

9.

Eine Bemerkung zur Zahlentheorie.

(Von Herrn Prof. Dr. Stern zu Göttingen.)

Wenn p eine Primzahl von der Form $8n+1$ und daher $p = c^2 + 2d^2$ ist, so hat man

$$1. \quad \pm 2c \equiv \frac{4n+1 \cdot 4n+2 \cdots 5n}{1 \cdot 2 \cdots n} \pmod{p}.$$

Dieses Theorem, welches in einem Aufsätze des Herrn Prof. *Jacobi* im 2ten Hefte des 30sten Bandes dieses Journals (S. 168) vorkommt, habe ich vor langer Zeit durch Induction gefunden und in etwas anderer Gestalt bekannt gemacht (Jahrbücher f. wissensch. Critik 1831 pg. 679), nemlich

$$2. \quad \pm 2c \equiv \frac{4n \cdots 3n+1}{1 \cdots n} \pmod{p}.$$

Dasselbe Theorem läßt sich aber noch einfacher ausdrücken. Es ist nemlich auch

$$3. \quad \pm 2c \equiv \frac{2n \cdots n+1}{1 \cdots n} \pmod{p},$$

und in dieser Formel muß das obere oder das untere Zeichen genommen werden, je nachdem c entweder in den Formen $8m+1$ und $8m+3$, oder in den Formen $8m+5$ und $8m+7$ enthalten ist.

Der Zusammenhang zwischen den Formeln (1.) und (2.) und der Formel (3.) ist nachzuweisen. Man hat nemlich

$$\begin{aligned} 2^n(1 \cdot 2 \cdot 3 \cdots n) &\equiv 2 \cdot 4 \cdot 6 \cdots 2n, \\ 2^n(4n+1 \cdots 5n) &\equiv 1 \cdot 3 \cdot 5 \cdots 2n-1, \end{aligned}$$

mithin

$$4. \quad 2^{2n}(4n+1 \cdots 5n) \equiv n+1 \cdots 2n.$$

Nun ist

$$2^{2n} \equiv \pm 1,$$

also

$$5. \quad \pm 1 \equiv \frac{5n \cdots 4n+1}{n+1 \cdots 2n};$$

wo das obere oder das untere Zeichen genommen werden muß, je nachdem die Zahl 2 ein biquadratischer Rest oder Nichtrest ist, d. h. je nachdem c in den

Formen $8m+1$ und $8m+7$ oder in den Formen $8m+3$ und $8m+5$ enthalten ist. Multiplicirt man die Formel (5.) mit der Formel (3.), so erhält man die Formel (1.), und man sieht, dafs in letzterer Formel das obere oder das untere Zeichen genommen werden mufs, je nachdem c in der Form $4n+1$ oder in $4n+3$ enthalten ist; wie es auch Herr Prof. *Jacobi* angegeben hat.

Die Formel (2.) gilt aber auch noch, wenn p eine Primzahl von der Form $8n+3$ ist, und es scheint mir hierin ein Beweis zu liegen, dafs die Theorie der Reste nicht die eigentliche Quelle solcher Sätze ist. Man hat nemlich, wenn $p = 8n+3 = c^2 + 2d^2$ ist,

$$6. \quad \pm 2c \equiv \frac{4n+1 \cdots 3n+2}{1 \cdots n},$$

und es mufs das obere oder das untere Zeichen genommen werden, je nachdem c entweder $= 8m+7$, $8m+5$, oder $= 8m+1$, $8m+3$ ist. Hieraus folgt, unter denselben Bedingungen:

$$7. \quad \pm 2c \equiv (-1)^n \cdot \frac{4n+2 \cdots 5n+1}{1 \cdots n}$$

und, mit Rücksicht auf die Congruenz

$$2^{2n}(4n+2 \cdots 5n+1) \equiv n+1 \cdots 2n,$$

auch

$$8. \quad \pm 2^{2n+1} \cdot c \equiv (-1)^n \cdot \frac{2n \cdots n+1}{1 \cdots n}.$$