht anwenden und müssen die Möglichkeit, dass $F(n)$ irgend eine Potenz von p_1 enthalte, zulassen; es ist in diesem Falle auch $f(\mu) = f\left(\frac{n}{p_1}\right)$ durch p_1 theilbar und da μ die kleinste Zahl ist, für welche $f(\mu)$ durch p_1 theilbar ist, ist in der That keine der Zahlen $f(v)$ durch p_1 theilbar, wenn $v < \frac{n}{p_1^{\alpha_1}}$ ist.

Hiemit ist die Richtigkeit des eingangs ausgesprochenen Theoremes vollständig nachgewiesen; natürlich gilt dasselbe nur für jene Zahlen $F(n)$, deren Argument durch keine der Primzahlen theilbar ist, welche die Bedingung (c) nicht erfüllen.

Wir wollen nun zwei specielle Formen der Function f näher betrachten.

§. 5.

Herr K. Zsigmondy hat in seiner Arbeit „Zur Theorie der Potenzreste“¹⁾ seinen Betrachtungen die Function $f(n) = a_1^n - a_2^n$ (a_1 und a_2 theilerfremd) zugrunde gelegt und bildet für diese Function den Ausdruck, den wir mit $F(n)$ bezeichnet haben; dieses

$F(n)$ bleibt offenbar dasselbe, wenn wir $f(n) = \frac{a_1^n - a_2^n}{a_1 - a_2}$ setzen, denn der Nenner $a_1 - a_2$ kommt im Zähler und Nenner von $F(n)$ in derselben Potenz vor. Die Function $\frac{a_1^n - a_2^n}{a_1 - a_2}$ erfüllt nun aber in der That die eingangs aufgestellten Bedingungen:

a) $f(1) = 1$.

b) $f(m)$ und $f(n)$ haben den größten gemeinsamen Theiler $f(d)$, wenn m und n den größten gemeinsamen Theiler d haben.

¹⁾ Monatshefte f. Math. u. Phys. 3. Jahrg. 1892.

c) Für jede Primzahl p , welche nicht in einer der Zahlen $a_1, a_2, a_1 - a_2$ aufgeht, ist $f(p-1) \equiv 0 \pmod{p}$.

d) Endlich kann $\frac{f(pn)}{f(n)}$ mit $f(n)$ höchstens einen Theiler von p gemein haben; dies folgt unmittelbar aus der Identität:

$$\frac{f(pn)}{f(n)} = (a_1 - a_2) \left\{ \frac{a_1^{(p-1)n} - a_2^{(p-1)n}}{a_1 - a_2} + \frac{a_2^n (a_1^{(p-2)n} - a_2^{(p-2)n})}{a_1 - a_2} + \dots \right. \\ \left. \dots + \frac{a_2^{(p-2)n} (a_1^n - a_2^n)}{a_1 - a_2} \right\} + p a_2^{(p-1)n},$$

da in der Klammer jeder Summand durch $f(n)$ theilbar ist und a_1 zu a_2 theilertremd ist.

Somit gilt bezüglich der Function $F(n)$ das eingangs ausgesprochene Theorem, welches Herr Zsigmondy auf andere Weise ableitet. Da die kleinste Zahl n , für welche $f(n)$ durch eine bestimmte Primzahl p theilbar ist, wie wir oben gesehen haben, immer ein Theiler von $p \pm 1$ ist, in diesem Falle also immer ein Theiler von $p-1$, so haben alle Primzahlen, welche in $F(n)$ aufgehen, ohne in n aufzugehen, die Gestalt $\lambda n + 1$; auf Grund dieser Bemerkung führt Herr Zsigmondy einen elementaren Beweis des Satzes, dass jede arithmetische Progression mit dem Anfangsgliede 1 unendlich viele Primzahlen enthält.

§. 6.

Wir wollen uns nun einem zweiten Beispiele zuwenden.

Es sei $f(n)$ gegeben durch die Recursionsformel:

$$f(n) = f(n-1) + \alpha f(n-2) \quad (\alpha \text{ ganz, positiv})$$

und die Anfangsbedingungen $f(1) = f(2) = 1$.

Diese Function erfüllt ebenfalls die Bedingungen (a), (b), (c), (d), wie wir zeigen wollen.

Aus der weiteren Recursionsformel:

$$f(n) = f(\lambda) f[n - (\lambda - 1)] + \alpha f(n-1) f(n-\lambda),$$

die man leicht von λ auf $\lambda + 1$ erschließen kann, erkennt man nämlich leicht, dass $f(m)$ und $f(n)$ den größten gemeinsamen Theiler $f(d)$ haben, wenn d der größte gemeinsame Theiler von m und n ist.

Man erhält ferner für $f(n)$, wenn man $P = 4\alpha + 1$ set die independente Darstellung:

$$f(n) = \frac{1}{2^{n-1}} \left\{ \binom{n}{1} + P \binom{n}{3} + P^2 \binom{n}{5} + \dots \right\} = \\ = \frac{1}{VP} \left\{ \left(\frac{1+V\bar{P}}{2} \right)^n - \left(\frac{1-V\bar{P}}{2} \right)^n \right\}.$$

Hieraus ergibt sich die Congruenz:

$$2^p f(p+1) \equiv 1 + P^{\frac{p-1}{2}} \pmod{p}.$$

Es ist somit $f(p+1)$ durch p theilbar, wenn P quadratischer Nichtrest von p ist.

Ist P quadratischer Rest von p , so erhalten wir die beiden Congruenzen:

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

woraus sich, wenn man die zweite Congruenz mit 2 multipliciert und von der ersten subtrahiert, ergibt:

$$2 \{ f(p+1) - f(p) \} = 2\alpha f(p-1) \equiv 0 \pmod{p}.$$

Ist also 2α nicht durch p theilbar, was wir annehmen wollen, so muss $f(p-1)$ durch p theilbar sein; es ist somit immer eine der beiden Zahlen $f(p-1)$ oder $f(p+1)$ durch p theilbar (mit Ausnahme jener Primzahlen p , welche eine der Zahlen 2α oder P theilen).

Was endlich die Bedingung (d) betrifft, so erhält man durch entsprechende Wahl von λ in obiger Recursionsformel folgende Transformation für $f(\rho n)$:

$$f(\rho n) = f(n) f[(\rho-1)n+1] + \alpha f(n-1) f[(\rho-1)n] = \\ = f(n) f[(\rho-1)n+1] + \alpha f(n-1) \{ f(n) f[(\rho-2)n+1] + \\ + \alpha f(n-1) f[(\rho-2)n] \} \\ = f(n) f[(\rho-1)n+1] + \alpha f(n-1) f(n) f[(\rho-2)n+1] + \\ + \alpha^2 f^2(n-1) f[(\rho-2)n] \\ = \dots \dots \dots \\ = f(n) \{ f[(\rho-1)n+1] + \alpha f(n-1) f[(\rho-2)n+1] + \\ + \alpha^2 f^2(n-1) f[(\rho-3)n+1] + \dots + \alpha^{e-1} f^{e-1}(n-1) \} \\ \frac{f(\rho n)}{f(n)} = \sum_{\lambda=1}^{\lambda=e} f^{\lambda-1} \alpha^{\lambda-1} (n-1) f[(\rho-\lambda)n+1]$$

$$\begin{aligned}
f[(\rho - \lambda)n + 1] &= f(n)f[(\rho - \lambda - 1)n + 2] + \\
&\quad + \alpha f(n-1)f[(\rho - \lambda - 1)n + 1] \\
f[(\rho - \lambda)n + 1] &\equiv \alpha f(n-1)f[(\rho - \lambda - 1)n + 1] \pmod{f(n)} \\
&\equiv \alpha^2 f^2(n-1)f[(\rho - \lambda - 2)n + 1] \pmod{f(n)} \\
&\equiv \dots\dots\dots \\
&\equiv \alpha^{\rho-\lambda} f^{\rho-\lambda}(n-1) \pmod{f(n)} \\
\frac{f(\rho n)}{f(n)} &\equiv \sum_{\lambda=1}^{\lambda=\rho} \alpha^{\lambda-1} f^{\lambda-1}(n-1) \alpha^{\rho-\lambda} f^{\rho-\lambda}(n-1) \equiv \\
&\equiv \rho \alpha^{\rho-1} f^{\rho-1}(n-1) \pmod{f(n)}.
\end{aligned}$$

α und $f(n)$ sind theilerfremd; denn jeder gemeinsame Theiler von α und $f(n)$ wäre auf Grund der Relation $f(n) = f(n-1) + \alpha f(n-2)$ ein Theiler von $f(n-1)$, ferner wegen $f(n-1) = f(n-2) + \alpha f(n-3)$ auch ein Theiler von $f(n-2)$ u. s. f., endlich ein Theiler von $f(1)$, das den Wert 1 hat; $f(n)$ und $f(n-1)$ sind aber ebenfalls theilerfremd, denn ihr größter gemeinsamer Theiler ist $f(1) = 1$, weil n und $n-1$ den größten gemeinsamen Theiler 1 haben. Somit ist in der That der größte gemeinsame Theiler von $\frac{f(\rho n)}{f(n)}$ und $f(n)$ ein Theiler von ρ . Somit sind auch für diese Functionen $f(n)$ die vier Bedingungen (a), (b), (c), (d) erfüllt.

§. 7.

Diese eben besprochenen Functionen $f(n)$ sind eine Verallgemeinerung der durch die Recursionsformel

$$f_1(n) = f_1(n-1) + f_1(n-2)$$

definierten Function; $f_1(n)$ ist das allgemeine Glied der Lamé'schen Reihe.

Diese Function hat Herr E. Lucas in Boncampagni's Bullettino di bibliografia e di storia, Tomo X, gelegentlich der Besprechung einiger Untersuchungen Fibonacci's einer eingehenden Discussion unterzogen. Die dort gegebene Unterscheidung der „facteurs propres“ und „facteurs impropres“ von $f_1(n)$ fällt im Wesentlichen mit der Aufstellung des Ausdrucks $F_1(n)$ zusammen; denn Herr Lucas bezeichnet als facteurs propres jene Primtheiler von $f(n)$, welche in keiner der Zahlen $f_1(1)$, $f_1(2)$, ..., $f_1(n-1)$ aufgehen.

Die durch obige allgemeinere Recursionsformel definierten Functionen $f(n)$ sind aber andererseits ein Specialfall jener Func-

tionen, welche Lejeune-Dirichlet in seiner Breslauer Habilitationsschrift untersuchte, und an welche Kronecker im 88. Bande der Sitzungsberichte der kgl. preuß. Akademie d. Wiss. einige Bemerkungen knüpft, unter welchen sich auch die Bildung eines der Function $F(n)$ analogen Ausdruckes findet.

§. 8.

Wir wollen nun annehmen, $P = 4\alpha + 1$ sei eine Primzahl und wollen den quadratischen Restcharacter von $F(n)$ bezüglich P untersuchen, n sei nicht theilbar durch P .

Aus der Form von $f(n)$

$$f(n) = \frac{1}{2^{n-1}} \left\{ \binom{n}{1} + P \binom{n}{3} + P^2 \binom{n}{5} + \dots \right\}$$

ergibt sich

$$2^{n-1} f(n) \equiv n \pmod{P}$$

und daraus:

$$\left(\frac{f(n)}{P} \right) = \left(\frac{n}{P} \right) \left(\frac{2}{P} \right)^{n-1}.$$

Für $F(n)$ wollen wir der Kürze wegen den Ausdruck:

$$F(n) = \prod_d f\left(\frac{n}{d}\right)^{\mu(d)}$$

setzen, wo sich das Productzeichen auf alle Theiler von n bezieht und die zahlentheoretische Function $\mu(x)$ den Wert 0 hat, wenn x durch ein Quadrat (außer 1) theilbar ist, sonst den Wert ± 1 , je nachdem die Anzahl der in x aufgehenden Primzahlen gerade oder ungerade ist.

Berücksichtigt man nun, dass in dem Ausdrücke $F(n)$ die im Zähler und Nenner stehenden Factoren die gleiche Rolle spielen, da das Legendre'sche Symbol immer den Wert ± 1 hat, so folgt:

$$\begin{aligned} \left(\frac{F(n)}{P} \right) &= \prod_d \left(\frac{f\left(\frac{n}{d}\right)}{P} \right)^{\mu(d)} = \prod_d \left\{ \left(\frac{n}{d} \right) \left(\frac{2}{P} \right)^{\frac{n}{d}-1} \right\}^{\mu(d)} = \\ &= \left(\frac{n}{P} \right)^{\sum \mu(d)} \cdot \prod_d \left(\frac{d}{P} \right)^{-\mu(d)} \cdot \left(\frac{2}{P} \right)^{\sum \frac{n}{d} \mu(d)} \cdot \left(\frac{2}{P} \right)^{-\sum \mu(d)} = \prod_d \left(\frac{d}{P} \right)^{\mu(d)}, \end{aligned}$$

denn die $\sum \mu(d) = 0$ und $\sum \frac{n}{d} \mu(d) = \varphi(n)$, also eine gerade Zahl. In dem nun erhaltenen Producte kommen nur solche Theiler in

Betracht, welche aus lauter verschiedenen Primzahlen bestehen, weil nur für diese die Function $\mu(d)$ von 0 verschieden ist. Ist nun n durch r verschiedene Primzahlen theilbar, deren eine p_i heiße, so wird p_i in $\binom{r-1}{\rho-1}$ Theilern von n aufgehen, welche aus ρ verschiedenen Primzahlen zusammengesetzt sind. Somit ist:

$$\left(\frac{F(n)}{P}\right) = \prod_i \left(\frac{p_i}{P}\right)^{\sum_{\rho=1}^{\rho=r} (-1)^\rho \binom{r-1}{\rho-1}}.$$

Für $r > 1$ reducirt sich der Exponent immer auf 0, und ist also $\left(\frac{F(n)}{P}\right) = 1$.

Für $r = 1$, d. h. $n = p^k$, ist $\left(\frac{F(n)}{P}\right) = \left(\frac{p}{P}\right)$.

Somit gilt folgender Satz:

Ist n eine Primzahlpotenz, so ist $F(n)$ quadratischer Rest, resp. Nichtrest von P , je nachdem die Primzahl, deren Potenz n ist, Rest oder Nichtrest von P ist.

Ist n aus mehreren Primzahlen zusammengesetzt, so ist $F(n)$ immer quadratischer Rest von P .

§. 9.

Auf Grund dieser Bemerkung wollen wir nun einen elementaren Beweis des Satzes führen, dass jede arithmetische Progression der Form $ax - 1$ ($x = 0, 1, 2, \dots$) unendlich viele Primzahlen enthält, wenn wir a als Primzahlpotenz voraussetzen.

$$a = p^l.$$

Wir bestimmen zu diesem Zwecke zu p eine zweite Primzahl P , welche die Form $P = 4a + 1$ hat, ohne dass a durch p theilbar ist, und quadratischer Nichtrest von p ist. Dann sei die Function $f(n)$ durch die Recursionsformel:

$$f(n) = f(n-1) + af(n-2) \quad f(1) = f(2) = 1$$

gegeben.

Bilden wir $F(p^l)$, so ist dies quadratischer Nichtrest von P ; es kann ferner keinen Primfactor enthalten, welcher in einer der Zahlen $f(1), f(2), \dots, f(p^l - 1)$ aufgeht; denn auf Grund des im §. 1 aufgestellten Theoremes könnte dieser Primfactor nur p sein, dann müsste aber schon $f\left(\frac{p^l}{p}\right) = f(1)$ auf Grund desselben Theo-

remes den Primfactor p haben, was nicht möglich ist. Sei nun m eine in $F(p^l)$ aufgehende Primzahl, so muss p^l ein Theiler von $m \pm 1$ sein, je nachdem P quadratischer Nichtrest oder Rest von m ist, oder, was dasselbe besagt, je nachdem m quadratischer Nichtrest oder Rest von P ist, weil $P = 4\alpha + 1$, also nach dem Reciprocitätsgesetze $\left(\frac{P}{m}\right) = \left(\frac{m}{P}\right)$ ist.

Da nun $F(p^l)$ quadratischer Nichtrest von P ist, so muss die Anzahl seiner Factoren, welche Nichtreste sind, eine ungerade sein; es muss daher $F(p^l)$ mindestens eine Primzahl enthalten, welche, um 1 vermehrt, durch p^l theilbar wird, also die Form $x p^l - 1$ hat.

$F(p^{l+i})$ muss analog mindestens eine Primzahl m' enthalten, welche, um 1 vermehrt, durch p^{l+i} theilbar wird und in keinem F mit kleinerem Argumente aufgeht. Somit hat auch

$$m' = x' p^{l+i} - 1 = (x' p^i) p^l - 1$$

die verlangte Form. Man erhält also für jedes i aus $F(p^{l+i})$ mindestens eine neue Primzahl der Form $x p^l - 1$, womit gezeigt ist, dass es unendlich viele Primzahlen dieser Form geben muss.

Abzählung der Primzahlen von der Form $100n + 3$.

Ich benütze diese Gelegenheit, um die Resultate einer Abzählung der in den ersten 9 Millionen natürlicher Zahlen vorhandenen Primzahlen der Form $100n + 3$ mitzuthellen, welche ein viel klarer ausgeprägtes Resultat bezüglich der Häufigkeit des Vorkommens dieser Primzahlen ergab, als es bei jenen der Form $100n + 1$ der Fall war, für welche ich eine analoge Untersuchung im Anzeiger der kais. Akademie d. Wissenschaften in Wien, math.-naturw. Cl. 1894, Nr. 1 veröffentlicht habe. Es hat sich nämlich ziemlich deutlich gezeigt, dass mehr als der $\varphi(100)^{\text{te}}$, d. i. 40. Theil aller Primzahlen dieses Gebietes die Form $100n + 3$ haben.

Die Zählungsergebnisse sind in der folgenden Tabelle zusammengestellt; die erste Colonne enthält die obere Grenze des immer von Null beginnenden Intervalles in Millionen als Einheiten; die zweite die Anzahl der in diesem Intervalle vorhandenen Primzahlen der Form $100n + 3$ und die dritte die Abweichung dieser Anzahl vom 40. Theile der in demselben Intervalle vorhandenen Primzahlmenge überhaupt.

Die Zählung wurde aus den Burckhardt-Glaisher-Daseschen Factorentafeln vorgenommen und sind die von Bertelsen ermittelten, von Gram im 17. Bande der Acta mathematica mitgetheilten Fehler derselben berücksichtigt worden.

0.1	237	— 3	1.1	2144	+ 1	2.1	3895	0
·2	447	— 3	·2	2329	+ 6	·2	4077	+ 10
·3	638	— 12	·3	2511	+ 10	·3	4245	+ 7
·4	831	— 16	·4	2685	+ 7	·4	4428	+ 21
·5	1033	— 5	·5	2878	+ 24	·5	4594	+ 17
·6	1229	+ 2	·6	3042	+ 14	·6	4766	+ 20
·7	1405	— 9	·7	3197	— 7	·7	4929	+ 13
·8	1598	— 1	·8	3373	— 4	·8	5103	+ 19
·9	1785	+ 3	·9	3548	— 3	·9	5277	+ 24
1.0	1969	+ 7	2.0	3712	— 11	3.0	5452	+ 32
3.1	5616	+ 29	4.1	7281	+ 37	5.1	8912	+ 38
·2	5790	+ 35	·2	7446	+ 38	·2	9072	+ 37
·3	5956	+ 33	·3	7607	+ 36	·3	9220	+ 21
·4	6133	+ 45	·4	7778	+ 45	·4	9391	+ 32
·5	6299	+ 45	·5	7949	+ 50	·5	9557	+ 37
·6	6467	+ 49	·6	8113	+ 52	·6	9703	+ 23
·7	6639	+ 54	·7	8276	+ 52	·7	9861	+ 21
·8	6789	+ 39	·8	8430	+ 44	·8	10030	+ 30
·9	6961	+ 46	·9	8591	+ 41	·9	10199	+ 38
4.0	7125	+ 46	5.0	8749	+ 36	6.0	10356	+ 35
6.1	10528	+ 47	7.1	12103	+ 28	8.1	13714	+ 63
·2	10682	+ 41	·2	12273	+ 40	·2	13858	+ 50
·3	10835	+ 33	·3	12428	+ 36	·3	14023	+ 58
·4	10986	+ 26	·4	12586	+ 37	·4	14191	+ 69
·5	11139	+ 20	·5	12743	+ 36	·5	14351	+ 73
·6	11302	+ 23	·6	12900	+ 36	·6	14492	+ 56
·7	11461	+ 24	·7	13061	+ 38	·7	14636	+ 43
·8	11610	+ 13	·8	13226	+ 47	·8	14782	+ 32
·9	11776	+ 19	·9	13384	+ 46	·9	14940	+ 34
7.0	11945	+ 29	8.0	13548	+ 54	9.0	15092	+ 30

In den einzelnen Millionen sind die Primzahlen der Form $100n + 3$ in folgenden Anzahlen vorhanden:

1969 1743 1740 1673 1624 1607 1589 1603 1544.

Die Abweichungen vom 40. Theil der Primzahlmengen in den betreffenden Millionen sind:

+ 7 — 18 + 43 + 14 — 10 — 1 — 6 + 25 — 24.

Unter den von Davis (Liouville's Journal 1866) berechneten 99 Primzahlen im Intervalle 100,000.000 bis 100,001.699 gibt es zwei Primzahlen, welche die Form $100n + 3$ haben, nämlich 100,001.203 und 100,001.303.