Theorie der quadratischen Kongruenzen.

Von **Lothar von Schrutka** in Wien.

1. Übliche Behandlungsmethode. In den Elementen der Zahlentheorie pflegt man bei der Behandlung der Kongruenzen zweiten Grades von der allgemeinsten Kongruenz dieser Art

$$Ax^2 + Bx + C \equiv 0 \,(m)$$

auszugehen und zu zeigen, wie sie auf eine reine Kongruenz zurückgeführt werden kann, dann aber nur die Theorie der reinen Kongruenzen zweiten Grades oder, anders ausgedrückt, die Theorie der quadratischen Reste weiter zu verfolgen.

In der vorliegenden Abhandlung unternehme ich es, die Theorie der Kongruenzen zweiten Grades systematisch zu behandeln, indem ich mich eines Prinzips bediene, das ich in einer früheren Arbeit „Theorie der Polygonalreste“ (Monatshefte für Mathematik und Physik, XVI. Jahrgang, Wien 1906, p. 167) zur Lösung einer speziellen Aufgabe dieser Art angewendet habe und das kurz als eine Abbildung geeignet gewählter rationaler Zahlen, die arithmetische Reihen bilden, auf die Reihe der ganzen Zahlen bezeichnet werden kann.

2. Absonderung des Absolutgliedes. Wird die Kongruenz zweiten Grades

$$Ax^2 + Bx + C \equiv 0 \,(m)$$

auf die Form

$$Ax^2 + Bx \equiv -C \,(m)$$

gebracht, so ist zu erkennen, daß sie als die Forderung angesehen werden kann, diejenigen Zahlen x zu ermitteln, für die der Ausdruck $Ax^2 + Bx$ einen nach dem Modul m einer bestimmten Zahl $-C$ kongruenten Wert annimmt.

Es wird daher das zahlentheoretische Verhalten des Ausdrucks $Ax^2 + Bx$ bei veränderlichem x näher zu untersuchen sein.

3. Erste Vereinfachung. Die in der Formel $Ax^2 + Bx$ enthaltenen Zahlen sind — x als ganzzahlig vorausgesetzt — jedenfalls ganz, wenn A und B selbst ganz sind, ferner aber auch dann, wenn A und B beide Brüche mit ungeradem Zähler und dem Nenner 2 sind, da ja stets

$$x^2 \equiv x \,(2)$$

ist. Wird daher

$$2A = T,\ B - A = U$$

gesetzt, so sind T, U zwei ganze Zahlen, die keiner Beschränkung unterworfen sind, und es ist

$$A = \frac{T}{2},\ B = \frac{T + 2U}{2},$$

$$Ax^2 + Bx = T \cdot \frac{x^2 + x}{2} + Ux.$$

Offenbar kann man aber, ohne etwas an Allgemeinheit zu verlieren, annehmen, daß A, daher auch T eine positive Zahl sei.

4. Die Transformation F. Es möge nun jeder ganzen Zahl a die (im allgemeinen gebrochene) Zahl

$$\alpha = F(a) = \frac{4a - T - 2U}{2T}$$

zugeordnet werden. Wird von der Bedingung, daß a ganz sein soll, abgesehen, so kann der Übergang von a zu $F(a)$, der kurz als die Transformation F bezeichnet werden möge, als eine Streckung der Zahlenlinie vom Punkte $\frac{T + 2U}{4 - 2T}$ aus im Verhältnis $1 : \frac{2}{T}$ beschrieben werden. Nur für $T = 2$ tritt an die Stelle der Streckung eine Translation um das Stück $\frac{1 + U}{2}$; insbesondere ist für $U = -1$ $F(a)$ mit a identisch.

Da T positiv vorausgesetzt wurde, so ist

$$F(a) \gtreqless F(b),$$

je nachdem $a \gtreqless b$ ist. Beziehungen der Gleichheit und Ungleichheit bleiben demnach bei der Transformation erhalten.

Die zu F inverse Funktion sei Φ:

$$a = \Phi(\alpha) = \frac{2T\alpha + T + 2U}{4};$$

Φ möge auch als Zeichen für die zu F inverse Transformation, der Übergang von $F(a)$ zu a oder von α zu $\Phi(\alpha)$ verwendet werden.

Was die Bezeichnung betrifft, so soll, wie es hier bereits geschehen ist, das kleine griechische Alphabet ausschließlich zur Bezeichnung der Zahlen von der Form $F(a)$ verwendet werden.

Schließlich seien noch folgende stehende Abkürzungen eingeführt:

$$\iota = F(0) = -\frac{T+2U}{2T},$$

$$\varepsilon = F(1) = \frac{4-T-2U}{2T},$$

$$\eta = F(2) = \frac{8-T-2U}{2T},$$

$$\rho = F(3) = \frac{12-T-2U}{2T},$$

$$f = \frac{(T+2U)(T+2U-4)}{8T}$$

5. Analoga der Addition und der Multiplikation. Ist

$$\alpha = F(a),\ \beta = F(b),$$

so ist sowohl $F(a+b)$ wie $F(ab)$ eine durch a und b, daher auch durch α und β bestimmte Zahl; es werde

$$F(a+b) = \frac{4(a+b)-T-2U}{2T} =$$

$$= \alpha+\beta-\iota = \alpha(+)\beta$$

$$F(ab) = \frac{4ab-T-2U}{2T} =$$

$$= \frac{T}{2}\alpha\beta + \frac{T+2U}{4}(\alpha+\beta) + f = \alpha(\cdot)\beta$$

gesetzt.

6. Rechengesetze für diese Verknüpfungen. Aus diesen Definitionen folgen unmittelbar für die mit den Zeichen $(+)$ und $(\cdot)$ belegten Verknüpfungen das kommutative Gesetz:

$$\alpha(+)\beta = \beta(+)\alpha,\ \alpha(\cdot)\beta = \beta(\cdot)\alpha,$$

das assoziative Gesetz:

$$[\alpha(+)\beta](+)\gamma = \alpha(+)[\beta(+)\gamma],\ [\alpha(\cdot)\beta](\cdot)\gamma = \alpha(\cdot)[\beta(\cdot)\gamma]$$

und das distributive Gesetz:

$$\alpha\,(\cdot)\,\gamma\,(+)\,\beta\,(\cdot)\,\gamma = [\alpha\,(+)\,\beta]\,(\cdot)\,\gamma.$$

Ferner ist

$$\alpha\,(+)\,\iota = \alpha,$$
$$\alpha\,(\cdot)\,\varepsilon = \alpha,$$
$$\alpha\,(\cdot)\,\iota = \iota.$$

7. Umkehrungen dieser Verknüpfungen. Die Umkehrungen dieser beiden Verknüpfungen existieren ebenfalls und sind eindeutig. Wird

$$F(-b) = \frac{-4b - T - 2U}{2T} = (-)\,\beta$$

gesetzt, so ist

$$\alpha\,(-)\,\beta = \alpha\,(+)\,[(-)\,\beta]$$

die Lösung der Gleichung

$$\beta\,(+)\,\xi = \alpha;$$

wird

$$F\left(\frac{1}{b}\right) = \frac{4\,\frac{1}{b} - T - 2U}{2T} = \frac{\varepsilon}{(\beta)} = \varepsilon\,(:)\,\beta$$

gesetzt, so ist

$$\alpha\,(:)\,\beta = \frac{\alpha}{(\beta)} = \alpha\,(\cdot)\,\frac{\varepsilon}{(\beta)}$$

die Lösung der Gleichung

$$\beta\,(\cdot)\,\xi = \alpha;$$

hiebei ist $\beta \neq \iota$ vorausgesetzt. Die Ausrechnung ergibt ohne Mühe

$$\alpha\,(-)\,\beta = \alpha - \beta + \iota,$$

$$\frac{\alpha}{(\beta)} = \frac{4\alpha - (T+2U)\beta - 4f}{2T\beta + T + 2U}.$$

8. Die direkte Operation dritter Stufe. Es werde noch

$$\overset{1}{\alpha}\,(\cdot)\,\overset{2}{\alpha}\,(\cdot)\,\cdots\,(\cdot)\,\overset{n}{\alpha} = \alpha^{(n)}$$

gesetzt. Unter $\alpha^{(1)}$ soll α, unter $\alpha^{(0)}$ ε, unter $\alpha^{(-n)}$ $\frac{\varepsilon}{(\alpha^{(n)})}$ verstanden werden.

Insbesondere ist

$$\alpha^{(2)} = \alpha\,(\cdot)\,\alpha = \frac{T}{2}\alpha^2 + \frac{T+2U}{2}\alpha + f = T\frac{\alpha^2+\alpha}{2} + U\alpha + f.$$

9. Allgemeiner Satz über die eingeführten Verknüpfungen. Durch entsprechende Kombination der Gleichungen in Nr. 5 und 7 ergibt sich folgender allgemeine Satz:

Ist

$$\Omega\,(+, -, \cdot, : \mid a, b, c, \ldots) = k$$

eine Kombination der Zeichen $+, -, \cdot, :$ und der Zahlen $a, b, c, \ldots$, also eine Rechenoperation, die aus Additionen, Subtraktionen, Multiplikationen und Divisionen besteht — Divisionen durch Null sollen überdies angeschlossen sein — und auf $a, b, c, \ldots$ angewendet das Resultat k ergibt; ist ferner

$$\alpha = F(a), \beta = F(b), \gamma = F(c), \ldots,$$

so ist die Ausführung der Operation

$$\Omega\,(+), (-), (\cdot), (:) \mid \alpha, \beta, \gamma, \ldots)$$

stets möglich, d. h. es tritt keine Zahl ι hinter dem Zeichen $(:)$ auf und es ist, wenn das Resultat mit $\varkappa$ bezeichnet wird,

$$\varkappa = F(k).$$

10. Teilbarkeit. Es braucht wohl kaum darauf hingewiesen zu werden, daß die bisherigen Resultate auch giltig bleiben, wenn $a = \Phi(\alpha), b = \Phi(\beta), c = \Phi(\gamma), \ldots$ keine ganzen Zahlen sind; im folgenden hingegen ist diese Bedingung wesentlich. Es ist nämlich auch möglich, alle zahlentheoretischen Begriffe von den Zahlen a auf die Zahlen $F(a)$ zu übertragen.

Wenn

$$\alpha = \beta\,(\cdot)\,\gamma$$

ist, so soll α durch β teilbar heißen. Der größte gemeinsame Teiler kann vermöge der Permanenz der Beziehungen der Ungleichheit (Nr. 4) durch einen dem Euklidischen vollkommen analogen Algorithmus bestimmt werden. Hierauf baut sich nun die ganze Zahlentheorie auf (Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, vierte Auflage, Braunschweig 1894, § 16). Also läßt sich für die Zahlen $F(a)$ eine vollständige Zahlentheorie entwickeln. Im folgenden sollen mit Übergehung aller Beweise nur die Hauptpunkte dieser Theorie berührt werden, soweit sie für die Anwendung, die das Ziel der ganzen Arbeit darstellt, notwendig sind.*)

*) Eine ausführlichere Darstellung, die sich übrigens hier fast Wort für Wort einfügen ließe, findet sich in meiner in Nr. 1 zitierten Abhandlung, Nr. 11 bis 31.

11. Primzahlen. Kongruenz der Zahlen. Lineare Kongruenz. Eine Zahl $\pi\,(>\varepsilon)$, die nur sich selbst und ε zum Teiler hat, heißt eine Primzahl. Die Zerfällung in Primzahlen — im Sinne der Operation $(\cdot)$ — ist eindeutig.

Wenn $\alpha\,(-)\,\beta$ durch μ teilbar ist, so heißen α, β nach (dem Modul) μ kongruent:

$$\alpha \equiv \beta\ (\mu).$$

Die lineare Kongruenz

$$\alpha\,(\cdot)\,\xi \equiv \beta\ (\mu)$$

hat eine und nur eine Wurzel, wenn α und μ teilerfremd sind; ist dagegen der größte gemeinsame Teiler δ von α und μ größer als ε, so hat sie $\Phi(\delta)$ oder keine Wurzel, je nachdem δ in β aufgeht oder nicht.

12. Analogon des Fermatschen Satzes. Wird $\varphi(\mu) = \varphi(\Phi\,\mu)$ wo $\varphi(m)$, wie üblich, die Anzahl der zu m teilerfremden Zahlen in der Reihe $0, 1, \ldots m-1$ bedeutet, gesetzt, so ist für jedes zu μ teilerfremde α

$$\alpha^{(\varphi(\mu))} \equiv \varepsilon\ (\mu).$$

Insbesondere ist für eine Primzahl π

$$\alpha^{(\Phi(\pi)-1)} \equiv \varepsilon\ (\pi).$$

13. Reste zweiten Grades. Analogon des Eulerischen Kriteriums. Analogon des Legendreschen Symbols. Bestimmung der Reste für einen gegebenen Modul.

Je nachdem die Kongruenz

$$\xi^{(2)} \equiv \delta\ (\mu),$$

wo δ zu μ teilerfremd ist, lösbar ist oder nicht, soll δ ein Rest zweiten Grades (oder kurz Rest) oder ein Nichtrest von μ heißen.

Für den Modul η ist jede Zahl Rest; für eine größere Primzahl π als Modul ist δ Rest oder Nichtrest, je nachdem

$$\delta^{\left(\frac{\nu}{2}\right)} \equiv (\pm)\ \varepsilon\ (\pi)$$

ist; hiebei ist $r = \varphi(\pi)$ gesetzt. Diese Zahl $(\pm)\,\varepsilon$ soll durch das Symbol $\left(\frac{\delta}{\pi}\right)$ bezeichnet werden. Es gilt $\left(\frac{\delta}{\pi}\right)(\cdot)\left(\frac{\delta'}{\pi}\right)\left(\frac{\delta\delta'}{\pi}\right)$. Ist δ Rest, so hat die Kongruenz

$$\xi^{(2)} \equiv \delta\ (\pi)$$

zwei Wurzeln.

Für den Modus $\pi^{(n)}$ gelten dieselben Resultate, dagegen verlangt der Modul $\eta^{(n)}$ eine besondere Behandlung. Nach dem Modul $\eta^{(2)}$ ist ε Rest, $(-)\,\varepsilon$ Nichtrest und die Kongruenz

$$\xi^{(2)} \equiv \varepsilon\ (\eta^{(2)})$$

hat die zwei Wurzeln $(\pm)\,\varepsilon$. Nach dem Modul $\eta^{(n)}$, wo $n \geqq 3$ ist, sind alle jene und nur jene Zahlen δ Reste, die $\equiv \varepsilon\,(\eta^{(3)})$ sind und die Kongruenz

$$\xi^{(2)} \equiv \delta\ (\eta^{(n)})$$

hat in diesem Fall vier Wurzeln.

Ist endlich der Modul μ zusammengesetzt

$$\mu = \eta^{(n_0)}(\cdot)\,\pi_1^{(n_1)}(\cdot)\cdots\pi_k^{(nk)},$$

σ ist eine Zahl δ nur dann Rest von μ, wenn sie Rest von $\eta^{(n_0)}, \pi_1^{(n_1)}, \ldots \pi_k^{(nk)}$ ist und die Anzahl der Wurzeln der Kongruenz

$$\xi^{(2)} \equiv \delta\ (\mu)$$

ist in diesem Falle gleich dem Produkt der Wurzelanzahlen für die genannten Moduln.

14. Bestimmung der Moduln, von denen eine gegebene Zahl Rest ist. Ergänzungssätze und Reziprozitätssatz. Die Zahl $(-)\,\varepsilon$ ist Rest oder Nichtrest der Primzahl π, je nachdem $\pi \equiv \nu(\cdot)\,\eta^{(2)}(\pm)\,\varepsilon$ ist. Die Zahl η ist Rest oder Nichtrest der Primzahl π, je nachdem π die Form $\nu(\cdot)\,\eta^{(3)}(\pm)\,\varepsilon$ oder die Form $\nu(\cdot)\,\eta^{(3)}(\pm)\,\rho$ hat.

Sind π und ϑ zwei voneinander und von η verschiedene Primzahlen, so gilt

$$\left(\frac{\pi}{\vartheta}\right)(\cdot)\left(\frac{\vartheta}{\pi}\right) = \left[(-)\,\varepsilon\right]^{\left(\frac{1}{2}\,\varphi(\pi)\cdot\frac{1}{2}\,\varphi(\vartheta)\right)}.$$

15. Die quadratische Kongruenz. Erste Bedingung für die Lösbarkeit. Die quadratische Kongruenz wurde in Nr. 2 und 3 auf die Form

$$T\frac{x^2+x}{2} + Ux \equiv -C\,(m)$$

gebracht; aus dieser ist sofort zu sehen, daß sie nur dann lösbar ist, wenn $-C$ durch den größten gemeinsamen Teiler D von T, U, m teilbar ist, in diesem Falle ist sie mit der Kongruenz

$$\frac{T}{D} \cdot \frac{x^2 + x}{2} + \frac{U}{D} \cdot x \equiv -\frac{C}{D} \left(\frac{m}{D}\right)$$

gleichwertig; jede Wurzel dieser Kongruenz liefert D Wurzeln der ursprünglichen. Es möge daher weiterhin angenommen werden, daß T, U, m nicht alle einen gemeinsamen Teiler haben.

16. Reguläre und irreguläre Moduln. Eigenschaften der regulären Moduln. Es möge nun bei gegebenen T jede ungerade Primzahl p irregulär oder regulär genannt werden, je nachdem sie in T aufgeht oder nicht; die Primzahl 2 hingegen soll regulär heißen, wenn $T \equiv 2\,(4)$ ist, sonst immer irregulär. Ferner heiße ein Modul dann und nur dann regulär, wenn er lauter reguläre Primfaktoren enthält, sonst irregulär.

Nach einem regulären Modul ist der Bruch $\frac{2}{T}$ stets einer gewissen ganzen (übrigens zu m teilerfremden) Zahl h kongruent:

$$\frac{2}{T} \equiv h\,(m).$$

In der Tat ist T zu jedem ungeraden Primfaktor p des Moduls teilerfremd und wenn m gerade ist, so muß $\frac{T}{2}$ nach der oben gegebenen Definition ungerade sein und man hat wieder

$$\frac{1}{\frac{T}{2}} \equiv h\,(m)$$

Hieraus folgt weiter, daß nach einem regulären Modul m jede Zahl

$$F(a) = \frac{4a - T - 2U}{2T},$$

einer ganzen Zahl, ferner auch die Zahl

$$f = \frac{(T + 2U)(T + 2U - 4)}{8T}$$

einer ganzen Zahl s kongruent ist. Denn man hat

$$F(a) \equiv h\left(a - \frac{T+2U}{4}\right)$$

$$f \equiv h \cdot \frac{T+2U}{4} \cdot \left(\frac{T+2U}{4} - 1\right)$$

und der hier auftretende Nenner 4 hebt sich in dem einzigen Falle, in dem er Schwierigkeiten bereiten könnte, nämlich bei einem geraden Modul m, weg; denn in diesem Falle ist (wie vorhin)

$$T \equiv 2\,(4),$$

ferner, weil T, U, m keinen gemeinsamen Teiler haben sollen,

$$U = 1\,(2),$$

somit $\frac{T+2U}{4}$ eine ganze Zahl.

Man kann endlich schließen, daß für einen regulären Modul m die Kongruenzen

$$\alpha \equiv \beta\,(m)$$

und

$$\alpha \equiv \beta\,(\mu)$$

wo $\mu = F(m)$ ist, äquivalent sind.

Setzt man nämlich $\Phi(\alpha) = a$, $\Phi(\beta) = b$, so lautet die erste Kongruenz

$$\frac{4a - T - 2U}{2T} \equiv \frac{4b - T - 2U}{2T}\,(m),$$

kann daher durch

$$ha \equiv hb\,(m),$$

$$a \equiv b\,(m)$$

ersetzt werden; diese Kongruenz ist aber nach dem Satz in Nr. 9 mit $\alpha \equiv \beta\,(\mu)$ äquivalent.

17. Lösbarkeit einer quadratischen Kongruenz nach einem regulären Modul. Aus der Kongruenz nach dem regulären Modul m:

$$T\frac{x^2+x}{2} + Ux \equiv -C\,(m)$$

oder

$$T\frac{x^2+x}{2}+Ux+s\equiv -C+s\,(m)$$

folgt, wenn γ und ξ durch die Kongruenzen

$$\gamma\equiv -C\,(m)$$
$$\xi\equiv x\,(m)$$

bestimmt werden,

$$T\frac{\xi^2+\xi}{2}+U\xi+f\equiv\gamma+f\,(m).$$

(Der gebrochene Koeffizient $\frac{T}{2}$ macht keinerlei Schwierigkeit, da bei geradem m auch T gerade ist.) Die letzte Kongruenz kann aber auf die Form

$$\xi^{(2)}\equiv\gamma+f\,(m)$$

gebracht und statt dieser kann nach dem letzten Satz in Nr. 16

$$\xi^{(2)}\equiv\gamma+f\big((\mu=F(m)\big).$$

gesetzt werden. Also ist die Zahl

$$\gamma+f=\gamma(+)\,[f+\iota]=\gamma(+)\left[\frac{(T+2U)(T+2U-4)}{8T}-\frac{T+2U}{2T}\right]=$$

$$=\gamma(+)\frac{(T+2U)(T+2U-8)}{8T}$$

Rest zweiten Grades des Moduls μ. Dafür kann nach Nr. 9 gesagt werden, die Zahl

$$\Phi\left(\gamma(+)\frac{(T+2U)(T+2U-8)}{8T}\right)=\Phi(\gamma)+\Phi\left(\frac{(T+2U)(T+2U-8)}{8T}\right)=$$

$$=\Phi(\gamma)+\frac{1}{4}\left(2T\frac{(T+2U)(T+2U-8)}{8T}+T+2U\right)=$$

$$=\Phi(\gamma)+\frac{(T+2U)(T+2U-4)}{16}$$

sei quadratischer Rest des Moduls m. Schließlich ist

$$\Phi(\gamma)=\Phi(-C)=\frac{-2TC+T+2U}{4}\,(m).$$

Das Resultat ist also folgendes:

Die Kongruenz

$$T\frac{x^2+x}{2}+Ux+C\equiv 0\,(m).$$

ist dann und nur dann lösbar, wenn die Zahl

$$\frac{-2TC+T+2U}{4}+\frac{(T+2U)\,(T+2U-4)}{16}=$$

$$=-\frac{T}{2}\cdot C+\left(\frac{T+2U}{4}\right)^2$$

quadratischer Rest von m ist; und die Anzahl der Wurzeln ist ebenso groß wie die der Wurzeln der Kongruenz

$$z^2\equiv -\frac{T}{2}C+\left(\frac{T+2U}{4}\right)^2(m).$$

Der Ausdruck rechts stimmt, wie leicht zu sehen, mit dem vierten Teil der negativen Diskriminante der quadratischen Kongruenz überein.

18. Lösbarkeit einer quadratischen Kongruenz nach einem beliebigen Modul. Es bleibt nun noch der Fall eines beliebigen Moduls M zu untersuchen. Man denke sich von M alle irregulären Primfaktoren $q\,q',\ldots$ abgetrennt und setze

$$M=q^n\cdot q'^{n'}\ldots m.$$

Es zeigt sich nun, daß, was die Lösbarkeit und die Wurzelanzahl der Kongruenz

$$T\frac{x^2+x}{2}+Ux+C\equiv 0$$

anbelangt, sich die beiden Moduln M und m vollständig gleich verhalten. Um dies nachzuweisen, ist nur zu zeigen, daß die Kongruenz

$$T\frac{x^2+x}{2}+Ux\equiv -C\,(q^n),$$

wo q eine irreguläre Primzahl ist, stets eine und nur eine Wurzel hat.

Es sei zunächst q ungerade, $=p$. Bedeuten k und l zwei Zahlen aus der Reihe

$$0,1,2,\ldots p^n-1,$$

so folgt aus der Kongruenz

$$T\frac{k^2+k}{2}+Uk\equiv T\frac{l^2+l}{2}+Ul\,(p^n),$$

daß

$$T\left(\frac{k^2+k}{2}-\frac{l^2+l}{2}\right)+U(k-l)\equiv 0\,(p^n),$$

$$[T(k+l+1)+2\,U](k-l)\equiv 0\,p^n)$$

sein muß. Nun geht p in T, aber nicht in $2\,U$ auf (weil ja sonst T, U, m den gemeinsamen Teiler p hätten), somit ist der Faktor $T(k+l+1)+2\,U$ zum Modul p^n teilerfremd und es muß $k\equiv l$ sein, daher nach der Voraussetzung k mit l zusammenfallen. Also kommen unter den echten Resten der Zahlen

$$T\frac{x^2+x}{2}+Ux$$

alle Zahlen $0, 1, \ldots p^n-1$ je einmal vor.

Es sei jetzt $q=2$; dann ist T entweder durch 4 teilbar oder ungerade. Im ersten Fall ist der Beweis ähnlich wie vorhin. Es seien k, l zwei Zahlen aus der Reihe

$$0, 1, 2, \ldots 2^n-1;$$

aus der Kongruenz

$$T\frac{k^2+k}{2}+Uk\equiv T\frac{l^2+l}{2}+Ul\,(2^n)$$

folgt

$$\left[\frac{T}{2}(k+l+1)+U\right](k-l)\equiv 0\,(2^n);$$

der Faktor $\frac{T}{2}(k+l+1)+U$ ist ungerade, weil $\frac{T}{2}$ gerade, U ungerade ist, also muß $k-l$ durch 2^n teilbar, mithin $k=l$ sein.

Ist dagegen T ungerade, so mögen k, l zwei Zahlen aus der Reihe

$$0, 1, 2, \ldots 2^{n+1}-1$$

sein. Aus der Kongruenz

$$T\frac{k^2+k}{2}+Uk\equiv T\frac{l^2+l}{2}+Ul\,(2^n)$$

folgt

$$[T(k+l+1)+2\,U](k-l)\equiv 0\,(2^{n+1}).$$

Da die Zahlen T und $T+2U$ beide ungerade sind, so hat die Kongruenz

$$T \cdot g \equiv T + 2U \,(2^{n+1})$$

eine und nur eine Lösung g, die überdies eine ungerade Zahl ist. Statt der letzten Kongruenz kann nun auch die Kongruenz

$$[k + l + g]\,(k - l) \equiv 0 \,(2^{n+1})$$

eingeführt werden. Da die Differenz der beiden Faktoren links $2l + g$, also ungerade ist, so kann sie nur erfüllt werden, indem einer der Faktoren durch den ganzen Modul 2^{n+1} teilbar ist. Es muß also entweder

$$k \equiv l \text{ oder } k \equiv -l - g \,(2^{n+1})$$

sein. Diese beiden Fälle sind stets streng geschieden, weil

$$l \not\equiv -l - g \,(2)$$

ist. Mithin erhält man, wenn in

$$T\frac{x^2 + x}{2} + Ux$$

alle Zahlen von 0 bis $2^{n+1} - 1$ eingesetzt werden, nach dem Modul 2^n jede Zahl genau zweimal, also ist jede Kongruenz

$$T\frac{x^2 + x}{2} + Ux + C \equiv 0 \,(2^n)$$

auflösbar.

Die Zählung der Wurzeln ist freilich in diesem Falle nicht in der gewöhnlichen Art durchführbar. In der Tat, ist x eine Wurzel der Kongruenz

$$T\frac{x^2 + x}{2} + Ux + C \equiv 0 \,(2^n),$$

so sind alle andern nicht, wie es sonst der Fall ist in der Formel

$$x + 2^n \cdot U,$$

sondern in den beiden Formeln

$$x + 2^{n+1} \cdot U, \quad -x - g + 2^{n+1} \cdot U$$

enthalten. Man kann nur sagen, daß sich unter je 2^n aufeinanderfolgenden Zahlen durchschnittlich eine Wurzel befindet; allerdings bekommt man durch Wahl der Teilungspunkte

$$\ldots, -\frac{g}{2} - 2^n, -\frac{g}{2}, -\frac{g}{2} + 2^n, -\frac{g}{2} + 2 \cdot 2^n, \ldots$$

Intervalle, die je eine Wurzel enthalten, aber die Wurzel steht erst in jedem zweiten der Intervalle wieder an derselben Stelle, während in den dazwischenliegenden Intervallen die Anordnung genau entgegengesetzt ist. Der Grund dieser Erscheinung liegt darin, daß die Koeffizienten der quadratischen Kongruenz $A = \frac{T}{2}$ und $B = \frac{T}{2} + U$ den Nenner 2 aufweisen, wenn auch die Formel $Ax^2 + Bx + C$ für alle ganzzahligen Werte von x selbst ganzzahlige Werte annimmt.