Kapitel 2. Kongruenzen

Wie sich in Kap. 1 gezeigt hat, ist der Teilbarkeitsbegriff für die Zahlentheorie fundamental. Die dort begonnenen Untersuchungen über Teilbarkeit ganzer Zahlen werden jetzt fortgesetzt, allerdings aus einem anderen Blickwinkel und unter Verwendung des neuen Begriffs der Kongruenz.

Obwohl ihrer ursprünglichen Definition nach eine Aussage über Teilbarkeit ganzer Zahlen, ist eine Kongruenzaussage mehr als nur eine nützliche Formulierung. Ihr Wert liegt hauptsächlich darin, daß man mit Kongruenzen bequem formal operieren kann, genauer gesagt, daß man mit ihnen weitgehend wie mit Gleichungen rechnen kann.

Historisch wurde die Bedeutung des Kongruenzbegriffs für die Zahlentheorie zuerst von GAUSS voll erkannt, der ihn ganz an den Anfang seiner *Disquisitiones Arithmeticae* stellte. Daran anschließend hat er eine sehr weitgehende und reichhaltige Theorie der Kongruenzen entwickelt, die sofort allgemein akzeptiert und zu einem bleibenden Bestandteil der Zahlentheorie wurde. Die wichtigsten Sätze dieser Theorie kommen in Kap. 2 (und im größten Teil von Kap. 3) zur Darstellung.

Einerseits werden dabei sehr viel ältere, klassische Teilbarkeitsergebnisse nach dem GAUSSschen Vorgang in der neuen Kongruenzensprache viel einfacher formuliert und bewiesen. Hierher gehört der in § 2 zu besprechende, vor mindestens eineinhalb Jahrtausenden in China und Indien in speziellen Varianten bekannte chinesische Restsatz. Auch die in § 3 darzustellenden zentralen Sätze von FERMAT, EULER und WILSON sind hier zu nennen. Diese finden z.B. bei Primzahltests Anwendung, in neuerer Zeit in der Theorie der geheimen Nachrichtenübermittlung.

Andererseits werden in Kap. 2 Resultate diskutiert, die zuerst von GAUSS selbst entdeckt worden sind und die sich (in neuerer Terminologie) vorwiegend mit der Struktur der primen Restklassengruppen auseinandersetzen. Genau wann diese zyklisch sind, wird in § 5 vollständig geklärt. Dort wird auch der Spezialfall eines allgemeineren gruppentheoretischen Satzes bewiesen, wonach prime

Restklassengruppen stets isomorph dem direkten Produkt geeigneter zyklischer Gruppen von Primzahlpotenzordnung sind.

§ 1. Lineare Kongruenzen

1. Definition der Kongruenz, elementare Eigenschaften. Seien $m \neq 0$, a, b ganze Zahlen. Man nennt a *kongruent (zu)* b *modulo* m genau dann, wenn $m|(a-b)$ gilt; man schreibt dies als

$$a \equiv b \pmod{m}.$$

Aus Satz 1.1.2(i), (ii), (ix) folgt insbesondere

r) $a \equiv a \pmod{m}$,

s) $a \equiv b \pmod{m} \quad \Rightarrow \quad b \equiv a \pmod{m}$,

t) $a \equiv b \pmod{m}, \quad b \equiv c \pmod{m} \quad \Rightarrow \quad a \equiv c \pmod{m}$.

Hieraus sieht man bereits, daß die Relation *kongruent modulo* m eine Äquivalenzrelation auf $\mathbb{Z}$ ist. Damit zerlegt sie $\mathbb{Z}$ in disjunkte Klassen, die sogenannten *Restklassen modulo* m. Insbesondere kann man wegen der Symmetrieregel s) einfachere Sprechweisen einführen, etwa "a und b sind modulo m kongruent" oder ähnlich; im Fall $m \not| (a-b)$ sagt man, a und b seien modulo m inkongruent, und schreibt $a \not\equiv b \pmod{m}$.

Aus der gegebenen Kongruenzdefinition folgen einige leichte Rechenregeln, die nachfolgend zusammengestellt seien.

Satz. *Sind a, b, c, d und $m \neq 0$ ganz, so gilt*

(i) $a \equiv b \pmod{m}, \quad c \equiv d \pmod{m} \quad \Rightarrow \quad a + c \equiv b + d \pmod{m}$;

(ii) $a \equiv b \pmod{m}, \quad c \equiv d \pmod{m} \quad \Rightarrow \quad ac \equiv bd \pmod{m}$;

(iii) $a \equiv b \pmod{m} \quad \Rightarrow \quad a^i \equiv b^i \pmod{m}$ *für alle* $i \in \mathbb{N}_0$;

(iv) $a \equiv b \pmod{m}, \quad f \in \mathbb{Z}[X] \quad \Rightarrow \quad f(a) \equiv f(b) \pmod{m}$.

Sind überdies alle $m_1, \ldots, m_k$ ganz und von Null verschieden und ist $m := \mathrm{kgV}(m_1, \ldots, m_k)$, so gilt

(v) $a \equiv b \pmod{m_\kappa}$ *für* $\kappa = 1, \ldots, k \quad \Leftrightarrow \quad a \equiv b \pmod{m}$.

Beweis. Indem man Satz 1.1.2(ix) mit $n_1 := a - b$, $n_2 := c - d$, $\ell_1 := 1$, $\ell_2 := 1$ anwendet, erhält man (i). Erneut nach (ix) jenes Satzes folgt aus $m|(a-b)$ bzw. $m|(c-d)$ die Gültigkeit von $m|(ac-bc)$ bzw. $m|(bc-bd)$, also $m|(ac-bd)$. Unter Zuhilfenahme von (ii) gewinnt man (iii) durch vollständige Induktion nach i; (iv) folgt aus den drei ersten, schon bewiesenen Regeln unmittelbar. Für (v) überlegt man, daß $m_\kappa|(a-b)$ für $\kappa = 1, \ldots, k$ nach dem Charakterisierungssatz 1.2.11 für das kgV bereits $m|(a-b)$ nach sich zieht; ist umgekehrt diese Teilbarkeitsbedingung erfüllt, so folgt aus $m_\kappa|m$ mittels Satz 1.1.2(vii) die Gültigkeit von $m_\kappa|(a-b)$ für $\kappa = 1, \ldots, k$. □

Bemerkung. Die Kongruenzschreibweise wird hier zur bequemen Notation von Teilbarkeitsaussagen eingeführt. Dementsprechend folgten die im obigen Satz zusammengestellten Rechenregeln für Kongruenzen leicht aus den in Satz 1.1.2 aufgeführten Regeln für den Umgang mit Teilbarkeitsbeziehungen. Wie obiger Satz belegt, kann man mit Kongruenzen *weitgehend* so rechnen (d.h. addieren, subtrahieren und multiplizieren), wie man dies von Gleichungen her gewöhnt ist. Wegen dieser starken Analogie hat GAUSS das Zeichen $\equiv$ für *kongruent* in Anlehnung an das übliche Gleichheitszeichen gewählt, vgl. hierzu auch die historischen Bemerkungen in 9. Diese große formale Ähnlichkeit mit den Gleichungen macht die Kongruenz zu einem überaus vorteilhaften technischen Hilfsmittel, das sich im folgenden noch oft bewähren wird, dessen Wirksamkeit sogleich im nächsten Abschnitt – vor der weiteren Entwicklung der allgemeinen Theorie – an einem Beispiel demonstriert werden soll.

2. Fermat–Zahlen. Darunter versteht man die Zahlen

$$F_n := 2^{2^n} + 1, \qquad n = 0, 1, \ldots.$$

Die fünf kleinsten sind 3, 5, 17, 257, 65537 und dies sind jeweils Primzahlen. FERMAT sprach 1640 in einem Brief an B. FRENICLE DE BESSY die Vermutung aus, daß auch die weiteren F_n Primzahlen seien. Er räumte aber ein, keinen Beweis für seine Behauptung zu besitzen, die wenig später von M. MERSENNE übernommen wurde. In einer Korrespondenz mit EULER während der Jahre 1729/30 lenkte GOLDBACH dessen Aufmerksamkeit auf FERMATs erwähnte Vermutung, die 1732 von EULER (Opera Omnia Ser. 1, II, 1–5) widerlegt werden konnte. EULER zeigte, daß F_5 *zusammengesetzt* ist, genauer, daß es von der Primzahl 641 geteilt wird. Ohne Taschenrechner, dafür mit dem Hilfsmittel der Kongruenzen, geht dies wie folgt:

Indem man zunächst Satz 1(iv) mit $f := (X-1)^4$ anwendet, folgt aus $5 \cdot 2^7 = 641 - 1$

$$5^4 \cdot 2^{28} = (641-1)^4 \equiv (-1)^4 = 1 \pmod{641}.$$

Andererseits ergibt sich aus $641 = 2^4 + 5^4$ die Kongruenz $5^4 \equiv -2^4 \pmod{641}$ und diese in die vorher erhaltene eingetragen führt zu

$$1 - F_5 = -2^4 \cdot 2^{28} \equiv 1 \pmod{641},$$

was $641 | F_5$ besagt. Tatsächlich hat EULER mit $F_5 = 641 \cdot 6700417$ sogar die Primfaktorzerlegung von F_5 gefunden.

Der Leser wird sich mit Recht fragen, wieso man gerade darauf kommt, die Teilbarkeit von F_5 durch 641 für möglich zu halten (und dann zu beweisen); dies wird durch Satz 3.2.11 erklärt werden.

In der Literatur finden sich mittlerweile eine ganze Reihe notwendiger und hinreichender Bedingungen dafür, daß F_n Primzahl ist. Allerdings ist bis heute noch keine Primzahl F_n mit $n \geq 5$ gefunden worden; man vergleiche hierzu auch die in 3.2.11 mitgeteilten Resultate.

Interessant ist aber, daß man die FERMAT–Zahlen für einen weiteren Beweis des EUKLIDschen Satzes 1.1.4 benützen kann, der ebenfalls nur auf die Primzahldefinition und auf einige der Regeln aus Satz 1.1.2 zurückgreift. EUKLIDs Satz ist eine direkte Konsequenz aus folgendem

Satz. *Für voneinander verschiedene ganze, nichtnegative m und n sind F_m und F_n zueinander teilerfremd.*

Beweis. Man definiert $G_n := 2^{2^n} - 1 = F_n - 2$ für $n = 0, 1, \ldots$ und sieht sofort $F_n G_n = G_{n+1}$ für dieselben n, was induktiv zu

$$G_n \prod_{\nu=n}^{m-1} F_\nu = G_m \quad \text{für } 0 \leq n \leq m \tag{1}$$

führt. Sei jetzt d eine natürliche, F_m und F_n teilende Zahl und o.B.d.A. sei $n < m$. Nach (1) wird G_m von d geteilt und wegen $F_m - G_m = 2$ muß dann d in 2 aufgehen. Wegen der Ungeradheit aller FERMAT–Zahlen muß $d = 1$ gelten. □

Bemerkung. Die FERMAT–Zahlen spielen z.B. auch in der Algebra eine gewisse Rolle, und zwar bei der Frage nach der Konstruierbarkeit des regulären h–Ecks bei gegebenem Umkreisradius allein mittels Zirkel und Lineal. GAUSS (*Disquisitiones Arithmeticae*, Artt. 335–366) hat gezeigt, daß diese Konstruktion unter den genannten Nebenbedingungen genau dann durchführbar ist, wenn h die Form $2^{n_0} F_{n_1} \cdot \ldots \cdot F_{n_r}$ hat mit $n_0, \ldots, n_r \in \mathbb{N}_0$ und paarweise verschiedenen $n_1, \ldots, n_r$, so daß sämtliche FERMAT–Zahlen F_{n_ρ} Primzahlen sind; dabei ist $r = 0$ erlaubt. Einige historische Anmerkungen zu dieser GAUSSschen Entdeckung folgen in 9.

3. Kürzungsregel. Regel (ii) von Satz 1 beinhaltet insbesondere: Wenn $a \equiv b \pmod{m}$ gilt, so auch $ac \equiv bc \pmod{m}$ bei beliebigem ganzem c. Daß die umgekehrte Schlußweise nicht immer richtig zu sein braucht, belegt folgendes Beispiel: Es ist zwar $9 \cdot 5 = 45 \equiv 15 = 3 \cdot 5 \pmod{10}$, aber nicht $9 \equiv 3 \pmod{10}$. Wieviel in dieser Richtung tatsächlich noch gesichert werden kann, entnimmt man folgender

Kürzungsregel. *Für ganze $m \neq 0$, a, b, c gilt die Äquivalenz*

$$ac \equiv bc \pmod{m} \quad \Leftrightarrow \quad a \equiv b \pmod{\frac{m}{(c,m)}}.$$

Beweis. Setzt man $c' := c/(c,m)$, $m' := m/(c,m)$, so sind c', m' nach Proposition 1.2.5(vii) teilerfremd. Wegen $ac \equiv bc \pmod{m} \Leftrightarrow m|(a-b)c \Leftrightarrow m'|(a-b)c'$ folgt dann $m'|(a-b)$ ($\Leftrightarrow a \equiv b \pmod{m'}$) aus der letzten Teilbarkeitsbedingung, wenn man Satz 1.2.6(i) investiert. Die umgekehrte Implikation der Kürzungsregel ist wegen $m|(c,m)\cdot(a-b) \Rightarrow m|c(a-b)$ trivial. □

Besonders herausgestellt sei noch der Fall der Kürzungsregel, wo m Primzahl ist.

Korollar. *Ist p eine Primzahl, so gilt für ganze a, b, c mit $p \nmid c$*

$$ac \equiv bc \pmod{p} \quad \Leftrightarrow \quad a \equiv b \pmod{p}.$$

4. Vollständige Restsysteme. Nach Satz 1.1.2(ii) sind die beiden Kongruenzen $a \equiv b \pmod{m}$ und $a \equiv b \pmod{-m}$ gleichbedeutend. Daher darf o.B.d.A. *im folgenden stets der Modul m als natürliche Zahl vorausgesetzt* werden. (Da zwei beliebige ganze Zahlen nach Satz 1.1.2(iii) modulo 1 stets kongruent sind, kann bei Bedarf noch o.B.d.A. $m \geq 2$ angenommen werden.)

Als nächstes soll eine äquivalente Formulierung des Kongruenzbegriffs gegeben werden. Sei für ganze n_1, n_2

$$n_1 \equiv n_2 \pmod{m}. \tag{1}$$

Nach dem Divisionsalgorithmus 1.2.2 gibt es ganze a_1, b_1, a_2, b_2, so daß

$$n_i = a_i m + b_i \quad \text{mit} \quad 0 \leq b_i < m \quad \text{für} \quad i = 1, 2$$

gilt. Wegen (1) bedeutet dies $m|(b_1 - b_2)$; wegen $|b_1 - b_2| < m$ und Satz 1.1.2(iv) muß $b_1 = b_2$ sein. Man hat also die

Proposition. *Sind die ganzen Zahlen n_1, n_2 modulo m kongruent, so lassen sie bei Division durch m (gemäß dem in 1.2.2 beschriebenen Algorithmus) dieselben Reste. Die Umkehrung gilt ebenfalls.*

Damit ist offenbar jede ganze Zahl zu genau einer Zahl der Menge

$$S_m := \{0, 1, \ldots, m-1\}$$

modulo m kongruent. Diesen Sachverhalt bringt man zum Ausdruck, indem man sagt, S_m sei *das kleinste nichtnegative Restsystem modulo m.*

Allgemeiner heißt jede Menge von m ganzen Zahlen, die paarweise inkongruent modulo m sind, ein *vollständiges Restsystem modulo m.* Nach der in 1 gegebenen Erklärung ist ein solches System nichts anderes als ein vollständiges Repräsentantensystem der Restklassen modulo m. Neben S_m ist ein anderes spezielles vollständiges Restsystem modulo m bisweilen im Gebrauch, das sogenannte *absolut kleinste Restsystem modulo m*, das ist die Menge S_m^* der ganzen Zahlen, die größer als $-\frac{1}{2}m$, aber kleiner oder gleich $\frac{1}{2}m$ sind. Z.B. ist danach $S_5^* = \{-2, -1, 0, 1, 2\}$ und $S_6^* = \{-2, -1, 0, 1, 2, 3\}$.

5. Lineare Kongruenzen. Sind a, c und $m > 0$ ganze Zahlen, so bezeichnet man

$$aX \equiv c \pmod{m} \tag{1}$$

als *lineare Kongruenz* (in *einer* Unbestimmten X). Genügt ein ganzes x der Bedingung $ax \equiv c \pmod{m}$, so sagt man, x löse (1). Jedes ganze, zu x modulo m kongruente x^* löst (1) ebenfalls; doch sind x, x^* im Sinne des Kongruenzenrechnens als nicht wesentlich voneinander verschiedene Lösungen anzusehen. Die Eigenschaft, (1) zu lösen oder nicht, ist also eine Eigenschaft, die einer ganzen Restklasse modulo m zukommt. Dementsprechend definiert man als *Lösungsanzahl von* (1) *modulo m* die Anzahl der modulo m inkongruenten ganzen x, die (1) lösen; dies ist nichts anderes als die Anzahl der in einem festen vollständigen Restsystem modulo m enthaltenen Lösungen von (1).

Im folgenden Satz wird die Lösungsanzahl von (1) modulo m bestimmt.

Satz. *Die Kongruenz (1) ist lösbar genau dann, wenn $(a, m)|c$ gilt; in diesem Falle ist die Lösungsanzahl von (1) modulo m gleich (a, m). Sind insbesondere a, m teilerfremd, so ist (1) modulo m eindeutig lösbar.*

Beweis. Ist (1) lösbar, so gibt es ganze x, y, so daß $ax + my = c$ gilt, woraus $(a, m)|c$ nach Satz 1.3.2 folgt. Sei nun umgekehrt diese Teilbarkeitsbedingung erfüllt. Mit $a' := a/(a, m)$, $c' := c/(a, m)$ und $m' := m/(a, m)$ sind a',

m' nach Proposition 1.2.5(vii) zueinander teilerfremd und somit gilt nach der Kürzungsregel bei ganzem x

$$ax \equiv c \pmod{m} \quad \Leftrightarrow \quad a'x \equiv c' \pmod{m'}. \tag{2}$$

Durchläuft nun x ein vollständiges Restsystem modulo m', so tut dies auch das Produkt $a'x$; denn dies sind ebenfalls m' ganze Zahlen, die modulo m' inkongruent sind: $a'x_1 \equiv a'x_2 \pmod{m'}$ impliziert ja $x_1 \equiv x_2 \pmod{m'}$, erneut nach der Kürzungsregel. Daher ist die Kongruenz rechts in (2) modulo m' eindeutig lösbar und *die* in $S_{m'}$ (vgl. 4) gelegene Lösung heiße x_0. Nun bestimmt man, genau welche der Zahlen $x_0 + tm'$, $t \in \mathbb{Z}$, in S_m liegen. Offenbar sind dies exakt die folgenden:

$$x_0, x_0 + m', \ldots, x_0 + ((a, m) - 1)m'.$$

Nach (2) genügen diese (1), womit der Satz bewiesen ist. □

Bemerkung. Ist a ganz und *zum Modul m teilerfremd*, so ist insbesondere die Kongruenz $aX \equiv 1 \pmod{m}$ eindeutig modulo m lösbar. Jedes ganze a' mit $aa' \equiv 1 \pmod{m}$ gehört daher einer festen, durch a bestimmten Restklasse modulo m an und kann daher als *die Inverse von a modulo m* bezeichnet werden; offenbar ist jedes solche a' zu m teilerfremd. Auch $a'X \equiv 1 \pmod{m}$ ist eindeutig modulo m lösbar und jede ganze Lösung liegt in derselben Restklasse modulo m wie das ursprüngliche a. Zwei ganze Zahlen, a, a' heißen *zueinander reziprok modulo m*, falls $aa' \equiv 1 \pmod{m}$ gilt.

6. Bruchschreibweise. Wie in Satz 5 gesehen, hat die Kongruenz 5(1) *bei teilerfremden a, m* genau eine Lösung modulo m, die man manchmal in der üblichen Form eines Bruchs, also $\frac{c}{a}$, aufschreibt. Damit werden aber nun *nicht* rationale Zahlen oder gar Kongruenzen zwischen solchen eingeführt, sondern man muß sich – vor allem am Anfang – die Interpretation dieser symbolischen Schreibweise genau vor Augen halten.

Wenn man dies tut, besteht der gewonnene Vorteil der Schreibweise darin, daß man mit ihrer Hilfe sehr bequem rechnen kann. Dies werde etwa an der Kongruenz $8X \equiv -1 \pmod{13}$ verdeutlicht, deren Lösung als $\frac{-1}{8}$ symbolisch hingeschrieben werden kann. Will man nun wissen, für welches $r \in S_{13}$ das Symbol $\frac{-1}{8}$ steht, geht man etwa so vor:

$$\frac{-1}{8} \equiv \frac{2 \cdot 13 - 1}{8 - 13} = -5 \pmod{13}.$$

$\frac{-1}{8}$ ist also modulo 13 als 8 zu interpretieren. Wie hier die Durchführung der Rechnung zeigt, kann man also im "Zähler" und "Nenner" beliebige Vielfache des Moduls (hier 13) addieren oder subtrahieren. Dies sieht man sofort ein, wenn man auf die Bedeutung des Symbols $\frac{-1}{8}$ zurückgeht. Danach ist $-5r \equiv 8r \equiv -1 \equiv 25 \pmod{13}$ und in $-5r \equiv 25 \pmod{13}$ darf nach der Kürzungsregel durch -5 gekürzt werden, was zu $r \equiv -5 \pmod{13}$ führt.

Obwohl dies aus dem bisher Gesagten bereits klar ist, sei nochmals ausdrücklich darauf hingewiesen, daß einem "Bruch" wie $\frac{-1}{8}$ keine *absolute* Bedeutung zukommt, sondern daß er stets *relativ* zu einem ganz bestimmten (zum "Nenner" teilerfremden) Modul interpretiert werden muß. So ist $\frac{-1}{8}$ z.B. modulo 11 als 4 zu interpretieren.

Bemerkung. Am Ende von 1 wurde angemerkt, daß man mit Kongruenzen weitgehend wie mit Gleichungen rechnen kann, da man Kongruenzen (nach demselben Modul) zueinander addieren, voneinander subtrahieren und miteinander multiplizieren kann. Nun kann man noch hinzufügen, daß man auch Divisionen wie gewohnt durchführen kann, vorausgesetzt der Divisor ist zum Modul teilerfremd. Ist der Modul insbesondere eine Primzahl, so nimmt die soeben formulierte Ausnahmebedingung eine besonders einfache Form an: Bei Primzahlmoduln dürfen auch Divisionen wie gewohnt ausgeführt werden, vorausgesetzt, der Divisor ist nicht kongruent Null nach dem Modul.

7. Restklassenring. In diesem und dem folgenden Abschnitt werden die bisherigen Entwicklungen über Kongruenzen vom algebraischen Standpunkt aus betrachtet. Ist m eine natürliche Zahl, so definiert man die (von m abhängige) Abbildung ψ von $\mathbb{Z}$ in die Menge der Restklassen modulo m dadurch, daß man jedem $a \in \mathbb{Z}$ diejenige Restklasse $\psi(a)$ zuordnet, der a angehört. Danach ist $a \equiv a' \pmod{m} \Leftrightarrow \psi(a) = \psi(a')$ klar; nach den Feststellungen in 4 hat $\psi(\mathbb{Z})$ genau m Elemente. In der Menge $\psi(\mathbb{Z})$ aller Restklassen modulo m definiert man sodann zwei Verknüpfungen $+$ und $\cdot$ durch folgende Vorschriften:

$$\psi(a) + \psi(b) := \psi(a+b) \quad \text{bzw.} \quad \psi(a) \cdot \psi(b) := \psi(ab) \tag{1}$$

für alle $a, b \in \mathbb{Z}$; dabei deutet das $+$ in $a+b$ auf die gewöhnliche Addition in $\mathbb{Z}$ hin. Daß diese Definitionen sinnvoll sind, ist eine leichte Konsequenz aus Satz 1(i), (ii). Da die Abbildung ψ des Integritätsrings $\mathbb{Z}$ auf $(\psi(\mathbb{Z}), +, \cdot)$ nach (1) ein Homomorphismus ist, ist $(\psi(\mathbb{Z}), +, \cdot)$ ein kommutativer Ring, der *Restklassenring modulo m* heißt. Sein Null– bzw. Einselement ist $\psi(0)$ bzw. $\psi(1)$; genau dann ist $\psi(0) \neq \psi(1)$, wenn $m \geq 2$ ist. Man hat nun folgenden

Satz. *Der Restklassenring modulo m ist genau dann ein Körper, wenn m Primzahl ist.*

Beweis. Der Fall $m = 1$ ist vorab behandelt; sei jetzt $m \geq 2$. Ist m zusammengesetzt, also $m = m_1 m_2$ mit ganzen m_1, m_2, die größer als 1 sind, so ist $\psi(0) = \psi(m) = \psi(m_1) \cdot \psi(m_2)$ nach (1). Wegen $0 < m_1, m_2 < m$ ist weder $\psi(m_1)$ noch $\psi(m_2)$ gleich dem Nullelement des Restklassenrings modulo m und also hat dieser Nullteiler. Ist jedoch m eine Primzahl, so sind nach (1) die Gleichungen $\psi(0) = \psi(m_1) \cdot \psi(m_2)$ und $\psi(0) = \psi(m_1 m_2)$ miteinander äquivalent und die letztere besagt $m | m_1 m_2$. Da m Primzahl ist, führt dies mit dem Charakterisierungs–Satz 1.2.7 zu $m | m_i$ für eines der $i = 1, 2$ und so ist $\psi(m_i) = \psi(0)$ für das entsprechende i. Der Restklassenring modulo m ist also für Primzahlen nullteilerfrei, insgesamt also ein Integritätsring; da dieser endlich ist, ist er nach einem einfachen Ergebnis der Algebra ein Körper. □

Man schreibt den Restklassenring modulo m als $\mathbb{Z}_m$ oder als $\mathbb{Z}/m\mathbb{Z}$. Die letztere Notation erinnert besser daran, daß der hier diskutierte Restklassenring modulo m Spezialfall einer aus der Algebra wohlbekannten Begriffsbildung ist, nämlich des Restklassenrings R/J eines kommutativen Rings R (hier $\mathbb{Z}$) nach einem Ideal $J \subset R$ (hier dem Hauptideal $m\mathbb{Z}$).

8. Prime Restklassengruppe. Ist a eine ganze, zu m teilerfremde Zahl, so sind für alle ganzen t auch m und $a+tm$ zueinander teilerfremd nach Proposition 1.2.5(v). Die Eigenschaft einer ganzen Zahl, zum Modul m teilerfremd zu sein, kommt also sogleich der ganzen Restklasse modulo m zu, in der die Zahl liegt. Eine Restklasse modulo m, deren jedes Element zu m teilerfremd ist, heißt eine *prime* (oder auch *teilerfremde*) *Restklasse modulo m*.

Um sämtliche verschiedenen primen Restklassen modulo m zu bestimmen, braucht man nur aus einem vollständigen Restsystem modulo m genau die zu m teilerfremden Zahlen herauszusuchen; diese müssen schon alle verschiedenen primen Restklassen modulo m repräsentieren. Bedient man sich dabei am bequemsten des kleinsten nichtnegativen Restsystems S_m modulo m aus 4, so enthält dieses nach der Definition der EULERschen Funktion φ in 1.4.11 genau $\varphi(m)$ zu m teilerfremde Zahlen; damit gibt es genau $\varphi(m)$ verschiedene prime Restklassen modulo m. Diese können von jedem System von $\varphi(m)$ paarweise modulo m inkongruenten, zu m teilerfremden ganzen Zahlen repräsentiert werden; jedes solche System heißt ein *primes Restsystem modulo m*. Z.B. bildet $\{1, 5, 7, 11\}$ ein primes Restsystem modulo 12.

Satz. *Die Menge der primen Restklassen modulo m bildet bezüglich der in 7 erklärten Verknüpfung $\cdot$ eine abelsche Gruppe, die sogenannte prime Restklassengruppe $\mathbb{Z}_m^*$ modulo m.*

Beweis. Sind a, b ganz und zu m teilerfremd, so ist nach Korollar 1.2.6 auch ab zu m teilerfremd. Anders gesagt: Sind $\psi(a)$, $\psi(b)$ prime Restklassen modulo m, so ist nach der zweiten Definition von 7(1) auch $\psi(a)\cdot\psi(b)$ eine prime Restklasse modulo m. Daher ist die im Satz genannte Menge gegenüber $\cdot$ abgeschlossen; außerdem gelten bezüglich dieser Verknüpfung Assoziativ– und Kommutativgesetz nach dem Beweis in 7. Sind weiter a, c ganz und zu m teilerfremd, so ist die nach Satz 5 modulo m eindeutig bestimmte Lösung von 5(1) ebenfalls zu m teilerfremd. Dies ist gleichbedeutend damit, daß die Gleichung

$$\psi(a)\cdot Y = \psi(c) \tag{1}$$

unter den genannten Bedingungen eine eindeutige Lösung hat, die wieder eine prime Restklasse modulo m ist, was den Satz beweist. □

Bemerkungen. 1) Wie gesehen ist die Ordnung der Gruppe $\mathbb{Z}_m^*$ gleich $\varphi(m)$. Im Falle eines Primzahlmoduls p ist diese Gruppe nichts anderes als $\mathbb{Z}_p^\times$, die multiplikative Gruppe des Körpers $\mathbb{Z}_p$.

2) Jetzt kann auch die in der Bemerkung zu 5 vereinbarte Redeweise, *jedes* dortige $a' \in \mathbb{Z}$ als *die* Inverse von a modulo m zu bezeichnen, voll akzeptiert werden: Gemeint ist damit jedes Element derjenigen primen Restklasse modulo m, die zu $\psi(a)$ in $\mathbb{Z}_m^*$ bezüglich $\cdot$ invers ist. Man beachte, daß $\psi(1)$ ersichtlich das Einselement der Gruppe $\mathbb{Z}_m^*$ ist.

3) Der Leser möge zur Übung nachweisen, daß $\mathbb{Z}_m^*$ genau die Einheitengruppe $E(\mathbb{Z}_m)$ des Restklassenrings $\mathbb{Z}_m$ modulo m ist, falls $m \geq 2$ gilt.

4) Es hat sich weitgehend eingebürgert, die Restklasse modulo m, der $a \in \mathbb{Z}$ angehört, mit $\overline{a}$ (anstelle von $\psi(a)$) zu notieren; $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ sind also sämtliche verschiedenen Restklassen modulo m.

9. Historische Anmerkungen. GAUSS beginnt seine *Disquisitiones Arithmeticae* mit der Erklärung "Si numerus a numerorum b, c differentiam metitur, b et c *secundum a congrui* dicuntur, sin minus *incongrui*: ipsum a *modulum* appellamus." In Art. 2 fährt er dann fort "numerorum congruentiam hoc signo, $\equiv$, in postero denotabimus, modulum ubi opus erit in clausulis adiungentes." In der Fußnote zu Art. 2 fügt er schließlich an: "Hoc signum propter magnam ana-

logiam quae inter aequalitatem atque congruentiam invenitur adoptavimus."*)

Nach dieser Festlegung der Terminologie entwickelte GAUSS a.a.O. sofort sehr weitgehend seine Theorie der Kongruenzen, die bald zu einem überaus wichtigen und bleibenden Bestandteil der Zahlentheorie werden sollte. Abgesehen vom Kongruenzenbegriff der Geometrie wurde hier, historisch erstmalig, rein formal mit einer Äquivalenzrelation operiert.

Es soll jedoch nicht unerwähnt bleiben, daß sich der zahlentheoretische Begriff der Kongruenz – eben so bezeichnet – vor GAUSS bereits ab 1730 in Briefen findet, die GOLDBACH an EULER geschrieben hat. GOLDBACH verwendet anstelle von $\equiv$ das Symbol $\perp\!\!\!\perp$; allerdings blieb bei ihm im Vergleich zu GAUSS der Kongruenzkalkül noch ganz in den Anfängen stecken.

Noch einige Worte zu der in der Bemerkung zu 2 angeschnittenen Frage nach der geometrischen Konstruierbarkeit des regulären h–Ecks. Explizite *geometrische* Konstruktionsverfahren des regelmäßigen h–Ecks für $h = 3, 5, 15$ (und damit auch für Vielfache, die Potenzen von 2 sind) waren bereits den Griechen wohlbekannt; Beschreibungen finden sich z.B. bei EUKLID (*Elemente* IV, §§ 2, 11, 16). GAUSS führte a.a.O. seinen Konstruierbarkeitsbeweis rein *algebraisch*. In Art. 354 gab er exemplarisch sämtliche (quadratischen) Gleichungen an, die für das regelmäßige 17–Eck nacheinander in geometrische Konstruktionen zu übersetzen blieben. Dieselbe Arbeit leisteten für das reguläre 257–Eck F.J. RICHELOT (J. Reine Angew. Math. *9*, 1–26 (1832)) bzw. J. HERMES für das reguläre 65537–Eck. Das in zehn Jahren entstandene, aber nie publizierte Werk von HERMES ist schwerer zugänglich und mit einem Hauch des Ungewöhnlichen behaftet: Das etwa 10000 handgeschriebene Seiten umfassende Manuskript wurde als Dissertation 1894 der Universität Königsberg in einem Koffer übergeben, der beide Weltkriege überstand und heute an der Universität Göttingen verwahrt wird.

§ 2. Simultane lineare Kongruenzen

1. Reduktion des Problems. Sind für $\kappa = 1, \ldots, k$ die Zahlen a_κ^*, c_κ^* und $m_\kappa^* > 0$ ganz, so wird nun in Verallgemeinerung von 1.5(1) ein System von k

*) ("Wenn die Zahl a in der Differenz der Zahlen b, c aufgeht, heißen b und c *nach a kongruent*, andernfalls *inkongruent*; a selbst nennen wir den *Modul*." — "Die Kongruenz von Zahlen notieren wir im folgenden mit dem Symbol $\equiv$; wenn nötig, fügen wir den Modul in Klammern an." — "Dieses Zeichen haben wir wegen der großen Ähnlichkeit gewählt, die zwischen Gleichung und Kongruenz besteht.")

linearen Kongruenzen in einer Unbestimmten X betrachtet:

$$a_1^* X \equiv c_1^* \pmod{m_1^*}, \ldots, a_k^* X \equiv c_k^* \pmod{m_k^*}. \tag{1}$$

Man interessiert sich dafür, ob es ganze x gibt, die *gleichzeitig* alle k linearen Kongruenzen in (1) lösen; daher spricht man bei (1) von einem System *simultaner* linearer Kongruenzen. Nach Satz 1.5 ist das System (1) sicher dann unlösbar, wenn $(a_\kappa^*, m_\kappa^*) \nmid c_\kappa^*$ für mindestens eines der κ gilt. Im weiteren sei daher $(a_\kappa^*, m_\kappa^*) | c_\kappa^*$ für $\kappa = 1, \ldots, k$ vorausgesetzt.

Schreibt man dann $d_\kappa^* := (a_\kappa^*, m_\kappa^*)$, $a_\kappa := a_\kappa^*/d_\kappa^*$, $c_\kappa := c_\kappa^*/d_\kappa^*$, $m_\kappa := m_\kappa^*/d_\kappa^*$ für $\kappa = 1, \ldots, k$, so ist das System (1) nach der Kürzungsregel 1.3 äquivalent mit dem neuen System

$$a_1 X \equiv c_1 \pmod{m_1}, \ldots, a_k X \equiv c_k \pmod{m_k}. \tag{2}$$

Dies bedeutet: Ein ganzes x löst (1) genau dann, wenn es (2) löst. Im System (2) gilt $(a_\kappa, m_\kappa) = 1$ für $\kappa = 1, \ldots, k$.

Ist nun $a'_\kappa \in \mathbb{Z}$ im Sinne der Bemerkung zu 1.5 die Inverse von a_κ modulo m_κ, so geht die κ–te Kongruenz in (2) durch Multiplikation mit a'_κ über in die äquivalente Kongruenz $X \equiv a'_\kappa c_\kappa \pmod{m_\kappa}$ und dies alles für $\kappa = 1, \ldots, k$. Demnach ist das System (2) gleichwertig mit folgendem neuen System

$$X \equiv c'_1 \pmod{m_1}, \ldots, X \equiv c'_k \pmod{m_k} \tag{3}$$

wobei $c'_\kappa := a'_\kappa c_\kappa$ für $\kappa = 1, \ldots, k$ gesetzt wurde.

Die Äquivalenz der Systeme (2) und (3) gilt bei beliebigen $m_1, \ldots, m_k \in \mathbb{N}$, nur daß in (2) für $\kappa = 1, \ldots, k$ die Bedingung $(a_\kappa, m_\kappa) = 1$ verlangt ist. In 2 werden beide Systeme vollständig behandelt unter der für viele Anwendungen ausreichenden Zusatzvoraussetzung, daß die Moduln $m_1, \ldots, m_k$ paarweise teilerfremd sind.

2. Paarweise teilerfremde Moduln. Hauptziel ist hier ein Ergebnis, für das sich in der Literatur eingebürgert hat die Bezeichnung

Chinesischer Restsatz. *Die natürlichen Zahlen $m_1, \ldots, m_k$ seien paarweise teilerfremd und m sei ihr kgV. Sind für $\kappa = 1, \ldots, k$ die c'_κ ganz, so hat das System 1(3) modulo m genau eine Lösung.*

Beweis. Es werde $n_\kappa := m/m_\kappa$ gesetzt; nach Satz 1.2.12B ist n_κ das Produkt der $m_1, \ldots, m_{\kappa-1}, m_{\kappa+1}, \ldots, m_k$. Hätte n_κ mit m_κ einen Primfaktor p gemeinsam, so müßte p in einem m_λ mit $\lambda \neq \kappa$ aufgehen, entgegen der paarweisen

Teilerfremdheit der $m_1, \ldots, m_k$. Somit ist $(m_\kappa, n_\kappa) = 1$ für $\kappa = 1, \ldots, k$; im Sinne der Bemerkung zu 1.5 sei n'_κ die Inverse von n_κ modulo m_κ, womit die ganze Zahl

$$x := \sum_{\kappa=1}^{k} c'_\kappa n_\kappa n'_\kappa \tag{1}$$

gebildet werde. Für jedes feste λ ist damit

$$x \equiv c'_\lambda + \sum_{\substack{\kappa=1 \\ \kappa\neq\lambda}}^{k} c'_\kappa n_\kappa n'_\kappa \equiv c'_\lambda \pmod{m_\lambda}$$

weil $m_\lambda | n_\kappa$ für jedes von λ verschiedene κ. Die Zahl x löst also das System 1(3).

Sei y irgendeine ganze, 1(3) genügende Zahl. Dann gilt $m_\kappa | (x - y)$ für $\kappa = 1, \ldots, k$, somit auch $m | (x - y)$ nach dem Charakterisierungs–Satz 1.2.11 für das kgV, was $y \equiv x \pmod{m}$ bedeutet. □

Korollar. *Sind die m_κ und m wie im chinesichen Restsatz, sind die a_κ, c_κ ganz und gilt $(a_\kappa, m_\kappa) = 1$ für $\kappa = 1, \ldots, k$, so hat das System 1(2) modulo m genau eine Lösung.*

Beweis. Unter den gemachten Voraussetzungen ist 1(2), wie in 1 gesehen, äquivalent zu 1(3), angewandt mit $c'_\kappa := a'_\kappa c_\kappa$, wobei a'_κ die Inverse von a_κ modulo m_κ bedeutet. Auf dieses System 1(3) wendet man den chinesischen Restsatz an. □

Bemerkung. Unter den Voraussetzungen des chinesischen Restsatzes bedeutet nach Satz 1.2.12B kgV der m_κ bzw. Produkt der m_κ dasselbe.

3. Anwendungen, numerische Beispiele. Vom *chinesischen* Restsatz spricht man, da Fragestellungen, die auf Probleme des Typs 1(3) hinauslaufen, schriftlich überliefert scheinbar erstmals im *Suan–ching**) des Chinesen SUN–TSU auftauchten. Er stellt dort u.a. folgende Aufgabe: "Wir haben eine gewisse Anzahl von Dingen, wissen aber nicht genau wieviele. Wenn wir sie zu je drei zählen, bleiben zwei übrig. Wenn wir sie zu je fünf zählen, bleiben drei übrig. Wenn wir sie zu je sieben zählen, bleiben zwei übrig. Wieviele Dinge sind es?" Offenbar läuft dies auf das simultane Kongruenzensystem

$$X \equiv 2 \pmod{3}, \quad X \equiv 3 \pmod{5}, \quad X \equiv 2 \pmod{7}$$

*) (*Handbuch der Arithmetik*)

vom Typ 1(3) mit paarweise teilerfremden Moduln hinaus, deren kgV hier 105 ist. Die n_1, n_2, n_3 bzw. ihre modulo m_1, m_2, m_3 Inversen n_1', n_2', n_3' aus dem Beweis des chinesischen Restsatzes sind hier 35, 21, 15 bzw. -1, 1, 1 (die letzteren natürlich nur modulo 3, 5, 7 eindeutig). Nach 2(1) ist $2 \cdot 35 \cdot (-1) + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 23$ *die* modulo 105 eindeutige Lösung von SUN–TSUs Aufgabe.

Als zweite Anwendung simultaner linearer Kongruenzen soll die (gewöhnliche) lineare Kongruenz 1.5(1) unter der Bedingung $(a, m) = 1$ nochmals besprochen werden. Nach Satz 1.5 weiß man zwar, daß 1.5(1) modulo m eindeutig lösbar ist. Jedoch ist für das tatsächliche Auffinden der Lösung durch die in 1.6 erläuterte Bruchschreibweise nicht unbedingt viel gewonnen, vor allem dann nicht, wenn der Modul m und eventuell auch noch a und c "groß" sind. Hat m die kanonische Primfaktorzerlegung $p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$, so ist 1.5(1) nach Satz 1.1(v) äquivalent zum System

$$aX \equiv c \pmod{p_1^{b_1}}, \ldots, aX \equiv c \pmod{p_k^{b_k}} \tag{1}$$

wobei $(a, p_\kappa^{b_\kappa}) = 1$ für $\kappa = 1, \ldots, k$ gilt. Dieses System vom Typ 1(2) ist nach dem Korollar zum chinesischen Restsatz modulo m eindeutig lösbar.

Ist nun ein "großer" Modul m aus "vielen kleineren" Primzahlpotenzen $p_\kappa^{b_\kappa}$ zusammengesetzt, so *kann* es ratsam sein, die modulo m eindeutige Lösung von 1.5(1) durch Lösen von (1) zu ermitteln.

Als Beispiel sei etwa die absolut kleinste Zahl gesucht, die die Kongruenz

$$883X \equiv -103 \pmod{2275}$$

löst. Wegen $2275 = 5^2 \cdot 7 \cdot 13$ lautet (1) hier

$$883X \equiv -103 \pmod{25}, \quad 883X \equiv -103 \pmod{7}, \quad 883X \equiv -103 \pmod{13}$$

oder äquivalent

$$8X \equiv -3 \pmod{25}, \quad X \equiv 2 \pmod{7}, \quad -X \equiv 1 \pmod{13}.$$

Dies ist nochmals gleichwertig mit

$$X \equiv 9 \pmod{25}, \quad X \equiv 2 \pmod{7}, \quad X \equiv -1 \pmod{13},$$

einem System vom Typ 1(3) mit paarweise teilerfremden Moduln. Die n_κ und n_κ' im Beweis des chinesischen Restsatzes ergeben sich hier zu 91, 325, 175 bzw. 11, -2, 11 und daher löst $9 \cdot 91 \cdot 11 + 2 \cdot 325 \cdot (-2) + (-1) \cdot 175 \cdot 11 = 5784$ das letzte Kongruenzensystem. Da die Lösung modulo 2275 eindeutig ist (883 ist Primzahl), ist -1041 die gesuchte Zahl.

Ein ähnliches Beispiel mit demselben Modul ist

$$3X \equiv 11 \pmod{2275}.$$

Hier könnte man natürlich analog wie soeben verfahren; nur führt in diesem Fall trotz des "großen" Moduls die Bruchschreibweise aus 1.6 ungleich schneller zum Ziel: Die Lösung modulo 2275 ist $\frac{11}{3} \equiv \frac{11+2275}{3} = 762$.

Es kommt also keinesfalls nur auf den Modul m an, sondern auch auf a und c, wie man die Lösung von 1.5(1) am besten anpackt.

4. Restklassenring als direkte Summe. Sind $G_1, \ldots, G_k$ (multiplikativ geschriebene) Gruppen mit den Einselementen $e_1, \ldots, e_k$, so führt man im kartesischen Produkt $G := G_1 \times \ldots \times G_k$ eine (multiplikativ geschriebene) Verknüpfung $\cdot$ dadurch ein, daß man zwei Elementen $(g_1, \ldots, g_k)$, $(g'_1, \ldots, g'_k)$ von G das Element $(g_1 g'_1, \ldots, g_k g'_k)$ von G zuordnet. Offenbar ist $(G, \cdot)$ eine Gruppe, das *direkte Produkt von* $G_1, \ldots, G_k$. Das Einselement der neuen Gruppe ist $(e_1, \ldots, e_k)$; sie ist jedenfalls dann abelsch, wenn alle G_κ abelsch sind.

Sind nun $R_1, \ldots, R_k$ Ringe, so betrachte man diese momentan als additive Gruppen und konstruiere daraus, wie soeben beschrieben, deren direkte Summe, welche R genannt werde; R ist bezüglich der eingeführten (komponentenweisen) Addition eine abelsche Gruppe. In R definiert man weiter eine (komponentenweise) Multiplikation, indem man zwei Elementen $(r_1, \ldots, r_k)$, $(r'_1, \ldots, r'_k)$ von R das Element $(r_1 r'_1, \ldots, r_k r'_k)$ von R zuordnet. Bezüglich der erklärten Addition und Multiplikation erweist sich R als Ring; dieser wird als die *direkte Summe der Ringe* $R_1, \ldots, R_k$ bezeichnet, symbolisch $R = R_1 \oplus \ldots \oplus R_k$.

Mit dem chinesischen Restsatz wird nun über die Struktur von $\mathbb{Z}_m$ bewiesen der

Satz. *Sei $m \geq 2$ ganz und seien die $m_1, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd mit $m_1 \cdot \ldots \cdot m_k = m$. Dann ist der Restklassenring modulo m isomorph zur direkten Summe der Restklassenringe modulo m_κ $(\kappa = 1, \ldots, k)$.*

Beweis. Es werde $R := \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_k}$ gesetzt. Definiert man die Abbildungen $\psi_\kappa : \mathbb{Z} \to \mathbb{Z}_{m_\kappa}$ für $\kappa = 1, \ldots, k$ analog zum Beginn von 1.7, so führt man nun $\Psi : \mathbb{Z} \to R$ ein durch $\Psi(a) := (\psi_1(a), \ldots, \psi_k(a))$. Die Surjektivität von Ψ ergibt sich aus dem chinesischen Restsatz: Denn sind $a_1, \ldots, a_k \in \mathbb{Z}$ beliebig vorgegeben, so ist das Kongruenzensystem $X \equiv a_1 \pmod{m_1}, \ldots, X \equiv a_k \pmod{m_k}$ vom Typ 1(3) lösbar. Nach 1.7(1) erweist sich weiter Ψ als Ringhomomorphismus, dessen Kern noch zu bestimmen bleibt. Ersichtlich ist $a \in$ Kern Ψ gleichbedeutend mit $a \equiv 0 \pmod{m_\kappa}$ für $\kappa = 1, \ldots, k$ und dieses mit $a \in m\mathbb{Z}$. Der Kern von

Ψ ist also das Ideal $m\mathbb{Z}$ in $\mathbb{Z}$ und nach einem aus der Algebra wohlbekannten Homomorphiesatz für Ringe sind R und $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ isomorph. □

5. Prime Restklassengruppe als direktes Produkt. Hauptziel ist hier folgender Satz, der es gestattet, die Struktur der primen Restklassengruppe modulo m vollständig aufzudecken.

Satz. *Sind $m, m_1, \ldots, m_k$ wie in Satz 4, so ist die prime Restklassengruppe modulo m isomorph zum direkten Produkt der primen Restklassengruppen modulo m_κ ($\kappa = 1, \ldots, k$).*

Dem Beweis wird vorausgeschickt das

Lemma. *Ist R die direkte Summe der kommutativen Ringe R_κ mit Einselement 1_κ für $\kappa = 1, \ldots, k$, so ist die Einheitengruppe von R das direkte Produkt der Einheitengruppen aller R_κ.*

Beweis. Ein $(r_1, \ldots, r_k) \in R$ gehört dann zur Einheitengruppe $E(R)$ von R, wenn es ein $(s_1, \ldots, s_k) \in R$ gibt mit $r_\kappa s_\kappa = 1_\kappa$ für $\kappa = 1, \ldots, k$; dies ist mit $r_\kappa \in E(R_\kappa)$ für $\kappa = 1, \ldots, k$ äquivalent und beweist

$$E(R) = E(R_1) \times \ldots \times E(R_k). \qquad \square$$

Beweis des Satzes. Sei $R := \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_k}$ und $\chi : R \to \mathbb{Z}_m$ ein Isomorphismus gemäß Satz 4. Nun wird $\chi(r) \in \mathbb{Z}_m^*$ für jedes $r \in E(R)$ überlegt: Zu $r := (r_1, \ldots, r_k) \in E(R)$ gibt es ein $s := (s_1, \ldots, s_k) \in R$ mit $r_\kappa s_\kappa = 1_\kappa$, weshalb $\chi(rs) = \chi(1_1, \ldots, 1_k) = \overline{1}$ ist, letzteres wegen der Isomorphieeigenschaft von χ ($\overline{1}$ ist die Restklasse modulo m, in der 1 liegt; vgl. Bemerkung 4 zu 1.8). Damit ist $\chi(r) \in \mathbb{Z}_m^*$ klar und die eingeschränkte Abbildung $\chi|_{E(R)}$ von $E(R)$ auf $\mathbb{Z}_m^*$ behält die Isomorphieeigenschaft. Nach dem Lemma in Verbindung mit Bemerkung 3 zu 1.8 ist $E(R) = \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_k}^*$. □

Wendet man den letzten Satz mit $k = 2$ an, so erhält man die bereits in Satz 1.4.11(i) festgestellte Multiplikativität der EULERschen Funktion φ erneut:

Korollar. *Sind $m_1, m_2 \in \mathbb{N}$ zueinander teilerfremd, so gilt $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.*

Bemerkung. Ist $\prod_{\kappa=1}^{k} p_\kappa^{\alpha_\kappa}$ die kanonische Zerlegung eines ganzen $m \geq 2$, so gilt nach dem hier gezeigten Satz

$$\mathbb{Z}_m^* \simeq \mathbb{Z}_{p_1^{\alpha_1}}^* \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}^*.$$

Die Struktur von $\mathbb{Z}_m^*$ ist also vollständig bekannt, wenn die Struktur der $\mathbb{Z}_{p^\alpha}^*$ bekannt ist; dies letztere Problem wird in 5.5 und 5.6 abschließend behandelt.

6. Historische Bemerkungen. Der zu Anfang von 3 erwähnte SUN–TSU muß zwischen 200 und 470 gelebt haben. In seinem *Handbuch* gibt er übrigens auch allgemeine Regeln zur Behandlung simultaner Kongruenzen (so die nach–GAUSSsche Terminologie) an. Der chinesische Mönch und Astronom I–HSING (682–727) dehnte diese Regeln weiter auf den Fall aus, wo die Moduln $m_1, \ldots, m_k$ des Systems 1(3) nicht mehr notwendig paarweise teilerfremd sind. Die chinesische Lösungsmethode — von K. MAHLER (Math. Nachr. *18*, 120–122 (1958)) in moderner Schreibweise erläutert — ist gänzlich von derjenigen verschieden, die hier zum Beweis des Restsatzes verwendet wurde.

Obiger Beweis des chinesischen Restsatzes, dessen Name inzwischen verständlich geworden ist, geht auf GAUSS (*Disquisitiones Arithmeticae*, Artt. 32–36) zurück; ohne Benützung der Kongruenzenschreibweise hatte EULER simultane Probleme des Typs 1(3) schon früher auf demselben Wege gelöst.

Ganz interessant ist vielleicht noch, daß auch in Indien spätestens im 6. Jahrhundert vor allem Astronomen, besonders die schon in 1.3.4 erwähnten ARYABHATA und BRAHMAGUPTA, simultane lineare Kongruenzen zu behandeln hatten. Die indische Methode dafür beruhte wesentlich auf dem euklidischen Algorithmus.

Daß in China, Indien und im Mittelalter dann im byzantinischen Raum vor allem Astronomen simultane Kongruenzen zu lösen hatten, hat folgenden Grund: Zahlreiche Kalenderprobleme und Fragestellungen im Zusammenhang mit den Umlaufbahnen von Planeten und anderen Himmelskörpern führen mathematisch (manchmal allerdings nur annähernd) auf Systeme des Typs 1(3).

§ 3. Die Sätze von Fermat, Euler und Wilson

1. Dirichlets Schubfachprinzip. Zunächst wird eine ganz einfache Tatsache explizit erwähnt, die in der Mathematik, insbesondere in der Zahlentheorie (auch in diesem Buch mehrfach), mit großem Erfolg angewandt werden kann.

Satz. *Sind M, N nicht leere Mengen, ist überdies N endlich und $f : M \to N$ eine Abbildung, so gilt: Ist $\#N < \#M$, so ist f nicht injektiv.*

Beweis. Zunächst ist $f(M)$ in N enthalten und somit endlich. Ist f injektiv, so gibt es zu jedem $n \in N$ höchstens ein $m \in M$ mit $f(m) = n$. Also ist $\#N \geq \#M$. □

Der hier festgestellte Sachverhalt wird üblicherweise äquivalent, jedoch in bildlicher Sprache formuliert als

Dirichletsches Schubfachprinzip. *Bei einer Verteilung von mehr als n Dingen auf n Schubfächer liegen in mindestens einem Fach mindestens zwei Dinge.*

2. Kongruenzverhalten von Potenzen. Im weiteren sei m eine feste natürliche Zahl. Für ganzes a werde die Folge $(a^i)_{i=0,1,\ldots}$ betrachtet und man interessiert sich dafür, welche Reste die Glieder $a^0, a^1, \ldots$ dieser Folge bei Division durch m lassen. Da es nach 1.1 und 1.4 genau m verschiedene Restklassen modulo m gibt, ist nach DIRICHLETs Schubfachprinzip klar, daß es unter den $m+1$ Zahlen $a^0, \ldots, a^m$ zwei geben muß, die modulo m zueinander kongruent sind. Es bezeichne h den kleinsten Exponenten, zu dem es ein $k > h$ gibt, so daß

$$a^k \equiv a^h \pmod{m} \tag{1}$$

gilt. Aus den vorigen Betrachtungen ist bereits $0 \leq h < m$ klar; selbstverständlich hängt h von a (und von m) ab. Bestimmt man nun noch k größer als h und minimal, so daß (1) zutrifft, so hat man weiter $0 \leq h < k \leq m$, wobei auch k von a (und m) abhängt.

Wegen Satz 1.1(iii) ist klar, daß sich bei $a_1 \equiv a_2 \pmod{m}$ die beiden Folgen $(a_1^i)_{i\in\mathbb{N}_0}$ bzw. $(a_2^i)_{i\in\mathbb{N}_0}$ modulo m nicht unterscheiden. Demnach sind *die Zahlen h und k Invarianten der ganzen Restklasse modulo m, der das speziell betrachtete a angehört.*

Sind h und k wie oben fixiert, so folgt aus Satz 1.1(ii) unmittelbar, daß $a^{i+(k-h)} \equiv a^i \pmod{m}$ genau für die $i \geq h$ gelten muß. Man sagt in diesem Zusammenhang, die Folge $(a^i)_{i\in\mathbb{N}_0}$ sei *modulo m periodisch* mit der *Periodenlänge* $k-h$ und der *Vorperiodenlänge* h; bei $h = 0$ heißt die Folge *modulo m reinperiodisch.*

Satz. *Für ganze $m > 0$ und a gilt: $(a^i)_{i\in\mathbb{N}_0}$ ist modulo m reinperiodisch genau dann, wenn m, a teilerfremd sind.*

Beweis. Bei $h = 0$ folgt aus (1) unmittelbar $(a, m) = 1$. Ist umgekehrt $(a, m) = 1$ und wird $h > 0$ angenommen, so folgt aus (1) mit der Kürzungsregel 1.3 die Kongruenz $a^{k-1} \equiv a^{h-1} \pmod{m}$, was der Definition von h widerspricht. □

Genau dann, wenn $(a, m) = 1$ ist, kann auch a^i modulo m eindeutig für negative ganze i definiert werden als die Lösung der Kongruenz $a^{-i}X \equiv 1 \pmod{m}$. In

diesem Fall kann sogar die zweifach unendliche Folge $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$ modulo m betrachtet werden. Wie man leicht nachweist, gilt für sie $a^{i+k} \equiv a^i \pmod{m}$ bei beliebigem ganzem i.

Wie das unterschiedliche Verhalten der Folge (a^i) modulo m erwarten läßt, je nachdem, ob a und m teilerfremd sind oder nicht, wird man sich im weiteren besonders für den Fall $(a, m) = 1$ interessieren. Hier bekommt die charakteristische Zahl k zunächst einen Namen: Bei teilerfremden a und m heißt die kleinste natürliche Zahl k, für die $a^k \equiv 1 \pmod{m}$ gilt, die *Ordnung von a modulo m*, in Zeichen $\mathrm{ord}_m a$. (In der älteren Literatur nannte man dies k manchmal den *Exponenten*, zu dem a modulo m gehört.)

3. Der "kleine" Fermatsche Satz. Zunächst wird der Spezialfall betrachtet, wo m Primzahl ist; dazu dient folgendes

Lemma. *Ist p eine Primzahl, so geht p in den Binomialkoeffizienten $\binom{p}{j}$ für $j = 1, \ldots, p-1$ auf.*

Beweis. Wegen $j!\binom{p}{j} = p \cdot \ldots \cdot (p-j+1)$ geht p in $j!\binom{p}{j}$ auf, aber nicht in $j!$. □

Satz von Fermat. *Sei p eine Primzahl. Dann gilt*

$$a^p \equiv a \pmod{p} \tag{1}$$

für jedes ganze a; für jedes ganze nicht durch p teilbare a gilt

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2}$$

Beweis. Bei $p \nmid a$ folgt (2) mit der Kürzungsregel 1.3 aus (1). Nun ist (1) für $a = 0$ richtig. Sei für ein $a \geq 0$ die Kongruenz (1) schon eingesehen; damit und aufgrund des Lemmas ist

$$(a+1)^p = \sum_{j=0}^{p} \binom{p}{j} a^j \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

Insbesondere ist also (1) auf dem vollständigen Restsystem S_p modulo p bewiesen und somit für alle ganzen a. □

Bemerkungen. 1) Bereits um 500 v. Chr. scheinen chinesische Mathematiker gewußt zu haben, daß $2^p - 2$ für jede Primzahl p durch p teilbar ist. In einem Brief vom 18. Oktober 1640 an FRENICLE DE BESSY teilte FERMAT ohne Beweis das obige Resultat mit. Es ist üblich geworden, dieses als "kleinen" FERMATschen Satz zu zitieren, da man den Terminus "FERMATscher Satz" einer anderen Behauptung FERMATs vorbehalten möchte, auf die in 4.2.7 eingegangen wird.

2) Der erste publizierte Beweis für (1) findet sich in einem nachgelassenen Manuskript von LEIBNIZ. Der oben geführte Beweis variiert den Ansatz von LEIBNIZ, der für natürliche a im wesentlichen so schloß: Für a Unbestimmte $X_1, \ldots, X_a$ liefert der Polynomiallehrsatz

$$(3) \qquad (X_1 + \ldots + X_a)^p = \sum_{j_1+\ldots+j_a=p} \frac{p!}{j_1! \ldots j_a!} X_1^{j_1} \cdot \ldots \cdot X_a^{j_a}$$

wobei rechts über alle a–Tupel $(j_1, \ldots, j_a)$ ganzer, nichtnegativer Zahlen der Summe p zu summieren ist. Setzt man in (3) für $X_1, \ldots, X_a$ jeweils 1 ein, so erscheint links a^p. Die Summanden rechts sind 1 für die a verschiedenen a–Tupel, bei denen genau ein j_α gleich p ist (und die restlichen daher verschwinden); für alle anderen a–Tupel ist die ganze Zahl $\frac{p!}{j_1! \ldots j_a!}$ durch p teilbar. Somit erscheint rechts eine natürliche, zu a modulo p kongruente Zahl.

4. Der Eulersche Satz. Ein zweiter, wesentlich anderer Ansatz zum Nachweis von 3(2) geht auf J. IVORY (New Ser. Math. Repository *1*, 6–8 (1806)) zurück, der den Vorteil besitzt, daß man mit ihm eine zu 3(2) analoge Formel bekommen kann, wenn der Modul nicht mehr notwendig Primzahl ist. Diese Verallgemeinerung der FERMATschen Kongruenz hat EULER (Opera Omnia Ser. 1, II, 531–555) entdeckt:

Satz von Euler. *Für natürliche m und ganze, zu m teilerfremde a gilt*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Dabei bezeichnet φ die EULERsche *Phi–Funktion aus 1.4.11.*

Beweis. Man setze $s := \varphi(m)$ und fixiere $\{g_1, \ldots, g_s\}$ als primes Restsystem modulo m. Wegen $(a, m) = 1$ ist auch $(ag_\sigma, m) = 1$ für $\sigma = 1, \ldots, s$ nach Korollar 1.2.6; weiter ist $ag_\sigma \not\equiv ag_{\sigma'} \pmod{m}$ für $\sigma \neq \sigma'$ nach der Kürzungsregel 1.3. Damit ist $\{ag_1, \ldots, ag_s\}$ ebenfalls ein primes Restsystem modulo m und so gibt es zu jedem Element des einen Restsystems genau ein modulo m kongruentes Element im anderen Restsystem. Also muß

$$(ag_1) \cdot \ldots \cdot (ag_s) \equiv g_1 \cdot \ldots \cdot g_s \pmod{m}$$

sein, woraus man wegen $(g_1 \cdot \ldots \cdot g_s, m) = 1$ EULERs Kongruenz erhält. □

Offenbar enthält der EULERsche Satz den "kleinen" FERMATschen in der Form 3(2). Den ersteren bezeichnet man auch oft als "Satz von FERMAT–EULER" oder "Satz von EULER–FERMAT", je nachdem, ob man die Anciennität der Entdeckung oder die größere Allgemeinheit der Aussage vornean stellen will.

Eine erste Folgerung aus dem für die Zahlentheorie überaus wichtigen FERMAT–EULERschen Satz ist das

Korollar. *Seien $m > 0$ und a ganz und zueinander teilerfremd. Ist $a^\ell \equiv 1 \pmod m$ für natürliches ℓ, so ist ℓ ein Vielfaches von $\operatorname{ord}_m a$; insbesondere wird $\varphi(m)$ von $\operatorname{ord}_m a$ geteilt.*

Beweis. Ist nämlich $k := \operatorname{ord}_m a$, so dividiere man ℓ mit Rest durch k, etwa $\ell = qk + r$, $0 \le r < k$. Dann ist nach Definition von $\operatorname{ord}_m a$ am Ende von 2

$$1 \equiv a^\ell = (a^k)^q a^r \equiv a^r \pmod m$$

woraus $r = 0$ wegen der Minimaleigenschaft von k folgt. Der FERMAT-EULERsche Satz erledigt den Sonderfall $\ell = \varphi(m)$. □

Bemerkung. Aus den Betrachtungen in 2 hatte sich $0 < \operatorname{ord}_m a \le m$ bei $(a, m) = 1$ ergeben; das Korollar verbessert dies auf $0 < \operatorname{ord}_m a \le \varphi(m)$. Es gibt unendlich viele m, für die bei geeignetem a mit $(a, m) = 1$ tatsächlich $\operatorname{ord}_m a = \varphi(m)$ gilt; genau mit dieser Problematik wird sich § 5 befassen.

5. Numerische Anwendungen. Bei der ersten Aufgabe zeigt sich, wie stark der FERMAT–EULERsche Satz in gewissen Situationen das praktische Rechnen vereinfachen kann. Man interessiert sich für die drei letzten Ziffern der Dezimaldarstellung von 9^{9^9}: Zunächst ist $9^{400} = 9^{\varphi(1000)} \equiv 1 \pmod{1000}$ und

$$9^9 = (80+1)^4 \cdot 9 \equiv (4 \cdot 80 + 1) \cdot 9 \equiv -79 \cdot 9 \equiv 89 \pmod{400}.$$

Daher ist modulo 1000

$$9^{9^9} \equiv 9^{89} = (10-1)^{89} \equiv -\binom{89}{2} \cdot 100 + 89 \cdot 10 - 1 \equiv 400 - 110 - 1 = 289$$

und somit endet die Dezimaldarstellung von 9^{9^9} mit den Ziffern 2, 8, 9.

Bei der zweiten Aufgabe geht es um die lineare Kongruenz

1.5(1) $$aX \equiv c \pmod m.$$

Im Fall $(a, m) = 1$ *eine* natürliche Zahl k mit $a^k \equiv 1 \pmod{m}$ zu kennen, ist von (im allgemeinen theoretischer) Bedeutung für die Lösung von 1.5(1). Denn dann braucht man 1.5(1) nur mit a^{k-1} zu multiplizieren und findet $a^{k-1}c$ als *die* Lösung modulo m. EULERs Satz garantiert somit $a^{\varphi(m)-1}c$ als die Lösung von 1.5(1).

Nimmt man sich daraufhin etwa die in 2.3 behandelte Kongruenz $883X \equiv -103 \pmod{2275}$ nochmals vor, so stellt man fest, daß

$$\varphi(2275) = \varphi(25)\varphi(7)\varphi(13) = 20 \cdot 6 \cdot 12 = 1440$$

beachtlich groß ist und nicht viel gewonnen scheint, wenn man $-883^{1439} \cdot 103$ als die Lösung modulo 2275 notiert. Da sich aufgrund des nachfolgenden Lemmas jedoch $\mathrm{ord}_{2275}883 = 20$ ergibt, kann die Lösung der vorgelegten Kongruenz modulo 2275 auch in der Form $-883^{19} \cdot 103$ aufgeschrieben werden. Nun können die 883^{2^j}, $j = 0, \ldots, 4$, rasch durch sukzessives Quadrieren zu $883, -636, -454, -909, 456$ ermittelt werden, was wegen der Darstellung $2^0 + 2^1 + 2^4$ des Exponenten 19 die Lösung modulo 2275 als $-103 \cdot 883 \cdot (-636) \cdot 456 \equiv -1041$ liefert, wie schon in 2.3 gesehen.

Lemma. *Seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd und $m := m_1 \cdot \ldots \cdot m_r$. Dann gilt für jedes ganze, zu m teilerfremde a*

$$\mathrm{ord}_m a = \mathrm{kgV}(\mathrm{ord}_{m_1} a, \ldots, \mathrm{ord}_{m_r} a).$$

Beweis. Setzt man $k := \mathrm{ord}_m a$ und $k_\rho := \mathrm{ord}_{m_\rho} a$ für $\rho = 1, \ldots, r$, so gilt: $a^k \equiv 1 \pmod{m} \Rightarrow a^k \equiv 1 \pmod{m_\rho}$ für alle ρ, also $k_\rho | k$ für alle ρ nach Korollar 4, also $K|k$ mit $K := \mathrm{kgV}(k_1, \ldots, k_r)$. Andererseits ist $a^{k_\rho} \equiv 1 \pmod{m_\rho}$ für alle ρ, also $a^K \equiv 1 \pmod{m_\rho}$ für dieselben ρ, was nach Satz 1.1(v) zu $a^K \equiv 1 \pmod{m}$ führt. Korollar 4 liefert $k|K$ und damit die Behauptung. □

Wegen $\mathrm{ord}_{25}883 = 20$, $\mathrm{ord}_7 883 = 1$, $\mathrm{ord}_{13}883 = 2$ ist also $\mathrm{ord}_{2275}883 = 20$, wie oben vorweggenommen wurde.

Bemerkung. Das hier gezeigte Lemma kommt z.B. auch in 5.1.7 zur Anwendung.

6. Zusammengesetzt oder Primzahl? In diesem Abschnitt soll kurz darauf eingegangen werden, wie man mit Hilfe des "kleinen" FERMATschen Satzes entscheiden kann, ob eine vorgelegte ganze Zahl $m > 1$ zusammengesetzt oder Primzahl ist. Zunächst erhält man aus dem FERMATschen Satz durch Kontraposition die

Proposition A. *Zu natürlichem m gebe es ein ganzes a mit $a^m \not\equiv a \pmod m$. Dann ist m zusammengesetzt.*

Tatsächlich ist a^m modulo m sehr schnell berechenbar: Wie in 5 bildet man dazu für $j = 0, 1, \ldots$ die Potenzen a^{2^j} modulo m durch wiederholtes Quadrieren; die dabei anfallenden Reste multipliziert man modulo m, wie es die dyadische Entwicklung von m (vgl. 5.1.1) verlangt. Auf diese Weise hat G.A. PAXSON (Math. Comp. *15*, 420 (1961)) gezeigt, daß die FERMAT–Zahl F_{13} wegen $3^{F_{13}} \not\equiv 3 \pmod{F_{13}}$ zusammengesetzt ist (vgl. 3.2.11).

Die Umkehrung von Proposition A gilt jedoch nicht, so daß man auf *diesem* Wege noch kein Primzahlkriterium erhält; man hat nämlich die (hier nicht zu beweisende)

Proposition B. *Es gibt zusammengesetzte ganze $m > 1$ mit $a^m \equiv a \pmod m$ für alle ganzen a.*

Beispiele für solche m sind $561 = 3 \cdot 11 \cdot 17$ und $1729 = 7 \cdot 13 \cdot 19$. Derartige m heißen CARMICHAEL–*Zahlen*; die Vermutung, daß es davon unendlich viele gibt, wurde von W. R. ALFORD, A. GRANVILLE und C. POMERANCE (Ann. Math. (2) *139*, 703–722 (1994)) bewiesen.

Das "richtige" Gegenstück zum "kleinen" FERMATschen Satz hat E. LUCAS (*Théorie des Nombres*, 1891) gefunden:

Proposition C. *Sei $m \geq 2$ ganz und es gebe ein ganzes, zu m teilerfremdes a mit $\mathrm{ord}_m a = m - 1$. Dann ist m Primzahl.*

Beweis. Nach Korollar 4 ist $(m-1) | \varphi(m)$, was zu $m - 1 \leq \varphi(m)$ führt. Wegen $m \geq 2$ ist andererseits $\varphi(m) \leq m - 1$, also $\varphi(m) = m - 1$, weshalb m Primzahl sein muß. □

Bemerkung. Die Aussage von Proposition *C* ist für die Praxis allerdings nicht sehr geeignet, denn bei großem m ist dieser Primzahltest vom algorithmischen Standpunkt aus viel zu langsam. In letzter Zeit sind eine ganze Reihe (auch algorithmisch schneller) Primzahltests entwickelt worden, wobei die Mehrzahl ganz wesentlich vom FERMAT–EULERschen Satz abhängt. Hier ist vor allem die Methode von L.M. ADLEMAN, C. POMERANCE und R. RUMELY (Ann. Math. (2) *117*, 173–206 (1983)) zu nennen, die von H. COHEN und H.W. LENSTRA JR. (Math. Comp. *42*, 297–330 (1984)) weiter verbessert wurde. Computerprogramme, die auf dieser Methode basieren, testen Zahlen mit 100 Dezimalstellen

in Sekundenschnelle auf Zusammengesetztheit. Einen sehr guten Überblick über die wichtigsten Primzahltests bis zum neuesten Stand erhält der interessierte Leser z.B. durch J.D. Dixon (Amer. Math. Monthly *91*, 333–352 (1984)), aber auch in den Monographien von E. Kranakis (*Primality and Cryptography*, Teubner, Stuttgart, and Wiley, Chichester etc., 1986), D.M. Bressoud (*Factorization and Primality Testing*, Springer, New York etc., 1989) oder R. Crandall und C. Pomerance (*Prime Numbers. A Computational Perspective*, Springer, New York etc., 2001 (2nd Ed. 2005)).

7. Fermat–Euler und geheime Nachrichtenübermittlung. Wie zuletzt erwähnt, hat man neuerdings überaus schnelle Methoden zur Entscheidung, ob eine vorgelegte natürliche Zahl m mit "vielen" Dezimalstellen Primzahl ist oder nicht. Erweist sich m als zusammengesetzt, so stellt sich das nächste Problem, seine kanonische Primfaktorzerlegung zu ermitteln. Die besten heute bekannten Algorithmen zur Herstellung dieser Zerlegung sind "sehr viel langsamer" als die oben genannten besten Primzahltests. Ist m etwa Produkt zweier verschiedener Primzahlen mit je 100 Dezimalstellen, so muß man für die effektive Faktorzerlegung eine Rechenzeit in der Größenordnung von 10^9 Jahren einplanen, selbst wenn man den derzeit (1987) besten Algorithmus und die schnellsten Computer verwendet. Diesen krassen Gegensatz zwischen schnellen Primzahltests und langsamer Faktorisierung nutzten R. Rivest, A. Shamir und L.M. Adleman, (Comm. ACM *21*, 120–128 (1978)), um eine einfache und elegante Methode der geheimen Nachrichtenübermittlung zu entwickeln, die im folgenden kurz beschrieben werden soll. Bemerkenswert ist, daß bei dieser Methode jeder Teilnehmer am genannten Übermittlungssystem seinen Chiffrierschlüssel (*fast* vollständig) öffentlich zugänglich macht.

Zunächst wählt sich jeder Teilnehmer des Systems zwei verschiedene Primzahlen p, q mit 100 Dezimalstellen; es stehen mehr als 10^{97} solcher Primzahlen zur Verfügung. Die schnellen Primzahltests gestatten jedem Teilnehmer eine rasche Abwicklung seiner individuellen Suche. Sodann bildet er $m := pq$ und wählt des weiteren eine (nicht zu kleine) natürliche Zahl e unterhalb m, die zu $\varphi(m) = (p-1)(q-1)$ teilerfremd ist. Wegen $(e, \varphi(m)) = 1$ kann er ganze x, y mit $ex + \varphi(m)y = 1$ nach Korollar 1.3.4 mit Hilfe des euklidischen Algorithmus bestimmen, von denen er nach Satz 1.3.3 außerdem $x, -y \in \mathbb{N}$ verlangen kann. Während er seine Zahlen p, q, $\varphi(m)$, x, y geheim hält, läßt der Teilnehmer im öffentlichen Verzeichnis des Nachrichtenübermittlungssystems (man denke etwa an ein Telefonbuch) seine charakteristischen Zahlen m und e abdrucken.

Will nun ein Teilnehmer des Systems einem anderen eine Nachricht geheim übermitteln, so schlägt er die Zahlen m, e des Empfängers im Verzeichnis nach. Sodann übersetzt der Absender seine in Buchstaben geschriebene Nachricht in

Zahlen gemäß $A = 01$, $B = 02$, …, $Z = 26$. Die so entstehende Ziffernfolge wird in Blöcke $\beta_1, \ldots, \beta_n$ geeigneter, aber gleicher Länge zerlegt, wobei am Ende gegebenenfalls irgendwie aufgefüllt wird. Nun wird γ_j gemäß $\beta_j^e \equiv \gamma_j \pmod m$ für $j = 1, \ldots, n$ gebildet und der Absender schickt die Folge der Blöcke $\gamma_1, \ldots, \gamma_n$ über das System an den Empfänger.

Dieser entschlüsselt die ankommende Blockfolge $\gamma_1, \ldots, \gamma_n$ leicht, indem er mittels des nur ihm bekannten x

$$\gamma_j^x \equiv \beta_j^{ex} = \beta_j^{1-\varphi(m)y} = \beta_j \left(\beta_j^{p-1}\right)^{(q-1)|y|} \pmod m \tag{1}$$

für $j = 1, \ldots, n$ bildet. Wird β_j von p geteilt, so auch γ_j und es gilt $\gamma_j^x \equiv \beta_j \pmod p$. Bei $p \not| \beta_j$ gilt $\beta_j^{p-1} \equiv 1 \pmod p$ nach dem FERMATschen Satz; (1) führt dann auch in diesem Fall zu $\gamma_j^x \equiv \beta_j \pmod p$. Ersetzung von p durch q ergibt schließlich $\gamma_j^x \equiv \beta_j \pmod m$ für $j = 1, \ldots, n$ und nach dieser Ermittlung der dechiffrierten Blöcke $\beta_1, \ldots, \beta_n$ kann der Empfänger die Buchstabenfolge lesen.

Ein von Absender und Empfänger verschiedener Teilnehmer des Systems, den die übermittelte Nachricht unbefugt interessiert, kennt zwar m, e und die Blockfolge $\gamma_1, \ldots, \gamma_n$; zur Entschlüsselung benötigt er aber ersichtlich x, an das er nur über eine der drei Zahlen p, q, $\varphi(m)$ herankommen kann. Die Berechnung einer dieser drei Zahlen läuft jedoch auf die Faktorisierung von m hinaus, welches 199 oder 200 Dezimalstellen hat und somit nach den Eingangsbemerkungen beim derzeitigen Stand der Dinge nicht in vernünftiger Zeit in seine beiden Primfaktoren zu zerlegen ist.

Bemerkung. Dem Leser, der in die hier angeschnittene Problematik weiter eindringen will, kann zum Selbststudium das bereits auf Seite 101 zitierte Buch von KRANAKIS ebenso empfohlen werden wie diejenigen von D.E.R. DENNING (*Cryptography and Data Security*, Addison–Wesley, Reading/Mass. etc., 1982) und von N. KOBLITZ (*A Course in Number Theory and Cryptography*, Springer, New York etc., 1987).

8. Satz von Wilson. *Eine ganze Zahl $m > 1$ ist Primzahl genau dann, wenn die Kongruenz $(m-1)! \equiv -1 \pmod m$ besteht.*

Beweis. Ist m zusammengesetzt, so geht die kleinste, m teilende Primzahl in $(m-1)!$ und in m auf und so kann die fragliche Kongruenz nicht gelten.

Sei nun $p := m$ eine Primzahl; weil die behauptete Kongruenz für $p = 2$ erfüllt ist, darf p künftig als ungerade vorausgesetzt werden. Da die Kongruenz $a^2 \equiv 1 \pmod p$ für ganzes a genau dann gilt, wenn entweder $a \equiv 1 \pmod p$ oder

$a \equiv -1 \pmod p$ zutrifft, kann man bei $p \geq 5$ die Menge der Zahlen $2, 3, \ldots, p-2$ in $\frac{1}{2}(p-3)$ Paare zueinander modulo p reziproker Partner zerlegen, so daß

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod p \tag{1}$$

gilt. Nach der Konvention über leere Produkte hat man (1) auch für $p = 3$ und Multiplikation von (1) mit $p-1$ liefert die behauptete Kongruenz. □

Bemerkung. Manuskripte von LEIBNIZ zeigen, daß dieser den WILSONschen Satz bereits vor 1683 gekannt haben muß. Publiziert wurde das Resultat offenbar zuerst von E. WARING (*Meditationes Algebraicae*, Cambridge, 1770), der es seinem Schüler J. WILSON zuschrieb. Erst J.L. LAGRANGE (Oeuvres III, 423–438) scheint dann 1771 wirklich einen *Beweis* für den WILSONschen Satz gefunden zu haben. Der angegebene Beweis geht auf GAUSS (*Disquisitiones Arithmeticae*, Art. 77) zurück.

9. Anwendung auf eine quadratische Kongruenz. Der Satz von WILSON liefert ersichtlich eine notwendige und hinreichende Bedingung dafür, daß eine ganze Zahl $m > 1$ Primzahl ist. Er ist vor allem für *theoretische* Untersuchungen von Bedeutung; eine erste Anwendung ist folgender

Satz. *Sei p eine Primzahl. Die quadratische Kongruenz*

$$X^2 \equiv -1 \pmod p \tag{1}$$

ist lösbar genau dann, wenn $p \not\equiv 3 \pmod 4$ ist. Insbesondere hat (1) bei $p = 2$ die eindeutige Lösung 1 modulo 2; bei $p \equiv 1 \pmod 4$ hat (1) genau die modulo p verschiedenen Lösungen $(\frac{p-1}{2})!$ und $-(\frac{p-1}{2})!$.

Beweis. Bei $p = 2$ wird (1) offenbar durch jede ungerade, aber keine gerade Zahl gelöst. Ist $p \equiv 1 \pmod 4$, so wird

$$\Big(\frac{p-1}{2}\Big)!^2 \equiv -1 \pmod p \tag{2}$$

behauptet, was dann die Lösbarkeit von (1) zeigt. Modulo p ist nämlich nach WILSONs Satz

$$-1 \equiv (p-1)! = \Big(\frac{p-1}{2}\Big)! \prod_{j=1}^{(p-1)/2} (p-j) \equiv (-1)^{(p-1)/2} \Big(\frac{p-1}{2}\Big)!^2 = \Big(\frac{p-1}{2}\Big)!^2$$

wenn man zuletzt $p \equiv 1 \pmod 4$ berücksichtigt.

Wird umgekehrt (1) von einem ganzen x bei ungerader Primzahl p gelöst, so gilt nach dem "kleinen" FERMATschen Satz

$$1 \equiv x^{p-1} = (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Wegen $p \geq 3$ muß hier die Zahl rechts gleich 1 sein, was $p \equiv 1 \pmod 4$ nach sich zieht. □

Bemerkung. In (1) tritt erstmals eine polynomiale, nicht lineare Kongruenz auf; solche Kongruenzen werden ausführlich in § 4 behandelt.

§ 4. Polynomiale Kongruenzen

1. Problemstellung. Sei m eine natürliche Zahl. In einer gegenüber 1.5 leicht abgewandelten Schreibweise wurde dort das Polynom $f := a_0 + a_1 X \in \mathbb{Z}[X]$ betrachtet und nach Bedingungen an a_0, a_1 (d.h. also an f) und m gefragt, unter denen es ganze x gibt, die der Kongruenz $f(x) \equiv 0 \pmod m$ genügen. Im Falle der Existenz solcher x wurde in Satz 1.5 außerdem die Anzahl der modulo m inkongruenten derartigen x bestimmt.

Diese Fragestellung wird nun deutlich verallgemeinert, indem man beliebige Polynome $f \in \mathbb{Z}[X]$ zuläßt. Jedes ganze x mit $f(x) \equiv 0 \pmod m$ heißt eine *Wurzel von f modulo m*. Nach Satz 1.1(iv) ist unmittelbar klar, daß mit x auch jedes ganze x' eine Wurzel von f modulo m ist, welches in derselben Restklasse modulo m liegt wie x. Daher versteht man genau wie in 1.5 unter der *Lösungsanzahl von*

$$f(X) \equiv 0 \pmod m \tag{1}$$

modulo m die Anzahl der modulo m inkongruenten ganzen x, die (1) lösen; in Zeichen $\rho_f(m)$. Klar ist danach $\rho_f(m) \leq m$ für alle $m \in \mathbb{N}$ ebenso wie $\rho_f(1) = 1$, gleichgültig wie $f \in \mathbb{Z}[X]$ gewählt ist.

2. Reduktion auf Primzahlpotenzmoduln. Im folgenden Satz wird das Problem der Lösung von 1(1) reduziert auf das Problem der Lösung der k polynomialen Kongruenzen

$$f(X) \equiv 0 \pmod{p_\kappa^{a_\kappa}} \tag{1}$$

für $\kappa = 1, \ldots, k$, wenn $\prod_{\kappa=1}^{k} p_\kappa^{a_\kappa}$ die kanonische Primfaktorzerlegung von m ist.

Satz. *Sei* $m = \prod_{\kappa=1}^{k} p_\kappa^{a_\kappa} \geq 2$ *wie soeben und* $f \in \mathbb{Z}[X]$. *Man erhält alle Wurzeln* $x_1, \ldots, x_t$ $(t := \rho_f(m))$ *von* f *modulo* m, *indem man zuerst für* $\kappa = 1, \ldots, k$ *alle Wurzeln* $x_1^{(\kappa)}, \ldots, x_{t_\kappa}^{(\kappa)}$ $(t_\kappa := \rho_f(p_\kappa^{a_\kappa}))$ *von* f *modulo* $p_\kappa^{a_\kappa}$ *bestimmt und anschließend für jedes dann mögliche* k*–Tupel* $(x_{\tau_1}^{(1)}, \ldots, x_{\tau_k}^{(k)})$ *das simultane System*

$$X \equiv x_{\tau_\kappa}^{(\kappa)} \pmod{p_\kappa^{a_\kappa}} \quad \text{für } \kappa = 1, \ldots, k \tag{2}$$

mittels chinesischem Restsatz löst. Insbesondere gilt $\rho_f(m) = \prod_{\kappa=1}^{k} \rho_f\big(p_\kappa^{a_\kappa}\big)$, *d.h. die zahlentheoretische Funktion* ρ_f *ist multiplikativ.*

Beweis. Ist x_τ eine Lösung von 1(1), so löst x_τ auch (1) für jedes $\kappa = 1, \ldots, k$. Deswegen existiert ein eindeutig bestimmtes k–Tupel $(x_{\tau_1}^{(1)}, \ldots, x_{\tau_k}^{(k)})$ mit $1 \leq \tau_\kappa \leq t_\kappa$ für $\kappa = 1, \ldots, k$, so daß x_τ das simultane System (2) löst.

Geht man umgekehrt von einem k–Tupel $(x_{\tau_1}^{(1)}, \ldots, x_{\tau_k}^{(k)})$ aus, so ist das simultane System (2) vom Typ 2.1(3) und also nach dem chinesischen Restsatz 2.2 modulo m eindeutig lösbar. Ist x diese Lösung, so muß x für jedes $\kappa = 1, \ldots, k$ die Kongruenz (1) lösen, da ja $x_{\tau_\kappa}^{(\kappa)}$ die dem Index κ entsprechende Kongruenz (1) löst. Also löst x auch 1(1) und man hat $x \equiv x_\tau \pmod{m}$ für genau ein τ mit $1 \leq \tau \leq t$. □

Bemerkung. Der Beweis lehrte insbesondere die Gleichwertigkeit von $t = 0$ und $t_\kappa = 0$ für mindestens ein κ, d.h. die Äquivalenz von Unlösbarkeit von 1(1) und von (1) für wenigstens ein κ. Die Idee, 1(1) auf (1) zu reduzieren, findet sich übrigens bereits in 2.3, vgl. dort Formel (1).

3. Überlegungen zur weiteren Reduktion. In 4 wird das in 2 angefallene Problem der Lösung von 2(1) auf dasjenige zurückgeführt, die Kongruenz $f(X) \equiv 0 \pmod{p_\kappa}$ zu lösen. Diese Reduktion wird durch folgende Betrachtungen vorbereitet.

Sei p eine Primzahl und $a \geq 2$ ganz. Seien $y_1, \ldots, y_s$ bzw. $z_1, \ldots, z_t$ genau die inkongruenten Wurzeln von $f \in \mathbb{Z}[X]$ modulo p^{a-1} bzw. p^a, wobei $s = 0$ oder $t = 0$ möglich sind. Da aus $p^a | f(z_\tau)$ folgt $p^{a-1} | f(z_\tau)$ für jedes $\tau = 1, \ldots, t$, muß jedes z_τ modulo p^{a-1} kongruent genau einem y_σ sein.

Danach ist klar: Ist $s \geq 1$ und sind alle inkongruenten Wurzeln $y_1, \ldots, y_s$ von f modulo p^{a-1} bereits bekannt, so braucht man zur Auffindung der Wurzeln von f modulo p^a lediglich für jedes $\sigma = 1, \ldots, s$ die p modulo p^a inkongruenten Zahlen

$$y_\sigma + x p^{a-1}, \quad x \in \{0, 1, \ldots, p-1\} \tag{1}$$

zu bilden und nachzusehen, für welche dieser x die Zahl (1) Wurzel von f modulo p^a ist.

Kann man nun x so bestimmen, daß (1) tatsächlich Wurzel von f modulo p^a ist? Zur Beantwortung dieser Frage wird in 4 ein systematischer Weg aufgezeigt.

4. Reduktion auf Primzahlmoduln. Zunächst sei daran erinnert, daß man für $f = \sum_{i\geq 0} a_i X^i \in \mathbb{Z}[X]$ die λ–te Ableitung definiert durch $f^{(0)} := f$ und $f^{(\lambda)} := \sum_{i\geq\lambda} \lambda!\binom{i}{\lambda} a_i X^{i-\lambda}$ für $\lambda \in \mathbb{N}$; selbstverständlich sind höchstens endlich viele der a_i von Null verschieden. Ersichtlich gilt $\frac{1}{\lambda!} f^{(\lambda)} \in \mathbb{Z}[X]$ für $\lambda \in \mathbb{N}_0$ und überdies die (rein algebraisch beweisbare) TAYLOR–Formel für Polynome

$$f(X+Y) = \sum_{\lambda\geq 0} \frac{1}{\lambda!} f^{(\lambda)}(X) Y^\lambda; \tag{1}$$

dabei sind X, Y zwei Unbestimmte. Schreibt man noch wie üblich f' anstelle von $f^{(1)}$ für die erste Ableitung von f, so kann man formulieren den

Satz. *Sei $f \in \mathbb{Z}[X]$, p eine Primzahl, $a \geq 2$ eine ganze Zahl und die ganze Zahl y sei Wurzel von f modulo p^{a-1}. Dann gilt:*

(i) *Ist $p | f'(y)$ und y nicht selbst Wurzel von f modulo p^a, so hat f modulo p^a keine Wurzel, die modulo p^{a-1} kongruent y ist.*

(ii) *Ist $p \nmid f'(y)$, so hat f modulo p^a genau eine Wurzel z, die modulo p^{a-1} kongruent y ist; z ergibt sich dabei in der Form $y + xp^{a-1}$, wo x die modulo p eindeutige Lösung folgender linearen Kongruenz ist*

$$f'(y)X \equiv -\frac{f(y)}{p^{a-1}} \pmod{p}. \tag{2}$$

(iii) *Ist $p | f'(y)$ und y selbst schon Wurzel von f modulo p^a, so hat f modulo p^a genau p Wurzeln, die modulo p^{a-1} kongruent y sind; diese ergeben sich in der Form $y + xp^{a-1}$, wo x ein vollständiges Restsystem modulo p durchläuft.*

Beweis. Mittels (1) stellt man sofort fest, daß $y + xp^{a-1}$ (vgl. 3(1)) Wurzel von f modulo p^a ist genau dann, wenn modulo p^a gilt

$$0 \equiv f(y + xp^{a-1}) = \sum_{\lambda\geq 0} \frac{1}{\lambda!} f^{(\lambda)}(y) x^\lambda p^{(a-1)\lambda} \equiv f(y) + f'(y) x p^{a-1}. \tag{3}$$

Dabei hat man $(a-1)\lambda \geq a$ für $\lambda \geq 2$ beachtet, was wegen $a \geq 2$ wahr ist; weiter ist die Ganzheit aller $\frac{1}{\lambda!}f^{(\lambda)}(y)$ berücksichtigt. Nun ist $\frac{f(y)}{p^{a-1}}$ nach Voraussetzung des Satzes ganz; die Kongruenz der Zahlen ganz links und ganz rechts in (3) modulo p^a ist daher nach Satz 1.3 damit äquivalent, daß x die lineare Kongruenz (2) löst. Nach Satz 1.5 ist diese aber genau dann lösbar, wenn $(f'(y), p) | f(y) p^{1-a}$ gilt, und in diesem Falle gibt es $(f'(y), p)$ modulo p inkongruente Lösungen. Die Lösungsanzahl von (2) ist also 0 bzw. 1 bzw. p und zwar genau dann, wenn $p | f'(y)$, $p^a \nmid f(y)$ bzw. $p \nmid f'(y)$ bzw. $p | f'(y)$, $p^a | f(y)$ gilt. Nacheinander sind dies genau die Fälle (i), (ii), (iii) im Satz. □

5. Polynomkongruenzen bei Primzahlmoduln. Zunächst wird der Begriff der Kongruenz zwischen ganzen Zahlen ausgedehnt zum Begriff der Kongruenz zwischen Polynomen in einer Unbestimmten mit ganzzahligen Koeffizienten: Für Primzahlen p heißen $f, g \in \mathbb{Z}[X]$ *kongruent modulo p* (in Zeichen: $f \equiv g \pmod{p}$ oder $f(X) \equiv g(X) \pmod{p}$, Negation: $f \not\equiv g \pmod{p}$) genau dann, wenn $a_i \equiv b_i \pmod{p}$ für alle ganzen $i \geq 0$ gilt, wobei $f = \sum_{i \geq 0} a_i X^i$, $g = \sum_{i \geq 0} b_i X^i$ ist.

Sei f wie soeben und 0 das Nullpolynom. Ist dann $f \not\equiv 0 \pmod{p}$, d.h. sind nicht alle a_i durch p teilbar, so heißt der größte Index i mit $p \nmid a_i$ *der Grad von f modulo p*. Dieser wird als $\partial(f; p)$ notiert in Anlehnung an den (gewöhnlichen) Grad eines Polynoms f, der in 1.5.7 durch $\partial(f)$ abgekürzt wurde.

Beispiel. Es werde das Polynom $f := 21 + 3X^2 + 24X^3$ betrachtet. Offenbar ist $f \equiv 0 \pmod{p}$ genau dann, wenn $p | (21, 3, 24)$, d.h. wenn $p = 3$ gilt. Weiter ist $\partial(f; 2) = 2$ und $\partial(f; p) = 3$ für alle Primzahlen $p > 3$.

Aus dem folgenden Satz wird ein Ergebnis über die Anzahl der inkongruenten Wurzeln eines ganzzahligen Polynoms modulo einer Primzahl abgeleitet.

Satz. *Seien $f \in \mathbb{Z}[X]$, p eine Primzahl und $f \not\equiv 0 \pmod{p}$. Sind die ganzen Zahlen $x_1, \ldots, x_s$ paarweise inkongruente Wurzeln von f modulo p, so gilt*

(i) die Kongruenz $f(X) \equiv g_s(X) \prod_{\sigma=1}^{s} (X - x_\sigma) \pmod{p}$ mit einem $g_s \in \mathbb{Z}[X]$, welches den Bedingungen $g_s \not\equiv 0 \pmod{p}$ und $\partial(g_s; p) = \partial(f; p) - s$ genügt,

(ii) die Ungleichung $s \leq \partial(f; p)$.

Korollar. *Für f, p wie im vorstehenden Satz gilt*

$$\rho_f(p) \leq \mathrm{Min}(p, \partial(f; p)).$$

Beweis des Satzes. Ersichtlich ist (ii) eine Konsequenz von (i), man beachte $\partial(g_s;p) \geq 0$. Die Aussage (i) wird durch Induktion nach s bewiesen. Bei $s = 0$ ist die Behauptung klar, man wähle einfach $g_0 := f$. Sei jetzt $\partial(f;p) > 0$ und es werde vorausgesetzt, daß (i) für ein $s \in \{0, \ldots, \partial(f;p)-1\}$ schon eingesehen ist. Hat f dann noch eine zu den $x_1, \ldots, x_s$ modulo p inkongruente Wurzel x_{s+1}, so gilt mit der Induktionsvoraussetzung

$$0 \equiv f(x_{s+1}) \equiv g_s(x_{s+1}) \prod_{\sigma=1}^{s} (x_{s+1} - x_\sigma) \pmod{p}.$$

Da p keine der Differenzen $x_{s+1} - x_\sigma$ im Produkt teilt, ist x_{s+1} eine Wurzel von g_s modulo p. Das letztere ist offenbar damit äquivalent, daß $\bar{x}_{s+1} \in \mathbb{Z}_p$ (vgl. 1.7 und Bemerkung 4 zu 1.8) Nullstelle von $\bar{g}_s \in \mathbb{Z}_p[X] \setminus \{\overline{0}\}$ ist, wobei $\bar{g}_s$ dadurch aus g_s hervorgeht, daß man sämtliche Koeffizienten von g_s durch ihre Restklassen modulo p ersetzt. Das Abspaltungslemma 1.5.8, angewandt mit $K := \mathbb{Z}_p$, $f := \bar{g}_s$, $c := \bar{x}_{s+1}$, garantiert die Existenz eines $\bar{g}_{s+1} \in \mathbb{Z}_p[X] \setminus \{\overline{0}\}$ mit

$$\bar{g}_s(X) = (X - \bar{x}_{s+1})\bar{g}_{s+1}(X) \quad \text{und} \quad \partial(\bar{g}_s) = 1 + \partial(\bar{g}_{s+1}). \tag{1}$$

Wählt man nun $g_{s+1} \in \mathbb{Z}[X]$, so daß sich bei Ersetzung seiner Koeffizienten durch ihre Restklassen modulo p gerade $\bar{g}_{s+1}$ ergibt, so ist modulo p

$$g_{s+1} \not\equiv 0, \quad g_s(X) \equiv (X - x_{s+1})g_{s+1}(X) \quad \text{und} \quad \partial(g_s;p) = 1 + \partial(g_{s+1};p)$$

wegen (1). Damit ist (i) induktiv bewiesen. □

Bemerkung. Ist p eine Primzahl, so hat das Polynom $X^{p-1} - 1$ nach dem "kleinen" FERMATschen Satz 3.3 die paarweise inkongruenten Wurzeln $1, 2, \ldots, p-1$ modulo p. Nach Teil (i) des obigen Satzes ist

$$X^{p-1} - 1 \equiv \prod_{\sigma=1}^{p-1} (X - \sigma) \pmod{p}$$

woraus in Gestalt von $-1 \equiv (p-1)! \pmod{p}$ der "nichttriviale" Teil des WILSONschen Satzes 3.8 nochmals folgt.

6. Ein Beispiel. Hier soll eine Anwendung der Ergebnisse dieses Paragraphen gegeben werden.

Für $f := X^2 + 1$ wurde in Satz 3.9 gezeigt: $\rho_f(2) = 1$ sowie $\rho_f(p)$ gleich 2 bzw. 0, je nachdem, ob die ungerade Primzahl p kongruent 1 bzw. 3 modulo 4 ist.

Wegen $\rho_f(4) = 0$ ist $\rho_f(2^a) = 0$ für alle ganzen $a \geq 2$. Sei jetzt $p \equiv 1 \pmod 4$. Dann ist nach Satz 3.9 und Satz 5(i) mit $y := (\frac{p-1}{2})!$

$$f \equiv (X - y)(X + y) \pmod p.$$

Wegen $p \not| f'(\pm y) = \pm 2y$ hat f modulo p^2 genau eine Wurzel z_1 bzw. z_2, die modulo p kongruent y bzw. $-y$ ist, und also hat man $\rho_f(p^2) = 2$. Dies ergibt sich aus Satz 4(ii). Wegen $p \not| y$ ist $p \not| z_1 z_2$ und so kann man das letzte Argument erneut anwenden und erhält $\rho_f(p^a) = 2$ für jedes $a \geq 1$. Wegen der in Satz 2 festgestellten Multiplikativität von ρ_f kann nun gesagt werden: $\rho_f(m)$ ist positiv genau dann, wenn $m = 2^\delta \prod_{\kappa=1}^{k} p_\kappa^{a_\kappa}$ gilt mit $\delta \in \{0, 1\}$, $k \in \mathbb{N}_0$ und $p_\kappa \equiv 1 \pmod 4$ für $\kappa = 1, \ldots, k$, falls $k > 0$; dann ist $\rho_f(m) = \prod_{\kappa=1}^{k} \rho_f(p_\kappa^{a_\kappa}) = 2^k$.

§ 5. Primitivwurzeln

1. Definition. In diesem Paragraphen wird eine Problematik wieder aufgenommen und fortgeführt, die bereits verschiedentlich in § 3 angeklungen ist. Begonnen wird mit der Ermittlung von $\operatorname{ord}_m a^i$ aus i und $\operatorname{ord}_m a$ in folgender

Proposition A. *Seien $m > 0$ und a ganze, teilerfremde Zahlen und sei $k := \operatorname{ord}_m a$. Dann gilt $\operatorname{ord}_m a^i = \frac{k}{(i,k)}$ für alle ganzen $i \geq 0$. Insbesondere sind genau die a^i wieder von der Ordnung k modulo m, für die $(i, k) = 1$ gilt.*

Beweis. Man setzt $k(i) := \operatorname{ord}_m a^i$, weiß dann $a^{ik(i)} \equiv 1 \pmod m$ und somit $k | ik(i)$ nach Korollar 3.4, also $\frac{k}{(i,k)} | k(i)$. Andererseits ist wegen $a^k \equiv 1 \pmod m$ auch $a^{ik/(i,k)} \equiv 1 \pmod m$, also $k(i) | \frac{k}{(i,k)}$ nach demselben Korollar, was die Behauptung beweist. □

Nun wird folgende, auf EULER zurückgehende Definition gegeben: Seien $m > 0$ und a ganze, teilerfremde Zahlen; genau dann, wenn $\operatorname{ord}_m a = \varphi(m)$ gilt, heißt a eine *Primitivwurzel modulo m*.

Wenn also a Primitivwurzel modulo m ist, sind $a, a^2, \ldots, a^{\varphi(m)}$ paarweise inkongruent modulo m nach 3.2. Außerdem sind diese $\varphi(m)$ Zahlen sämtliche zu m teilerfremd und bilden somit in ihrer Gesamtheit ein primes Restsystem modulo m, vgl. 1.8. Hat man umgekehrt ein ganzes a, für das $a, a^2, \ldots, a^{\varphi(m)}$ ein primes Restsystem modulo m bilden, so ist offenbar a eine Primitivwurzel modulo m. Die hier festgestellte Äquivalenz kann in der Sprache von 1.8 formuliert werden als

Proposition B. *Für ganze Zahlen $m > 0$ sind gleichbedeutend:*
(i) Modulo m gibt es eine Primitivwurzel.
(ii) Die prime Restklassengruppe modulo m ist zyklisch.

Ohne die Frage nach der Existenz von Primitivwurzeln modulo einem vorgegebenen m schon jetzt zu klären, sagt

Proposition C. *Sei $m > 0$ ganz. Wenn es modulo m überhaupt Primitivwurzeln gibt, so existieren genau $\varphi(\varphi(m))$ paarweise modulo m inkongruente.*

Beweis. Sei a eine Primitivwurzel modulo m; dann ist $\mathrm{ord}_m a = \varphi(m)$. Nach Proposition A sind genau die a^i wieder Primitivwurzeln modulo m, für die $(i, \varphi(m)) = 1$ gilt, was die Behauptung liefert. □

Ob es zu einem vorgegebenen natürlichen m überhaupt Primitivwurzeln gibt, ist im Moment noch eine offene Frage, die erst in 5 vollständig geklärt sein wird. Betrachtet man beispielsweise die Fälle m gleich 14 bzw. 15, so ist $\varphi(m)$ gleich 6 bzw. 8. Modulo 14 sind die Potenzen von 3 gleich 3, 9, -1, -3, -9, 1; somit ist 3 eine Primitivwurzel modulo 14 und wegen $\varphi(\varphi(14)) = 2$ muß es noch genau eine weitere geben, vgl. Proposition C. Es zeigt sich, daß diese 5 modulo 14 ist. Wegen $\mathrm{ord}_{15} 1 = 1$, $\mathrm{ord}_{15} a = 2$ für $a \equiv -1, \pm 4 \pmod{15}$ und $\mathrm{ord}_{15} a = 4$ für $a \equiv \pm 2, \pm 7 \pmod{15}$ gibt es modulo 15 keine Primitivwurzeln.

2. Primitivwurzeln modulo Primzahlen. Der hier zu zeigende Satz beinhaltet insbesondere, daß es Primitivwurzeln modulo jeder Primzahl gibt. Dies wurde von J.H. Lambert (Opera Mathematica II, 198–213) behauptet. Euler (Opera Omnia Ser. 1, III, 240–281) gab einen nicht ganz kompletten Beweis, während Gauss (*Disquisitiones Arithmeticae*, Artt. 52–55) mit einer Methode, die unten vorgeführt wird, zeigen konnte

Satz. *Sei p eine Primzahl und $d > 0$ ein Teiler von $p - 1$. Dann existieren genau $\varphi(d)$ modulo p inkongruente ganze Zahlen, die modulo p die Ordnung d haben. Insbesondere gibt es $\varphi(p-1)$ modulo p inkongruente Primitivwurzeln modulo p.*

Beweis. Sei nämlich T ein primes Restsystem modulo p. Für alle $t \in T$ ist $(\mathrm{ord}_p t) | (p-1)$ und für ganzes $d > 0$ mit $d | (p-1)$ bezeichne $\psi(d)$ die Anzahl der $t \in T$ mit $\mathrm{ord}_p t = d$. Klar ist

$$\sum_{d|(p-1)} \psi(d) = p - 1. \tag{1}$$

Nun ist entweder $\psi(d) = 0$ oder es gibt ein $t_0 \in T$ mit $\mathrm{ord}_p t_0 = d$; im zweiten Fall sind $t_0, t_0^2, \ldots, t_0^d$ paarweise inkongruent modulo p und sie sind Wurzeln von $f_d := X^d - 1$ modulo p. Andererseits kann f_d nach Korollar 4.5 höchstens d modulo p inkongruente Wurzeln haben. Das heißt aber: Jede Wurzel von f_d modulo p ist kongruent t_0^i für genau ein $i \in \{1, \ldots, d\}$. Nun interessieren offenbar genau diejenigen i mit $\mathrm{ord}_p t_0^i = d$. Nach Proposition 1A sind dies genau die zu d teilerfremden $i \in \{1, \ldots, d\}$ und davon gibt es $\varphi(d)$ Stück. Bei $\psi(d) > 0$ gilt also $\psi(d) = \varphi(d)$, d.h. $\varphi(d) \geq \psi(d)$ für alle positiven Teiler d von $(p-1)$. Aus Satz 1.4.11(iii) und (1) ergibt sich dann

$$p - 1 = \sum_{d|(p-1)} \varphi(d) \geq \sum_{d|(p-1)} \psi(d) = p - 1,$$

was $\psi(d) = \varphi(d)$ nun für alle positiven Teiler d von $p-1$ impliziert. □

Oftmals nützlich ist noch das als Nebenergebnis angefallene

Korollar. *Ist p eine Primzahl und kennt man eine Primitivwurzel t_0 modulo p, so sind die $\varphi(p-1)$ Potenzen t_0^i mit zu $p-1$ teilerfremdem $i \in \{1, \ldots, p-1\}$ genau die sämtlichen Primitivwurzeln modulo p.*

Bemerkungen. 1) In der Bemerkung zu 3.4 wurde (in der in 1 eingeführten Sprechweise) angekündigt, daß es zu unendlich vielen $m \in \mathbb{N}$ Primitivwurzeln gibt. Dies ist natürlich im obigen Satz enthalten.

2) Mittels Proposition 1B kann für Primzahlen p aus dem Hauptergebnis des gegenwärtigen Abschnitts geschlossen werden: *Die prime Restklassengruppe modulo p ist zyklisch.* Anders ausgedrückt: *Die multiplikative Gruppe $\mathbb{Z}_p^\times$ des Körpers $\mathbb{Z}_p$* (vgl. 1.7) *ist zyklisch.* Dies ist Spezialfall eines allgemeineren Satzes aus der Algebra: Ist K ein Körper, so ist jede *endliche* Untergruppe von $K^\times$ zyklisch.

3. Tabellen für Primitivwurzeln. Es sei eine kurze Tabelle für die sämtlichen $\varphi(p-1)$ Primitivwurzeln modulo der Primzahlen $p < 50$ angefügt.

p	$\varphi(p-1)$	Primitivwurzeln modulo p
2	1	1
3	1	2
5	2	2,3
7	2	3,5
11	4	2,6,7,8
13	4	2,6,7,11
17	8	3,5,6,7,10,11,12,14
19	6	2,3,10,13,14,15
23	10	5,7,10,11,14,15,17,19,20,21
29	12	2,3,8,10,11,14,15,18,19,21,26,27
31	8	3,11,12,13,17,21,22,24
37	12	2,5,13,15,17,18,19,20,22,24,32,35
41	16	6,7,11,12,13,15,17,19,22,24,26,28,29,30,34,35
43	12	3,5,12,18,19,20,26,28,29,30,33,34
47	22	5,10,11,13,15,19,20,22,23,26,29,30,31,33,35,38,39,40,41,43,44,45

Es soll beispielsweise erklärt werden, wie hier die 22 Primitivwurzeln modulo 47 gefunden wurden. Nach Korollar 3.4 gilt $\mathrm{ord}_{47}a \in \{1, 2, 23, 46\}$ für alle ganzen, nicht durch 47 teilbaren Zahlen a. Wegen $2^{12} = 4096 = 47 \cdot 87 + 7 \equiv 7 \pmod{47}$ ist $2^{24} \equiv 49 \equiv 2 \pmod{47}$, also $\mathrm{ord}_{47}2 = 23$. Weiter gilt wegen $3^5 \equiv 8 \pmod{47}$, $3^{11} \equiv 4 \pmod{47}$ die Kongruenz $3^{23} \equiv 1 \pmod{47}$, was zu $\mathrm{ord}_{47}3 = 23$ führt. Nach dem "kleinen" FERMAT–Satz 3.3 ist $4^{23} = 2^{46} \equiv 1 \pmod{47}$, also auch $\mathrm{ord}_{47}4 = 23$ und als kleinste positive Primitivwurzel modulo 47 kommt erst 5 in Frage. Wegen $5^{23} \equiv -1 \pmod{47}$ ist tatsächlich $\mathrm{ord}_{47}5 = 46$, also 5 *eine* Primitivwurzel modulo 47. Nach Korollar 2 erhält man daraus leicht *alle* Primitivwurzeln modulo 47.

Bei dem hier durchgeführten Beispiel sieht es so aus, als hätte man zur Ermittlung einer ersten Primitivwurzel modulo 47 einfach die Zahlen 2, 3, 4, 5 nacheinander durchprobiert. Es gibt aber manche Hilfen, die das Probierverfahren oft abkürzen; eine solche ist enthalten im

Lemma. *Sei $m \in \mathbb{N}$ und die ganzen Zahlen a_1, a_2 seien zu m teilerfremd; weiter seien $\mathrm{ord}_m a_1$, $\mathrm{ord}_m a_2$ zueinander teilerfremd. Dann gilt*

$$\mathrm{ord}_m a_1 a_2 = (\mathrm{ord}_m a_1)(\mathrm{ord}_m a_2).$$

Beweis. Ist $k := \mathrm{ord}_m a_1 a_2$ und $k_i := \mathrm{ord}_m a_i$ für $i = 1, 2$, so folgt aus $a_i^{k_i} \equiv 1 \pmod{m}$ sofort $a_i^{k_1 k_2} \equiv 1 \pmod{m}$ für $i = 1, 2$ und daraus $(a_1 a_2)^{k_1 k_2} \equiv$

$1 \pmod m$, woraus man $k|k_1k_2$ erhält. Andererseits führt $a_1^k a_2^k \equiv 1 \pmod m$ zu $a_1^{kk_2} \equiv 1 \pmod m$, also $k_1|kk_2$; wegen $(k_1, k_2) = 1$ bedeutet dies $k_1|k$. Analog folgt $k_2|k$ und somit $k_1k_2|k$, erneut wegen $(k_1, k_2) = 1$. Mit $k = k_1k_2$ hat man die Behauptung. □

Aufgrund dieses Lemmas kann man schon in dem Moment eine Primitivwurzel modulo 47 angeben, wo man $\mathrm{ord}_{47}2 = 23$ erkannt hat, also sofort nach dem ersten (Fehl–)Versuch, eine möglichst kleine Primitivwurzel modulo 47 zu finden. Wegen $\mathrm{ord}_{47}(-1) = 2$, $\mathrm{ord}_{47}2 = 23$ ist nämlich nach dem Lemma $\mathrm{ord}_{47}(-2) = 2 \cdot 23 = 46$ und so ist $-2 \equiv 45$ eine Primitivwurzel modulo 47. Dies ist die letzte in der $p = 47$ entsprechenden Zeile obiger Tabelle; auch aus ihr ergeben sich selbstverständlich sämtliche weiteren Primitivwurzeln derselben Zeile mittels Korollar 2.

Nach diesem Korollar ist es einleuchtend, warum in den meisten Tafeln über Primitivwurzeln, die man in der Literatur findet, meistens nur die *kleinste positive* Primitivwurzel modulo der Primzahlen p angegeben ist. Die erste umfangreichere solche Tafel für $p < 1000$ findet sich bei C.G.J. Jacobi (*Canon Arithmeticus*, 1839; Neuausgabe: Akademie–Verlag, Berlin, 1956). Wesentlich weitreichender ist das Tafelwerk für $p \leq 50021$ von A.E. Western und J.C.P. Miller (*Tables of Indices and Primitive Roots*, University Press, Cambridge, 1968).

Bemerkungen. 1) Ein Blick auf obige Tabelle suggeriert, daß für jede Primzahl $p \neq 3$ das Produkt aller $\varphi(p-1)$ inkongruenten Primitivwurzeln modulo p kongruent $1 \pmod p$ ist; der Leser möge dies als Übung beweisen.

2) Betrachtet man obige Tabelle nicht "horizontal", sondern "vertikal", so hat E. Artin (Collected Papers, viii–x) im Jahre 1927 die Vermutung geäußert, daß jedes vorgegebene ganze $a \neq -1$, das keine Quadratzahl ist, Primitivwurzel modulo p für unendlich viele Primzahlen p ist. Daß hier die Ausnahmen $a \neq -1, 0$ ganz natürlich sind, ist klar. Ist a eine positive Quadratzahl, etwa $a = b^2$, so ist $a^{(p-1)/2} = b^{p-1} \equiv 1 \pmod p$ für alle ungeraden Primzahlen p mit $p \not| a$; modulo aller genügend großen p können diese a also sicher keine Primitivwurzeln sein. Einen bedeutenden Fortschritt in Richtung auf die noch offene Artinsche Vermutung hat C. Hooley (J. Reine Angew. Math. *225*, 209–220 (1967)) erzielt, allerdings unter Annahme der Richtigkeit einer anderen derzeit unbewiesenen Hypothese. Ohne jede unbewiesene Voraussetzung konnte D.R. Heath-Brown (Quart. J. Math. Oxford (2) *37*, 27–38 (1986)) ein überaus interessantes Resultat sichern, aus dem z.B. folgt, daß bis auf höchstens zwei Ausnahmen jede Primzahl a Primitivwurzel modulo p für unendlich viele Primzahlen p ist.

4. Zu welchen Moduln sind Primitivwurzeln möglich? Um diese Frage möglichst präzise beantworten zu können, sei vorausgeschickt folgendes

Lemma. *Sind $m_1, m_2 \in \mathbb{N}$ und $a \in \mathbb{Z}$ paarweise teilerfremd und ist $n_i \in \mathbb{N}$ Vielfaches von $\operatorname{ord}_{m_i} a$ für $i = 1, 2$, so ist $\frac{n_1 n_2}{(n_1, n_2)}$ Vielfaches von $\operatorname{ord}_{m_1 m_2} a$.*

Beweis. Bei $k_i := \operatorname{ord}_{m_i} a$, $k := \operatorname{ord}_{m_1 m_2} a$ gilt $k = \operatorname{kgV}(k_1, k_2) = \frac{k_1 k_2}{(k_1, k_2)}$ nach Lemma 3.5 und Satz 1.2.12A. Weiter gilt $n_i = k_i \ell_i$ für $i = 1, 2$ mit geeignetem $\ell_i \in \mathbb{N}$ nach Voraussetzung. Die Behauptung ist also mit $\frac{k_1 k_2}{(k_1, k_2)} \mid \frac{k_1 k_2 \ell_1 \ell_2}{(k_1 \ell_1, k_2 \ell_2)}$, d.h. mit $(k_1 \ell_1, k_2 \ell_2) \mid \ell_1 \ell_2 (k_1, k_2)$ äquivalent und letzteres ist direkt einsichtig. □

Das soeben gezeigte Lemma gestattet es nun, die Moduln, zu denen es Primitivwurzeln geben kann, weitgehend einzuschränken.

Proposition. *Modulo $m \in \mathbb{N}$ existieren höchstens dann Primitivwurzeln, wenn m gleich 1, 2, 4, p^α, $2p^\alpha$ mit ungerader Primzahl p und natürlichem α ist.*

Beweis. Für a, m_1, m_2 wie im Lemma gilt $(\operatorname{ord}_{m_i} a) \mid \varphi(m_i)$ für $i = 1, 2$ nach Korollar 3.4. Unter Berücksichtigung der Multiplikativität von φ (vgl. Satz 1.4.11(i)) und der Teilerfremdheit von m_1, m_2 ist $\frac{\varphi(m_1 m_2)}{(\varphi(m_1), \varphi(m_2))}$ nach dem Lemma Vielfaches von $\operatorname{ord}_{m_1 m_2} a$. Dies bedeutet: Modulo solcher $m \in \mathbb{N}$, die eine Zerlegung $m = m_1 m_2$ mit teilerfremden $m_1, m_2 \in \mathbb{N}$ und $(\varphi(m_1), \varphi(m_2)) > 1$ zulassen, kann es keine Primitivwurzeln geben.

Es werde erst der Fall betrachtet, daß m von einer ungeraden Primzahl geteilt wird, etwa von p. Sei hier $m = p^\alpha m'$ mit $m', \alpha \in \mathbb{N}$, $p \not| m'$; wegen $p^\alpha \geq 3$ und Korollar 1.4.11(iv) ist $\varphi(p^\alpha)$ gerade. Wenn also modulo m eine Primitivwurzel existiert, muß $\varphi(m')$ ungerade, also gleich 1 sein; dies läßt nur m' gleich 1 oder 2 zu.

Um den Fall $m = 2^\alpha$ zu behandeln, wird behauptet, daß bei ungeradem ganzem u die Kongruenz

$$u^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha} \quad \text{für } \alpha = 3, 4, \ldots \tag{1}$$

gilt. Zunächst hat man $u^2 = (2v+1)^2 = 4v(v+1) + 1 \equiv 1 \pmod 8$ mit ganzem v wegen der Ungeradheit von u; dies beweist (1) für $\alpha = 3$. Sei nun (1) schon für ein $\alpha \geq 3$ als richtig erkannt; (1) ist äquivalent mit einer Gleichung $u^{2^{\alpha-2}} = 1 + 2^\alpha w$ bei geeignetem ganzem w. Durch Quadrieren folgt hieraus $u^{2^{\alpha-1}} = 1 + 2^{\alpha+1} w + 2^{2\alpha} w^2 \equiv 1 \pmod{2^{\alpha+1}}$ und dies ist (1) für $\alpha + 1$ anstelle von α.

Wegen $\varphi(2^\alpha) = 2^{\alpha-1}$ ist $(\operatorname{ord}_{2^\alpha} u) \mid \frac{1}{2}\varphi(2^\alpha)$ nach (1) für $\alpha = 3, 4, \ldots$ und jedes ungerade ganze u. Da jede Primitivwurzel modulo 2^α, $\alpha > 2$, ungerade sein müßte, kann es solche nach der zuletzt festgestellten Teilbarkeitsbeziehung nicht geben. □

5. Bestimmung aller Moduln mit Primitivwurzeln. Die Aussage der letzten Proposition geht auf GAUSS (*Disquisitiones Arithmeticae*, Art. 92) zurück. Implizit findet sich im gleichen Werk schon an früherer Stelle, daß es zu den in der Proposition genannten Moduln tatsächlich Primitivwurzeln gibt. Damit ist auch klar, warum am Ende von 1 Primitivwurzeln modulo 14, jedoch nicht modulo 15 gefunden werden konnten.

Um das volle GAUSSsche Ergebnis beweisen zu können, benötigt man folgendes

Lemma . *Zu jeder Primzahl p gibt es eine Primitivwurzel a modulo p mit $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

Beweis. Bei ganzem a_1 und $a_2 := a_1 + p$ gilt nach Lemma 3.3

$$a_2^p = \sum_{j=0}^{p} \binom{p}{j} a_1^j p^{p-j} \equiv a_1^p \pmod{p^2}. \tag{1}$$

Nach dem "kleinen" FERMATschen Satz 3.3 ist $a_j^p = a_j + b_j p$ mit ganzem b_j für $j = 1, 2$; dies in (1) eingetragen führt unter Berücksichtigung der Kürzungsregel 1.3 zur Kongruenz $b_2 \equiv b_1 - 1 \pmod{p}$ und so ist höchstens eines der b_1, b_2 durch p teilbar. Nun wähle man a_1 als Primitivwurzel modulo p, was nach Satz 2 möglich ist; a_2 ist ebenfalls Primitivwurzel modulo p. Nach den Feststellungen über die b_j ist aber $p^2 \not| (a_j^p - a_j)$ für mindestens ein j. □

Satz von Gauss. *Modulo $m \in \mathbb{N}$ existieren genau dann Primitivwurzeln, wenn m gleich 1, 2, 4, p^α, $2p^\alpha$ mit ungerader Primzahl p und natürlichem α ist.*

Beweis. Zunächst sind 1, 1, 3 Primitivwurzeln modulo 1, 2, 4 in dieser Reihenfolge. Für den Rest des Beweises seien p, α wie im Satz.

Sei a eine Primitivwurzel modulo p^α; dann gibt es auch eine *ungerade* Primitivwurzel $\hat{a}$ modulo p^α: Man nehme für $\hat{a}$ etwa die ungerade der beiden Zahlen a und $a+p^\alpha$ und hat $(\hat{a}, 2p^\alpha) = 1$. Für $k := \operatorname{ord}_{2p^\alpha} \hat{a}$ gilt $k | \varphi(2p^\alpha) \Leftrightarrow k | (p-1)p^{\alpha-1}$ nach Korollar 3.4; da $\hat{a}^k \equiv 1 \pmod{2p^\alpha}$ die Kongruenz $\hat{a}^k \equiv 1 \pmod{p^\alpha}$ impliziert, ist $(p-1)p^{\alpha-1} | k$, erneut nach Korollar 3.4. Man hat also $k = (p-1)p^{\alpha-1} = \varphi(2p^\alpha)$ und so ist $\hat{a}$ Primitivwurzel modulo $2p^\alpha$.

Im folgenden muß lediglich noch gezeigt werden, daß es modulo p^α Primitivwurzeln gibt. Dazu wird a dem vorausgeschickten Lemma gemäß gewählt und

$$a^{(p-1)p^{\alpha-2}} \not\equiv 1 \pmod{p^\alpha} \tag{2}$$

für $\alpha = 2, 3, \ldots$ behauptet. Während (2) für $\alpha = 2$ mit dem Lemma erledigt ist, werde nun (2) für ein $\alpha \geq 2$ als richtig vorausgesetzt. Unter Beachtung von $\varphi(p^{\alpha-1}) = (p-1)p^{\alpha-2}$ folgt aus (2) mit dem FERMAT–EULERschen Satz 3.4

$$a^{(p-1)p^{\alpha-2}} = 1 + bp^{\alpha-1} \tag{3}$$

mit ganzem, nicht durch p teilbarem b. Aus (3) ergibt sich durch Potenzieren

$$a^{(p-1)p^{\alpha-1}} = (1 + bp^{\alpha-1})^p = 1 + bp^{\alpha} + cp^{2\alpha-1} \tag{4}$$

mit ganzem c wegen $p|\binom{p}{2}$, vgl. Lemma 3.3. Mit Rücksicht auf $2\alpha - 1 \geq \alpha + 1$ für $\alpha \geq 2$ und $p \nmid b$ beinhaltet (4) die Richtigkeit von (2) für $\alpha + 1$ anstelle von α.

Ist a weiterhin dem Lemma gemäß gewählt, so ist es zu p^α teilerfremd, und man kann $\ell := \mathrm{ord}_{p^\alpha} a$ definieren. Nach Korollar 3.4 ist $\ell | \varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Andererseits folgt aus $a^\ell \equiv 1 \pmod{p^\alpha}$ erst recht $a^\ell \equiv 1 \pmod{p}$ und somit $(p-1)|\ell$ wegen $\mathrm{ord}_p a = p - 1$. Damit muß $\ell = (p-1)p^\beta$ mit einem $\beta \in \{0, \ldots, \alpha - 1\}$ gelten, d.h. $a^{(p-1)p^\beta} \equiv 1 \pmod{p^\alpha}$. Wegen (2) ist hier $\beta \leq \alpha - 2$ unmöglich und so bleibt nur $\beta = \alpha - 1$, was $\mathrm{ord}_{p^\alpha} a = \ell = (p-1)p^{\alpha-1} = \varphi(p^\alpha)$ beweist. □

Bemerkung. Nach dem GAUSSschen Satz und Proposition 1B ist die prime Restklassengruppe $\mathbb{Z}^*_{p^\alpha}$ modulo p^α für natürliche α und Primzahlen p genau dann zyklisch, wenn nicht gleichzeitig $p = 2$ und $\alpha \geq 3$ gelten. Daher kann nach der Bemerkung zu 2.5 gesagt werden:

Ist $m \geq 2$ eine ganze Zahl mit der kanonischen Zerlegung $\prod_{\kappa=1}^{k} p_\kappa^{\alpha_\kappa}$, so ist $\mathbb{Z}^*_m$ isomorph zum direkten Produkt der primen Restklassengruppen modulo $p_\kappa^{\alpha_\kappa}$ für $\kappa = 1, \ldots, k$ und diese letzteren sind sämtliche zyklisch, falls nur $8 \nmid m$ gilt. Ist jedoch $8|m$ und etwa $p_1 = 2$, so ist $\mathbb{Z}^*_{p_1^{\alpha_1}}$ sicher *nicht* zyklisch.

Dennoch muß $\mathbb{Z}^*_m$ auch in diesem Fall isomorph dem direkten Produkt geeigneter zyklischer Gruppen von Primzahlpotenzordnung sein; dies lehrt der Hauptsatz über endliche abelsche Gruppen von G. FROBENIUS und L. STICKELBERGER (J. Reine Angew. Math. *86*, 217–262 (1879)). Für die Darstellung von $\mathbb{Z}^*_m$ bei $8|m$ als direktes Produkt zyklischer Gruppen reicht es offenbar nach den vorstehenden Erörterungen, $\mathbb{Z}^*_{2^\alpha}$ bei $\alpha \geq 3$ noch als direktes Produkt geeigneter zyklischer Gruppen von Primzahlpotenzordnung auszudrücken, was im folgenden Abschnitt geschehen soll.

6. Zweierpotenzen als Moduln. Dazu wird vorangestellt folgendes

Lemma. *Bei ungeradem ganzem u sind äquivalent:*
(i) $\operatorname{ord}_{2^\alpha} u = 2^{\alpha-2}$ *für alle* $\alpha = 3, 4, \ldots$.
(ii) $u \equiv \pm 3 \pmod 8$.

Beweis. In beiden Fällen $u \equiv \pm 1 \pmod{2^3}$ ist $u^2 \equiv 1 \pmod{2^4}$ und daher induktiv $u^{2^{\alpha-3}} \equiv 1 \pmod{2^\alpha}$ für alle $\alpha \geq 4$, also $(\operatorname{ord}_{2^\alpha} u) | 2^{\alpha-3}$ für dieselben α und die Gleichung in (i) kann hier nicht gelten.

Sei nun $u \equiv \pm 3 \pmod 8$. Dann ist $u^{2^\beta} - 1 = 2^{\beta+2} v_\beta$ für alle $\beta \in \mathbb{N}$ mit ungeradem ganzem v_β. Für $\beta = 1$ ist dies nämlich leicht ersichtlich und, wenn die Gleichung für ein $\beta \geq 1$ wahr ist, ist $u^{2^\beta} + 1 = 2w_\beta$ mit $w_\beta := 1 + 2^{\beta+1} v_\beta$ ungerade, also $u^{2^{\beta+1}} - 1 = 2^{\beta+3} v_\beta w_\beta =: 2^{\beta+3} v_{\beta+1}$ mit ungeradem $v_{\beta+1}$.

Nach 4(1) gilt $\operatorname{ord}_{2^\alpha} u = 2^\beta$ mit natürlichem $\beta \leq \alpha - 2$ für $\alpha \geq 3$. Andererseits ist nach der letzten Feststellung $2^\alpha | (u^{2^\beta} - 1) = 2^{\beta+2} v_\beta$, also $\alpha \leq \beta + 2$ wegen der Ungeradheit von v_β. Daher ist $\operatorname{ord}_{2^\alpha} u = 2^\beta = 2^{\alpha-2}$ für $\alpha \geq 3$. □

Satz. *Bei ganzem $\alpha \geq 3$ und $u \equiv \pm 3 \pmod 8$ bilden die folgenden $\varphi(2^\alpha) = 2^{\alpha-1}$ Zahlen ein primes Restsystem modulo 2^α*

$$u, u^2, u^3, \ldots, u^{2^{\alpha-2}}, -u, -u^2, \ldots, -u^{2^{\alpha-2}}. \tag{1}$$

Beweis. Da u ungerade ist, sind offenbar alle $2^{\alpha-1}$ Zahlen (1) zum Modul 2^α teilerfremd. Wegen der Implikation (ii) ⇒ (i) des Lemmas sind die ersten $2^{\alpha-2}$ Zahlen in (1) paarweise inkongruent modulo 2^α; dasselbe gilt für die zweiten $2^{\alpha-2}$ Zahlen in (1). Andererseits ist auch jede der ersten $2^{\alpha-2}$ Zahlen in (1) zu jeder der zweiten teilerfremd: Denn wäre $u^i \equiv -u^j \pmod{2^\alpha}$ für $1 \leq i, j \leq 2^{\alpha-2}$, o.B.d.A. mit $j \leq i$, so wäre $u^{i-j} \equiv -1 \pmod{2^\alpha}$ nach der Kürzungsregel 1.3. Daraus würde $u^{2(i-j)} \equiv 1 \pmod{2^{\alpha+1}}$ folgen, also erneut nach dem Lemma $2^{\alpha-1} | 2(i-j)$, was wegen $0 \leq i - j < 2^{\alpha-2}$ zu $i = j$ führt, damit zu $1 \equiv -1 \pmod{2^\alpha}$, was wegen $\alpha \geq 3$ nicht geht. □

Aus dem vorstehenden Satz ergibt sich unmittelbar das

Korollar. *Seien $\alpha \geq 3$ und $u \equiv \pm 3 \pmod 8$ feste ganze Zahlen. Dann gibt es zu jedem ungeraden ganzen c ein modulo 2 bzw. $2^{\alpha-2}$ eindeutig bestimmtes ganzes i_0 bzw. i_{-1}, so daß gilt*

$$c \equiv (-1)^{i_0} u^{i_{-1}} \pmod{2^\alpha}. \tag{2}$$

Die Bedeutung der Existenz von Primitivwurzeln modulo m liegt vor allem in folgender, in 1 erkannten Tatsache: Ist a eine feste Primitivwurzel modulo m, so gibt es zu jedem ganzen c mit $(c, m) = 1$ ein modulo $\varphi(m)$ eindeutig bestimmtes ganzes i mit

$$c \equiv a^i \pmod{m}. \tag{3}$$

Formel (2) hat als Analogon zu (3) im Falle des Moduls 2^α, $\alpha \geq 3$, angesehen zu werden, zu dem es nach dem GAUSSschen Satz keine Primitivwurzeln gibt.

Bemerkung. Aus dem obigen Korollar folgt: Sind $\alpha \geq 3$ und $u \equiv \pm 3 \pmod 8$ feste ganze Zahlen, so ist die prime Restklassengruppe $\mathbb{Z}^*_{2^\alpha}$ modulo 2^α direktes Produkt ihrer von den Restklassen $\overline{-1}$ bzw. $\bar{u}$ modulo 2^α erzeugten zyklischen Untergruppen der Primzahlpotenzordnung 2 bzw. $2^{\alpha-2}$. (Man vergleiche die Bemerkung zu 5 sowie zur Schreibweise die Bemerkung 4 zu 1.8.)

7. Basisdarstellung. Die Darstellungen 6(2) bzw. 6(3) für zum Modul teilerfremde ganze Zahlen gelten nur für sehr spezielle Moduln; der folgende Satz verallgemeinert diese Darstellungen auf beliebige natürliche Moduln.

Satz. *Sei m eine natürliche Zahl mit der kanonischen Zerlegung $\prod_{\kappa=0}^{k} p_\kappa^{\alpha_\kappa}$, wobei $p_0 := 2$ vereinbart sei; dabei sind α_0 und k ganz und nichtnegativ, jedoch seien $\alpha_1, \ldots, \alpha_k$ positiv, falls k positiv ist. Für $\kappa = 0, \ldots, k$ sei $q_\kappa := p_\kappa^{\alpha_\kappa}$ gesetzt. Die ganze Zahl a_0 genüge den Kongruenzen*

$$a_0 \equiv -1 \pmod{q_0}, \quad a_0 \equiv 1 \pmod{\frac{m}{q_0}} \tag{1}$$

und, falls k positiv ist, seien a_κ feste Primitivwurzeln modulo q_κ mit

$$a_\kappa \equiv 1 \pmod{\frac{m}{q_\kappa}} \tag{2}$$

für $\kappa = 1, \ldots, k$. Dann gilt für jedes zu m teilerfremde ganze c

(i) im Falle $\alpha_0 \leq 2$: Es gibt genau ein $(i_0, \ldots, i_k) \in \mathbb{N}_0^{k+1}$, $i_\kappa < \varphi(q_\kappa)$ für $\kappa = 0, \ldots, k$ mit

$$c \equiv a_0^{i_0} \cdot \ldots \cdot a_k^{i_k} \pmod{m}; \tag{3}$$

(ii) im Falle $\alpha_0 \geq 3$: Es gibt genau ein $(i_{-1}, i_0, \ldots, i_k) \in \mathbb{N}_0^{k+2}$, $i_{-1} < \frac{1}{2}\varphi(q_0)$, $i_0 < 2$ und $i_\kappa < \varphi(q_\kappa)$ für $\kappa = 1, \ldots, k$ mit

$$c \equiv a_{-1}^{i_{-1}} a_0^{i_0} \cdot \ldots \cdot a_k^{i_k} \pmod{m}. \tag{4}$$

Dabei hat die ganze Zahl a_{-1} den Kongruenzen

$$a_{-1} \equiv u \pmod{q_0}, \quad a_{-1} \equiv 1 \pmod{\frac{m}{q_0}} \tag{5}$$

zu genügen, wenn die ganze Zahl u vorab gemäß $u \equiv \pm 3 \pmod 8$ fixiert wurde.

Beweis. Zunächst sind die Wahlen (1) bzw. (5), letzteres bei $\alpha_0 \geq 3$, für a_0 bzw. a_{-1} nach dem chinesischen Restsatz 2.2 (sogar modulo m eindeutig) möglich. Ist $k \geq 1$, so gibt es nach dem GAUSSschen Satz 5 für jedes $\kappa = 1, \ldots, k$ eine Primitivwurzel a'_κ modulo q_κ. Erneut nach dem chinesischen Restsatz ist das System

$$X \equiv a'_\kappa \pmod{q_\kappa}, \qquad X \equiv 1 \pmod{\frac{m}{q_\kappa}}$$

dann für jedes $\kappa = 1, \ldots, k$ (modulo m eindeutig) lösbar; jede derartige Lösung a_κ ist wegen $a_\kappa \equiv a'_\kappa \pmod{q_\kappa}$ eine Primitivwurzel modulo q_κ, die außerdem der Bedingung (2) genügt.

Wegen $(c, m) = 1 \Leftrightarrow (c, q_\kappa) = 1$ für $\kappa = 0, \ldots, k$ existiert nach der Feststellung zu 6(3) genau ein $i_\kappa \in \{0, \ldots, \varphi(q_\kappa) - 1\}$ mit

$$c \equiv a_\kappa^{i_\kappa} \pmod{q_\kappa}; \tag{6}$$

bei $\alpha_0 \leq 2$ trifft dies für $\kappa = 0, \ldots, k$ zu, bei $\alpha_0 \geq 3$ lediglich für $\kappa = 1, \ldots, k$.

Sei erst $\alpha_0 \leq 2$ und $\kappa \in \{0, \ldots, k\}$ fixiert. Nach (1) und (2) ist $a_\lambda \equiv 1 \pmod{\frac{m}{q_\lambda}}$ für $\lambda = 0, \ldots, k$, also erst recht $a_\lambda \equiv 1 \pmod{q_\kappa}$ für dieselben λ, aber $\lambda \neq \kappa$ (man beachte $q_\kappa | \frac{m}{q_\lambda}$). Wegen (6) und der letzten Feststellung ist

$$c \equiv a_0^{i_0} \cdot \ldots \cdot a_k^{i_k} \pmod{q_\kappa};$$

da dies für $\kappa = 0, \ldots, k$ zutrifft, ist die Existenz *einer* Darstellung (3) gesichert. Aus

$$a_0^{i_0} \cdot \ldots \cdot a_k^{i_k} \equiv a_0^{j_0} \cdot \ldots \cdot a_k^{j_k} \pmod{m} \tag{7}$$

mit $i_\kappa, j_\kappa \in \{0, \ldots, \varphi(q_\kappa) - 1\}$ für $\kappa = 0, \ldots, k$ folgt dieselbe Kongruenz modulo q_κ anstatt modulo m, wegen $a_\lambda \equiv 1 \pmod{q_\kappa}$ für $\lambda \neq \kappa$ also $a_\kappa^{i_\kappa} \equiv a_\kappa^{j_\kappa} \pmod{q_\kappa}$, was nach den Feststellungen bei 6(3) zu $i_\kappa = j_\kappa$ für $\kappa = 0, \ldots, k$ führt.

Sei jetzt $\alpha_0 \geq 3$ und $\kappa \in \{1, \ldots, k\}$ fixiert. Nach 6(2) ist mit $i_0 \in \{0, 1\}$, $i_{-1} \in \{0, \ldots, \frac{1}{2}\varphi(q_0) - 1\}$ wegen (1) und (5)

$$c \equiv u^{i_{-1}}(-1)^{i_0} \equiv a_{-1}^{i_{-1}} a_0^{i_0} \pmod{q_0}$$

also wegen den aus (2) folgenden Kongruenzen $a_\kappa \equiv 1 \pmod{q_0}$ für $\kappa = 1, \ldots, k$

$$c \equiv a_{-1}^{i_{-1}} a_0^{i_0} \cdot \ldots \cdot a_k^{i_k} \pmod{q_0}.$$

Dieselbe Kongruenz hat man modulo q_κ für $\kappa = 1, \ldots, k$ anstatt modulo q_0; man braucht ja nur (6) und $a_\lambda \equiv 1 \pmod{q_\kappa}$ für $\lambda = -1, 0, \ldots, k$, $\lambda \neq \kappa$ (für $\lambda = -1$ vgl. (5)) zu beachten. Damit ist die Existenz *einer* Darstellung (4) gesichert mit den dort genannten Bedingungen an $i_{-1}, \ldots, i_k$. Deren Eindeutigkeit möge sich der Leser selbst überlegen, ausgehend von einer zu (7) analogen Kongruenz. □

Bemerkungen. 1) Ist α_0 im vorstehenden Satz gleich 0 oder 1, so kann a_0 gleich 1 gewählt werden, so daß der erste Faktor rechts in (3) nicht in Erscheinung tritt.

2) Ist allgemein eine multiplikativ geschriebene abelsche Gruppe G direktes Produkt zyklischer Untergruppen $G_1, \ldots, G_k$ von G und wird G_κ von g_κ für $\kappa = 1, \ldots, k$ erzeugt, so heißt $\{g_1, \ldots, g_k\}$ eine *Basis* von G. Mittels einer solchen Basis läßt sich jedes $g \in G$ eindeutig in der Form

$$g_1^{i_1} \cdot \ldots \cdot g_k^{i_k} \tag{8}$$

ausdrücken; man nennt (8) die Basisdarstellung von g. Wendet man diese Begriffsbildung auf die prime Restklassengruppe $\mathbb{Z}_m^*$ an, so wird man unter Beachtung der Bemerkungen zu 5 und 6 die Kongruenzen (3) und (4) im Satz als *Basisdarstellung* der zum Modul teilerfremden ganzen Zahlen bezeichnen.

3) Die Basisdarstellung (3) bzw. (4) ist von größter Bedeutung z.B. beim Beweis des Satzes 3.2.10 von Dirichlet über Primzahlen in arithmetischen Progressionen, vgl. K. Prachar [20], S. 99ff.