Lineare Chiffren

Klaus Pommerening
Fachbereich Mathematik
der Johannes-Gutenberg-Universität
Saarstraße 21
D-55099 Mainz

16. Januar 2000, letzte Revision 17. August 2008

Lineare Chiffren wurden von dem Mathematiker Lester Hill 1929 vorgeschlagen und erregten einiges Aufsehen (vor allem bei Mathematikern); sie wurden aber wegen ihrer allzu offensichtlichen Schwächen nie ernsthaft eingesetzt. Ihre eigentliche Bedeutung liegt darin, dass hier erstmals systematisch algebraische Methoden in die Kryptologie eingeführt wurden, und dass dabei deutlich wurde, welche Bedeutung Linearität für die Kryptoanalyse hat.

Diese Chiffren verwenden lineare Algebra (oder Matrizenrechnung) über dem Ring der ganzen Zahlen $\mathbb{Z}$ oder seinen endlichen Restklassenringen $\mathbb{Z}/n\mathbb{Z}$. Daher folgt hier zunächst ein zahlentheoretisch-algebraischer Einschub.

8.1 Der EUKLIDische Algorithmus

Der Euklidische Algorithmus liefert den größten gemeinsamen Teiler (ggT) zweier ganzer Zahlen,

$$\mathrm{ggT}(a,b) = \max\{d \in \mathbb{Z} \mid d|a, d|b\}$$

Wenn man der Einfachheit halber noch $\mathrm{ggT}(0,0) = 0$ setzt, hat man die Funktion

$$\mathrm{ggT} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{N}$$

mit den folgenden Eigenschaften:

Hilfssatz 1 *Für beliebige $a, b, c, q \in \mathbb{Z}$ gilt:*
(i) $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,a)$.
(ii) $\mathrm{ggT}(a,-b) = \mathrm{ggT}(a,b)$.
(iii) $\mathrm{ggT}(a,0) = |a|$.
(iv) $\mathrm{ggT}(a-qb,b) = \mathrm{ggT}(a,b)$.

Beweis. Trivial; für (iv) verwendet man die Äquivalenz $d|a, b \Longleftrightarrow d|a-qb, b$. ◇

Der Euklidische Algorithmus wird gewöhnlich als Folge von Divisionen mit Rest aufgeschrieben:

$$r_0 = |a|, r_1 = |b|, \ldots, r_{i-1} = q_i r_i + r_{i+1},$$

wobei q_i der ganzzahlige Quotient und r_{i+1} der eindeutig bestimmte Divisionsrest mit $0 \leq r_{i+1} < r_i$ ist. Ist dann $r_n \neq 0$ und $r_{n+1} = 0$, so ist $r_n = \mathrm{ggT}(a,b)$. Denn aus Hilfssatz 1 folgt

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(r_0,r_1) = \mathrm{ggT}(r_1,r_2) = \ldots = \mathrm{ggT}(r_n,0) = r_n.$$

Da außerdem

$$r_1 > r_2 > \ldots > r_i \geq 0 \quad \text{für alle } i,$$

wird die Abbruchbedingung $r_{n+1} = 0$ nach spätestens $n \leq |b|$ Iterationsschritten (also Divisionen) erreicht.

Eine kleine Erweiterung liefert sogar noch mehr. Es ist nämlich jedes r_i ganzzahlige Linearkombination der beiden vorhergehenden Divisionsreste, also auch von $|a|$ und $|b|$:

$$r_{i+1} \in \mathbb{Z}r_i + \mathbb{Z}r_{i-1} \subseteq \ldots \subseteq \mathbb{Z}r_1 + \mathbb{Z}r_0 = \mathbb{Z}a + \mathbb{Z}b;$$

für r_0 und r_1 ist das trivial, und allgemein folgt es durch Induktion: Sei schon $r_j = |a|x_j + |b|y_j$ für $0 \leq j \leq i$. Dann folgt

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= |a|x_{i-1} + |b|y_{i-1} - q_i|a|x_i - q_i|b|y_i \\ &= |a|(x_{i-1} - q_i x_i) + |b|(y_{i-1} - q_i y_i). \end{aligned}$$

Diese Überlegung liefert gleich eine explizite Konstruktion für die Koeffizienten mit; sie erfüllen nämlich die Rekursionsformeln

$$x_{i+1} = x_{i-1} - q_i x_i \quad \text{mit} \quad x_0 = 1, x_1 = 0,$$

$$y_{i+1} = y_{i-1} - q_i y_i \quad \text{mit} \quad y_0 = 0, y_1 = 1,$$

die bis auf die Startwerte mit der Formel für die r_i übereinstimmen:

$$r_{i+1} = r_{i-1} - q_i r_i \quad \text{mit} \quad r_0 = |a|, r_1 = |b|.$$

Der **erweiterte Euklidische Algorithmus** (auch Algorithmus von LAGRANGE genannt) ist die Zusammenfassung dieser drei Rekursionsformeln. Damit ist gezeigt (wenn man die Vorzeichen von x_n und y_n passend justiert):

Satz 1 *Der erweiterte Euklidische Algorithmus liefert in endlich vielen Schritten zu zwei ganzen Zahlen a und b den größten gemeinsamen Teiler d und ganzzahlige Koeffizienten x und y mit $ax + by = d$.*

Bemerkungen

1. Das kleinste gemeinsame Vielfache berechnet man nach der Formel

   $$\mathrm{kgV}(a, b) = \frac{ab}{\mathrm{ggT}(a, b)}$$

   ebenfalls effizient.

2. Der größte gemeinsame Teiler mehrerer Zahlen kann man nach der Formel

   $$\mathrm{ggT}(\ldots(\mathrm{ggT}(\mathrm{ggT}(a_1, a_2), a_3)\ldots, a_r)$$

   berechnen; hier sind noch kleine Optimierungen möglich. Analoges gilt für das kleinste gemeinsame Vielfache.

8.2 Analyse des EUKLIDischen Algorithmus

Ein kleines Problem hat sich im vorigen Abschnitt eingeschlichen: Zwar sind die Quotienten und Divisionsreste sicher durch die Eingabeparameter beschränkt; aber die Koeffizienten x_i und y_i sind auf den ersten Blick nicht kontrollierbar. Wie kann man garantieren, dass es hier nicht zu einem Überlauf bei der üblichen Ganzzahl-Arithmetik mit beschränkter Stellenzahl kommt? Nun, das Wachstum wird durch die folgende Überlegung kontrolliert:

Hilfssatz 2 *Für die Koeffizienten x_i und y_i im erweiterten Euklidischen Algorithmus gilt:*

(i) $x_i > 0$, *wenn i gerade,* $x_i \leq 0$, *wenn i ungerade, und* $|x_{i+1}| \geq |x_i|$ *für* $i = 1, \ldots, n$.

(ii) $y_i \leq 0$, *wenn i gerade,* $y_i > 0$, *wenn i ungerade, und* $|y_{i+1}| \geq |y_i|$ *für* $i = 2, \ldots, n$.

(iii) $x_{i+1}y_i - x_i y_{i+1} = (-1)^{i+1}$ *für* $i = 0, \ldots, n$; *insbesondere sind x_i und y_i stets teilerfremd für* $i = 0, \ldots, n+1$.

(iv) $|x_i| \leq |b|, |y_i| \leq |a|$ *für* $i = 0, \ldots, n+1$, *falls* $b \neq 0$ *bzw.* $a \neq 0$.

Beweis. (Nur angedeutet.) (i), (ii) und (iii) zeigt man durch Induktion. Aus $0 = r_{n+1} = |a|x_{n+1} + |b|y_{n+1}$ folgt dann $x_{n+1}|b$ und $y_{n+1}|a$. $\diamond$

Von besonderem Interesse ist, dass der Euklidische Algorithmus sehr effizient ist – die Zahl der Iterationsschritte wächst nur linear mit der *Stellenzahl* der Eingabeparameter, die gesamte Rechenzeit quadratisch. Es ist eine ziemlich genaue Analyse möglich, die wie folgt aussieht.

Die Divisionskette habe die Länge n (o. B. d. A. $b \neq 0$). Wie groß muss b dann mindestens sein? Es ist $r_n \geq 1, r_{n-1} \geq 2$ und $r_{i-1} \geq r_i + r_{i+1}$. Die FIBONACCI-Zahlen F_n sind rekursiv definiert durch

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad \text{für } n \geq 2.$$

Durch Induktion erhält man also $r_i \geq F_{n+2-i}$, wobei der Induktionsanfang heißt: $r_n \geq 1 = F_2$, $r_{n-1} \geq 2 = F_3$; insbesondere folgt $|b| \geq F_{n+1}$. Anders formuliert:

Satz 2 (BINET 1841) *Für $a, b \in \mathbb{Z}$ mit $0 < b < F_{n+1}$ ergibt der Euklidische Algorithmus den größten gemeinsamen Teiler in höchstens $n-1$ Iterationsschritten.*

Zusatz. *Das gilt auch für $b = F_{n+1}$, außer wenn $a \equiv F_{n+2} \equiv F_n \pmod{b}$.*

Damit haben wir eine elegante mathematische Formulierung, aber noch keine Lösung. Jedoch ist das Wachstum der FIBONACCI-Zahlen sehr genau bekannt. Man kann es durch den goldenen Schnitt $\varphi = \frac{1+\sqrt{5}}{2}$ ausdrücken; es ist $\varphi^2 - \varphi - 1 = 0$.

Hilfssatz 3 *Für eine reelle Zahl $c \in \mathbb{R}$ und einen Index $k \in \mathbb{N}$ sei $F_k > c \cdot \varphi^k$ und $F_{k+1} > c \cdot \varphi^{k+1}$. Dann gilt $F_n > c \cdot \varphi^n$ für alle $n \geq k$.*

Beweis. (Durch Induktion.)

$$F_n = F_{n-1} + F_{n-2} > c\varphi^{n-1} + c\varphi^{n-2} = c\varphi^{n-2}(\varphi + 1) = c\varphi^n$$

für $n \geq k + 2$. $\diamond$

Korollar 1 $F_{n+1} > 0.43769 \cdot \varphi^{n+1}$ *für* $n \geq 2$.

Beweis.

$$\begin{aligned} \varphi^2 &= \varphi + 1 = \frac{3 + \sqrt{5}}{2}, \\ \varphi^3 &= \varphi^2 + \varphi = 2 + \sqrt{5}, \\ \varphi^4 &= \varphi^3 + \varphi^2 = \frac{7 + 3\sqrt{5}}{2}. \end{aligned}$$

Daraus folgt

$$\begin{aligned} \frac{F_3}{\varphi^3} &= \frac{2}{2 + \sqrt{5}} = \frac{2(\sqrt{5} - 2)}{1} = 2\sqrt{5} - 4 > 0.47, \\ \frac{F_4}{\varphi^4} &= \frac{3 \cdot 2}{7 + 3\sqrt{5}} = \frac{6(7 - 3\sqrt{5})}{49 - 45} = \frac{21 - 9\sqrt{5}}{2} > 0.43769 \end{aligned}$$

und daraus die Behauptung. $\diamond$

Korollar 2 *Seien $a, b \in \mathbb{Z}$ mit $b \geq 2$. Dann ist die Anzahl der Iterationsschritte im Euklidischen Algorithmus für* $\mathrm{ggT}(a, b)$ *kleiner als* $0.718 + 4.785 \cdot {}^{10}\log(b)$.

Beweis. Wenn die Divisionskette die Länge n hat, ist $b \geq F_{n+1}$,

$$b \geq F_{n+1} > 0.43769 \cdot \varphi^{n+1},$$

$${}^{10}\log(b) > {}^{10}\log(0.43769) + (n+1) \cdot {}^{10}\log(\varphi) > -0.35884 + 0.20898 \cdot (n+1),$$

also $n < 0.718 + 4.785 \cdot {}^{10}\log(b)$. $\diamond$

Etwas gröber, aber einfacher zu merken, ist die folgende Version:

Korollar 3 *Seien $a, b \in \mathbb{Z}$ mit $b \geq 2$. Dann ist die Anzahl der Iterationsschritte im Euklidischen Algorithmus für* $\mathrm{ggT}(a, b)$ *kleiner als fünfmal die Zahl der Dezimalstellen von b außer für $b = 8, a \equiv 5 \pmod 8$, wo man 5 Iterationsschritte braucht.*

Berücksichtigt man noch die Stellenzahl der vorkommenden Zahlen und den Aufwand für die Multiplikation und Division langer Zahlen, kommt man auf eine Rechenzeit, die quadratisch mit der Stellenzahl wächst, wie im folgenden gezeigt wird.

Hat a (bezüglich der Basis B) die Stellenzahl m und b die Stellenzahl p, so ist der Aufwand für die erste Division alleine schon $\leq c \cdot (m-p) \cdot p$; dabei ist c eine Konstante, die höchstens zweimal so groß ist wie die, die den Aufwand für die „Rückmultiplikation Quotient $\times$ Divisor“ beschreibt. Für B wird man bei heutigen Rechnerarchitekturen in der Regel 2^{32} annehmen, und als primitive Operationen werden die Grundrechenschritte Addition, Subtraktion, Multiplikation, Division mit Rest und Vergleich von einstelligen Zahlen (zur Basis B) gezählt. Zum Glück nehmen im Verlauf der euklidischen Divisionskette die zu dividierenden Zahlen exponentiell ab. Der Divisionsschritt

$$r_{i-1} = q_i r_i + r_{i+1}$$

benötigt noch $\leq c \cdot {}^B\log(q_i) {}^B\log(r_i)$ primitive Operationen, die gesamte Divisionskette also

$$\begin{aligned} A(a,b) &\leq c \cdot \sum_{i=1}^{n} {}^B\log(q_i) {}^B\log(r_i) \leq c \cdot {}^B\log|b| \cdot \sum_{i=1}^{n} {}^B\log(q_i) \\ &= c \cdot {}^B\log|b| \cdot {}^B\log(q_1 \cdots q_n). \end{aligned}$$

Das Produkt der q_i lässt sich weiter abschätzen:

$$|a| = r_0 = q_1 r_1 + r_2 = q_1(q_2 r_2 + r_3) + r_2 = \ldots = q_1 \cdots q_n r_n + \cdots \geq q_1 \cdots q_n;$$

also haben wir die grobe Abschätzung

$$A(a,b) \leq c \cdot {}^B\log|b| \cdot {}^B\log|a|.$$

Satz 3 *Die Anzahl der primitiven Operationen im Euklidischen Algorithmus für ganze Zahlen a und b der Stellenzahlen $\leq m$ ist $\leq c \cdot m^2$.*

Der Aufwand für den Euklidischen Algorithmus mit Input a und b ist also nicht wesentlich größer als der für die Multiplikation von a und b. Eine feinere Abschätzung soll hier nicht durchgeführt werden; ebensowenig werden mögliche Verbesserungen diskutiert. Erwähnt soll aber werden, dass ein Verfahren von LEHMER erlaubt, einen großen Anteil der Langzahl-Divisionen im Euklidischen Algortithmus durch primitive Operationen zu ersetzen.

8.3 Kongruenzdivision

Der erweiterte Euklidische Algorithmus liefert nun eine Lösung des nicht ganz trivialen Problems, im Ring $\mathbb{Z}/n\mathbb{Z}$ der ganzen Zahlen $\bmod n$ effizient zu dividieren.

Satz 4 *Gegeben seien $n \in \mathbb{N}, n \geq 2$, und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(b, n) = d$. Genau dann ist a in $\mathbb{Z}/n\mathbb{Z}$ durch b teilbar, wenn $d|a$. Ist dies der Fall, so gibt es genau d Lösungen z von $zb \equiv a \pmod{n}$ mit $0 \leq z < n$, und je zwei solche unterscheiden sich um ein Vielfaches von n/d. Ist $d = xn + yb$ und $a = td$, so ist $z = yt$ Lösung.*

Beweis. Ist a durch b teilbar, $a \equiv bz \pmod{n}$, so $a = bz + kn$, also $d|a$. Ungekehrt sei $a = td$. Nach Satz 1 findet man x, y mit $nx + by = d$; also ist $nxt + byt = a$ und $byt \equiv a \pmod{n}$. Ist auch $a \equiv bw \pmod{n}$, so $b(z-w) \equiv 0 \pmod{n}$, also $z - w$ Vielfaches von n/d. $\diamond$

Ein expliziter Algorithmus für die Division ist dem Beweis von Satz 4 direkt zu entnehmen. Wichtig – und wesentlich einfacher zu formulieren – ist der Spezialfall $d = 1$:

Korollar 1 *Ist b zu n teilerfremd, so ist jedes a in $\mathbb{Z}/n\mathbb{Z}$ eindeutig durch b teilbar.*

Die Berechnung des Inversen y zu b folgt dann, da $d = 1$, sofort aus der Formel $1 = nx + by$; es ist nämlich $by \equiv 1 \pmod{n}$.

Korollar 2 $(\mathbb{Z}/n\mathbb{Z})^\times = \{b \bmod n \mid \mathrm{ggT}(b, n) = 1\}$.

Die invertierbaren Elemente im Ring $\mathbb{Z}/n\mathbb{Z}$ sind also genau die Restklassen der zu n teilerfremden ganzen Zahlen. Der wichtigste Fall ist: $n = p$ Primzahl. Dann gilt

Korollar 3 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ *ist ein Körper.*

Beweis. Ist $b \in \mathbb{F}_p, b \neq 0$, so gibt es genau ein $c \in \mathbb{F}_p$ mit $bc = 1$. $\diamond$

Korollar 4 (Kleiner Satz von Fermat) $a^p \equiv a \pmod{p}$ *für alle $a \in \mathbb{Z}$.*

Beweis. Die Elemente $\neq 0$ von $\mathbb{F}_p$ bilden die multiplikative Gruppe $\mathbb{F}_p^\times$. Da die Ordnung eines Elements stets Teiler der Gruppenordnung ist, gilt $a^{p-1} \equiv 1 \pmod{p}$ wenn a zu p teilerfremd ist. Andernfalls gilt $p|a$, also $a \equiv 0 \equiv a^p \pmod{p}$. $\diamond$

8.4 Der chinesische Restalgorithmus

Das chinesische Restproblem ist die Frage nach der Lösung simultaner Kongruenzen. Der einfachste erwähnenswerte Fall geht so:

Satz 5 (Chinesischer Restsatz) *Seien m und n teilerfremde natürliche Zahlen ≥ 1 und a, b beliebige ganze Zahlen. Dann gibt es genau eine ganze Zahl x, $0 \leq x < mn$, mit*

$$x \equiv a \pmod{m}, \; x \equiv b \pmod{n}.$$

Beweis. Die Eindeutigkeit folgt so: Ist auch y eine solche Zahl, so $y = x + km = x + ln$ mit ganzen Zahlen k und l, und $km = ln$. Da m und n teilerfremd sind, folgt $n|k$, $k = cn$,

$$y = x + cmn \equiv x \pmod{mn}.$$

Für den Existenzbeweis setzt man $x = a + tm$ an; dann ist $x \equiv a \pmod{m}$ erfüllt, und

$$x \equiv b \pmod{n} \Longleftrightarrow b - a \equiv x - a \equiv tm \pmod{n}.$$

Ein solches t existiert aber nach Satz 4. Die so gefundene Lösung x wird noch $\bmod(mn)$ reduziert. $\diamond$

Der Beweis ist konstruktiv und leicht in einen Algorithmus umzusetzen. Im allgemeinen Fall, für mehrfache Kongruenzen, lautet das chinesische Restproblem so:

- Gegeben sind q paarweise teilerfremde ganze Zahlen $n_1, \ldots, n_q \geq 1$ und q ganze Zahlen $a_1, \ldots, a_q$.
- Gesucht ist eine ganze Zahl x mit $x \equiv a_i \pmod{n_i}$ für $i = 1, \ldots q$.

Man kann Satz 5 entsprechend verallgemeinern. Interessanter ist aber eine abstrakte Formulierung, die auch die Interpolationsaufgabe für Polynome mit einschließt; auch in dieser allgemeinen Formulierung erkennt man Satz 5 samt Beweis leicht wieder, wenn man daran denkt, dass für ganze Zahlen m und n mit größtem gemeinsamen Teiler d gilt:

$$m, n \text{ teilerfremd} \Longleftrightarrow d = 1 \Longleftrightarrow \mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}.$$

Satz 6 (Allgemeiner chinesischer Restsatz) *Sei R ein kommutativer Ring mit Einselement, $q \geq 1$, $\mathfrak{a}_1, \ldots, \mathfrak{a}_q \trianglelefteq R$ Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$. Seien Elemente $a_1, \ldots, a_q \in R$ gegeben. Dann gibt es ein $x \in R$ mit $x - a_i \in \mathfrak{a}_i$ für $i = 1, \ldots, q$, und die Restklasse $x \bmod \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_q$ ist eindeutig bestimmt.*

Beweis. Die Eindeutigkeit ist auch hier einfach: Ist $x - a_i, y - a_i \in \mathfrak{a}_i$, so $x - y \in \mathfrak{a}_i$; gilt das für alle i, so $x - y \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_q$.

Die Existenz wird durch Induktion über q bewiesen. Im Fall $q = 1$ nimmt man $x = a_1$. Sei nun $q \geq 2$ und y mit $y - a_i \in \mathfrak{a}_i$ für $i = 1, \ldots, q-1$ schon gefunden. Idee: Zu y kann man ein $s \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ addieren, ohne das bisher erreichte, nämlich die Lösung der ersten $q-1$ Kongruenzen, wieder aufzugeben. Benötigt wird dazu die Aussage: Zu jedem $r \in R$ gibt es ein $s \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ mit $r - s \in \mathfrak{a}_q$, oder, anders ausgedrückt,

$$(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}) + \mathfrak{a}_q = R.$$

Zum Beweis dieser Zwischenbehauptung wählt man $c_i \in \mathfrak{a}_i$ für $i = 1, \ldots, q-1$ und $b_1, \ldots, b_{q-1} \in \mathfrak{a}_q$ mit $b_i + c_i = 1$. Dann ist

$$1 = (b_1 + c_1) \cdots (b_{q-1} + c_{q-1}) = c_1 \cdots c_{q-1} + b$$

mit $c_1 \cdots c_{q-1} \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ und $b \in \mathfrak{a}_q$.

Nun wird zu $a_q - y \in R$ ein $s \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ gewählt mit $a_q - y - s \in \mathfrak{a}_q$ und dann $x = y + s$ gesetzt. Dann ist $x \equiv y \equiv a_i \pmod{\mathfrak{a}_i}$ für $i = 1, \ldots, q-1$ und $x \equiv y + s \equiv a_q \pmod{\mathfrak{a}_q}$. $\diamond$

Bemerkungen und Beispiele

1. Ist $R = \mathbb{Z}$ oder sonst ein Hauptidealring und $\mathfrak{a}_i = Rn_i$, so ist $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_q = R(n_1 \cdots n_q)$. Daraus erhält man die übliche Formulierung des chinesischen Restsatzes.

2. Ist R ein Hauptidealring, so ist läuft die Konstruktion der Lösung wie folgt: Ist $\mathfrak{a}_i = Rn_i$, so wird s in der Zwischenbehauptung so gewählt, dass $s = tn_1 \cdots n_{q-1}$ mit

   $$r - tn_1 \cdots n_{q-1} \in Rn_q$$

   (Kongruenzdivision mod n_q). Ein expliziter Algorithmus für das chinesische Restproblem existiert also, wenn einer für die Kongruenzdivision existiert, auf jeden Fall also für $R = \mathbb{Z}$.

3. Im Fall $R = \mathbb{Z}$ berechnet man iterativ

   $$\begin{aligned} x_1 = a_1 \bmod n_1, &\qquad s_1 = n_1, \\ t_i \text{ mit } 0 \leq t_i \leq n_i - 1 &\quad \text{und } a_i - x_{i-1} - t_i s_{i-1} \in Rn_i, \\ x_i = x_{i-1} + t_i s_{i-1}, &\qquad s_i = s_{i-1} n_i. \end{aligned}$$

   Insbesondere ist $s_k = n_1 \cdots n_k$. Durch Induktion beweist man sofort $0 \leq x_i \leq s_i - 1$ für alle i. Am Ende erhält man die Lösung $x = x_q$. Die

eben durchgeführte Überlegung garantiert, dass kein Zwischenergebnis einen Überlauf erzeugt. Der Aufwand besteht im wesentlichen aus $q-1$ Kongruenzdivisionen und $2\cdot(q-1)$ gewöhnlichen Ganzzahlmultiplikationen. Der Gesamtaufwand ist also ungefähr $cq\times$ dem Aufwand für eine Langzahl-Multiplikation mit einer kleinen Konstanten c.

4. Die allgemeine Gestalt der Lösungsformel ist

$$x = x_1 + t_1 n_1 + \cdots + t_{q-1} n_1 \cdots n_{q-1}.$$

5. Als Beispiel wird die Aufgabe von Sun-Tsu aus dem 1. Jahrhundert behandelt, die in unserer Schreibweise so heißt: Finde x mit

$$x \equiv 2 \pmod 3,\ x \equiv 3 \pmod 5,\ x \equiv 2 \pmod 7.$$

   Der Algorithmus liefert der Reihe nach:

$$\begin{aligned} x_1 = 2, &\quad s_1 = 3, \\ 1 - 3t_2 \in 5\mathbb{Z}, &\quad t_2 = 2, \\ x_2 = 2 + 2\cdot 3 = 8, &\quad s_2 = 15, \\ -6 - 15t_3 \in 7\mathbb{Z}, &\quad t_3 = 1, \\ x = x_3 = 8 + 1\cdot 15 = 23. & \end{aligned}$$

6. Für den Polynomring $K[T]$ über einem Körper K erhält man die Lösung des Interpolationsproblems. Der Algorithmus ist dabei gerade das Interpolationsverfahren von Newton.

8.5 Die EULERsche phi-Funktion

Eine wichtige Anwendung des chinesischen Restsatzes ist die folgende; sinnvollerweise wird hier stets $n \geq 2$ vorausgesetzt. Die ganzen Zahlen $\bmod n$ bilden den Ring $\mathbb{Z}/n\mathbb{Z}$. Die *multiplikative Gruppe* $\bmod n$, die (auch in der Kryptologie) oft vorkommt, ist besteht genau aus den invertierbaren Elementen dieses Rings und wird abgekürzt als

$$\mathbb{M}_n := (\mathbb{Z}/n\mathbb{Z})^\times.$$

Ihre Ordnung wird durch die EULERsche φ-Funktion beschrieben:

$$\varphi(n) = \#\mathbb{M}_n = \#\{a \in [0 \cdots n-1] \mid a \text{ teilerfremd zu } n\}.$$

Korollar 1 *Sind m und n teilerfremd, so ist $\varphi(mn) = \varphi(m)\varphi(n)$.*

Beweis. Die Aussage des chinesischen Restsatzes bedeutet gerade, dass der natürliche Ring-Homomorphismus

$$F\colon \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto (x \bmod m, x \bmod n),$$

bijektiv, also sogar ein Ring-Isomorphismus ist. Außerdem ist $F(\mathbb{M}_{mn}) = (\mathbb{M}_m \times \mathbb{M}_n)$. Also ist

$$\varphi(mn) = \#\mathbb{M}_{mn} = \#\mathbb{M}_m \cdot \#\mathbb{M}_n = \varphi(m)\varphi(n),$$

wie behauptet. $\diamond$

Ist p prim, so $\varphi(p) = p - 1$, allgemeiner $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$, wenn $e \geq 1$, denn p^e hat genau die Teiler px mit $1 \leq x \leq p^{e-1}$. Aus Korollar 1 folgt also:

Korollar 2 *Ist $n = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung (alle $e_i \geq 1$), so*

$$\varphi(n) = n \cdot \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

8.6 Matrizen über Ringen

Sei R ein Ring (kommutativ mit 1). Die „multiplikative Gruppe“ von R ist die Gruppe der inverbaren Elemente, also

$$R^\times = \{a \in R \mid ab = 1 \text{ für ein } b \in R\} = \{a \in R \mid a|1\}.$$

Ebenso betrachtet man in der (nichtkommutativen) R-Algebra $M_{qq}(R)$ der $q \times q$-Matrizen über R die Gruppe der invertierbaren Elemente

$$GL_q(R) = \{A \in M_{qq}(R) \mid AB = \mathbf{1}_q \text{ für ein } B \in M_{qq}(R)\}.$$

Die Determinante definiert eine multiplikative Abbildung

$$\mathrm{Det}\colon M_{qq}(R) \longrightarrow R.$$

Klar ist:

$$A \in GL_q(R) \Longrightarrow AB = \mathbf{1}_q \text{ für ein } B \Longrightarrow \mathrm{Det}\, A \cdot \mathrm{Det}\, B = \mathrm{Det}\, \mathbf{1}_q = 1$$

$$\Longrightarrow \mathrm{Det}\, A \in R^\times.$$

Zum Beweis der Umkehrung betrachtet man die adjungierte Matrix $\tilde{A} = (\tilde{a}_{ij})$ mit

$$\tilde{a}_{ij} = A_{ji} = \mathrm{Det} \begin{pmatrix} a_{11} & \dots & a_{1,i-1} & a_{1,i+1} & \dots & a_{1q} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{j-1,1} & \dots & a_{j-1,i-1} & a_{j-1,i+1} & \dots & a_{j-1,q} \\ a_{j+1,1} & \dots & a_{j+1,i-1} & a_{j+1,i+1} & \dots & a_{j+1,q} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{q1} & \dots & a_{q,i-1} & a_{q,i+1} & \dots & a_{qq} \end{pmatrix}$$

Damit kann man zeigen:

Satz 7 *Für $A \in M_{qq}(R)$ gilt*
(i) $A\tilde{A} = \mathrm{Det}\, A \cdot \mathbf{1}_q$.
(ii) $A \in GL_q(R) \Longleftrightarrow \mathrm{Det}\, A \in R^\times$*; ist dies der Fall, so*

$$A^{-1} = \frac{1}{\mathrm{Det}\, A}\tilde{A}.$$

Beweis. (i) ist der Determinanten-Entwicklungssatz.
(ii) folgt sofort aus (i). $\diamond$

Beispiel. Im Falle $R = \mathbb{Z}/n\mathbb{Z}$ kann man das so formulieren:

$$A \in M_{qq} \text{ ist invertierbar } \mod n \Longleftrightarrow \mathrm{Det}\, A \text{ ist zu } n \text{ teilerfremd.}$$

Bemerkungen

1. Der Rechenaufwand zur Berechnung der inversen Matrix A^{-1} beträgt bei naiver Anwendung von (ii):

   - Eine $q \times q$-Determinante aus $q!$ Summanden zu je q Faktoren,
   - q^2 Stück $(q-1) \times (q-1)$-Determinanten.

   Das ist sehr ineffizient – nämlich exponentiell in q.

2. Mit GAUSSscher Elimination sinkt der Aufwand auf $\mathrm{O}(q^3)$. Der Haken dabei ist, dass beim exakten Rechnen rationale Zahlen mit *riesigen* Zählern und Nennern auftreten.

3. Ein modifiziertes rein ganzzahliges Eliminationsverfahren ist effizienter, siehe im nächsten Abschnitt, kann aber immer noch recht große Zwischenergebnisse liefern.

4. Eine Alternative beruht auf dem chinesischen Restsatz: Ein Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ induziert einen R-Algebra-Homomorphismus $\varphi_q\colon M_{qq}(R) \longrightarrow M_{qq}(R')$. Ist $A \in M_{qq}$ invertierbar, so

   $$\varphi_q(A)\varphi_q(A^{-1}) = \varphi_q(AA^{-1}) = \varphi_q(\mathbf{1}_q) = \mathbf{1}_q,$$

   also ist auch $\varphi(A)$ invertierbar.

   Allgemeiner gilt $\operatorname{Det} \varphi_q(A) = \varphi(\operatorname{Det} A)$, d.h., das Diagramm

   $$\begin{array}{ccc} M_{qq}(R) & \xrightarrow{\varphi_q} & M_{qq}(R') \\ {\scriptstyle \operatorname{Det}}\downarrow & & \downarrow{\scriptstyle \operatorname{Det}} \\ R & \xrightarrow[\varphi]{} & R' \end{array}$$

   ist kommutativ.

   Im Fall $R = \mathbb{Z}$ kann man die Restklassen-Homomorphismen $\mathbb{Z} \longrightarrow \mathbb{F}_p$ (p prim) für genügend viele Primzahlen p ausnützen – so dass deren Produkt garantiert $> \operatorname{Det} A$ ist –, indem man:

   - alle $\operatorname{Det} A \bmod p$, also in den Körpern $\mathbb{F}_p$ berechnet (ohne riesige Zwischenergebnisse!),
   - $\operatorname{Det} A$ daraus mit dem chinesischen Restsatz bestimmt.

8.7 Ganzzahlige Elimination

Wie löst man lineare Gleichungssysteme über dem Ring $\mathbb{Z}$ der ganzen Zahlen? Wie berechnet man Determinanten? Wie findet man eine inverse Matrix? Wie in der bekannten linearen Algebra über Körpern ist auch in der allgemeineren Situation über Ringen die *Trigonalisation* von Matrizen der Schlüssel zu effizienten Algorithmen.

Einen etwas hinreichend allgemeinen Rahmen liefern folgende drei Klassen von Ringen (kommutativ, nullteilerfrei, mit 1):

- **faktorielle Ringe** = ZPE-Ringe: Alle Elemente haben eine Primzerlegung, insbesondere gibt es zu je zwei Elementen einen größten gemeinsamen Teiler ggT.
- **Hauptidealringe:** Jedes Ideal ist Hauptideal. Hauptidealringe sind faktoriell, und jeder ggT zweier Elemente lässt sich linear aus diesen kombinieren.
- **Euklidische Ringe:** Es gibt eine Division mit Rest. Euklidische Ringe sind Hauptidealringe; ein ggT zweier Elemente lässt sich samt seiner linearen Darstellung effizient mit dem erweiterten euklidischen Algorithmus bestimmen.

Die Menge der invertierbaren Matrizen mit Determinate 1 wird als $SL_n(R) \subseteq GL_n(R)$ bezeichnet.

Hilfssatz 4 *Sei R ein Hauptidealring, $a_1, \ldots, a_n \in R$, d ein* $\mathrm{ggT}(a_1, \ldots, a_n)$. *Dann gibt es eine invertierbare Matrix $U \in SL_n(R)$ mit*

$$U \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Beweis. Sind alle $a_i = 0$, ist die Behauptung trivial. Ansonsten kann man (nach einer eventuellen Permutation, die als Permutationmatrix in U aufgenommen wird – evtl. muss eine 1 durch eine -1 ersetzt werden, um die Determinante zu 1 zu machen) o. B. d. A. $a_1 \neq 0$ annehmen. Da der Fall $n = 1$ ebenfalls trivial ist, kann man auch $n \geq 2$ annehmen.

Sei $d_2 := \mathrm{ggT}(a_1, a_2)$ (gemeint ist *ein* ggT) – dann ist $d_2 \neq 0$ – und allgemeiner $d_i = \mathrm{ggT}(a_1, \ldots, a_i) = \mathrm{ggT}(d_{i-1}, a_i)$ für $i = 3, \ldots, n$. Nun ist $d_2 = c_1 a_1 + c_2 a_2$ Linearkombination. Damit gilt die Gleichung

$$\begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} c_1 a_1 + c_2 a_2 \\ -\frac{a_2 a_1}{d_2} + \frac{a_1 a_2}{d_2} \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \end{pmatrix}$$

mit der invertierbaren Koeffizientenmatrix

$$C = \begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \quad \text{mit } \operatorname{Det} C = \frac{c_1 a_1}{d_2} + \frac{c_2 a_2}{d_2} = 1.$$

Dann geht es mit vollständiger Induktion weiter: Im allgemeinen Schritt sei schon

$$U' \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d' \\ 0 \\ \vdots \\ 0 \\ a_i \\ \vdots \\ a_n \end{pmatrix} \qquad \text{mit } a_i \neq 0$$

erreicht. Dann formt man genauso wie eben zwei Koordinaten um:

$$\begin{pmatrix} d' \\ a_i \end{pmatrix} \rightsquigarrow \begin{pmatrix} d'' \\ 0 \end{pmatrix};$$

damit wird sukzessive die Matrix U aufgebaut. $\diamond$

Bemerkung. Die Inverse der Matrix C im Beweis ist

$$C^{-1} = \begin{pmatrix} \frac{a_1}{d_2} & -c_2 \\ \frac{a_2}{d_2} & c_1 \end{pmatrix}$$

Daraus folgt, dass U und U^{-1} zusammen durch höchstens $n-1$-fache Anwendung des euklidischen Algorithmus bestimmbar sind, dazu $n-1$ Multiplikationen von $n \times n$-Matrizen und höchstens $n-1$ Multiplikationen von Permutationsmatrizen.

Damit lassen sich Matrizen trigonalisieren. (Eine genauere Betrachtung führt zur Hermiteschen Normalform.)

Satz 8 (i) *Sei R ein Hauptidealring und $A \in M_{pq}(R)$. Dann gibt es eine invertierbare Matrix $U \in SL_p(R)$ so dass $H = UA$ die Gestalt*

$$\begin{pmatrix} * & \dots & * \\ & \ddots & \vdots \\ & & * \\ 0 & & \end{pmatrix} \quad \textit{für } p \geq q, \qquad \begin{pmatrix} * & \dots & \dots & * \\ & \ddots & \dots & \\ 0 & & * & \end{pmatrix} \quad \textit{für } p < q$$

hat.

(ii) *Ist R euklidisch, so lassen sich U und U^{-1} gemeinsam mit höchstens $\frac{p(p-1)}{2}$ Durchführungen eines erweiterten euklidischen Algorithmus bestimmen.*

Spezialfall. Zu einer quadratischen Matrix $A \in M_{pp}(R)$ wird $H = UA$ bestimmt. Dann ist

$$\operatorname{Det} A = \operatorname{Det} H = h_{11} \cdots h_{pp}.$$

Ist A invertierbar, so ist $A^{-1} = (U^{-1}H)^{-1} = H^{-1}U$. Dabei ist H^{-1} für die Dreiecksmatrix H trivial zu bestimmen. Determinantenberechnung und Invertierung sind also auf die Trigonalisierung zurückgeführt.

Beweis. Der Beweis besteht in der Angabe eines Algorithmus. Sei $r := \min\{p, q\}$. Der Algorithmus wird initialisiert durch

$$H := A, \quad U := \mathbf{1}_p, \quad V := \mathbf{1}_p.$$

Es wird eine Schleife über $j = 1, \ldots r$ durchgeführt; invariante Relationen sind dabei $UA = H$, $UV = \mathbf{1}_p$.

- Im j-ten Durchlauf sehe H zu Beginn so aus:

$$\begin{pmatrix} * & & & & \\ & \ddots & & & * \\ & & * & & \\ & & & h_{jj} & \\ & 0 & & \vdots & \\ & & & h_{pj} & \end{pmatrix}$$

  Falls $h_{jj} = \ldots = h_{pj} = 0$, sind wir mit diesem Durchlauf fertig. Sonst wird nach dem Hilfssatz eine Matrix $U' \in SL_{p-j+1}(R)$ zusammen mit $(U')^{-1}$ gewonnen mit

$$U' \begin{pmatrix} h_{jj} \\ \ldots \\ h_{pj} \end{pmatrix} = \begin{pmatrix} d_j \\ 0 \\ \ldots \\ 0 \end{pmatrix}$$

  Es ist $\left(\begin{smallmatrix} \mathbf{1} & 0 \\ 0 & U' \end{smallmatrix}\right) \in SL_p(R)$. Man setzt als Ergebnis des Schleifendurchlaufs

$$U := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} U, \quad H := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} H, \quad V := V \begin{pmatrix} \mathbf{1} & 0 \\ 0 & (U')^{-1} \end{pmatrix}.$$

Nach dem letzten Schleifendurchlauf haben U und H die gewünschte Gestalt. $\diamond$

Zum Gesamtaufwand kommen noch je $\frac{p(p-1)}{2}$ Matrizen-Multiplikationen und Multiplikationen mit Permutationsmatrizen hinzu. Der Gesamtaufwand

ist daraus aber nicht unmittelbar abzulesen, da die Größe der Zwischenergebnisse nicht ohne weiteres abgeschätzt werden kann. Man erhält durch genauere Überlegungen einen Aufwand von $O(m^2n^5)$, wenn alle Einträge von A höchstens m-stellig sind und $n = \max(p, q)$. Diese Schranke ist durch Optimierungen noch verbesserbar.

Wie invertiert man nun eine Matrix $A \in GL_q(\mathbb{Z}/n\mathbb{Z})$? Dazu fasst man A als ganzzahlige Matrix auf und bestimmt nach Satz 8 ein $U \in SL_q(\mathbb{Z})$, so dass $H = UA$ ganzzahlige obere Dreiecksmatrix ist. Bei Reduktion mod$n$ bleibt die Gleichung $H = UA$ erhalten und ebenso $A^{-1} = H^{-1}U$; da A mod n invertierbar ist, müssen alle Diagonalelemente von H mod n invertierbar sein.

8.8 Die Hill-Chiffre

Beschreibung

Das **Alphabet** ist $\Sigma = \mathbb{Z}/n\mathbb{Z}$ mit der Struktur als endlicher Ring.

Der **Schlüsselraum** ist $K = GL_l(\mathbb{Z}/n\mathbb{Z})$, die multiplikative Gruppe der invertierbaren Matrizen. Die Größe des Schlüsselraums wird in Abschnitt 8.9 abgeschätzt.

Verschlüsselt wird blockweise, wobei l die Blocklänge ist: Für $k \in GL_l(\mathbb{Z}/n\mathbb{Z})$ und $(a_1, \ldots, a_l) \in (\mathbb{Z}/n\mathbb{Z})^l$ ist

$$\begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix} = f_k(a_1, \ldots, a_l) = k \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix}$$

oder in ausgeschriebener Form

$$c_i = \sum_{j=1}^{l} k_{ij} a_j \quad \text{für } i = 1, \ldots, l.$$

Entschlüsselt wird mit der inversen Matrix:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix} = k^{-1} \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix}.$$

Verwandte Chiffren

Spezialfall: Wird k als Permutationsmatrix P_σ zur Permutation $\sigma \in \mathcal{S}_l$ gewählt, so ist die Verschlüsselungsfunktion f_k die Blocktransposition zu σ.

Verallgemeinerung: Die affine Chiffre. Hier wird ein Schlüssel

$$(k, b) \in GL_l(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^l$$

gewählt; verschlüsselt wird nach der Formel

$$c = ka + b.$$

Wählt man hier k als die Einheitsmatrix, so erhält man als Spezialfall wiederum die Belaso-Chiffre mit Schlüssel b.

Anmerkung: Bei der von Hill vorgeschlagenen Original-Chiffre wird vor Anwendung der linearen Abbildung zunächst noch das Alphabet permutiert, d. h., die Zuordnung der Buchstaben zu den Zahlen $0, \ldots, 25$ wird als Teil des Schlüssels angesehen.

Beispiel

Zur Illustration ein „Spielzeug-Beispiel“ mit ganz unvernünftig kleiner Dimension $l = 2$ und

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Dann ist $\operatorname{Det} k = 77 - 24 = 53 \equiv 1 \bmod 26$ und

$$k^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

Zur Umrechnung von Zahlen in Buchstaben ist es nützlich, die Tabelle

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

zur Hand zu haben. Damit wird der Klartext `Herr` $= (7, 4, 17, 17)$ verschlüsselt zu

$$\begin{aligned} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} &= \begin{pmatrix} 77 + 32 \\ 21 + 28 \end{pmatrix} = \begin{pmatrix} 109 \\ 49 \end{pmatrix} = \begin{pmatrix} 5 \\ 23 \end{pmatrix}, \\ \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 17 \\ 17 \end{pmatrix} &= \begin{pmatrix} 187 + 136 \\ 51 + 119 \end{pmatrix} = \begin{pmatrix} 323 \\ 170 \end{pmatrix} = \begin{pmatrix} 11 \\ 14 \end{pmatrix}, \end{aligned}$$

also $f_k(\texttt{Herr}) = (5, 23, 11, 14) = \texttt{FXLO}$.

Zur Probe die Entschlüsselung:

$$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} = \begin{pmatrix} 35 + 414 & 77 + 252 \\ 115 + 253 & 253 + 154 \end{pmatrix} = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

Bewertung

\+ Wesentlich stärker als die Blocktransposition und die Belaso-Chiffre.

\+ Die Geheimtexte sind sehr gut gleichverteilt; ein Angriff mit nichts als Geheimtext findet keine Anhaltspunkte.

\− Sehr anfällig für einen Angriff mit bekanntem Klartext, siehe Abschnitt 8.10.

8.9 Die Anzahl invertierbarer Matrizen in einem Restklassenring

Ziel ist, eine möglichst genaue Vorstellung davon zu bekommen, wie groß die Anzahl

$$\nu_{ln} := \#GL_l(\mathbb{Z}/n\mathbb{Z})$$

der invertierbaren $l \times l$-Matrizen über dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ ist.

Im Spezialfall $l = 1$ ist ν_{1n} die Anzahl der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ selbst, und das ist der Wert $\varphi(n)$ der EULERschen φ-Funktion.

Eine *obere Schranke* für ν_{ln} ist leicht gefunden:

$$\nu_{ln} \leq \#M_{ll}(\mathbb{Z}/n\mathbb{Z}) = n^{l^2}.$$

Eine *untere Schranke* erhält man aus der Beobachtung, dass Matrizen der Gestalt (über einem Ring R)

$$\begin{pmatrix} 1 & & \\ & \ddots & \\ * & & 1 \end{pmatrix} \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_l \end{pmatrix} \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

stets invertierbar sind, wenn $d_1, \ldots, d_l \in R^\times$. Dadurch erhält man eine injektive Abbildung

$$R^{\frac{l(l-1)}{2}} \times (R^\times)^l \times R^{\frac{l(l-1)}{2}} \longrightarrow GL_l(R).$$

(Beweis der Injektivität: **Übungsaufgabe.**) Daraus folgt die Abschätzung

$$\nu_{ln} \geq n^{\frac{l(l-1)}{2}} \cdot \varphi(n)^l \cdot n^{\frac{l(l-1)}{2}} = n^{l^2-l} \cdot \varphi(n)^l.$$

Zusammengefasst:

Satz 9

$$n^{l^2-l} \cdot \varphi(n)^l \leq \nu_{ln} \leq n^{l^2}.$$

Bemerkungen

1. Die Idee, Matrizen in der Form $A = UDV$ wie oben zu schreiben – mit einer Diagonalmatrix D, einer unteren Dreiecksmatrix U mit Einser-Diagonale sowie einer oberen Dreiecksmatrix V mit ebenfalls Einser-Diagonale – ist gleichzeitig eine geeignete Methode, invertierbare Matrizen zu konstruieren, ohne lange zu probieren und Determinanten auszurechnen. Man erhält „fast alle“ invertierbaren Matrizen auf diese Weise – in der Theorie der algebraischen Gruppen ist dies die „große BRUHAT-Zelle“. Solche Matrizen sind auch wegen der Formel $A^{-1} = V^{-1}D^{-1}U^{-1}$ leicht zu invertieren.

2. Aus zwei unteren Schranken für die φ-Funktion, die hier ohne Beweis angegeben werden, ergeben sich handlichere Schranken für ν_{ln}. Die erste Abschätzung ist

$$\varphi(n) > \frac{6}{\pi^2} \cdot \frac{n}{\ln n} \quad \text{für } n \geq 7.$$

Daraus folgt für $n \geq 7$

$$\nu_{ln} > n^{l^2-l} \cdot \left(\frac{6}{\pi^2} \cdot \frac{n}{\ln n} \right)^l = \frac{6^l}{\pi^{2l}} \cdot \frac{n^{l^2}}{(\ln n)^l}.$$

3. Die andere Schranke ist

$$\varphi(n) > \frac{n}{2 \cdot \ln \ln n} \quad \text{für fast alle } n.$$

Daraus folgt

$$\nu_{ln} > \frac{1}{(2 \cdot \ln \ln n)^l} \cdot n^{l^2}$$

oder auch

$$\frac{1}{(2 \cdot \ln \ln n)^l} \quad < \quad \frac{\nu_{ln}}{n^{l^2}} \quad < \quad 1$$

für fast alle n.

Fazit: „Sehr viele“ bis „fast alle“ Matrizen in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ sind invertierbar. Was das im einzelnen bedeutet, wird weiter unten noch etwas genauer beleuchtet.

Beispiel. Für $n = 26$ lässt sich die untere Schranke aus Satz 9 noch stark vergröbern zu einer sehr übersichtlichen Form: Da $\varphi(26) = 12$, folgt

$$\nu_{l,26} \geq 26^{l^2-l} 12^l > 16^{l^2-l} 8^l = 2^{4l^2-l}.$$

Daraus erhält man die Abschätzungen $\nu_{2,26} > 2^{14}$, $\nu_{3,26} > 2^{33}$, $\nu_{4,26} > 2^{60}$, $\nu_{5,26} > 2^{95}$, so dass die HILL-Chiffre spätestens bei der Blockgröße 5 vor vollständiger Schlüsselsuche sicher ist.

Es gibt auch eine genaue Formel für ν_{ln}, die jetzt hergeleitet wird.

Hilfssatz 5 *Sei $n = p$ prim. Dann ist*

$$\nu_{lp} = p^{l^2} \cdot \rho_{lp} \quad \textit{mit} \quad \rho_{lp} = \prod_{i=1}^{l} \left(1 - \frac{1}{p^i} \right).$$

Insbesondere geht die relative Häufigkeit von invertierbaren Matrizen, ρ_{lp}, bei festem l mit wachsendem p gegen 1.

Beweis. Man baut eine invertierbare Matrix Spalte für Spalte auf und zählt jeweils die Möglichkeiten. Da $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein Körper ist, ist die erste Spalte ein beliebiger Vektor $\neq 0$. Davon gibt es $p^l - 1$ Stück.

Seien nun schon i Spalten gewählt; diese müssen linear unabhängig sein und spannen daher einen Unterraum von $\mathbb{F}_p^l$ aus p^i Elementen auf. Die $(i+1)$-te Spalte ist dann ein beliebiger Vektor außerhalb dieses Unterraums, und davon gibt es $p^l - p^i$ Stück. Insgesamt sind das

$$\prod_{i=0}^{l-1}(p^l - p^i) = \prod_{i=0}^{l-1} p^l(1 - p^{i-l}) = p^{l^2} \prod_{j=1}^{l} \left(1 - \frac{1}{p^j}\right)$$

Möglichkeiten. $\diamond$

Hilfssatz 6 *Sei $n = p^e$ mit p prim und $e \geq 1$. Dann gilt:*

(i) *Sei $A \in M_{ll}(\mathbb{Z})$. Dann ist $A \bmod n$ in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ genau dann invertierbar, wenn $A \bmod p$ in $M_{ll}(\mathbb{F}_p)$ invertierbar ist.*

(ii) *Die Anzahl der invertierbaren Matrizen in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ ist*

$$\nu_{ln} = p^{el^2} \cdot \rho_{lp}.$$

(iii) *Die relative Häufigkeit invertierbarer Matrizen in $M_{ll}(\mathbb{Z}/p^e\mathbb{Z})$ ist ρ_{lp}, unabhängig vom Exponenten e.*

Beweis. (i) Da $\mathrm{ggT}(p, \mathrm{Det}\, A) = 1 \Longleftrightarrow \mathrm{ggT}(n, \mathrm{Det}\, A) = 1$, sind beide Aussagen zu $p \nmid \mathrm{Det}\, A$ äquivalent.

(ii) O. B. d. A. habe A nur Einträge in $[0 \ldots n-1]$. Dann schreibt man $A = pQ + R$ mit allen Einträgen von R in $[0 \ldots p-1]$ und allen von Q in $[0 \ldots p^{e-1} - 1]$. Nun ist $A \bmod n$ genau dann invertierbar, wenn $R \bmod p$ invertierbar ist; für R gibt es nach Hilfssatz 5 ν_{lp} Möglichkeiten und für Q noch $p^{(e-1)l^2}$. Zusammen ist das die behauptete Formel.

(iii) folgt direkt aus (ii). $\diamond$

Hilfssatz 7 *Sind m und n teilerfremd, so ist $\nu_{l,mn} = \nu_{lm}\nu_{ln}$.*

Beweis. Der vom chinesischen Restsatz gelieferte Ring-Isomorphismus

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

wird zu einem Isomorphismus der (nichtkommutativen) Ringe

$$M_{ll}(\mathbb{Z}/mn\mathbb{Z}) \longrightarrow M_{ll}(\mathbb{Z}/m\mathbb{Z}) \times M_{ll}(\mathbb{Z}/n\mathbb{Z})$$

fortgesetzt. Die Behauptung folgt, weil sie die Gleichheit der jeweiligen Anzahlen von invertierbaren Elementen aussagt. $\diamond$

Daraus folgt durch Induktion unmittelbar:

Satz 10 *Für $n \in \mathbb{N}$ gilt*

$$\nu_{ln} = n^{l^2} \cdot \prod_{\substack{p\ prim \\ p|n}} \rho_{lp}.$$

Insbesondere hängt die relative Häufigkeit invertierbarer Matrizen, $\rho_{ln} = \nu_{ln}/n^{l^2}$ nicht von den Exponenten der Primfaktoren in n ab; die explizite Formel heißt

$$\rho_{ln} = \prod_{\substack{p\ prim \\ p|n}} \rho_{lp} = \prod_{\substack{p\ prim \\ p|n}} \prod_{i=1}^{l} \left(1 - \frac{1}{p^i}\right).$$

Beispiel. Für $n = 26$ ergibt die explizite Formel die Werte $\nu_{1,26} = 12$, $\nu_{2,26} = 157{\cdot}248$, $\nu_{3,26} = 1{\cdot}634{\cdot}038{\cdot}189{\cdot}056 \approx 1.6 \cdot 10^{12}$. Der Vergleich des letzteren Werts mit der oben hergeleiteten unteren Schranke $2^{33} \approx 8 \cdot 10^9$ zeigt, wie grob diese ist.

Übungsaufgabe. Sei $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... die aufsteigende Folge der Primzahlen. Sei $n_r = p_1 \cdots p_r$ für $r \geq 1$. Zeige, dass bei festem l

$$\lim_{r\to\infty} \rho_{ln_r} = 0.$$

D. h., der Anteil der invertierbaren Matrizen schwindet immer mehr. *Anleitung*: Sei ζ die RIEMANNsche ζ-Funktion. Welchen Wert hat ζ in den natürlichen Zahlen $i \geq 1$?

8.10 Kryptoanalyse der HILL-Chiffre

Die Blocklänge

Die Blocklänge l kann man dadurch bestimmen, dass alle Geheimtextlängen Vielfache von l sind – zumindest wenn das Verfaheren „in Reinkultur“, d. h. ohne verschleiernde Modifikationen, angewendet wurde. Notfalls hilft aber auch das (etwas lästige) Durchprobieren aller in Frage kommenden Längen.

Bekannter Klartext

Die Kryptoanalyse der HILL-Chiffre ist fast nur mit bekanntem Klartext erfolgversprechend – dann aber fast trivial. Zur erfolgreichen Kryptoanalyse reichen in der Regel l bekannte Klartextblöcke, also bekannter Klartext der Länge l^2. (Das ist ja im wesentlichen auch die Länge des Schlüssels, wie in Abschnitt 8.9 hergeleitet.)

Seien $(a_{11}, \ldots, a_{l1})$, $\ldots$, $(a_{1l}, \ldots, a_{ll})$ die bekannten Klartextblöcke mit den zugehörigen Geheimtextblöcken $(c_{11}, \ldots, c_{l1})$, $\ldots$, $(c_{1l}, \ldots, c_{ll})$.

Daraus ergibt sich die Matrizen-Gleichung

$$\begin{pmatrix} k_{11} & \ldots & k_{1l} \\ \vdots & \ddots & \vdots \\ k_{l1} & \ldots & k_{ll} \end{pmatrix} \begin{pmatrix} a_{11} & \ldots & a_{1l} \\ \vdots & \ddots & \vdots \\ a_{l1} & \ldots & a_{ll} \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1l} \\ \vdots & \ddots & \vdots \\ c_{l1} & \ldots & c_{ll} \end{pmatrix}$$

oder kurz geschrieben: $kA = C$ in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$. Falls zufällig A invertierbar ist, kann man sofort nach k auflösen und erhält den Schlüssel

$$k = CA^{-1}.$$

Die Matrix-Inversion ist effizient nach Abschnitt 8.7. Ferner ist A nach Abschnitt 8.9 mit hoher Wahrscheinlichkeit invertierbar. Falls das nicht der Fall ist, benötigt man geringfügig mehr bekannten Klartext. Die Details der Lösung werden hier nicht ausgeführt. Statt dessen ein Beispiel.

Beispiel

In dem Beispiel aus Abschnitt 8.8 – gedacht als Teil eines längeren Textes – sei der Klartext `Herr` bekannt. Er bildet zwei Blöcke und somit die Matrix

$$A = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

Deren Determinante ist $\operatorname{Det} A = 17 \cdot (7 \cdot 1 - 4 \cdot 1) = 17 \cdot 3 = 51 \equiv -1 \bmod 26$; der Kryptoanalytiker hat also Glück und kann sofort invertieren:

$$A^{-1} = \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix}.$$

Daraus ergibt sich die Schlüsselmatrix:

$$k = \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Die affine Chiffre

Für die affine Chiffre $c = ka + b$ braucht man im allgemeinen $l + 1$ bekannte Klartextblöcke $a_0, \ldots, a_l$. Durch Differenzenbildung erhält man

$$\begin{aligned} c_l - c_0 &= k \cdot (a_l - a_0), \\ &\ldots \\ c_l - c_{l-1} &= k \cdot (a_l - a_{l-1}). \end{aligned}$$

Dadurch ist die Kryptoanalyse auf die der Hill-Chiffre mit l bekannten Klartextblöcken reduziert.

Fazit

Linearität in einer Chiffre macht sie extrem anfällig für einen Angriff mit bekanntem Klartext, weil lineare Gleichungssysteme so leicht lösbar sind – zumindest über den Ringen, in denen man praktisch rechnen kann.

Daher wird man für die Konstruktion von sicheren Chiffren zur Vermeidung von Angriffen mit bekanntem Klartext auf Nichtlinearität setzen: Algebraische Gleichungen höheren Grades sind sehr viel schwerer lösbar. Daher der Merksatz:

Bekannter Klartext ist der natürliche Feind der Linearität.

Übungsaufgabe. Hill hatte vorgeschlagen, vor Anwendung der linearen Abbildung das Alphabet zu permutieren, d. h., eine monoalphabetische Substitution vorzuschalten. Wie wirkt sich dies auf die Kryptoanalyse aus?