

Zahlentheoretische Methoden in der Kryptographie

Vorlesungsskript von Arne Winterhof

23. Januar 2004

Dieses Skript ist die schriftliche Ausarbeitung einer Vorlesung, die ich im Wintersemester 2001/2002 an der Universität Wien gehalten haben. Für die Unterstützung beim Schreiben bedanke ich mich bei Frau Paula Rossi, für Korrekturen bei meinen Studenten.

Arne Winterhof

Inhaltsverzeichnis

1	Zahlentheoretische Grundlagen	4
1.1	Teilbarkeit und Euklidischer Algorithmus	4
1.2	Kongruenzen und Eulersche φ -Funktion	7
1.3	Quadratische Reste und Reziprozität	10
1.4	Summen von Legendre-Symbolen	15
1.5	Laufzeiten von arithmetischen Operationen und Algorithmen . . .	18
1.6	Quadratwurzeln modulo p	22
2	Einfache Kryptosysteme	24
2.1	Grundbegriffe	24
2.2	Lineare Substitutionschiffre	24
2.3	Verschlüsselungsmatrizen	25
3	Public-Key Kryptosysteme	27
3.1	Grundlagen	27
3.2	Das RSA-Verfahren	28
3.3	Diskreter Logarithmus und Diffie-Hellman Schlüsselaustausch . . .	28
4	Sicherheitsanalyse	30
4.1	Interpolation der Diffie-Hellman Abbildung	30
4.2	Interpolation des diskreten Logarithmus	31
4.3	Darstellung des diskreten Logarithmus als lineare Rekursionsfolge	32
5	Algorithmen zur Berechnung des diskreten Logarithmus	33
5.1	Direkte Suche	33
5.2	Baby-Step Giant-Step Algorithmus	33
5.3	Index-Calculus	34
6	Faktorisierungsalgorithmen	37
6.1	Sieb des Eratosthenes	37
6.2	Fermat-Faktorisierung	37
6.3	Pollards ρ -Methode	38
6.4	Quadratwurzelfaktorisierung	39

6.5	Das quadratische Sieb	41
7	Primzahlerzeugung	43
7.1	Pseudoprimzahltests	43
7.1.1	Fermat Test	43
7.1.2	Solovay-Strassen Test	44
7.1.3	Miller-Rabin Test	45
7.2	Primzahltests	47
7.2.1	Lucas-Lehmer Test	47
7.2.2	Der $n - 1$ Test	49
7.2.3	Bestimmung primitiver Wurzeln	49
8	Zur Komplexität der Diffie-Hellman Abbildung und des diskreten Logarithmus	50
8.1	Vandermonde-Determinante	50
8.2	Der Grad der Diffie-Hellman Abbildung	51
8.3	Untere Schranken für das Gewicht	52
8.4	Weitere untere Schranken für den Grad	54
8.5	Eine explizite Formel für den diskreten Logarithmus	55
8.6	Explizite Darstellungen als Rekursionsfolge	57

Kapitel 1

Zahlentheoretische Grundlagen

1.1 Teilbarkeit und Euklidischer Algorithmus

Definition 1 Eine ganze Zahl b heißt durch eine ganze Zahl $a \neq 0$ teilbar, wenn es eine ganze Zahl x mit $b = ax$ gibt.

Schreibweise: $a|b$.

Ist b nicht durch a teilbar : $a \nmid b$.

Lemma 1

1. $a|0$ für alle ganzen Zahlen $a \neq 0$.
2. $a|b \Rightarrow a|bc$ für alle ganzen Zahlen c .
3. $a|b$ und $b|c \Rightarrow a|c$.
4. $a|b$ und $a|c \Rightarrow a|bx + cy$ für alle ganzen Zahlen x und y .
5. $a|b$ und $b|a \Rightarrow a = \pm b$.
6. Für natürliche Zahlen a, b gilt: $a|b \Rightarrow a \leq b$.
7. $m \neq 0$: $a|b \Rightarrow ma|mb$.

Beweis: Trivial. □

Lemma 2 (Divisionsalgorithmus)

Zu ganzen Zahlen a und b mit $a > 0$ gibt es eindeutig bestimmte ganze Zahlen q und r mit

$$b = qa + r, \quad 0 \leq r < a.$$

Beweis: Die Zahl r ist die kleinste nichtnegative ganze Zahl der Form $b - aq$, $q \in \mathbb{Z}$, womit auch q bestimmt ist. Gäbe es ein weiteres Paar (q_1, r_1) mit $b = aq_1 + r_1$ und $r < r_1 < a$ so gilt $r_1 - r = a(q - q_1)$ also $a|r_1 - r$, was Lemma 1(6.) widerspricht. \square

Definition 2 Eine ganze Zahl mit $a|b$ und $a|c$ heißt gemeinsamer Teiler von b und c . Falls $bc \neq 0$, so gibt es einen größten gemeinsamen Teiler $\text{ggT}(b, c)$.

Satz 1 (Euklidischer Algorithmus)

Seien b und $c > 0$ ganze Zahlen. Wiederholte Anwendung des Divisionsalgorithmus liefert:

$$\begin{array}{lll} b & = & cq_1 + r_1 & 0 < r_1 < c \\ c & = & r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2q_3 + r_3 & 0 < r_3 < r_2 \\ \dots & & \dots & \dots \\ r_{j-2} & = & r_{j-1}q_j + r_j & 0 < r_j < r_{j-1} \\ r_{j-1} & = & r_jq_{j+1} & \end{array}$$

Es gilt $\text{ggT}(b, c) = r_j$ und durch Rückwärtseinsetzen erhält man $\text{ggT}(b, c) = bx + cy$ mit ganzen Zahlen x und y .

Beweis: Die Folge r_1, r_2, \dots fällt streng monoton und bricht daher nach endlich vielen Schritten ab. Wegen $r_{j-1} = r_jq_{j+1}$ teilt r_j nach Lemma 1(4.) r_{j-1} und somit

$$\begin{array}{l} r_{j-2} = r_{j-1}q_j + r_j \\ r_{j-3} = r_{j-2}q_{j-1} + r_{j-1} \\ \vdots \\ c = r_1q_2 + r_2 \\ b = cq_1 + r_1. \end{array}$$

Ein gemeinsamer Teiler d von b und c teilt auch

$$\begin{array}{l} r_1 = b - cq_1 \\ r_2 = c - r_1q_1 \\ \vdots \\ r_j = r_{j-2} - r_{j-1}q_j. \end{array}$$

\square

Beispiel: $\text{ggT}(1547, 560)$

$$\begin{aligned}1547 &= 2 \cdot 560 + 427 \\560 &= 1 \cdot 427 + 133 \\427 &= 3 \cdot 133 + 28 \\133 &= 4 \cdot 28 + 21 \\28 &= 1 \cdot 21 + 7 \\21 &= 3 \cdot 7\end{aligned}$$

$$\begin{aligned}7 &= 28 - 21 = 28 - (133 - 4 \cdot 28) \\&= 5 \cdot 28 - 133 = 5(427 - 3 \cdot 133) - 133 \\&= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16(560 - 427) \\&= 21 \cdot 427 - 16 \cdot 560 = 21(1547 - 2 \cdot 560) - 16 \cdot 560 \\&= 21 \cdot 1547 - 58 \cdot 560\end{aligned}$$

Definition 3 Eine natürliche Zahl $p > 1$ ohne echte Teiler, d.h. 1 und p sind die einzigen Teiler, heißt Primzahl.

Satz 2 (Fundamentalsatz der Zahlentheorie)

Die Zerlegung einer beliebigen natürlichen Zahl $n > 1$ in Primzahlen ist (bis auf die Reihenfolge) eindeutig.

Beweis: Angenommen n sei die kleinste natürliche Zahl mit zwei verschiedenen Primfaktorzerlegungen

$$n = p_1 \dots p_r = q_1 \dots q_s, \quad r, s > 1.$$

Dann kann kein p_i mit einem q_j übereinstimmen. Sei o.B.d.A. $p_1 < q_1$ und

$$N := (q_1 - p_1)q_2q_3 \dots q_s = p_1(p_2 \dots p_r - q_2 \dots q_s) < n.$$

Wegen $p_1 \nmid (q_1 - p_1)$ haben wir zwei verschiedene Zerlegungen von N im Widerspruch zu $N < n$. \square

Kanonische Zerlegung: $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\alpha_1, \dots, \alpha_r \in \mathbb{N}$.

$$\begin{aligned}n &= p_1^{\alpha_1} \dots p_r^{\alpha_r}, \quad \alpha_1, \dots, \alpha_r \geq 0 \\m &= p_1^{\beta_1} \dots p_r^{\beta_r}, \quad \beta_1, \dots, \beta_r \geq 0 \\ \text{ggT}(n, m) &= p_1^{\min(\alpha_1, \beta_1)} \dots p_r^{\min(\alpha_r, \beta_r)}.\end{aligned}$$

Beispiel:

$$\begin{aligned}1547 &= 7 \cdot 13 \cdot 17 \\560 &= 2^4 \cdot 5 \cdot 7 \\ \text{ggT}(1547, 560) &= 7\end{aligned}$$

Folgerung: p Primzahl: $p|ab \Rightarrow p|a$ oder $p|b$.

1.2 Kongruenzen und Eulersche φ -Funktion

Definition 4 Sei $0 \neq m \in \mathbb{Z}$. Zwei ganze Zahlen a, b heißen kongruent modulo m genau dann, wenn $m|a - b$.

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

Lemma 3 Die Relation \equiv ist eine Äquivalenzrelation, d. h.

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Außerdem gilt:

4. $a \equiv b \pmod{m}$ und $d|m \Rightarrow a \equiv b \pmod{d}$
5. $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$, $\text{ggT}(m, n) = 1 \Rightarrow a \equiv b \pmod{mn}$.

Beweis: Trivial. □

Definition 5 Die ganzen Zahlen modulo m , bezeichnet $\mathbb{Z}/m\mathbb{Z}$, ist die Menge der Restklassen $a \pmod{m} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{m}\}$, $a \in \mathbb{Z}$.

Lemma 4 $\mathbb{Z}/m\mathbb{Z}$ ist ein kommutativer Ring mit 1.

Beweis: Trivial. □

Lemma 5 Die Elemente $a \pmod{m} \in \mathbb{Z}/m\mathbb{Z}$ mit multiplikativen Inversen (die Einheiten) sind genau die Elemente mit $\text{ggT}(a, m) = 1$. Sie bilden bzgl. der Multiplikation eine Gruppe (Bezeichnung: $\mathbb{Z}/m\mathbb{Z}^*$).

Beweis: Sei $d := \text{ggT}(a, m)$. Aus $ab \equiv 1 \pmod{m}$, d. h. $m|ab - 1$ folgt $d|ab - 1$. Wegen $d|a$ und $\text{ggT}(a, ab - 1) = 1$ gilt $d = 1$. Falls $d = 1$ so liefert der Euklidische Algorithmus ganze Zahlen x, y mit $1 = ax + my$ also $ax \equiv 1 \pmod{m}$. Die zweite Aussage ist trivial. □

Definition 6 (Eulersche φ -Funktion)

$$\varphi(n) := |\{1 \leq b \leq n \mid \text{ggT}(b, n) = 1\}| = |\mathbb{Z}/m\mathbb{Z}^*|.$$

Bemerkung: $\varphi(1) = 1$

p Primzahl $\Rightarrow \varphi(p) = p - 1$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\alpha \in \mathbb{N}$

Lemma 6 (Kleiner Satz von Fermat)

Sei p eine Primzahl, dann gilt für jede ganze Zahl a :

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

und

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

falls $p \nmid a$.

Beweis: Gelte zunächst $p \nmid a$. Die Zahlen $0, a, 2a, \dots, (p-1)a$ sind modulo p verschieden, denn aus $ia \equiv ja \pmod{p}$ folgt $p \mid (i-j)a$ und somit $p \mid (i-j)$. Wegen $i, j < p$ gilt $i = j$. Es folgt $a \cdot 2a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$ und somit $a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$. Wegen $p \nmid (p-1)!$ gilt $a^{p-1} \equiv 1 \pmod{p}$ und somit $a^p \equiv a \pmod{p}$.

Falls $p \mid a$ dann ist $a^p \equiv a \pmod{p}$ trivial. □

Korollar 1 Für $p \nmid a$ gilt:

$$n \equiv m \pmod{p-1} \Rightarrow a^n \equiv a^m \pmod{p}.$$

Beispiel: Berechne $2^{10^6} \pmod{7}$.

$$10^6 \equiv 4^6 \equiv 16^3 \equiv 4^3 \equiv 4 \pmod{6} \Rightarrow 2^{10^6} \equiv 2^4 \equiv 2 \pmod{7}.$$

Satz 3 (Chinesischer Restsatz)

Seien m_1, m_2 natürliche Zahlen mit $\text{ggT}(m_1, m_2) = 1$ und a_1, a_2 weitere ganze Zahlen. Dann haben die Kongruenzen

$$x \equiv a_1 \pmod{m_1} \quad \text{und} \quad x \equiv a_2 \pmod{m_2}$$

gemeinsame Lösungen. Je zwei Lösungen sind kongruent modulo $m_1 m_2$.

Beweis: Eindeutigkeit: Seien x_1 und x_2 zwei Lösungen, so gilt $x_1 \equiv x_2 \pmod{m_1}$ und $\pmod{m_2}$ also $x_1 \equiv x_2 \pmod{m_1 m_2}$ nach Lemma 3(5.).

Existenz: Seien n_1 und n_2 ganze Zahlen mit

$$m_2 n_1 \equiv 1 \pmod{m_1} \quad \text{bzw.} \quad m_1 n_2 \equiv 1 \pmod{m_2}.$$

Dann ist $x = a_1 m_2 n_1 + a_2 m_1 n_2$ eine gemeinsame Lösung beider Kongruenzen. \square

Beispiel: Bestimme alle gemeinsamen Lösungen von $x \equiv 1 \pmod{3}$ und $x \equiv 2 \pmod{4}$.

Methode 1: $x \equiv 1, 4, 7$ oder $10 \pmod{12}$ und $x \equiv 2, 6$ oder $10 \pmod{12}$ also $x \equiv 10 \pmod{12}$.

Methode 2: Aus $4n_1 \equiv 1 \pmod{3}$ folgt $n_1 \equiv 1 \pmod{3}$ und aus $3n_2 \equiv 1 \pmod{4}$ folgt $n_2 \equiv 3 \pmod{4}$. Also ist $x \equiv 1 \cdot 4 \cdot 1 + 2 \cdot 3 \cdot 3 \equiv 10 \pmod{12}$.

Korollar 2 Die Eulersche φ -Funktion ist multiplikativ, d.h.

$$\varphi(mn) = \varphi(m) \varphi(n), \quad \text{wenn } \text{ggT}(m, n) = 1.$$

Beweis: Zu j mit $1 \leq j \leq mn$ definiere j_1 und j_2 durch

$$j \equiv j_1 \pmod{m}, \quad 0 \leq j_1 < m,$$

$$j \equiv j_2 \pmod{n}, \quad 0 \leq j_2 < n.$$

Nach dem chinesischen Restsatz, Satz 3, ist j durch j_1 und j_2 eindeutig bestimmt. Es gilt

$$\begin{aligned} \text{ggT}(mn, j) = 1 &\Leftrightarrow \text{ggT}(m, j) = \text{ggT}(n, j) = 1 \\ &\Leftrightarrow \text{ggT}(m, j_1) = \text{ggT}(n, j_2) = 1. \end{aligned}$$

Die Anzahl der j_1 mit $\text{ggT}(m, j_1) = 1$ ist $\varphi(m)$ und die Anzahl der j_2 mit $\text{ggT}(n, j_2) = 1$ ist $\varphi(n)$. Also ist die Anzahl $\varphi(mn)$ der j mit $\text{ggT}(mn, j) = 1$ gleich $\varphi(m) \cdot \varphi(n)$. \square

Beispiel: $\varphi(90) = \varphi(2 \cdot 3^2 \cdot 5) = \varphi(2)\varphi(3^2)\varphi(5) = 1 \cdot 6 \cdot 4 = 24$.

Lemma 7 (Euler-Fermat)

Ist $\text{ggT}(a, m) = 1$, so gilt $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Beweis: Analog Lemma 6. \square

Korollar 3 Für $a \in \mathbb{Z}$ mit $\text{ggT}(a, m) = 1$ gilt:

$$n_1 \equiv n_2 \pmod{\varphi(m)} \Rightarrow a^{n_1} \equiv a^{n_2} \pmod{m}.$$

Beispiel: Berechne $2^{10^6} \pmod{77}$.

$$\varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$$

$$10^6 \equiv 100^3 \equiv 40^3 \equiv 1600 \cdot 40 \equiv 40 \cdot 40 \equiv 40 \pmod{60}$$

$$2^{10^6} \equiv 2^{40} \equiv 1024^4 \equiv 23^4 \equiv 100 \equiv 23 \pmod{77}$$

Einfacher:

$$10^6 \equiv 4 \pmod{6} \Rightarrow 2^{10^6} \equiv 2^4 \equiv 2 \pmod{7}$$

$$10^6 \equiv 0 \pmod{10} \Rightarrow 2^{10^6} \equiv 1 \pmod{11}$$

Chinesischer Restsatz: $2^{10^6} \equiv 23 \pmod{77}$

Lemma 8 Für $n \in \mathbb{N}$ gilt

$$\sum_{d|n} \varphi(d) = n.$$

Beweis: Ist $n = p^\alpha$, so gilt

$$\sum_{d|n} \varphi(d) = \sum_{j=0}^{\alpha} \varphi(p^j) = 1 + (p-1) + (p^2-p) + \dots + p^\alpha - p^{\alpha-1} = p^\alpha.$$

Es bleibt zu zeigen, dass $F(n) = \sum_{d|n} \varphi(d)$ multiplikativ ist. Sei $n = mk$ mit $\text{ggT}(m, k) = 1$. Dann läßt sich jeder Teiler d von n als $d = d_1 d_2$ mit $d_1|m$ und $d_2|k$ schreiben. Somit gilt

$$\begin{aligned} F(n) &= \sum_{d_1|m, d_2|k} \varphi(d_1 d_2) = \sum_{d_1|m, d_2|k} \varphi(d_1) \varphi(d_2) \\ &= \left(\sum_{d_1|m} \varphi(d_1) \right) \left(\sum_{d_2|k} \varphi(d_2) \right) = F(m) F(k). \end{aligned}$$

□

1.3 Quadratische Reste und Reziprozität

Im ganzen Abschnitt sei $p > 2$ eine Primzahl.

Definition 7 $\mathbb{Z}/p\mathbb{Z}[X] := \{\sum_{j=0}^n a_j X^j \mid a_j \in \mathbb{Z}/p\mathbb{Z}, a_n \neq 0, n \in \mathbb{N} \cup \{0\}\}$ heißt Polynomring über $\mathbb{Z}/p\mathbb{Z}$. Die Elemente $f(X) = \sum_{j=0}^n a_j X^j$ heißen Polynome und $\text{grad}(f) := n$ der Grad von f . Ein Element $a \in \mathbb{Z}/p\mathbb{Z}$ mit $f(a) \equiv 0 \pmod{p}$ heißt Nullstelle von f .

Bemerkung: Analog zur Teilbarkeit in \mathbb{Z} kann man Teilbarkeit in $\mathbb{Z}/p\mathbb{Z}[X]$ definieren und erhält einen Euklidischen Algorithmus für Polynome (Polynomdivision).

Lemma 9 Ein Polynom $f(X)$ über $\mathbb{Z}/p\mathbb{Z}$ vom Grad n , $n \in \mathbb{N}$, hat höchstens n Nullstellen.

Beweis: Ein Polynom vom Grad $n = 0$ hat keine Nullstelle. Sei $\text{grad}(f) = n > 0$ und gelte die Behauptung für alle Polynome vom Grad $n-1$. Hätte $f(X)$ mehr als n Nullstellen und sei x_0 eine Nullstelle, so würde Polynomdivision durch $(X - x_0)$ ein Polynom vom Grad $n-1$ mit mindestens n Nullstellen liefern. □

Definition 8 Die Ordnung von $a \in \mathbb{Z}$ mit $p \nmid a$ ist das kleinste $d > 0$ mit $a^d \equiv 1 \pmod{p}$.

Bezeichnung: $\text{ord}_p(a)$.

Lemma 10 Die Ordnung von $a \in \mathbb{Z}$ mit $p \nmid a$ teilt $p - 1$.

Beweis: Gelte $a^d \equiv 1 \pmod{p}$ mit $d \nmid p - 1$. Dann existieren q und $0 < r < d$ mit $p - 1 = dq + r$ und es gilt

$$a^r \equiv a^{p-1-dq} \equiv a^{p-1}(a^d)^{-q} \equiv 1 \pmod{p}$$

nach Voraussetzung und Lemma 6. Wegen $0 < r < d$ ist d nicht die Ordnung von a . \square

Satz 4 $\mathbb{Z}/p\mathbb{Z}^*$ ist zyklisch, d.h. es gibt ein Element g , dessen Potenzen alle Elemente von $\mathbb{Z}/p\mathbb{Z}^*$ durchlaufen.

Beweis: Hat $a \in \mathbb{Z}/p\mathbb{Z}^*$ die Ordnung $d \mid p - 1$, so auch alle Elemente der Form a^j mit $\text{ggT}(j, d) = 1$, denn mit $1 = jx + dy$ folgt aus

$$1 \equiv a^{jd'} \equiv a^{jxd'} \equiv a^{(1-dy)d'} \equiv a^{d'} \pmod{p},$$

dass $d' \geq d$ ist. Für Elemente a^j mit $t = \text{ggT}(j, d) > 1$ gilt

$$a^{jd/t} \equiv (a^d)^{j/t} \equiv 1 \pmod{p}.$$

Nach Lemma 9 hat das Polynom $X^d - 1$ außer a^j , $0 \leq j < d$, keine weiteren Nullstellen. $\mathbb{Z}/p\mathbb{Z}^*$ enthält also kein oder genau $\varphi(d)$ Elemente der Ordnung d . Nach Lemma 8 müssen aber genau $\varphi(d)$ Elemente der Ordnung $d \mid p - 1$, insbesondere der Ordnung $d = p - 1$, existieren. \square

Definition 9 Man nennt $a \in \mathbb{Z}/p\mathbb{Z}^*$ einen quadratischen Rest modulo p , wenn $X^2 - a$ eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}^*$ hat. Anderenfalls heißt a quadratischer Nichtrest modulo p .

Definition 10 Das Legendre-Symbol $\left(\frac{a}{p}\right)$ ist definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{falls } p \mid a \\ 1, & \text{falls } a \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1, & \text{falls } a \text{ quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

Lemma 11

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

Beweis: Für $p|a$ ist die erste Aussage trivial. Gelte jetzt $p \nmid a$. Nach Satz 4 ist $a = g^j$ und a ist genau dann quadratischer Rest, wenn j gerade ist. Außerdem ist $a^{(p-1)/2} \equiv g^{j(p-1)/2} \equiv 1 \pmod{p}$ genau dann, wenn $j(p-1)/2$ durch $p-1$ teilbar und somit j gerade ist. Die zweite Aussage folgt aus der ersten. \square

Lemma 12

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Beweis: Sei b quadratischer Nichtrest modulo p . Mit a durchläuft auch ab alle Restklassen modulo p . Es gilt also

$$S := \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = \sum_{a=0}^{p-1} \left(\frac{ab}{p}\right) = \left(\frac{b}{p}\right) \sum_{a=0}^{p-1} \left(\frac{a}{b}\right) = -S$$

und damit $S = 0$. \square

2. *Beweis:* Sei $g \in \mathbb{Z}/p\mathbb{Z}$ ein Element der Ordnung $p-1$. Dann gilt:

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{g^j}{p}\right) = \sum_{j=1}^{p-1} (-1)^j = 0.$$

\square

Lemma 13

$$(X + Y)^p \equiv X^p + Y^p \pmod{p}.$$

Beweis: Nach dem Binomischen Lehrsatz gilt:

$$(X + Y)^p \equiv \sum_{j=0}^p \binom{p}{j} X^{p-j} Y^j \pmod{p}.$$

Für $1 \leq j < p$ ist die ganze Zahl $\binom{p}{j} = p \frac{(p-1)!}{j!(p-j)!}$ durch p teilbar, da alle Faktoren des Nenners kleiner als p sind. Es folgt $\binom{p}{j} \equiv 0 \pmod{p}$ für $1 \leq j < p$ und damit die Behauptung. \square

Bemerkung: Ist f ein *irreduzibles Polynom*, d. h. ein Polynome ohne echte Teiler, vom Grad n über $\mathbb{Z}/p\mathbb{Z}$ und α eine Nullstelle von f , so ist $\mathbb{F}_{p^n} := \mathbb{Z}/p\mathbb{Z}(\alpha) = \{a_1 + a_2\alpha + \dots + a_n\alpha^{n-1} \mid a_1, \dots, a_n \in \mathbb{Z}/p\mathbb{Z}\}$ ein Erweiterungskörper von $\mathbb{Z}/p\mathbb{Z}$ mit p^n Elementen. Mit einer q -ten Einheitswurzel ξ über $\mathbb{Z}/p\mathbb{Z}$ ist dann eine Nullstelle ξ von $X^q - 1$ aus einem Erweiterungskörper gemeint.

Lemma 14 Sei $q > 2$ eine Primzahl und $\xi \neq 1$ eine q -te Einheitswurzel über $\mathbb{Z}/p\mathbb{Z}$. Dann gilt für $G := \sum_{j=0}^{q-1} \binom{j}{q} \xi^j$:

$$G^2 \equiv (-1)^{(q-1)/2} q \pmod{p}.$$

Beweis:

$$\begin{aligned}
G^2 &\equiv \sum_{j,k=1}^{q-1} \binom{j}{q} \binom{-k}{q} \xi^{j-k} \\
&\equiv \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \binom{jk}{q} \xi^{j-k} \\
&\stackrel{k=jl}{\equiv} (-1)^{(q-1)/2} \sum_{j=1}^{q-1} \sum_{l=1}^{q-1} \binom{j^2 l}{q} \xi^{j(1-l)} \\
&\equiv (-1)^{(q-1)/2} \sum_{l=1}^{q-1} \binom{l}{q} \sum_{j=0}^{q-1} \xi^{j(1-l)} \pmod{p}.
\end{aligned}$$

Wegen

$$\sum_{j=0}^{q-1} \xi^{j(1-l)} = \begin{cases} (\xi^{q(1-l)} - 1) / (\xi^{1-l} - 1) = 0, & l \neq 1, \\ q, & l = 1, \end{cases}$$

gilt

$$G^2 \equiv (-1)^{(q-1)/2} q \pmod{p}.$$

□

Lemma 15

$$G^p \equiv (-1)^{(p-1)(q-1)/4} \binom{q}{p} G \pmod{p}.$$

Beweis: Nach Lemma 14 gilt:

$$\begin{aligned}
G^p &\equiv (G^2)^{\frac{p-1}{2}} G \equiv ((-1)^{(q-1)/2} q)^{(p-1)/2} G \\
&\equiv (-1)^{(p-1)(q-1)/4} q^{(p-1)/2} G \equiv (-1)^{(p-1)(q-1)/4} \binom{q}{p} G \pmod{p}.
\end{aligned}$$

□

Satz 5 (Quadratisches Reziprozitätsgesetz)

Für zwei Primzahlen $p, q > 2$ gilt

$$\binom{p}{q} = (-1)^{(p-1)(q-1)/4} \binom{q}{p}.$$

Beweis: Es gilt

$$\begin{aligned}
 G^p &\equiv \left(\sum_{j=0}^{q-1} \binom{j}{q} \xi^j \right)^p \equiv \sum_{j=0}^{q-1} \binom{j}{q} \xi^{jp} \\
 &\equiv \sum_{j=0}^{q-1} \binom{p}{q} \binom{jp}{q} \xi^{jp} \\
 &\stackrel{l=jp}{\equiv} \binom{p}{q} \sum_{l=0}^{q-1} \binom{l}{q} \xi^l \equiv \binom{p}{q} G \pmod{p}.
 \end{aligned}$$

Mit Lemma 15 bekommt man das Ergebnis. □

Beispiel: Ist 7411 quadratischer Rest modulo 9283?

$$\begin{aligned}
 \left(\frac{7411}{9283} \right) &= - \left(\frac{9283}{7411} \right) = - \left(\frac{1872}{7411} \right) = - \left(\frac{12^2 \cdot 13}{7411} \right) = - \left(\frac{13}{7411} \right) \\
 &= - \left(\frac{7411}{13} \right) = - \left(\frac{1}{13} \right) = -1.
 \end{aligned}$$

Lemma 16 (Ergänzungssatz)

$$\left(\frac{2}{p} \right) = (-1)^{(p^2-1)/8}.$$

Beweis: Sei ξ eine primitive achte Einheitswurzel (d. h. keine erste, zweite oder vierte Einheitswurzel) über $\mathbb{Z}/p\mathbb{Z}$. Dann folgt wegen $\xi^4 \equiv -1 \pmod{p}$ sofort $\xi^2 + \xi^{-2} \equiv 0 \pmod{p}$, damit

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

und schließlich wegen $(\xi + \xi^{-1})^p \equiv \xi^p + \xi^{-p} \pmod{p}$ im Fall $p \equiv \pm 1 \pmod{8}$, dass

$$\left(\frac{2}{p} \right) \equiv 2^{(p-1)/2} \equiv (\xi + \xi^{-1})^{p-1} \equiv \frac{\xi^p + \xi^{-p}}{\xi + \xi^{-1}} \equiv 1 \pmod{p},$$

und analog im Fall $p \equiv \pm 3 \pmod{8}$, dass

$$\left(\frac{2}{p} \right) \equiv -1 \pmod{p}.$$

□

Definition 11 (Jacobi-Symbol) Sei a eine ganze Zahl und n eine positive ungerade Zahl mit Primfaktorzerlegung $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Dann definieren wir

$$\left(\frac{a}{n} \right) = \left(\frac{a}{p_1} \right)^{\alpha_1} \cdots \left(\frac{a}{p_r} \right)^{\alpha_r}.$$

Bemerkungen: 1. Quadratisches Reziprozitätsgesetz und Ergänzungssatz gelten auch für zusammengesetzte Zahlen. Zum Beweis muss man zeigen, dass die rechten Seiten der beiden Gesetze *stark multiplikativ* sind. (Eine Funktion $F(n)$ heißt stark multiplikativ, wenn $F(km) = F(k)F(m)$ für alle natürlichen Zahlen k und m gilt.)

2. Falls $\left(\frac{a}{n}\right) = 1$ und n keine Primzahl ist, so muss a kein Quadrat modulo n sein.

Beispiele:

$$\begin{aligned} 1. \quad \left(\frac{7411}{9283}\right) &= -\left(\frac{1872}{7411}\right) = -\left(\frac{16}{7411}\right) \left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right) = -\left(\frac{40}{117}\right) \\ &= -\left(\frac{2}{117}\right) \left(\frac{5}{117}\right) = \left(\frac{5}{117}\right) = \left(\frac{2}{5}\right) = -1. \end{aligned}$$

2. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = 1$ aber 2 ist kein quadratischer Rest modulo 15.

1.4 Summen von Legendre-Symbolen

Lemma 17 Sei x eine ganze Zahl mit $p \nmid x$. Dann gilt

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \left(\frac{a+x}{p}\right) = -1.$$

Beweis: Wegen $\left(\frac{a}{p}\right) = \left(\frac{a^{-1}}{p}\right)$ für $p \nmid a$ gilt

$$S := \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \left(\frac{a+x}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{(a+x)a^{-1}}{p}\right).$$

Durchläuft a alle Restklassen $1, \dots, p-1 \pmod p$, so durchläuft $(a+x)a^{-1}$ alle Restklassen bis auf $1 \pmod p$. Es ist also

$$S = \sum_{b=2}^{p-1} \left(\frac{b}{p}\right) = -\left(\frac{1}{p}\right) = -1$$

nach Lemma 12. □

Lemma 18 Für $N = 1, \dots, p$ gilt:

$$\sum_{j=0}^{p-1} \left| \sum_{n=0}^{N-1} \left(\frac{j+n}{p}\right) \right|^2 = N(p-N).$$

Beweis: Es gilt

$$S := \sum_{j=0}^{p-1} \left| \sum_{n=0}^{N-1} \left(\frac{j+n}{p} \right) \right|^2 = \sum_{n,m=0}^{N-1} \sum_{j=0}^{p-1} \left(\frac{j+n}{p} \right) \left(\frac{j+m}{p} \right).$$

Nach Lemma 17 ist die innere Summe gleich -1 , falls $n \neq m$ und anderenfalls gleich $p-1$. Also gilt

$$S = N(p-1) - N(N-1) = N(p-N).$$

□

Satz 6 Für $N = 1, \dots, p$ und $a \in \mathbb{Z}$ gilt:

$$S := \left| \sum_{n=0}^{N-1} \left(\frac{a+n}{p} \right) \right| \leq 1 + (3N(p-N))^{\frac{1}{3}}.$$

Beweis: Es gilt

$$\left| \sum_{n=0}^{N-1} \left(\frac{\pm j + a + n}{p} \right) \right| \geq S - 2j, \quad j = 1, \dots, \left\lfloor \frac{S}{2} \right\rfloor.$$

(Mit $\lfloor x \rfloor$ wird die größte ganze Zahl $\leq x$ bezeichnet.) Mit $t := 2\lfloor \frac{S}{2} \rfloor \leq S$ erhält man

$$\begin{aligned} \sum_{j=0}^{p-1} \left| \sum_{n=0}^{N-1} \left(\frac{j+a+n}{p} \right) \right|^2 &\geq S^2 + 2((S-t)^2 + (S-t+2)^2 + \dots + (S-2)^2) \\ &\geq t^2 + 2(0^2 + 2^2 + 4^2 + \dots + (t-2)^2) = \frac{t^3 + 2t}{3} \geq \frac{t^3}{3}. \end{aligned}$$

(Den letzten Schritt kann man induktiv zeigen.) Lemma 18 impliziert

$$\frac{1}{3}t^3 \leq \sum_{j=0}^{p-1} \left| \sum_{n=0}^{N-1} \left(\frac{j+a+n}{p} \right) \right|^2 = N(p-N).$$

Mit $S \leq t+1$ erhalten wir die Behauptung. □

Bemerkungen: Mit weniger elementaren Methoden kann man Satz 6 deutlich verbessern. Allgemein kann man z. B. $S < p^{1/2} \ln p$ zeigen.

Korollar 4 Der kleinste (positive) quadratische Nichtrest modulo p ist kleiner gleich

$$\left\lfloor \sqrt{3p-2} \right\rfloor + 1.$$

Beweis: Sind $1, \dots, N$ quadratische Reste, so gilt nach Satz 6

$$N = \sum_{n=1}^N \left(\frac{n}{p} \right) \leq 1 + (3N(p-N))^{1/3}$$

und daher

$$(N-1)^3 - N + 1 \leq (N-1)^3 \leq 3N(p-N)$$

und daher die Behauptung. \square

Satz 7 (Weil) Sei $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ ein Polynom mit Hauptkoeffizient 1, das kein Quadrat eines Polynoms ist, so gilt:

$$\left| \sum_{a=0}^{p-1} \left(\frac{f(a)}{p} \right) \right| \leq (\text{grad}(f) - 1)p^{1/2}.$$

Beweis: Siehe z. B. Lidl/Niederreiter: Finite Fields, Theorem 5.41. \square

Bemerkung: Ist $f(X)$ von der Form $f(X) = g(X)^2$ mit einem Polynom $g(X)$ ohne Nullstellen in $\mathbb{Z}/p\mathbb{Z}$, so ist offensichtlich die Summe gleich p .

Satz 8 Sei $1 \leq N < p$ und $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ ein Polynom mit Hauptkoeffizient 1, das kein Quadrat in $\mathbb{Z}/p\mathbb{Z}[X]$ ist. Dann gilt

$$\left| \sum_{n=0}^{N-1} \left(\frac{f(n)}{p} \right) \right| < N^{1/2}(3\text{grad}(f) - 1)^{1/2}p^{1/4} + p^{1/2}.$$

Beweis: Zunächst gilt für jede ganze Zahl $k \geq 0$,

$$\left| \sum_{n=0}^{N-1} \left(\frac{f(n)}{p} \right) - \sum_{n=0}^{N-1} \left(\frac{f(n+k)}{p} \right) \right| \leq 2k.$$

Dann haben wir für jede ganze Zahl K mit $1 \leq K \leq p$

$$K \left| \sum_{n=0}^{N-1} \left(\frac{f(n)}{p} \right) \right| \leq W + K(K-1), \quad (1.1)$$

wobei

$$\begin{aligned} W &= \left| \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \left(\frac{f(n+k)}{p} \right) \right| \\ &\leq \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \left(\frac{f(n+k)}{p} \right) \right|. \end{aligned}$$

Mit der Cauchy-Schwarz Ungleichung erhält man

$$\begin{aligned} W^2 &\leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \left(\frac{f(n+k)}{p} \right) \right|^2 \\ &\leq N \sum_{n=0}^{p-1} \left| \sum_{k=0}^{K-1} \left(\frac{f(n+k)}{p} \right) \right|^2 \\ &= N \sum_{k,m=0}^{K-1} \sum_{n=0}^{p-1} \left(\frac{f(n+k)f(n+m)}{p} \right). \end{aligned}$$

Sei $d \leq \text{grad}(f)$ die Anzahl der verschiedenen Nullstellen von $f(X)$ und $f(X) = \prod_{j=1}^d (X - \nu_j)^{c_j}$ die Faktorisierung von $f(X)$ (im sogenannten Zerfällungskörper über $\mathbb{Z}/p\mathbb{Z}$). Da $f(X)$ kein Quadrat ist existiert ein h mit $1 \leq h \leq d$ und $c_h \not\equiv 0 \pmod{2}$. Falls

$$k = m + \nu_h - \nu_j \quad \text{für ein } j \text{ mit } 1 \leq j \leq d, \quad (1.2)$$

dann schätzen wir die Summe trivial mit p ab. (Es existieren höchstens d mögliche Indizes m , die (1.2) für gegebenes k und h erfüllen.) Ist $k \neq m + \nu_h - \nu_j$ für alle j mit $1 \leq j \leq d$, dann ist das Polynom $F(X) = f(X+k)f(X+m)$ kein Quadrat und hat $\text{grad}(F) \leq 2\text{grad}(f)$. Daher darf Satz 7 auf die innere Summe angewendet werden und wir erhalten

$$W^2 < NKdp + NK^2(2\text{grad}(f) - 1)p^{1/2}.$$

Wählt man

$$K = \lceil p^{1/2} \rceil,$$

($\lceil x \rceil$ ist die kleinste ganze Zahl $\geq x$) so erhält man

$$\frac{W^2}{K^2} < N(3\text{grad}(f) - 1)p^{1/2}$$

und die Behauptung aus (1.1). \square

1.5 Laufzeiten von arithmetischen Operationen und Algorithmen

Definition 12 Die Darstellung einer natürlichen Zahl n als

$$n = d_{k-1}2^{k-1} + d_{k-2}2^{k-2} + \dots + d_12 + d_0$$

mit $d_0, d_1, \dots, d_{k-2}, d_{k-1} \in \{0, 1\}$ heißt eine Binärdarstellung (Bitdarstellung) von n , $d_0, d_1, \dots, d_{k-2}, d_{k-1}$ heißen Bits von n und n eine k -Bit Zahl.

Schreibweise: $n = (d_{k-1}d_{k-2} \dots d_1d_0)_2$.

Die Addition bzw. Subtraktion zweier Bits unter Berücksichtigung von Überträgen heißt eine Bitoperation.

Beispiel:

1. $(11001001)_2 = 128 + 64 + 8 + 1 = 201$

2. Addition:

$$\begin{array}{r} 1\ 1\ 1\ 1\ 0\ 0\ 0 \\ +\ 0\ 0\ 1\ 1\ 1\ 1\ 0 \\ \hline (1\ 1\ 1\ 1) \\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0 \end{array}$$

3. Subtraktion:

$$\begin{array}{r} 1\ 1\ 1\ 1\ 0\ 0\ 0 \\ -\ 0\ 0\ 1\ 1\ 1\ 1\ 0 \\ \hline (1\ 1\ 1\ 1) \\ 1\ 0\ 1\ 1\ 0\ 1\ 0 \end{array}$$

4. Multiplikation:

$$\begin{array}{r} 11101 \cdot 1101 : \\ 1\ 1\ 1\ 0\ 1 \\ +\ 1\ 1\ 1\ 0\ 1 \\ +\ 1\ 1\ 1\ 0\ 1 \\ \hline 1\ 1\ 1\ 0\ 1 \\ (1\ 1\ 1\ 1) \\ +\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1 \\ \hline (1) \\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1 \end{array}$$

5. Division:

$$\begin{array}{r} 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1 : 1\ 0\ 0\ 1\ 1\ 1 = 1\ 0\ 1 + \frac{110}{100111} \\ -\ 1\ 0\ 0\ 1\ 1\ 1 \\ \hline 1\ 0\ 1\ 1\ 0\ 1 \\ -\ 1\ 0\ 0\ 1\ 1\ 1 \\ \hline 1\ 1\ 0 \end{array}$$

Abkürzung: $\log n := \log_2 n$

Lemma 19 *Seien n und m zwei k -Bit Zahlen.*

1. *Die Zahl n kann als k -Bit Zahl mit $k = \lfloor \log n \rfloor + 1$ dargestellt werden.*
2. *Addition und Subtraktion von n und m benötigen höchstens k Bitoperationen.*
3. *Multiplikation und Division von n und m benötigen höchstens k^2 Bitoperationen.*

Beweis: 1. und 2. sind trivial. 3. Die Multiplikation besteht aus höchstens $k - 1$ Additionen von k -Bit Zahlen und somit aus höchstens $k(k - 1) < k^2$ Bitoperationen. Die Division besteht aus höchstens k Subtraktionen von k -Bit Zahlen. \square

Definition 13 (O-Notation) Seien f und g Abbildungen von \mathbb{N} in die positiven reellen Zahlen. Wir definieren

$$f(n) = O(g(n)),$$

falls eine positive Konstante c und eine natürliche Zahl n_0 existieren, so dass

$$f(n) \leq cg(n) \quad \text{für } n \geq n_0.$$

Beispiel:

$$\begin{aligned} 2n^2 + 3n - 3 &= O(n^2) \\ n^2 &= O(n^3) \quad \text{aber} \quad n^3 \neq O(n^2) \\ \ln n &= O(n^\varepsilon), \quad \varepsilon > 0, \end{aligned}$$

da nach l'Hospital $\lim_{n \rightarrow \infty} \frac{\ln n}{n^\varepsilon} = 0$,

$$\log_b n = O(\log n), \quad b > 1.$$

Definition 14 Ein Algorithmus mit natürlichen Zahlen $\leq n$, der $O(\log^d n)$ Bitoperationen benötigt, heißt *polynomial*.

Bemerkung: Seien $m \leq n$ zwei ganze Zahlen. Nach Lemma 19 benötigt die Addition von m und n $O(\log n)$ und die Multiplikation von n und m $O(\log^2 n)$ Bitoperationen. Es existiert ein Algorithmus, der für die Multiplikation nur

$$O(\log n \log \log n \log \log \log n)$$

Bitoperationen benötigt (Schönhage/Strassen, 1971).

Satz 9 Der größte gemeinsame Teiler zweier natürlicher Zahlen $c \leq b$ kann mit dem Euklidischen Algorithmus in $O(\log^3 b)$ Bitoperationen berechnet werden.

Beweis: Jede Division mit Rest benötigt $O(\log^2 b)$ Bitoperationen. Mit den Bezeichnungen aus Satz 1 müssen wir zeigen, dass j mit $r_j = \text{ggT}(b, c)$ die Gleichung $j = O(\log b)$ erfüllt. Dazu zeigen wir, dass $r_{l+2} < r_l/2$ für $l = 1, 2, \dots, j-2$ gilt. Ist $r_{l+1} \leq r_l/2$, so gilt sofort $r_{l+2} < r_{l+1} \leq r_l/2$. Ist $r_{l+1} > r_l/2$, so ist $r_l = 1 \cdot r_{l+1} + r_{l+2}$ und daher $r_{l+2} = r_l - r_{l+1} < r_l/2$. \square

Korollar 5 Eine Lösung der Kongruenz $ax \equiv 1 \pmod m$, $\text{ggT}(a, m) = 1$, kann in $O(\log^3 m)$ Bitoperationen berechnet werden.

Lemma 20 (Repeated-Squaring)

Die modulare Exponentiation $b^n \bmod m$ kann in $O(\log n \log^2 m)$ Bitoperationen durchgeführt werden.

Beweis: Wir berechnen zunächst

$$b, b^2, b^4, \dots, b^{2^t} \bmod m \quad \text{mit } t = \lfloor \log n \rfloor.$$

Jedes Quadrieren bzw. jedes Reduzieren modulo m benötigt $O(\log^2 m)$ Bitoperationen. Sei $n = (n_t n_{t-1} \dots n_0)_2$ die Bitdarstellung von n , so gilt

$$b^n \equiv b^{n_0} b^{2n_1} \dots b^{2^t n_t} \bmod m,$$

d.h. wir benötigen höchstens t weitere Multiplikationen, so dass der gesamte Algorithmus $O(\log n \log^2 m)$ Bitoperationen braucht. \square

Korollar 6 Man kann mit $O(\log^3 p)$ Bitoperationen entscheiden, ob $a \in \mathbb{Z}/p\mathbb{Z}^*$ ein quadratischer Rest modulo p ist.

Beweis: Lemma 11 und Lemma 20. \square

Bemerkung: Man kann zeigen, dass das Jacobi-Symbol $\left(\frac{a}{n}\right)$ in $O(\log a \log n)$ Bitoperationen ausgewertet werden kann, so dass sogar $O(\log^2 p)$ statt $O(\log^3 p)$ im Korollar gilt.

Lemma 21 Sei n eine natürliche Zahl. Der Wert $\lfloor \sqrt{n} \rfloor$ kann in $O(\log^3 n)$ Bitoperationen berechnet werden.

Beweis: Sei n eine k -Bitzahl, so ist $2^{\lfloor k/2 \rfloor} = (100 \dots 0)_2$ eine erste Näherung für $\lfloor \sqrt{n} \rfloor$. Die weiteren Bits bestimmt man durch sukzessives Probieren (eine Multiplikation pro Bit). \square

Lemma 22 Seien p und q Primzahlen und $n = pq$. Dann läßt sich $\varphi(n)$ aus n , p und q in $O(\log n)$ Bitoperationen berechnen. Umgekehrt lassen sich p und q aus n und $\varphi(n)$ in $O(\log^3 n)$ Bitoperationen berechnen.

Beweis: Ist n gerade, so gilt $p = 2$ und $q = \frac{n}{2}$ also $\varphi(n) = \frac{n}{2} - 1$.

Sei n ungerade. $\varphi(n) = (p-1)(q-1) = n+1 - (p+q)$ kann mit zwei Addition und einer Subtraktion aus p und q berechnet werden.

Wenn umgekehrt n und $\varphi(n)$ bekannt sind, so folgt aus $n = pq$ und $\varphi(n) = n+1 - (p+q)$ die quadratische Gleichung

$$n = ((n+1) - \varphi(n) - q)q$$

in q , die nach dem vorigen Lemma in $O(\log^3 n)$ Bitoperationen berechnet werden kann. \square

1.6 Quadratwurzeln modulo p

Lemma 23 *Ist $p \equiv 3 \pmod{4}$, so können Quadratwurzeln in $\mathbb{Z}/p\mathbb{Z}$ in $O(\log^3 p)$ Bitoperationen berechnet werden.*

Beweis: $x = a^{(p+1)/4}$ ist eine Lösung von $x^2 \equiv a \pmod{p}$ und kann nach Lemma 20 in $O(\log^3 p)$ Bitoperationen berechnet werden. \square

Lemma 24

1. *Ein quadratischer Nichtrest modulo p kann deterministisch mit $O(p^{1/2} \log^3 p)$ Bitoperationen bestimmt werden.*
2. *Probabilistisch kann ein quadratischer Nichtrest modulo p mit einer erwarteten Anzahl von $O(\log^3 p)$ Bitoperationen bestimmt werden.*

Beweis: Nach Lemma 6 kann man mit $O(\log^3 p)$ Bitoperationen entscheiden, ob ein Element quadratischer Nichtrest ist. Deterministisch testet man der Reihe nach die Elemente $2, 3, \dots$. Nach Korollar 4 braucht man höchstens $O(p^{1/2})$ Elemente zu testen. Probabilistisch ist die Wahrscheinlichkeit, dass ein zufällig gewähltes Element aus $\mathbb{Z}/p\mathbb{Z}^*$ ein quadratischer Nichtrest ist gleich $1/2$. Nach mehreren Versuchen bekommt man mit sehr hoher Wahrscheinlichkeit einen quadratischen Nichtrest. \square

Bemerkungen:

1. Nach Satz 16 ist 2 ein quadratischer Nichtrest, falls $p \equiv \pm 3 \pmod{8}$.
2. Im allgemeinen kann man zeigen, dass der kleinste quadratische Nichtrest von der Größenordnung $O(p^{1/4e^{1/2}+\varepsilon})$ ist.

Satz 10 (Algorithmus von Tonelli)

Sei a ein quadratischer Rest modulo p . Kennt man einen quadratischen Nichtrest g modulo p , so bestimmt der folgende Algorithmus eine Lösung der Kongruenz $x^2 \equiv a \pmod{p}$ in $O(\log^4 p)$ Bitoperationen.

1. *Stelle $p - 1$ als $p - 1 = 2^s t$ mit ungeradem t dar.*
2. *Setze $e_1 = 0$ und berechne g^{-1} .*
3. *Für $i = 2, \dots, s$ setze*

$$e_i = \begin{cases} 2^{i-1} + e_{i-1}, & \text{falls } (ag^{-e_{i-1}})^{(p-1)/2^i} \not\equiv 1 \pmod{p}, \\ e_{i-1}, & \text{sonst.} \end{cases}$$

4. *Setze $h \equiv ag^{-e_s} \pmod{p}$.*
5. *Setze $x \equiv g^{e_s/2} h^{(t+1)/2} \pmod{p}$.*

Beweis: Zunächst zeigen wir, dass $x = g^{e_s/2}h^{(t+1)/2}$ eine Lösung der Kongruenz ist. Dazu zeigt man zunächst induktiv, dass

$$(ag^{-e_i})^{(p-1)/2^i} \equiv 1 \pmod{p}, \quad i = 1, 2, \dots, s.$$

Damit erhält man

$$x^2 \equiv g^{e_s}h^{t+1} \equiv a(ag^{-e_s})^{(p-1)/2^s} \equiv a \pmod{p}.$$

Analyse des Algorithmus:

1. Schritt: $s = O(\log p)$ Divisionen a $O(\log^2 p)$ Bitoperationen.
2. Schritt: eine Inversion also $(O(\log^3 p))$ Bitoperationen.
3. Schritt: $s = O(\log p)$ Potenzen a $O(\log^3 p)$ Bitoperationen.
4. Schritt: $O(\log^3 p)$ Bitoperationen.
5. Schritt: $O(\log^3 p)$ Bitoperationen.

□

Beispiel: Berechne eine Quadratwurzel von 10 mod 13. Dann ist $p-1 = 12 = 2^2 \cdot 3$ also $t = 3$ und $s = 2$. Weiterhin ist 2 ein quadratischer Nichtrest modulo 13 und $2^{-1} \equiv 7 \pmod{13}$. Wir haben $(10 \cdot 7^0)^3 \equiv -1 \pmod{13}$ also $e_2 = 2$, $h \equiv 10 \cdot 7^2 \equiv 9 \pmod{13}$ und $x \equiv 2 \cdot 9^2 \equiv 6 \pmod{13}$.

Kapitel 2

Einfache Kryptosysteme

2.1 Grundbegriffe

Kryptographie: Wissenschaft geheimer Nachrichtenübermittlungen.

Klartext: Nachricht, die übermittelt werden soll.

Chiffretext: verschlüsselte Nachricht.

Chiffrierung: Verschlüsselung.

Dechiffrierung: Entschlüsselung.

Schlüssel: Informationsträger für die Verschlüsselung des Klartextes bzw. die Entschlüsselung des Chiffretextes.

Alphabet: Menge von "Zeichen" aus denen die Nachricht besteht.

Nachrichtenblock: ein einzelnes Zeichen, ein Zeichenpaar, Zeichentripel oder allgemein ein n -Tupel von Zeichen.

Chiffrierungs-Transformation: Abbildung f von der Menge aller Klartext-Nachrichtenblöcke \mathcal{P} in die Menge aller Chiffretextblöcke \mathcal{C} .

Dechiffrierungs-Transformation: Abbildung f^{-1} , die aus dem Chiffretext den Klartext wieder herstellt.

Kryptosystem: $\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$.

2.2 Lineare Substitutionschiffre

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}/m\mathbb{Z}$$

$$f(x) \equiv ax + b \pmod{m}, \quad a, b \in \mathbb{Z}, \quad \text{ggT}(a, m) = 1$$

$$f^{-1}(y) \equiv a^{-1}(y - b) \pmod{m}$$

Chiffrierungsschlüssel: (a, b)

Dechiffrierungsschlüssel: $(a^{-1}, -a^{-1}b)$

Beispiel: $m = 26$, $f(x) = 7x + 12$, $f^{-1}(x) = 15x + 2$:

	<i>B</i>	<i>E</i>	<i>C</i>	<i>K</i>	<i>E</i>	<i>N</i>	<i>B</i>	<i>A</i>	<i>U</i>	<i>E</i>	<i>R</i>
<i>x</i>	1	4	2	10	4	13	1	0	20	4	17
$f(x)$	19	14	0	4	14	25	19	12	22	14	1
<i>y</i>	4	1	12	25	4	11					
$f^{-1}(y)$	10	17	0	13	10	11					

Nachteil: Bei längeren Texten kann man mit Häufigkeitsanalysen (E ist der häufigste (17,4%) und N der zweithäufigste (9,8%) Buchstabe der deutschen Sprache) einen Teil des Textes erraten. Hier reichen zwei Paare (x_1, y_1) und (x_2, y_2) mit $f(x_1) \equiv y_1 \pmod{m}$ und $f(x_2) \equiv y_2 \pmod{m}$ und $\text{ggT}(x_2 - x_1, m) = 1$, um den Schlüssel (a, b) zu berechnen:

$$y_1 \equiv ax_1 + b \pmod{m}$$

$$y_2 \equiv ax_2 + b \pmod{m}$$

$$y_2 - y_1 \equiv a(x_2 - x_1) \pmod{m}$$

$$a \equiv (x_2 - x_1)^{-1}(y_2 - y_1) \pmod{m}$$

$$b \equiv y_1 - (x_2 - x_1)^{-1}(y_2 - y_1)x_1 \pmod{m}$$

Abhilfe:

1. Verschlüsselung von längeren Blöcken, d. h. z. B. $\mathcal{P} = \mathcal{C} = \mathbb{Z}/m^2\mathbb{Z}$. (Die Häufigkeiten verschiedener Paare in der deutschen Sprache liegen schon viel dichter beieinander (EN 3,88%, ER 3,75%, CH 2,75%). Allerdings reicht immer noch die Kenntnis von lediglich zwei Paaren (x_1, y_1) , (x_2, y_2) , mit $f(x_1) = y_1$, $f(x_2) = y_2$, zur Berechnung des Schlüssels aus.
2. Verschlüsselungsmatrizen, d. h. $\mathcal{P} = \mathcal{C} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

2.3 Verschlüsselungsmatrizen

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \pmod{m},$$

$$D := ad - bc \quad \text{mit} \quad \text{ggT}(D, m) = 1$$

$$f^{-1} \left(\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) \equiv D^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} y_1 - e_1 \\ y_2 - e_2 \end{pmatrix} \pmod{m}$$

Beispiel: $m = 26$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$, $D = -5$, $\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

	NO	AN	SW	ER
$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$	$\begin{pmatrix} 13 \\ 14 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 13 \end{pmatrix}$	$\begin{pmatrix} 18 \\ 22 \end{pmatrix}$	$\begin{pmatrix} 4 \\ 17 \end{pmatrix}$

$$f \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \begin{pmatrix} 16 \\ 21 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} \begin{pmatrix} 24 \\ 16 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix}$$

Bemerkung: Um die Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

zu bestimmen braucht man mindestens drei Vektorpaare $(\vec{x}_1, \vec{y}_1), (\vec{x}_2, \vec{y}_2), (\vec{x}_3, \vec{y}_3)$ mit

$$f(\vec{x}_i) \equiv \vec{y}_i \pmod{m}, \quad i = 1, 2, 3.$$

$$\begin{aligned} \vec{y}_1 &\equiv A\vec{x}_1 + \vec{b} \pmod{m} & \vec{y}_1 - \vec{y}_3 &\equiv A(\vec{x}_1 - \vec{x}_3) \pmod{m} \\ \vec{y}_2 &\equiv A\vec{x}_2 + \vec{b} \pmod{m} & \Rightarrow \vec{y}_2 - \vec{y}_3 &\equiv A(\vec{x}_2 - \vec{x}_3) \pmod{m} \\ \vec{y}_3 &\equiv A\vec{x}_3 + \vec{b} \pmod{m} \\ & \Rightarrow (\vec{y}_1 - \vec{y}_3 \quad \vec{y}_2 - \vec{y}_3) & \equiv A \underbrace{(\vec{x}_1 - \vec{x}_3 \quad \vec{x}_2 - \vec{x}_3)}_{=:C} \end{aligned}$$

Ist C invertierbar, so kann man A aus der letzten Kongruenz berechnen.

Kapitel 3

Public-Key Kryptosysteme

3.1 Grundlagen

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}.$$

Ist wie in Kapitel 2 die Umkehrabbildung f^{-1} effizient berechenbar, so heißt das obige Kryptosystem *symmetrisch* (oder *Private-Key Kryptosystem*). Ist f^{-1} nicht effizient berechenbar, so handelt es sich um ein *Public-Key Kryptosystem* (oder *asymmetrisches Kryptosystem*).

Bemerkung: Bei symmetrischen Systemen kann jeder, der verschlüsseln kann, auch entschlüsseln.

Authentikation:

A soll B beweisen, dass er wirklich A ist.

f_A öffentlicher Schlüssel von A , f_A^{-1} privater Schlüssel von A .

f_B öffentlicher Schlüssel von B , f_B^{-1} privater Schlüssel von B .

A und B einigen sich auf eine *Unterschrift* P von A .

A berechnet $C := f_B f_A^{-1}(P)$.

B berechnet $f_A f_B^{-1}(C) = P$ und weiß, dass nur A die Nachricht P gesendet haben kann, da nur A den Schlüssel f_A^{-1} hat.

Schlüsselaustausch: Die Schlüssel f_A und f_B können öffentlich gemacht werden, ohne dass ein potentieller Angreifer damit entschlüsseln kann. Insbesondere müssen sich A und B nicht a priori auf einen Schlüssel einigen.

3.2 Das RSA-Verfahren

RSA (Rivest, Shamir, Adleman)-Schlüsselerzeugung:

A macht folgendes:

1. Erzeuge zwei große Primzahlen p und q von etwa derselben Größe.
2. Berechne $n = pq$ und $\varphi(n) = (p - 1)(q - 1)$.
3. Wähle $1 < e < \varphi(n)$ mit $\text{ggT}(e, \varphi(n)) = 1$.
4. Berechne mit dem Euklidischen Algorithmus $1 < d < \varphi(n)$, so dass

$$ed \equiv 1 \pmod{\varphi(n)}.$$

5. Der öffentliche Schlüssel von A ist (n, e) , der private ist d .

RSA-Verschlüsselung:

B macht folgendes:

1. Hole den öffentlichen Schlüssel (n, e) von A .
2. Stelle die Nachricht m als Element aus $\{0, 1, \dots, n - 1\}$ dar.
3. Berechne $c \equiv m^e \pmod{n}$ mit Repeated-Squaring.
4. Übermittle c an A .

A macht folgendes:

- Berechne mit dem privaten Schlüssel d die Nachricht $c^d \equiv m \pmod{n}$ (nach Euler-Fermat).

RSA-Annahme: Sei $n = pq$, $1 < e < \varphi(n)$ mit $\text{ggT}(e, \varphi(n)) = 1$ und $c \in \mathbb{Z}$, dann kann $m \in \mathbb{Z}$ mit $m^e \equiv c \pmod{n}$ (ohne Kenntnis von p oder q) nicht effizient berechnet werden.

Bemerkung: Die Sicherheit des RSA-Verfahrens beruht auf der Annahme, dass eine Zahl $n = pq$ nicht effizient in seine Faktoren p und q zerlegt werden kann (*Faktorisierungsproblem*).

3.3 Diskreter Logarithmus und Diffie-Hellman Schlüsselaustausch

Definition 15 Sei $b \in \mathbb{Z}/p\mathbb{Z}^*$ und $a \equiv b^x \pmod{p}$ mit $0 \leq x \leq p - 1$. Dann heißt x der diskrete Logarithmus (oder Index) von a zur Basis b .

Bezeichnung: $\text{ind}_b(a) = x$.

Beispiel: $p = 19 : \text{ind}_2(7) = 6$

Diffie-Hellman Schlüsselaustausch:

1. A und B einigen sich auf eine (große) Primzahl p und ein Element $a \in \mathbb{Z}/p\mathbb{Z}^*$ (mit großer Ordnung), d. h. (a, p) ist öffentlich.
2. A wählt einen persönlichen Schlüssel x und veröffentlicht $a^x \bmod p$.
 B wählt einen persönlichen Schlüssel y und veröffentlicht $a^y \bmod p$.
3. A berechnet den Schlüssel $K \equiv (a^y)^x \bmod p$.
 B berechnet den Schlüssel $K \equiv (a^x)^y \bmod p$.

Nachrichten werden dann mit einem einfachen Kryptosystem (s. Kapitel 2) und dem Schlüssel $K \in \mathbb{Z}$ verschlüsselt.

Diffie-Hellman Annahme:

Aus a^x und a^y ist (ohne Kenntnis von x oder y) a^{xy} nicht effizient berechenbar.

Bemerkung: Die Sicherheit des Diffie-Hellman Schlüsselaustausches beruht auf der Annahme, dass der diskrete Logarithmus nicht effizient berechnet werden kann (*DL-Problem*).

Beispiel: Lineare Verschiebungschiffre

$$y \equiv x + K \bmod 26$$

mit Schlüssel K .

Bestimmung von K mit Diffie-Hellman:

$p = 53, a = 2,$

$A: x = 29, 2^{29} \equiv 45 \bmod 53, K \equiv 12^{29} \equiv 21 \bmod 53$

$B: y = 19, 2^{19} \equiv 12 \bmod 53, K \equiv 45^{19} \equiv 21 \bmod 53$

Kapitel 4

Sicherheitsanalyse

4.1 Interpolation der Diffie-Hellman Abbildung

Definition 16 Sei $g \in \mathbb{Z}/p\mathbb{Z}^*$ ein Element der Ordnung $p - 1$. (g heißt auch primitive Wurzel modulo p .) Die Abbildung

$$D : \mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/p\mathbb{Z}^* \rightarrow \mathbb{Z}/p\mathbb{Z}^*$$

mit

$$D(g^x, g^y) \equiv g^{xy} \pmod{p} \quad \text{für } 0 \leq x, y \leq p - 2$$

heißt Diffie-Hellman Abbildung.

Bemerkungen:

1. Die Sicherheit des Diffie-Hellman Schlüsselaustausches beruht auf der Annahme, dass man keine einfach auszuwertende Form von D hat.
2. Wegen

$$g^{2xy} \equiv g^{(x+y)^2} g^{-x^2} g^{-y^2} \pmod{p}$$

und da nach Abschnitt 1.6 Quadratwurzeln modulo p effizient berechenbar sind (wir kennen den quadratischen Nichtrest g), können wir die Abbildung

$$d : \mathbb{Z}/p\mathbb{Z}^* \rightarrow \mathbb{Z}/p\mathbb{Z}^*$$

mit

$$d(g^x) \equiv g^{x^2} \pmod{p} \quad \text{für } 0 \leq x \leq p - 2$$

anstelle der Diffie-Hellman Abbildung betrachten.

Satz 11 Sei $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ mit

$$f(g^x) \equiv g^{x^2} \pmod{p}, \quad x \in S$$

für eine Teilmenge $S \subseteq \{1, \dots, p - 1\}$ der Kardinalität $|S| = p - 1 - s$, so gilt

$$\text{grad}(f) \geq p - 3 - 2s.$$

Beweis: Sei R die Menge der $x \in \{0, \dots, p-2\}$ mit $f(g^x) \equiv g^{x^2} \pmod{p}$ und $f(g^{x+1}) \equiv g^{(x+1)^2} \pmod{p}$. Dann gilt

$$|R| \geq p - 1 - 2s.$$

Mit $u := g^x$ und $x \in R$ gilt

$$f(gu) \equiv f(g^{x+1}) \equiv g^{(x+1)^2} \equiv g^{2x+1} g^{x^2} \equiv gu^2 f(u) \pmod{p}.$$

Das Polynom

$$h(X) = gX^2 f(X) - f(gX)$$

hat also mindestens $|R|$ Nullstellen und ist wegen $\text{grad}(h) = \text{grad}(f) + 2$ nicht das Nullpolynom. Daher gilt

$$\text{grad}(f) + 2 = \text{grad}(h) \geq |R| \geq p - 1 - 2s.$$

□

4.2 Interpolation des diskreten Logarithmus

Satz 12 Sei $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ mit

$$\text{ind}_g(n) \equiv f(n) \pmod{p}, \quad n \in S$$

für eine Teilmenge $S \subseteq \mathbb{Z}/p\mathbb{Z}^*$ der Kardinalität $|S| = p - 1 - s$. Dann gilt

$$\text{grad}(f) \geq p - 2 - 2s.$$

Beweis: Sei R die Menge der $n \in \mathbb{Z}/p\mathbb{Z}^*$ mit

$$\text{ind}_g(n) \equiv f(n) \pmod{p} \quad \text{und} \quad \text{ind}_g(gn) \equiv f(gn) \pmod{p}.$$

Dann gilt $|R| \geq p - 1 - 2s$. Wir haben $\text{ind}_g(gn) \equiv 1 + \text{ind}_g(n) \pmod{p}$ falls $n \neq g^{p-2}$. Daher gilt

$$f(gn) \equiv \text{ind}_g(gn) \equiv 1 + \text{ind}_g(n) \equiv 1 + f(n) \pmod{p}$$

für $n \in R$ mit $n \neq g^{p-2}$. Deshalb hat das Polynom $h(X) = f(gX) - f(X) - 1$ mindestens $|R| - 1$ Nullstellen in $\mathbb{Z}/p\mathbb{Z}^*$ und ist wegen $h(0) \equiv -1 \pmod{p}$ nicht das Nullpolynom. Daher erhalten wir

$$\text{grad}(f) \geq \text{grad}(h) \geq |R| - 1 \geq p - 2 - 2s.$$

□

4.3 Darstellung des diskreten Logarithmus als lineare Rekursionsfolge

Definition 17 Eine ganzzahlige Folge s_0, s_1, \dots heißt eine (binäre) lineare Rekursionsfolge der Ordnung d , wenn sie eine Rekursionsvorschrift

$$s_{d+n} \equiv a_{d-1}s_{d+n-1} + a_{d-2}s_{d+n-2} + \dots + a_0s_n \pmod{2}, \quad n \geq 0$$

mit $a_0, \dots, a_{d-1} \in \{0, 1\}$ erfüllt.

Satz 13 Sei $1 \leq N < p$ und s_0, s_1, \dots eine ganzzahlige lineare Rekursionsfolge der Ordnung d , die

$$\text{ind}_g(n) \equiv s_n \pmod{2}, \quad 1 \leq n \leq N$$

erfüllt. Dann gilt

$$d > \frac{N}{7p^{1/2} + 1}.$$

Beweis: Da die Aussage anderenfalls trivial ist, dürfen wir annehmen, dass $N \geq 7p^{1/2} + d$ ist.

Mit $a_d = 1$ haben wir

$$\sum_{i=0}^d a_i \text{ind}_g(n+i) \equiv 0 \pmod{2}, \quad 1 \leq n \leq N-d.$$

Äquivalent dazu ist, dass $n^{a_0}(n+1)^{a_1} \dots (n+d)^{a_d}$ quadratischer Rest modulo p ist. Daher haben wir

$$\left| \sum_{n=1}^{N-d} \left(\frac{n}{p}\right)^{a_0} \dots \left(\frac{n+d}{p}\right)^{a_d} \right| = N-d.$$

Andererseits gilt nach Satz 8

$$\begin{aligned} N-d &< (N-d)^{1/2}(3(d+1)-1)^{1/2}p^{1/4} + p^{1/2} \\ &\leq (N-d)^{1/2}d^{1/2}p^{1/4} \left(\sqrt{5} + \frac{p^{1/4}}{(N-d)^{1/2}} \right) \\ &< \sqrt{7}(N-d)^{1/2}d^{1/2}p^{1/4}, \end{aligned}$$

woraus die Behauptung folgt. □

Kapitel 5

Algorithmen zur Berechnung des diskreten Logarithmus

geg.: g primitive Wurzel modulo p , $a \in \mathbb{Z}/p\mathbb{Z}^*$
ges.: $x = \text{ind}_g(a)$

5.1 Direkte Suche

Berechne $g^0, g^1, g^2, \dots \pmod p$ bis $a \equiv g^x \pmod p$ erreicht ist.

Lemma 25 Die direkte Suche berechnet den diskreten Logarithmus in $\mathbb{Z}/p\mathbb{Z}$ in $O(p \log^2 p)$ Bitoperationen.

5.2 Baby-Step Giant-Step Algorithmus

1. Setze $m = \lceil \sqrt{p-1} \rceil$.
2. Erstelle eine Tabelle (Baby-Step)

j	0	1	2	...	$m-1$
$g^j \pmod p$	$g^0 \pmod p$	$g^1 \pmod p$	$g^2 \pmod p$...	$g^{m-1} \pmod p$
3. Berechne $g^{-m} \pmod p$ und setze $a_0 = a$.
4. Für $i = 0, \dots, m-1$
 - (a) Teste, ob a_i in der zweiten Zeile der obigen Tabelle steht und lese das zugehörige j ab.
 - (b) Falls ja, setze $x = im + j$. Stopp.
 - (c) Setze $a_{i+1} \equiv a_i g^{-m} \pmod p$ (Giant-Step).

Satz 14 Der Baby-Step Giant-Step Algorithmus berechnet den diskreten Logarithmus in $\mathbb{Z}/p\mathbb{Z}$ in $O(p^{1/2} \log^2 p)$ Bitoperationen.

Beweis: Zunächst zeigen wir, dass $a \equiv g^x \pmod p$. Die Darstellung von $x = im + j$ mit $0 \leq j \leq m - 1$ ist eindeutig und es gilt

$$g^j \equiv a_i \equiv a_{i-1}g^{-m} \equiv a_{i-2}g^{-2m} \equiv \dots \equiv a_0g^{-im} \equiv ag^{-im} \pmod p.$$

Analyse des Algorithmus:

1. $O(\log^3 p)$ Bitoperationen nach Lemma 21.
2. m Multiplikationen a $O(\log^2 p)$ also insgesamt $O(p^{1/2} \log^2 p)$ Bitoperationen.
3. Invertieren und Potenzieren in jeweils $O(\log^3 p)$ Bitoperationen.
4. Höchstens $m = O(p^{1/2})$ Multiplikationen in c) also $O(p^{1/2} \log^2 p)$ Bitoperationen.

□

Beispiel: $p = 113, g = 3, a = 57$

1. $m = 11$.

$$2. \begin{array}{c|cccccccccc} j & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline 3^j \pmod{113} & 1 & 3 & 9 & 27 & 81 & 17 & 51 & 40 & 7 & 21 & 63 \end{array}$$

3. $g^{-1} \equiv 3^{-1} \equiv 38 \pmod{113}, g^{-m} \equiv 38^{11} \equiv 58 \pmod{113}$.

$$4. \begin{array}{c|cccccccccc} i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline a_i \equiv 57 \cdot 58^i \pmod{113} & 57 & 29 & 100 & 37 & 112 & 55 & 26 & 39 & 2 & 3 \end{array}$$

$$\text{ind}_3(57) = 9 \cdot 11 + 1 = 100$$

5.3 Index-Calculus

1. Wähle eine Teilmenge $S = \{p_1, \dots, p_t\} \subseteq \{1, \dots, p-1\}$, so dass ein wesentlicher Anteil der Zahlen $\{1, 2, \dots, p-1\}$ als Produkt von Elementen aus S ausgedrückt werden kann.
(Wähle z.B. für S die ersten Primzahlen, so dass mindestens ein Drittel der Zahlen $1, \dots, p-1$ als Produkt von Elementen aus S geschrieben werden kann.)
2. (a) Wähle (zufällig) k mit $0 \leq k \leq p-2$ und berechne $g^k \pmod p$.

- (b) Versuche $g^k \bmod p$ (aufgefasst als ganze Zahl zwischen 1 und $p - 1$) als Produkt von Elementen aus S zu schreiben:

$$g^k \equiv \prod_{i=1}^t p_i^{c_i} \bmod p, \quad c_i \geq 0.$$

Falls dies gelingt, logarithmiere beide Seiten:

$$k \equiv \sum_{i=1}^t c_i \operatorname{ind}_g(p_i) \bmod (p - 1). \quad (5.1)$$

- (c) Wiederhole (a) und (b) bis $t + c$ verschiedene Gleichungen der Form (5.1) erzeugt wurden (c ist eine kleine natürliche Zahl, so dass das entstandene Gleichungssystem mit hoher Wahrscheinlichkeit eine eindeutige Lösung besitzt).
3. Löse das in 2. erzeugte lineare Gleichungssystem, um $\operatorname{ind}_g(p_i)$, $1 \leq i \leq t$, zu bestimmen.
4. (a) Wähle (zufällig) k mit $0 \leq k \leq p - 2$ und berechne $a \cdot g^k \bmod p$.
 (b) Versuche $a \cdot g^k \bmod p$ als Produkt von Elementen aus S zu schreiben:

$$ag^k \equiv \prod_{i=1}^t p_i^{d_i} \bmod p, \quad d_i \geq 0.$$

Falls der Versuch nicht gelingt, wähle in (a) ein anderes k . Anderenfalls ergibt Logarithmieren:

$$x \equiv \operatorname{ind}_g a \equiv \sum_{i=1}^t d_i \operatorname{ind}_g p_i - k \bmod (p - 1).$$

Beispiel: $p = 229, g = 6, a = 13$

1. $S = \{2, 3, 5, 7, 11\}$

2.

$$\begin{array}{rcl}
 6^{100} & \equiv & 180 \equiv 2^2 \cdot 3^2 \cdot 5 \pmod{229} \\
 6^{18} & \equiv & 176 \equiv 2^4 \cdot 11 \pmod{229} \\
 6^{12} & \equiv & 165 \equiv 3 \cdot 5 \cdot 11 \pmod{229} \\
 6^{62} & \equiv & 154 \equiv 2 \cdot 7 \cdot 11 \pmod{229} \\
 6^{143} & \equiv & 198 \equiv 2 \cdot 3^2 \cdot 11 \pmod{229} \\
 6^{206} & \equiv & 210 \equiv 2 \cdot 3 \cdot 5 \cdot 7 \pmod{229}
 \end{array}$$

$$\begin{array}{rcl}
 100 & \equiv & 2\text{ind}_6(2) + 2\text{ind}_6(3) + \text{ind}_6(5) & \pmod{228} \\
 18 & \equiv & 4\text{ind}_6(2) + \text{ind}_6(11) & \pmod{228} \\
 12 & \equiv & \text{ind}_6(3) + \text{ind}_6(5) + \text{ind}_6(11) & \pmod{228} \\
 62 & \equiv & \text{ind}_6(2) + \text{ind}_6(7) + \text{ind}_6(11) & \pmod{228} \\
 143 & \equiv & \text{ind}_6(2) + 2\text{ind}_6(3) + \text{ind}_6(11) & \pmod{228} \\
 206 & \equiv & \text{ind}_6(2) + \text{ind}_6(3) + \text{ind}_6(5) + \text{ind}_6(7) & \pmod{228}
 \end{array}$$

3. $\text{ind}_6(2) = 21, \text{ind}_6(3) = 208, \text{ind}_6(5) = 98, \text{ind}_6(7) = 107, \text{ind}_6(11) = 162.$

4. $k = 77: \quad ag^k \equiv 13 \cdot 6^{77} \equiv 147 \equiv 3 \cdot 7^2 \pmod{229}$
 $\text{ind}_6(13) \equiv \text{ind}_6(3) + 2\text{ind}_6(7) - 77 \equiv 117 \pmod{228}.$

Bemerkung:

1. Der Hauptschritt 2. (b) wird ungefähr t mal ausgeführt und benötigt $O(\log p)$ Divisionen.
2. Bei günstiger Wahl der Menge S ist der Index-Calculus Algorithmus schneller als der Baby-Step Giant-Step Algorithmus.
3. Ein Algorithmus heißt *subexponential*, falls er $O(p^\varepsilon)$ Bitoperationen für alle $\varepsilon > 0$ benötigt. (Z.B. $2^{(\log p)^{1/2}} = O(p^\varepsilon), \varepsilon > 0.$) Der Index-Calculus Algorithmus gehört zur Klasse der subexponentialen Algorithmen.

Kapitel 6

Faktorisierungsalgorithmen

geg.: $n = pq$

ges.: p und q , $p < q$

6.1 Sieb des Eratosthenes

Für $t = 2, 3, 5, 7, \dots$ teste, ob n durch t teilbar ist.

Lemma 26 *Das Sieb des Eratosthenes berechnet einen Faktor von n in*

$$O(n^{1/2} \log^2 n)$$

Bitoperationen.

Bemerkung: Das Sieb des Eratosthenes ist effizient, falls p klein ist.

6.2 Fermat-Faktorisierung

Vorbemerkungen:

1. Wegen $p = \frac{p+q}{2} + \frac{p-q}{2}$ und $q = \frac{p+q}{2} - \frac{p-q}{2}$ gilt $n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.
2. Nach Lemma 21 kann $\lfloor \sqrt{n} \rfloor$ effizient berechnet werden.

Algorithmus:

1. Berechne $a = \lfloor \sqrt{n} \rfloor$.
2. Für $t = 1, 2, \dots$ berechne $b = \lfloor \sqrt{(a+t)^2 - n} \rfloor$ und teste ob $n = (a+t)^2 - b^2$.
Falls ja, so gilt $p = a + t - b$ und $q = a + t + b$.

Bemerkung: Der Algorithmus ist effizient, falls p und q dicht bei einander liegen.

Beispiel: Faktorisiere $n = 200819$.

1. $a = \lfloor \sqrt{200819} \rfloor = 448$.
2. $t = 1 : b = \lfloor \sqrt{449^2 - 200819} \rfloor = \lfloor \sqrt{782} \rfloor = 27 \neq \sqrt{782}$
 $t = 2 : b = \lfloor \sqrt{450^2 - 200819} \rfloor = \lfloor \sqrt{1681} \rfloor = 41 = \sqrt{1681}$
 $p = 448 + 2 - 41 = 409$
 $q = 448 + 2 + 41 = 491$
 $n = 409 \cdot 491$

6.3 Pollards ρ -Methode

Sei S eine endliche Menge der Kardinalität n , $f : S \rightarrow S$ eine Funktion, $x_0 \in S$ und x_0, x_1, \dots die durch $x_{i+1} = f(x_i)$, $i \geq 0$, definierte Folge. Da S endlich ist, muss die Folge schließlich periodisch sein. Insbesondere existieren $0 \leq i < j$ mit $x_i = x_j$.

Lemma 27 Sei $l = 1 + \lfloor \sqrt{2\lambda n} \rfloor$. Dann ist der Anteil der Paare (f, x_0) , für die x_0, \dots, x_l verschieden sind, wobei f alle Abbildungen von S in S und x_0 alle Elemente von S durchläuft, kleiner als $e^{-\lambda}$.

Beweis: Die gesamte Anzahl der Paare (f, x_0) ist n^{n+1} und die Anzahl der Paare (f, x_0) , für die x_0, \dots, x_l verschieden sind, ist $n^{n-l} \prod_{j=0}^l (n-j)$, der Anteil also

$$h(n, l) := \frac{\prod_{j=0}^l (n-j)}{n^{l+1}} = \prod_{j=0}^l \left(1 - \frac{j}{n}\right).$$

Nun gilt wegen $\ln(1-x) < -x$ für $x < 1$:

$$\ln h(n, l) = \sum_{j=0}^l \ln \left(1 - \frac{j}{n}\right) < -\frac{1}{n} \sum_{j=0}^l j = -\frac{l(l+1)}{2n} < -\frac{l^2}{2n} < -\lambda$$

und somit $h(n, e) < e^{-\lambda}$. □

Lemma 28 (Floyd) Der Erwartungswert für das kleinste $m \geq 0$ mit $x_m = x_{2m}$ ist $m = O(\sqrt{n})$.

Beweis: Ist l_1 die Vorperiode und l_2 die Periode von x_0, x_1, \dots , dann gilt für $m = l_2(1 + \lfloor l_1/l_2 \rfloor) > l_1$ die Gleichung $x_m = x_{2m}$. Nach dem vorherigen Lemma hat $m \leq l_1 + l_2 =: l$ den Erwartungswert $O(\sqrt{n})$. \square

Algorithmus (Pollards ρ -Methode):

1. Setze $a_0 = 2, b_0 = 2$.
2. Für $i = 1, 2, \dots$
 - 2.1 Setze $a_i \equiv a_{i-1}^2 + 1 \pmod n, b_i \equiv (b_{i-1}^2 + 1)^2 + 1 \pmod n$.
 - 2.2 Berechne $d = \text{ggT}(a_i - b_i, n)$.
 - 2.3 Falls $1 < d < n$, so ist d ein nichttrivialer Faktor von n .
 - 2.4 Falls $d = n$, dann beende den Algorithmus mit einer Fehlermeldung.

Bemerkungen:

1. Unter der Annahme, dass das Polynom $f(x) = x^2 + 1$ sich wie eine zufällige Funktion verhält, bestimmt Pollards ρ -Algorithmus in einer erwarteten Anzahl von $O(n^{1/4} \log^3 n)$ Bitoperationen einen nichttrivialen Teiler von n .
2. Im seltenen Fall $d = n$ kann man z.B. statt $f(x) = x^2 + 1$ das Polynom $f(x) = x^2 + 2$ wählen und den modifizierten Algorithmus starten.

Beispiel: $n = pq = 1927$

i	a_i	b_i	d
0	2	2	—
1	5	26	1
2	26	1631	1
3	677	411	1
4	1631	1850	1
5	902	1005	1
6	411	205	1
7	1273	535	41

6.4 Quadratwurzelfaktorisierung

Lemma 29 Seien x, y und n ganze Zahlen. Falls $x^2 \equiv y^2 \pmod n$ aber $x \not\equiv \pm y \pmod n$, dann sind $\text{ggT}(x - y, n)$ und $\text{ggT}(x + y, n)$ nichttriviale Teiler von n .

Beweis: Nach Voraussetzung gilt $n \mid x^2 - y^2 = (x - y)(x + y)$ aber $n \nmid (x - y)$ und $n \nmid (x + y)$. Also muss n einen nichttrivialen gemeinsamen Teiler mit $x - y$ bzw. $x + y$ haben. \square

Beispiel: $n = 35, 2^2 \equiv 12^2 \pmod{35}$
 $\text{ggT}(12 - 2, 35) = 5, \text{ggT}(12 + 2, 35) = 7$

Lemma 30 Ist $n = pq$ mit Primzahlen p und q und a eine ganze Zahl mit $\text{ggT}(a, n) = 1$, so besitzt die Kongruenz $x^2 \equiv a^2 \pmod{n}$ genau vier Lösungen (zwei davon sind $x \equiv \pm a \pmod{n}$).

Beweis: Die Kongruenzen $x^2 \equiv a^2 \pmod{p}$ und $x^2 \equiv a^2 \pmod{q}$ haben nach Lemma 9 jeweils genau zwei Lösungen $x \equiv \pm a \pmod{p}$ bzw. $x \equiv \pm a \pmod{q}$. Nach dem chinesischen Restsatz gibt es also genau vier Lösungen von $x^2 \equiv a^2 \pmod{pq}$. \square

Beispiel: $n = 35 = 5 \cdot 7$, $x^2 \equiv 4 \pmod{35}$ hat vier Lösungen.:

$$x^2 \equiv 4 \pmod{5} \Rightarrow x \equiv \pm 2 \pmod{5} \Rightarrow x \equiv \pm 2, \pm 3, \pm 7, \pm 8, \pm 12, \pm 13, \pm 17 \pmod{35}$$

$$x^2 \equiv 4 \pmod{7} \Rightarrow x \equiv \pm 2 \pmod{7} \Rightarrow x \equiv \pm 2, \pm 5, \pm 9, \pm 12, \pm 16 \pmod{35}$$

$$\Rightarrow x \equiv \pm 2, \pm 12 \pmod{35}$$

Algorithmus: geg.: $n = pq$

ges.: x, y mit $x^2 \equiv y^2 \pmod{n}$ aber $x \not\equiv \pm y \pmod{n}$

1. Wähle $S = \{p_1, p_2, \dots, p_t\}$, wobei p_j die j -te Primzahl ist.
2. (a) Für $i = 1, 2, \dots, t+1$ wähle (zufällig) $a_i \in \{0, \dots, n-1\}$ und berechne $b_i \equiv a_i^2 \pmod{n}$.
(b) Schreibe (falls möglich)

$$b_i = \prod_{j=1}^t p_j^{e_{ij}}, \quad e_{ij} \geq 0.$$

Anderenfalls wähle ein neues a_i .

3. Finde eine Teilmenge $T \subseteq \{1, \dots, t+1\}$, so dass $\prod_{i \in T} b_i$ ein Quadrat ist, indem man aus den $t+1$ binären Vektoren $\underline{v}_i \equiv (e_{i1}, \dots, e_{it}) \pmod{2}$, $1 \leq i \leq t+1$, eine nichttriviale Darstellung des Nullvektors bestimmt.
4. Wähle $x = \prod_{i \in T} a_i$ und $y = \sqrt{\prod_{i \in T} b_i}$.
5. Falls $x \not\equiv \pm y \pmod{n}$: Stopp.
Falls $x \equiv \pm y \pmod{n}$ suche in 3. eine andere Teilmenge T .

Beispiel: $n = 17111$

1. $S = \{2, 3\}$

2.

i	a_i	b_i	$\underline{v}_i := (e_{i1} \ e_{i2} \ e_{i3})$
1	6047	2	1 0 0
2	16444	3	0 1 0
3	4847	6	1 1 0
4	3396	2	1 0 0

3. $\underline{v}_1 + \underline{v}_2 + \underline{v}_3 \equiv \underline{0} \pmod{2}$
 $a_1 \cdot a_2 \cdot a_3 \equiv 6 \equiv \sqrt{b_1 b_2 b_3} \pmod{17111}$
 $\underline{v}_2 + \underline{v}_3 + \underline{v}_4 \equiv \underline{0} \pmod{2}$
 $a_2 \cdot a_3 \cdot a_4 \equiv 7236 \not\equiv \pm 6 \pmod{17111}$
4. $x \equiv 7236 \pmod{17111}, \quad y \equiv 6 \pmod{17111}$

$$\text{ggT}(x - y, n) = \text{ggT}(7230, 17111) = 241$$

$$17111 = 71 \cdot 241$$

6.5 Das quadratische Sieb

Vorbemerkungen: 1. Die Wahrscheinlichkeit, dass eine ganze Zahl b als Produkt kleiner Primzahlen darstellbar ist, ist groß, falls b (betragsmäßig) klein ist.

2. Ist $|x|$ klein, so ist $|(x + \lfloor \sqrt{n} \rfloor)^2 - n|$ ebenfalls klein.

3. Gilt $a^2 \equiv b^2 \pmod{n}$ mit $0 \leq a < b < n$ und $a < \sqrt{n}$, so ist $b \geq \sqrt{n}$.

Algorithmus:

1. Setze $S = \{p_1, \dots, p_t\}$, wobei $p_1 = -1$ und $p_j, 2 \leq j \leq t$, die $(j - 1)$ -te Primzahl mit $\left(\frac{n}{p_j}\right) = 1$ ist.
2. Berechne $m = \lfloor \sqrt{n} \rfloor$.
3. Wähle x in der Reihenfolge $0, 1, -1, 2, -2, \dots$
Für $i = 1, 2, \dots, t + 1$:
 - (a) Berechne $b_i = (x + m)^2 - n$.
 - (b) Falls möglich schreibe $b_i = \prod_{j=1}^t p_j^{e_{ij}}, e_{ij} \geq 0$, anderenfalls wähle das nächste x . Setze $a_i = x + m$ und $\underline{v}_i := (e_{i1} \dots e_{it}) \pmod{2}$.
4. Finde $\emptyset \neq T \subseteq \{1, 2, \dots, t + 1\}$ mit $\sum_{i \in T} \underline{v}_i \equiv \underline{0} \pmod{2}$.
5. Berechne $x \equiv \prod_{i \in T} a_i \pmod{n}$.
6. Berechne $e_j = \sum_{i \in T} e_{ij} / 2, 1 \leq j \leq t$.
7. Berechne $y \equiv \prod_{j=1}^t p_j^{e_j} \pmod{n}$.
8. Falls $x \equiv \pm y \pmod{n}$ finde eine neue Teilmenge T mit $\sum_{i \in T} \underline{v}_i \equiv \underline{0} \pmod{2}$ und gehe zu 5.

9. Berechne $d = \text{ggT}(x - y, n)$.

Beispiel: $n = 24961$

1. $S = \{-1, 2, 3, 5, 13, 23\}$
 (7, 11, 17 und 19 erfüllen nicht $\left(\frac{n}{p}\right) = 1$.)

2. $m = \lfloor \sqrt{24961} \rfloor = 157$

3.

i	x	$b_i = (x + m)^2 - n$	$a_i = x + m$	\underline{v}_i
1	0	$-312 = -2^3 \cdot 3 \cdot 13$	157	(111010)
2	1	3	158	(001000)
3	-1	$-625 = -5^4$	156	(100000)
4	2	$320 = 2^6 \cdot 5$	159	(000100)
5	-2	$-936 = -2^3 \cdot 3^2 \cdot 13$	155	(110010)
6	4	$960 = 2^6 \cdot 3 \cdot 5$	161	(001100)
7	-6	$-2160 = -2^4 \cdot 3^3 \cdot 5$	151	(101100)

($x = \pm 3, \pm 5$ liefert b_i mit einem Primfaktor, der nicht in S liegt.)

4. $\underline{v}_1 + \underline{v}_2 + \underline{v}_5 \equiv \underline{0} \pmod{2} \Rightarrow T = \{1, 2, 5\}$

5. $x \equiv a_1 a_2 a_5 \equiv 936 \pmod{n}$

6. $e_1 = 1, e_2 = 3, e_3 = 2, e_4 = 0, e_5 = 1, e_6 = 0$.

7. $y \equiv -2^3 \cdot 3^2 \cdot 13 \equiv 24025 \pmod{n}$

8. $x \equiv 936 \equiv -24025 \equiv -y \pmod{n}$

9. $\underline{v}_3 + \underline{v}_6 + \underline{v}_7 \equiv \underline{0} \pmod{2} \Rightarrow T = \{3, 6, 7\}$

10. $x \equiv a_3 a_6 a_7 \equiv 23405 \pmod{n}$

11. $e_1 = 1, e_2 = 5, e_3 = 2, e_4 = 3, e_5 = 0, e_6 = 0$

12. $y \equiv -2^5 \cdot 3^2 \cdot 5^3 \equiv 13922 \pmod{n}$.

13. $x \equiv 23405 \not\equiv \pm 13922 \pmod{n}$
 $\text{ggT}(x - y, n) = \text{ggT}(9483, 24961) = 109$
 $n = 109 \cdot 229$

Bemerkungen:

1. Bei geeigneter Wahl von t ist das quadratische Sieb subexponential.

2. Ist n kein quadratischer Rest modulo p , so kann p nicht b_i teilen. (Anderenfalls hätten wir $n \equiv (x + m)^2 \pmod{p}$.) Daher kann man in 1. die Primzahlen mit $\left(\frac{n}{p}\right) = -1$ weglassen.

Kapitel 7

Primzahlerzeugung

7.1 Pseudoprimzahltests

7.1.1 Fermat Test

Vorbemerkung: Falls $a^{n-1} \not\equiv 1 \pmod n$ für ein $2 \leq a \leq n-2$, so ist nach dem kleinen Fermat n zusammengesetzt.

Definition 18 Sei n eine natürliche Zahl und gelte $a^{n-1} \equiv 1 \pmod n$ für ein a mit $\text{ggT}(a, n) = 1$, so heißt n eine Pseudoprimzahl zur Basis a .

Lemma 31 Sei n eine zusammengesetzte Zahl, so gilt $a^{n-1} \equiv 1 \pmod n$ für alle a mit $\text{ggT}(a, n) = 1$ oder für höchstens $\varphi(n)/2$ verschiedene a mit $1 \leq a \leq n-1$ und $\text{ggT}(a, n) = 1$.

Beweis: Ist n Pseudoprimzahl zu den Basen a_1 und a_2 mit $\text{ggT}(a_1, n) = \text{ggT}(a_2, n) = 1$, so ist n Pseudoprimzahl zur Basis $a_1 a_2^{-1}$.

Seien $1 \leq a_1, \dots, a_s \leq n-1$ alle Elemente mit $a_1^{n-1} \equiv \dots \equiv a_s^{n-1} \equiv 1 \pmod n$, $\text{ggT}(a_i, n) = 1$, $1 \leq i \leq s$, und b ein Element mit $b^{n-1} \not\equiv 1 \pmod n$, $\text{ggT}(b, n) = 1$. Dann sind alle Elemente $a_1 b, \dots, a_s b$ keine Pseudoprimzahlbasen für n , woraus $s \leq \varphi(n)/2$ folgt. \square

Definition 19 Eine zusammengesetzte Zahl n mit $a^{n-1} \equiv 1 \pmod n$ für alle a mit $\text{ggT}(a, n) = 1$ heißt Carmichael-Zahl.

Algorithmus:

Eingabe: n (Testzahl), t (Sicherheitsparameter)

1. Für $i = 1, \dots, t$:
 - (a) Wähle a mit $2 \leq a \leq n-2$.
 - (b) Berechne $r := a^{n-1} \pmod n$.

(c) Falls $r \not\equiv 1 \pmod n$: n ist zusammengesetzt, stopp.

2. n ist wahrscheinlich prim.

Lemma 32 Sei n eine zusammengesetzte ungerade Zahl. Ist n quadratfrei, so ist n eine Carmichael-Zahl genau dann, wenn $p-1|n-1$ für jeden Primteiler p von n .

Beweis: Sei $n = p_1 \cdots p_r$ und $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$. Aus $p_i - 1 | n - 1$ für $1 \leq i \leq r$ folgt $a^{n-1} \equiv (a^{p_i-1})^{(n-1)/(p_i-1)} \equiv 1 \pmod{p_i}$, $1 \leq i \leq r$. Nach dem Chinesischen Restsatz gilt also $a^{n-1} \equiv 1 \pmod n$ und n ist eine Carmichael-Zahl. Gilt $p_i - 1 \nmid n - 1$ für ein $1 \leq i \leq r$ und ist g eine primitive Wurzel modulo p_i , so existiert ein a mit $a \equiv g \pmod{p_i}$ und $a \equiv 1 \pmod{n/p_i}$. Dann gilt aber $\text{ggT}(a, n) = 1$ und $1 \equiv a^{n-1} \equiv g^{n-1} \pmod{p_i}$ würde im Widerspruch zu $p_i - 1 \nmid n - 1$ stehen. \square

Beispiel: $n = 561 = 3 \cdot 11 \cdot 17$ ist eine Carmichael-Zahl, da 560 durch $3 - 1$, $11 - 1$ und $17 - 1$ teilbar ist.

Bemerkungen: 1. Eine nicht quadratfreie Zahl kann keine Carmichael-Zahl sein.
2. Es gibt unendlich viele Carmichael-Zahlen.
3. Falls n eine zusammengesetzte Zahl ist, die keine Carmichael-Zahl ist, so erkennt der Fermat Test n als zusammengesetzt mit Wahrscheinlichkeit mindestens $1 - (1/2)^t$.

7.1.2 Solovay-Strassen Test

Vorbemerkung: Falls $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod n$ für ein a mit $2 \leq a \leq n - 2$, so ist n zusammengesetzt nach Lemma 11.

Definition 20 Ist n eine zusammengesetzte Zahl und $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod n$ für ein a mit $\text{ggT}(a, n) = 1$, so heißt n eine Euler-Pseudoprimzahl zur Basis a .

Lemma 33 Ist n eine Euler-Pseudoprimzahl zur Basis a , so ist n eine Pseudoprimzahl zur Basis a .

Beweis: Trivial. \square

Beispiel: 91 ist Pseudoprimzahl zur Basis 3, aber wegen $3^{45} \equiv 27 \pmod{91}$ ist 91 keine Euler-Primzahl zur Basis 3.

Algorithmus:

1. Für $i = 1, \dots, t$:
 - (a) Wähle a mit $2 \leq a \leq n - 2$.

- (b) Berechne $r := a^{(n-1)/2} \bmod n$.
- (c) Falls $r \not\equiv \pm 1 \pmod n$: n ist zusammengesetzt, stopp.
- (d) Berechne $s := \left(\frac{a}{n}\right)$.
- (e) Falls $r \not\equiv s \pmod n$: n ist zusammengesetzt, stopp.

2. n ist wahrscheinlich prim.

7.1.3 Miller-Rabin Test

Lemma 34 Sei p eine Primzahl, $p - 1 = 2^s r$ mit $2 \nmid r$ und $2 \leq a \leq p - 2$, dann gilt entweder $a^r \equiv 1 \pmod p$ oder $a^{2^j r} \equiv -1 \pmod p$ für ein $0 \leq j \leq s - 1$.

Beweis: Nach dem kleinen Fermat gilt $a^{p-1} \equiv a^{2^s r} \equiv 1 \pmod p$. Ist $a^{2^j r} \equiv 1 \pmod p$ für ein j mit $1 \leq j \leq s$, so gilt $a^{2^{j-1} r} \equiv \pm 1 \pmod p$. Deshalb ist entweder $a^{2^j r} \equiv -1 \pmod p$ für ein $0 \leq j \leq s - 1$ oder $a^{2^j r} \equiv 1 \pmod p$ für $0 \leq j \leq s$. \square

Definition 21 Sei n eine ungerade zusammengesetzte Zahl, $n - 1 = 2^s r$ mit ungeradem r und a eine ganze Zahl mit $\text{ggT}(a, n) = 1$. Falls entweder $a^r \equiv 1 \pmod n$ oder es existiert ein $0 \leq j \leq s - 1$ mit $a^{2^j r} \equiv -1 \pmod n$, so heißt n eine strenge Pseudoprimzahl zur Basis a .

Lemma 35 Falls $n \equiv 3 \pmod 4$, so ist n genau dann eine strenge Pseudoprimzahl zur Basis a , wenn n eine Euler-Pseudoprimzahl zur Basis a ist.

Beweis: Da $(n - 1)/2$ nach Voraussetzung ungerade ist, ist n eine strenge Pseudoprimzahl zur Basis a genau dann, wenn $a^{(n-1)/2} \equiv \pm 1 \pmod n$ ist.

Ist n eine Euler-Pseudoprimzahl zur Basis a , so gilt $a^{(n-1)/2} \equiv \pm 1 \pmod n$.

Gilt $a^{(n-1)/2} \equiv \pm 1 \pmod n$, so ist

$$\left(\frac{a}{n}\right) = \left(\frac{a(a^2)^{(n-3)/4}}{n}\right) = \left(\frac{a^{(n-1)/2}}{n}\right) = \left(\frac{\pm 1}{n}\right) = \pm 1.$$

\square

Lemma 36 Ist n eine strenge Pseudoprimzahl zur Basis a , so ist n eine Euler-Pseudoprimzahl zur Basis a .

Beweis: Fall 1: $a^r \equiv 1 \pmod n$

Es gilt

$$a^{(n-1)/2} \equiv a^{2^{s-1} r} \equiv 1 \pmod n$$

und

$$\left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^r = \left(\frac{a^r}{n}\right) = \left(\frac{1}{n}\right) = 1.$$

Fall 2: $a^{(n-1)/2} \equiv -1 \pmod n$

Ist p Primteiler von n und $p-1 = 2^{s'} r'$ mit ungeradem r' . Dann gilt $s' \geq s$ und

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{falls } s' = s, \\ 1, & \text{falls } s' > s, \end{cases}$$

denn aus $a^{(n-1)/2} \equiv a^{2^{s-1}r} \equiv -1 \pmod n$ folgt

$$a^{2^{s-1}r'r} \equiv -1 \pmod p.$$

Wegen $1 \equiv a^{p-1} \equiv a^{2^{s'}r'} \equiv a^{2^{s'}r'r} \pmod p$ muss $s' \geq s$ gelten. Falls $s' = s$, so gilt

$$\left(\frac{a}{p}\right) \equiv \left(\frac{a}{p}\right)^r \equiv a^{(p-1)r/2} \equiv a^{2^{s'-1}r'r} \equiv -1 \pmod p.$$

Falls $s' > s$ so, gilt

$$\left(\frac{a}{p}\right) \equiv a^{2^{s'-1}r'r} \equiv (a^{2^{s-1}r'r})^{2^{s'-s}} \equiv 1 \pmod p.$$

Sei k die Anzahl der Primteiler p von n mit $s' = s$ (in ihrer Vielfachheit gezählt).

Wegen

$$p \equiv \begin{cases} 1 + 2^s \pmod{2^{s+1}}, & \text{falls } s' = s, \\ 1 \pmod{2^{s+1}}, & \text{falls } s' > s, \end{cases}$$

gilt

$$n = \prod p \equiv (1 + 2^s)^k \equiv 1 + k2^s \pmod{2^{s+1}}.$$

Andererseits gilt

$$n = 2^s r + 1 \equiv 2^s + 1 \pmod{2^{s+1}}$$

und daher ist k ungerade. Schließlich haben wir

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p}\right) = (-1)^k = -1.$$

Fall 3: $a^{2^j r} \equiv -1 \pmod n$ mit $0 \leq j \leq s-2$

Wegen $a^{(n-1)/2} \equiv 1 \pmod n$ müssen wir $\left(\frac{a}{n}\right) = 1$ zeigen. Analog dem vorherigen

Fall zeigt man für einen Primteiler p von n mit $p-1 = 2^{s'} r'$:

$$s' \geq j+1 \text{ und } \left(\frac{a}{p}\right) = \begin{cases} -1, & \text{falls } s' = j+1, \\ 1, & \text{falls } s' > j+1. \end{cases}$$

Die Behauptung folgt analog dem vorherigen Fall. □

Beispiel: 65 ist Pseudoprime zu den Basen $a = 1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64,$

Euler-Pseudoprime zu den Basen $a = 1, 8, 14, 18, 47, 51, 57, 64$
 und strenge Pseudoprime zu $a = 1, 8, 18, 47, 57, 64$.

Algorithmus:

1. Schreibe $n - 1 = 2^s r$ mit ungeradem r .
2. Für $i = 1, \dots, t$:
 - (a) Wähle (zufällig) a mit $2 \leq a \leq n - 2$.
 - (b) Berechne $y := a^r \pmod n$.
 - (c) Falls $y \neq \pm 1$:
 - i. Setze $j = 1$.
 - ii. Solange $j \leq s - 1$ und $y \not\equiv -1 \pmod n$:
 - A. Ersetze y durch $y^2 \pmod n$.
 - B. Falls $y \equiv 1$: n ist zusammengesetzt, stopp.
 - C. Ersetze j durch $j + 1$.
 - iii. Falls $y \not\equiv -1 \pmod n$: n ist zusammengesetzt, stopp.
3. n ist wahrscheinlich prim.

7.2 Primzahltests

7.2.1 Lucas-Lehmer Test

Definition 22 Für $s \geq 2$ heißt eine Zahl der Form $2^s - 1$ Mersenne-Zahl. Falls $2^s - 1$ eine Primzahl ist, so heißt $2^s - 1$ Mersenne-Primzahl.

Beispiel: $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ sind Primzahlen.
 $2^4 - 1 = 15$, $2^6 - 1 = 63$, $2^{11} - 1 = 2047 = 23 \cdot 89$ sind keine Primzahlen.

Lemma 37 Für $s \geq 3$ ist $n = 2^s - 1$ genau dann eine Primzahl, wenn s Primzahl ist und die Folge

$$u_0 = 4, \quad u_{k+1} \equiv u_k^2 - 2 \pmod n, \quad k \geq 0,$$

die Bedingung $u_{s-2} \equiv 0 \pmod n$ erfüllt.

Beweis: Wegen $2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 1)$ ist $2^s - 1$ nur dann Primzahl, wenn s Primzahl ist.

Sei q ein Primteiler von n und

$$f(X) = X^2 - 2^{(s+1)/2}X - 1 = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta \in \mathbb{Z}/q\mathbb{Z}[X]$$

mit Nullstellen α, β in einem Erweiterungskörper von $\mathbb{Z}/q\mathbb{Z}$. Dann gilt

$$\alpha + \beta = 2^{(s+1)/2} \quad \text{und} \quad \alpha\beta = -1.$$

Mit vollständiger Induktion zeigt man:

$$u_k \equiv \alpha^{2^{k+1}} + \beta^{2^{k+1}} \pmod{q}.$$

$k = 0$:

$$\alpha^2 + \beta^2 \equiv (\alpha + \beta)^2 - 2\alpha\beta \equiv 2^{s+1} + 2 \equiv 4 \equiv u_0 \pmod{q}.$$

$k \rightarrow k + 1$:

$$\begin{aligned} u_{k+1} &\equiv u_k^2 - 2 \equiv (\alpha^{2^{k+1}} + \beta^{2^{k+1}})^2 - 2 \equiv \alpha^{2^{k+2}} + \beta^{2^{k+2}} + 2(\alpha\beta)^{2^{k+1}} - 2 \\ &\equiv \alpha^{2^{k+2}} + \beta^{2^{k+2}} + 2(-1)^{2^{k+1}} - 2 \equiv \alpha^{2^{k+2}} + \beta^{2^{k+2}} \pmod{q}. \end{aligned}$$

Ist n eine Primzahl, so gilt wegen $n \equiv -1 \pmod{8}$:

$$\left(\frac{6}{n}\right) = \left(\frac{2}{n}\right) \left(\frac{3}{n}\right) = -1.$$

Die Nullstellen $\alpha, \beta = 2^{(s-1)/2} \pm \frac{1}{2}\sqrt{2^{s+1} + 4}$ liegen also wegen $2^{s+1} + 4 \equiv 6 \pmod{n}$ nicht in $\mathbb{Z}/n\mathbb{Z}$. Daher gilt $\alpha = \beta^n$ bzw. $\beta = \alpha^n$ wegen $f(\beta^n) \equiv f(\beta)^n \equiv 0 \pmod{n}$ bzw. $f(\alpha^n) \equiv f(\alpha)^n \equiv 0 \pmod{n}$, woraus

$$\alpha^{n+1} \equiv \beta^{n+1} \equiv \alpha\beta \equiv -1 \pmod{n}$$

und somit

$$-2 \equiv \alpha^{n+1} + \beta^{n+1} \equiv \alpha^{2^s} + \beta^{2^s} \equiv u_{s-1} \equiv u_{s-2}^2 - 2 \pmod{n}$$

und daher $u_{s-2} \equiv 0 \pmod{n}$ folgt.

Ist $u_{s-2} \equiv 0 \pmod{n}$ mit zusammengesetztem n und q ein Teiler von n mit $q^2 \leq n$, so gilt

$$\alpha^{2^{s-1}} + \beta^{2^{s-1}} \equiv 0 \pmod{q}$$

und somit

$$\alpha^{2^s} + (\alpha\beta)^{2^{s-1}} \equiv 0 \pmod{q}$$

also $\alpha^{2^s} \equiv -1 \pmod{q}$ und $\alpha^{2^{s+1}} \equiv 1 \pmod{q}$. Andererseits gilt $\alpha \equiv \beta^q \equiv \alpha^{q^2} \pmod{q}$ also $\alpha^{q^2-1} \equiv 1 \pmod{q}$, woraus $2^{s+1}|q^2 - 1$ folgt im Widerspruch zu $q^2 - 1 < n < 2^{s+2}$. \square

7.2.2 Der $n - 1$ Test

Lemma 38 (Pocklington) Sei $n - 1 = q^k r$ mit einer Primzahl q und $q \nmid r$. Falls eine ganze Zahl a mit

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{und} \quad \text{ggT}(a^{(n-1)/q} - 1, n) = 1$$

existiert, so gilt für jeden Primteiler p von n :

$$p \equiv 1 \pmod{q^k}.$$

Beweis: Es gilt $a^{n-1} \equiv 1 \pmod{p}$, weshalb die Ordnung t von a modulo p ein Teiler von $n - 1 = q^k r$ ist. Wegen $\text{ggT}(a^{(n-1)/q} - 1, n) = 1$ gilt $a^{(n-1)/q} \not\equiv 1 \pmod{p}$ und somit $t \nmid (n - 1)/q = q^{k-1} r$, woraus $q^k | t | p - 1$ folgt. \square

Korollar 7 Sei $n - 1 = fr$ mit $f > \sqrt{n} - 1$ und $\text{ggT}(f, r) = 1$. Falls ein a mit $a^{n-1} \equiv 1 \pmod{n}$ und $\text{ggT}(a^{(n-1)/q} - 1, n) = 1$ für jeden Primfaktor q von f , so ist n eine Primzahl.

Beweis: Sei n zusammengesetzt und p der kleinste Primfaktor von n , also $p \leq \sqrt{n}$. Nach dem vorherigen Lemma gilt $p \equiv 1 \pmod{q^k}$, falls $q^k | f$ aber $q^{k+1} \nmid f$ für alle Primteiler q von f . Nach dem Chinesischen Restsatz gilt also $p \equiv 1 \pmod{f}$ und daher $p \geq f + 1 > \sqrt{n}$, was einen Widerspruch ergibt. \square

7.2.3 Bestimmung primitiver Wurzeln

Algorithmus:

Eingabe: Primzahl p und Faktorisierung von $p - 1 = p_1^{e_1} \cdots p_r^{e_r}$

Ausgabe: eine primitive Wurzel g modulo p

1. Wähle (zufällig) ein Element $g \in \mathbb{Z}/p\mathbb{Z}^*$
2. Für $i = 1, \dots, r$: Falls $g^{(p-1)/p_i} \equiv 1 \pmod{p}$, dann gehe zu 1.
3. g ist eine primitive Wurzel modulo p .

Bemerkungen: 1. Die Wahrscheinlichkeit, dass ein zufällig gewähltes Element eine primitive Wurzel ist, ist $\varphi(p - 1)/(p - 1)$.

2. Die Korrektheit des Algorithmus folgt aus der Tatsache, dass die Ordnung eines Elementes ein Teiler von $p - 1$ sein muss.

Kapitel 8

Zur Komplexität der Diffie-Hellman Abbildung und des diskreten Logarithmus

8.1 Vandermonde-Determinante

Lemma 39 Seien $a_1, \dots, a_n \in \mathbb{Z}/p\mathbb{Z}$, $n \geq 2$, und

$$A_n = \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix}.$$

Dann gilt

$$\text{Det}A_n = \prod_{1 \leq j < i \leq n} (a_i - a_j).$$

Beweis: $n = 2$:

$$\text{Det}A_2 = \begin{vmatrix} 1 & a_1 \\ 1 & a_2 \end{vmatrix} = a_2 - a_1.$$

$n - 1 \rightarrow n$: Wir ziehen von jeder Spalte beginnend mit der letzten bis zur zweiten die jeweils mit a_1 multipliziert vorausgehende Spalte ab und erhalten

$$\text{Det}A_n = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & a_2 - a_1 & a_2^2 - a_1 a_2 & \dots & a_2^{n-1} - a_1 a_2^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n - a_1 & a_n^2 - a_1 a_n & \dots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix}$$

$$\begin{aligned}
&= \prod_{i=2}^n (a_i - a_1) \begin{vmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & a_2 & a_2^2 & \dots & a_2^{n-2} \\ 0 & 1 & a_3 & a_3^2 & \dots & a_3^{n-2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & a_n & a_n^2 & \dots & a_n^{n-2} \end{vmatrix} \\
&= \prod_{i=2}^n (a_i - a_1) \cdot \prod_{2 \leq j < i \leq n} (a_i - a_j)
\end{aligned}$$

nach Induktionsvoraussetzung. □

Korollar 8 Seien $a_1, \dots, a_n \in \mathbb{Z}/p\mathbb{Z}$ alle verschieden, so ist A_n invertierbar.

8.2 Der Grad der Diffie-Hellman Abbildung

Lemma 40 Sei g ein primitives Element modulo p .

$$f(X, Y) = - \sum_{i,j=0}^{p-2} g^{-ij} X^i Y^j \in \mathbb{Z}/p\mathbb{Z}[X, Y]$$

ist das eindeutig bestimmte Polynom mit $\text{grad}_X(f), \text{grad}_Y(f) \leq p-2$ mit der Eigenschaft

$$f(g^x, g^y) = g^{xy} \quad \text{für } 0 \leq x, y \leq p-2.$$

Beweis: Für $1 \leq k \leq p-2$ gilt

$$\sum_{j=0}^{p-2} g^{jk} = (g^k - 1)^{-1} (g^{(p-1)k} - 1) = 0.$$

Damit gilt

$$- \sum_{i,j=0}^{p-2} g^{-ij} g^{ix} g^{jy} = - \sum_{i=0}^{p-2} g^{ix} \sum_{j=0}^{p-2} g^{j(y-i)} = g^{xy}.$$

Fixieren wir y und sei $h(X) = h(X, g^y)$ ein Polynom vom Grad $\leq p-2$ mit der Eigenschaft $h(g^x) = g^{xy}$. Dann hat das Polynom $H(X) = h(X) - f(X, g^y)$ vom Grad $\leq p-2$ mindestens $p-1$ Nullstellen und muss daher das Nullpolynom sein. Es gilt also $h(X, g^y) = f(X, g^y)$ für jedes $0 \leq y \leq p-2$ und somit $h(X, Y) = f(X, Y)$. □

Satz 15 Sei g eine primitive Wurzel modulo p und N eine natürliche Zahl. Sei $f(X, Y) \in \mathbb{Z}/p\mathbb{Z}[X, Y]$ ein Polynom mit der Eigenschaft

$$f(g^x, g^y) = g^{xy}, \quad 0 \leq x, y \leq N-1.$$

Dann gilt für den totalen Grad von $f(X, Y)$:

$$\text{grad}(f) \geq N-1.$$

Beweis: Da das Ergebnis sonst trivial wäre, beschränken wir uns auf den Fall $\text{grad}_X(f), \text{grad}_Y(f) \leq N - 1$, d. h.

$$f(X, Y) = \sum_{i,j=0}^{N-1} c_{i,j} X^i Y^j.$$

Die Koeffizienten c_{ij} sind durch folgende Matrixgleichung eindeutig bestimmt:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & g & \cdots & g^{N-1} \\ \vdots & \vdots & & \vdots \\ 1 & g^{N-1} & \cdots & g^{(N-1)(N-1)} \end{pmatrix} \underbrace{\begin{pmatrix} c_{0,0} & \cdots & c_{0,N-1} \\ \vdots & & \vdots \\ c_{N-1,0} & \cdots & c_{N-1,N-1} \end{pmatrix}}_C = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & g & \cdots & g^{N-1} \\ \vdots & \vdots & & \vdots \\ 1 & g^{N-1} & \cdots & g^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & g & \cdots & g^{N-1} \\ \vdots & \vdots & & \vdots \\ 1 & g^{N-1} & \cdots & g^{(N-1)(N-1)} \end{pmatrix}^{-1}.$$

Alle Matrizen sind invertierbar, weshalb auch C invertierbar ist. Insbesondere existiert in jeder Zeile von C ein von Null verschiedener Eintrag, woraus die Behauptung folgt. \square

Bemerkung: Analoge Ergebnisse lassen sich für Elemente g mit beliebiger Ordnung herleiten. Außerdem läßt sich das Ergebnis auf andere Mengen, die (x, y) durchlaufen, verallgemeinern. Man benötigt für den Beweis lediglich, dass einer der Bereiche für x oder y aus aufeinanderfolgenden Zahlen besteht.

8.3 Untere Schranken für das Gewicht

Definition 23 Das Gewicht eines Polynoms $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ ist die Anzahl der von 0 verschiedenen Koeffizienten.

Schreibweise: $w(f)$.

Lemma 41 Sei $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ ein vom Nullpolynom verschiedenes Polynom vom Grad $\leq p - 2$. Hat $f(X)$ mindestens N Nullstellen in $\mathbb{Z}/p\mathbb{Z}^*$, so gilt

$$w(f) \geq (p - 1)/(p - 1 - N).$$

Beweis: Sei g eine primitive Wurzel modulo p und $t := w(f)$. Sei weiterhin A die Anzahl der $0 \leq x \leq p - 2$ mit $f(g^x) \not\equiv 0 \pmod{p}$ und T die Anzahl der Paare (y, i) , $0 \leq y \leq p - 2$, $0 \leq i \leq t - 1$, mit $f(g^{y+i}) \not\equiv 0 \pmod{p}$. Unter Berücksichtigung von $g^{p-1} \equiv 1 \pmod{p}$ sieht man $T = tA$.

Sei $f(X) = \sum_{j=0}^{t-1} a_{n_j} X^{n_j}$ mit $a_{n_j} \neq 0$, $0 \leq j \leq t-1$. Angenommen, für ein

$0 \leq y \leq p-2$ gelte $f(g^{y+i}) = \sum_{j=0}^{t-1} a_{n_j} \cdot g^{n_j(y+i)} \equiv 0 \pmod{p}$ für $0 \leq i \leq t-1$,

also

$$(a_{n_0} \ a_{n_1} \ \dots \ a_{n_{t-1}}) \underbrace{\begin{pmatrix} g^{n_0 y} & g^{n_0(y+1)} & \dots & g^{n_0(y+t-1)} \\ g^{n_1 y} & g^{n_1(y+1)} & \dots & g^{n_1(y+t-1)} \\ \vdots & \vdots & & \vdots \\ g^{n_{t-1} y} & g^{n_{t-1}(y+1)} & \dots & g^{n_{t-1}(y+t-1)} \end{pmatrix}}_G = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Weiterhin gilt

$$\text{Det}G = \prod_{j=0}^{t-1} g^{n_j y} \underbrace{\text{Det} \begin{pmatrix} 1 & g^{n_0} & \dots & g^{n_0(t-1)} \\ 1 & g^{n_1} & \dots & g^{n_1(t-1)} \\ \vdots & \vdots & & \vdots \\ 1 & g^{n_{t-1}} & \dots & g^{n_{t-1}(t-1)} \end{pmatrix}}_A.$$

A ist eine invertierbare Vandermonde-Matrix und somit G invertierbar und

$$(a_{n_0} \ a_{n_1} \ \dots \ a_{n_{t-1}}) = (0 \ 0 \ \dots \ 0),$$

was einen Widerspruch ergibt. Somit existiert zu jedem $0 \leq y \leq p-2$ ein $0 \leq i \leq t-1$ mit $f(g^{y+1}) \not\equiv 0 \pmod{p}$, woraus $T = tA \geq p-1$ folgt. Wegen $A \leq p-1-N$ gilt

$$t \geq \frac{p-1}{A} \geq \frac{p-1}{p-1-N}.$$

□

Satz 16 Sei $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ mit $f(g^x) \equiv g^{x^2} \pmod{p}$, $x \in S$ für eine Teilmenge $S \subseteq \{1, \dots, p-1\}$ der Kardinalität $|S| = p-1-s$, so gilt

$$w(f) \geq (p-1)/4s.$$

Beweis: Nach dem Beweis von Satz 11 hat das Polynom $h(X) = gX^2 f(X) - f(gX)$ mindestens $p-1-2s$ Nullstellen also $w(h) \geq (p-1)/2s$. Offensichtlich gilt aber $w(h) \leq 2w(f)$. □

Satz 17 Sei $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ mit

$$\text{ind}_g(n) \equiv f(n) \pmod{p}, \quad n \in S$$

für eine Teilmenge $S \subseteq \mathbb{Z}/p\mathbb{Z}^*$ der Kardinalität $|S| = p-1-s$. Dann gilt

$$w(f) \geq (p-1)/(2s+1) - 1.$$

Beweis: Nach dem Beweis von Satz 12 hat das Polynom $h(X) = f(gX) - f(X) - 1$ mindestens $p-2-2s$ Nullstellen also $w(h) \geq (p-1)/(2s+1)$. Offensichtlich gilt $w(f) \geq w(h) - 1$. □

8.4 Weitere untere Schranken für den Grad

Satz 18 Sei $p \geq 3$ und $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ mit

$$\text{ind}_g(x) \equiv f(x) \pmod{p}, \quad x \in S,$$

für $S \subseteq \{1, \dots, p-1\}$, dann gilt

$$\text{grad}(f) \geq \frac{|S|(|S|-1)}{2(p-2)}.$$

Beweis: Betrachte $D = \{a \equiv yx^{-1} \pmod{p} \mid 2 \leq a \leq p-1, x, y \in S\}$. Offensichtlich gilt $|D| \leq p-2$. Andererseits existiert ein $a \in D$ mit mindestens $|S|(|S|-1)/|D|$ Darstellungen $a \equiv yx^{-1} \pmod{p}, x, y \in S$. Sei $R = \{1 \leq x \leq p-1 \mid \text{ind}_g(x) \equiv f(x) \pmod{p} \text{ und } \text{ind}_g(ax) \equiv f(ax) \pmod{p}\}$.

Es gilt $|R| \geq |S|(|S|-1)/(p-2)$. Entweder haben wir für $x \in R$:

$$f(ax) \equiv \text{ind}_g(ax) \equiv \text{ind}_g(a) + \text{ind}_g(x) \equiv \text{ind}_g(a) + f(x) \pmod{p}$$

oder

$$f(ax) \equiv \text{ind}_g(ax) \equiv \text{ind}_g(a) + \text{ind}_g(x) - p + 1 \equiv \text{ind}_g(a) + f(x) + 1 \pmod{p}.$$

Daher hat entweder das Polynom

$$h_1(aX) = f(aX) - f(X) - \text{ind}_g(a)$$

oder das Polynom

$$h_2(aX) = f(aX) - f(X) - \text{ind}_g(a) - 1$$

mindestens $|R|/2$ Nullstellen. Wegen $h_1(0) \equiv -\text{ind}_g(a) \not\equiv 0 \pmod{p}$ wegen $a \not\equiv 1 \pmod{p}$ und $h_2(0) \equiv -\text{ind}_g(a) - 1 \not\equiv 0 \pmod{p}$ wegen $0 \leq \text{ind}_g(a) \leq p-2$ hat entweder $h_1(X)$ oder $h_2(X)$ mindestens den Grad $|R|/2 \geq |S|(|S|-1)/2(p-2)$. Offensichtlich gilt $\text{grad}(f) \geq \text{grad}(h_1)$ bzw. $\text{grad}(h_2)$, woraus die Behauptung folgt. \square

Satz 19 Sei $f(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ mit

$$f(g^x) \equiv g^{x^2} \pmod{p}, \quad x \in S,$$

für $S \subseteq \{0, \dots, p-2\}$, dann gilt

$$\text{grad}(f) \geq \frac{|S|^2}{2(p-1)} - \frac{2(p-1)}{|S|}.$$

Beweis: Sei $K := \lfloor \frac{2(p-1)}{|S|} \rfloor$ und $S_i := \{(x-i) \bmod (p-1) \mid x \in S\}$, $i = 0, \dots, K$. Dann gilt

$$(K+1)|S| - \sum_{0 \leq i < j \leq K} |S_i \cap S_j| = \sum_{i=0}^K |S_i| - \sum_{0 \leq i < j \leq K} |S_i \cap S_j| \leq \left| \bigcup_{i=0}^K S_i \right| \leq p-1.$$

Daher existiert ein Paar (i, j) , $0 \leq i < j \leq K$ mit

$$|S \cap S_{i-j}| = |S_i \cap S_j| \geq \frac{2|S|}{K} - \frac{2(p-1)}{K(K+1)}.$$

Sei $k = j - i$, so gilt für $x \in S \cap S_k$

$$g^{x^2} \equiv f(g^x) \pmod{p} \quad \text{und} \quad g^{(x+k)^2} \equiv f(g^{x+k}) \pmod{p},$$

also

$$f(g^{x+k}) \equiv g^{(x+k)^2} \equiv g^{x^2} g^{2kx} g^{k^2} \equiv g^{2kx} g^{k^2} f(g^x).$$

Das Polynom

$$h(X) = g^{k^2} X^{2k} f(X) - f(g^k X)$$

vom Grad $\text{grad}(h) = \text{grad}(f) + 2k \leq \text{grad}(f) + 2K$ hat also mindestens

$$|S \cap S_k| \geq \frac{2|S|}{K} - \frac{2(p-1)}{K(K+1)}$$

Nullstellen, woraus $\text{grad}(f) \geq \frac{2|S|}{K} - \frac{2(p-1)}{K(K+1)} - 2K$ und somit die Behauptung folgt. \square

Bemerkung: Satz 11 und 12 sind nur dann nicht trivial, wenn $|S| \geq (p+1)/2$. Satz 18 und 19 sind auch dann nicht trivial, wenn $|S| \geq \sqrt{2(p-2)} - 1$ bzw. $|S| \geq (2(p-1))^{2/3}$.

8.5 Eine explizite Formel für den diskreten Logarithmus

Lemma 42 Für eine ganze Zahl $j \geq 0$ gilt

$$\sum_{c=0}^{p-1} c^j \equiv \begin{cases} 0 \pmod{p}, & \text{falls } j = 0 \text{ oder } j \not\equiv 0 \pmod{p-1}, \\ -1 \pmod{p}, & \text{falls } j \neq 0 \text{ und } j \equiv 0 \pmod{p-1}, \end{cases}$$

wobei $0^0 := 1$.

Beweis: Für $j \equiv 0 \pmod{p-1}$ ist das Ergebnis trivial. Für $j \not\equiv 0 \pmod{p-1}$ gilt

$$\sum_{c=0}^{p-1} c^j \equiv \sum_{c=1}^{p-1} c^j \equiv \sum_{n=0}^{p-2} g^{nj} \equiv (g^j - 1)^{-1} (g^{j(p-1)} - 1) \equiv 0 \pmod{p}.$$

□

Lemma 43 Für $p \geq 3$ und $0 \leq k \leq p-1$ gilt

$$\sum_{\substack{c=0 \\ c \neq 1}}^{p-1} (1-c)^{-1} c^k \equiv k \pmod{p}.$$

Beweis: Mit $d := 1 - c$ gilt

$$\begin{aligned} \sum_{\substack{c=0 \\ c \neq 1}}^{p-1} (1-c)^{-1} c^k &\equiv \sum_{d=1}^{p-1} d^{p-2} (1-d)^k \\ &\equiv \sum_{i=0}^k \binom{k}{i} (-1)^i \sum_{d=1}^{p-1} d^{p-2+i} \equiv - \binom{k}{1} (-1) \equiv k \pmod{p} \end{aligned}$$

nach Lemma 42.

□

Satz 20 Für $1 \leq a \leq p-1$, $p \geq 3$, gilt

$$\text{ind}_g(a) \equiv -1 + \sum_{j=1}^{p-2} (g^{-j} - 1)^{-1} a^j \pmod{p}.$$

Beweis: Mit $k = \text{ind}_g(a) + 1$ und wegen

$$c^{\text{ind}_g(a)} = g^{\text{ind}_g(c) \text{ind}_g(a)} = a^{\text{ind}_g(c)}, \quad 1 \leq c \leq p-1$$

gilt nach Lemma 43

$$\begin{aligned} \text{ind}_g(a) &\equiv -1 + \sum_{c=2}^{p-1} (1-c)^{-1} c^{\text{ind}_g(a)+1} \\ &\equiv -1 + \sum_{c=2}^{p-1} (c^{-1} - 1)^{-1} a^{\text{ind}_g(c)} \equiv -1 + \sum_{j=1}^{p-2} (g^{-j} - 1)^{-1} a^j \pmod{p}. \end{aligned}$$

□

8.6 Explizite Darstellungen als Rekursionsfolge

Lemma 44 Sei $p \equiv 1 \pmod{4}$. Mit der Konvention $\text{ind}_g(0) := p - 1 \equiv 0 \pmod{2}$ gilt

$$\text{ind}_g(p - 1 + n) \equiv \text{ind}_g(p - 2 + n) + \text{ind}_g(p - 3 + n) + \dots + \text{ind}_g(n) \pmod{2}, \quad n \geq 0.$$

Beweis:

$$\begin{aligned} \sum_{i=0}^{p-1} \text{ind}_g(i + n) &\equiv \sum_{k=0}^{p-1} \text{ind}_g(k) \equiv \sum_{j=0}^{p-2} \text{ind}_g(g^j) \\ \sum_{j=0}^{p-2} j &\equiv (p-2) \frac{p-1}{2} \equiv \frac{p-1}{2} \equiv 0 \pmod{2}. \end{aligned}$$

□

Bemerkung: Für $p \equiv 1 \pmod{8}$ existiert eine nichttriviale Rekursion für den diskreten Logarithmus der Ordnung $\frac{p-1}{2}$, für $p \equiv 3 \pmod{8}$ ist $\text{ind}_g(p+n) \equiv \text{ind}_g(n) \pmod{2}$ die kürzeste Rekursion, für $p \equiv 5 \pmod{8}$ ist die Rekursion im Lemma die kürzeste und für $p \equiv 7 \pmod{8}$ existiert eine Rekursion der Ordnung $\frac{p+1}{2}$.

Beispiel:

$$1. \quad p = 3, g = 2$$

n	0	1	2
$\text{ind}_2(n)$	2	0	1

Aus $a_2 \text{ind}_2(n+2) + a_1 \text{ind}_2(n+1) + a_0 \text{ind}_2(n) \equiv 0 \pmod{2}$, $n \geq 0$, folgt $a_0 \equiv a_1 \equiv a_2 \equiv 0 \pmod{2}$.

$$2. \quad p = 5, g = 2$$

n	0	1	2	3	4
$\text{ind}_2(n)$	4	0	1	3	2

Aus $a_3 \text{ind}_2(n+3) + a_2 \text{ind}_2(n+2) + a_1 \text{ind}_2(n+1) + a_0 \text{ind}_2(n) \equiv 0 \pmod{2}$ folgt $a_0 \equiv a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod{2}$.

$$3. \quad p = 7, g = 3$$

n	0	1	2	3	4	5	6
$\text{ind}_3(n)$	6	0	2	1	4	5	3

$\text{ind}_3(n+3) + \text{ind}_3(n+2) + \text{ind}_3(n+1) + \text{ind}_3(n) \equiv 0 \pmod{2}$, $n \geq 0$.

Literaturverzeichnis

- [1] N. Koblitz: A course in number theory and cryptography, Springer 1987.
- [2] A. Menezes, P. Oorschot und S. Vanstone: Handbook of applied cryptography, CRC Press, 1997.
- [3] I. Niven und H. Zuckerman: Einführung in die Zahlentheorie I und II, Bibliographisches Institut, 1976.
- [4] I. Shparlinski: Number theoretic methods in cryptography, Birkhäuser, 1999.