

Zahlentheoretische Methoden in der Kryptographie

Vorlesungsskript von Arne Winterhof

27. Januar 2006

Dieses Skript ist die schriftliche Ausarbeitung einer Vorlesung, die ich im Wintersemester 2005/2006 an der JKU Linz gehalten habe.

Arne Winterhof

Inhaltsverzeichnis

1	Zahlentheoretische Grundlagen	1
1.1	Teilbarkeit und Euklidischer Algorithmus	1
1.2	Kongruenzen und Eulersche φ -Funktion	3
1.3	Quadratische Reste und Reziprozität	6
1.4	Summen von Legendre-Symbolen	11
1.5	Laufzeiten von arithmetischen Operationen und Algorithmen . . .	14
1.6	Quadratwurzeln modulo p	17
2	Einfache Kryptosysteme	20
2.1	Grundbegriffe	20
2.2	Lineare Substitutionschiffre	20
2.3	Verschlüsselungsmatrizen	21
2.4	Stromchiffren und lineare Komplexität	22
3	Public-Key Kryptosysteme	24
3.1	Grundlagen	24
3.2	Das RSA-Verfahren	25
3.3	Diskreter Logarithmus und Diffie-Hellman Schlüsselaustausch . . .	26
4	Faktorisierungsalgorithmen	27
4.1	Sieb des Eratosthenes	27
4.2	Fermat-Faktorisierung	27
4.3	Pollards ρ -Methode	28
4.4	Quadratwurzelfaktorisierung	29
4.5	Das quadratische Sieb	30
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	Interpolationspolynome	36
6.1	Interpolation der Diffie-Hellman Abbildung	36

6.2	Interpolation des diskreten Logarithmus	37
6.3	Interpolation der RSA-Abbildung	38
6.4	Interpolation einiger faktorisierender Funktionen	38
7	Primzahlerzeugung	40
7.1	Pseudoprimzahltests	40
7.1.1	Fermat Test	40
7.1.2	Solovay-Strassen Test	41
7.1.3	Miller-Rabin Test	42
7.2	Primzahltests	44
7.2.1	Lucas-Lehmer Test	44
7.2.2	Der $n - 1$ Test	46
7.2.3	Der AKS-Test	46
8	Elliptische Kurven in der Kryptographie	48
8.1	Definition und Gruppenstruktur	48
8.2	Der Diffie-Hellman Schlüsselaustausch mit elliptischen Kurven . .	50
8.3	Primzahltest und Faktorisierung mit elliptischen Kurven	50
8.3.1	Primzahltest	51
8.3.2	Faktorisierung	52

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. $m \neq 0$: $a|b \Rightarrow ma|mb$.

Lemma 2 (Divisionsalgorithmus)

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

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

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:

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

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

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

Ein gemeinsamer Teiler d von b und c teilt auch

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

□

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

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

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

Aufgaben

1. Beweise Lemma 1.
2. Bestimme $\text{ggT}(1547, 560)$ mit dem Euklidischen Algorithmus.
3. Bestimme $\text{ggT}(1547, 560)$ mit Hilfe der kanonischen Zerlegungen von 1547 und 560.

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

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

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

Lemma 5 Die Elemente $a \bmod m \in \mathbb{Z}/m\mathbb{Z}$ 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. $m \mid ab - 1$ folgt $d \mid ab - 1$. Wegen $d \mid a$ 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. \square

Definition 6 (Eulersche φ -Funktion)

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

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. \square

Korollar 1 Für $p \nmid a$ gilt:

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

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

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

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

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

Lemma 7 (Euler-Fermat)

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

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

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

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

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

□

Aufgaben

1. Beweise Lemma 3.
2. Beweise Lemma 4.
3. Berechne $2^{10^6} \bmod 7$.
4. Bestimme alle gemeinsamen Lösungen von $x \equiv 1 \pmod{3}$ und $x \equiv 2 \pmod{4}$.
5. Berechne $\varphi(90)$.
6. Beweise Lemma 7.
7. Berechne $2^{10^6} \bmod 77$.

1.3 Quadratische Reste und Reziprozität

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

Definition 7 $\mathbb{Z}/p\mathbb{Z}[X] := \{\sum_{j=0}^n a_j X^j : a_j \in \mathbb{Z}/p\mathbb{Z}, a_n \neq 0, n \in \mathbb{N} \cup \{0\}\}$ 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 . Wir definieren $\text{grad}(0) = -1$.

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 , $n \in \mathbb{N} \cup \{0\}$, 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. \square

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 $d|p-1$, 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 $d|p-1$, 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

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

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:

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = \sum_{j=0}^{p-2} \left(\frac{g^j}{p}\right) = \sum_{j=0}^{p-2} (-1)^j = 0.$$

\square

Lemma 13

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

Bemerkung: Ist f ein irreduzibles Polynom, d. h. ein Polynom ohne echte Teiler, vom Grad n über $\mathbb{Z}/p\mathbb{Z}$ und α eine Nullstelle von f , so ist $\mathbb{F}_{p^n} := \mathbb{Z}/p\mathbb{Z}(\alpha) := \{a_1 + a_2\alpha + \dots + a_n\alpha^{n-1} : a_1, \dots, a_n \in \mathbb{Z}/p\mathbb{Z}\}$ 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:

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

wobei hier Lemma 12 benutzt wurde. 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 $p, q > 2$, $p \neq q$, gilt

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

Beweis: Es gilt mit Lemma 13

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

Mit Lemma 15 bekommt man das Ergebnis. \square

Lemma 16 (Ergänzungssatz)

$$\binom{2}{p} = (-1)^{(p^2-1)/8}.$$

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

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

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

$$\binom{2}{p} \equiv -1 \pmod{p}.$$

\square

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.

Aufgaben

1. Beweise Lemma 13.
2. Ist 7411 quadratischer Rest modulo 9283? Benutze nur das Legendre-Symbol.
3. Berechne $\left(\frac{7411}{9283}\right)$ mit dem Jacobi-Symbol.
4. Berechne $\left(\frac{2}{15}\right)$. Ist 2 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. \square

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). □

Aufgaben

1. Berechne $\sum_{a=1}^N \left(\frac{a}{p}\right)$ für $1 \leq N \leq p-1$ und $p = 5, 7, 11$.
2. Bestimme den kleinsten quadratischen Nichtrest modulo p für $p = 3, 5, 7, 11, 13, 17, 19$.
3. Warum ist der kleinste quadratische Nichtrest modulo p eine Primzahl?
4. Bestimme das kleinste p für das der kleinste quadratische Nichtrest modulo p gleich 5 bzw. 7 ist.

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

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

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.

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 $b^n \pmod{m}$ kann in $O(\log n \log^2 m)$ Bitoperationen durchgeführt werden.

Beweis: Wir berechnen zunächst

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

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

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

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

Aufgaben

1. Welche Zahl hat die Binärdarstellung $(11001001)_2$?
2. Gib die Binärdarstellung von 1109 an.
3. Berechne schriftlich
 - a) $(1111000)_2 + (0011110)_2$,
 - b) $(1111000)_2 - (0011110)_2$,
 - c) $(11101)_2 \cdot (1101)_2$,
 - d) $(11001001)_2 : (100111)_2$.
4. Beweise Lemma 19.
5. Zeige, dass $n^c = O(e^n)$ für jede positive Konstante c gilt, aber die Umkehrung $e^n = O(n^c)$ falsch ist.

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 Corollary 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.

□

Aufgabe

- Berechne eine Quadratwurzel von 10 mod 13
- a) durch Berechnen der Quadrate modulo 13,
 - b) mit dem Algorithmus von Tonelli.

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

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:

$$\begin{array}{rcl} y_1 & \equiv & ax_1 + b \pmod{m} \\ y_2 & \equiv & ax_2 + b \pmod{m} \\ \hline y_2 - y_1 & \equiv & a(x_2 - x_1) \pmod{m} \\ \hline a & \equiv & (x_2 - x_1)^{-1}(y_2 - y_1) \pmod{m} \\ b & \equiv & y_1 - (x_2 - x_1)^{-1}(y_2 - y_1)x_1 \pmod{m} \end{array}$$

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

Aufgaben

1. Betrachte die lineare Substitution $f(x) \equiv 7x + 12 \pmod{26}$. Wir identifizieren unser Alphabet mit $\mathbb{Z}/26\mathbb{Z}$ durch die Zuordnung $A \rightarrow 0 \pmod{26}$, $B \rightarrow 1 \pmod{26}, \dots, Z \rightarrow 25 \pmod{26}$.
 - a) Verschlüssel das Wort BECKENBAUER mit obiger Substitution.
 - b) Welches Wort wurde zu 4 1 12 25 4 11 verschlüsselt?
2. Von einer linearen Substitution $f(x) = ax + b \pmod{31}$ sind $f(2) = 5$ und $f(3) = 10$ bekannt.
 - a) Berechne a und b .
 - b) Berechne f^{-1} .

2.3 Verschlüsselungsmatrizen

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

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

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

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

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.

Aufgabe

Sei A eine 2×2 Matrix über $\mathbb{Z}/26\mathbb{Z}$ und $f(\vec{x}) = A\vec{x}$. Gelte weiterhin $f(13, 14) = (16, 21)$, $f(0, 13) = (13, 0)$ und $f(18, 22) = (24, 16)$.

a) Berechne A .

b) Identifiziere unser Alphabet wieder mit $\mathbb{Z}/26\mathbb{Z}$. Verschlüsselt das Wort NO AN SW ER.

2.4 Stromchiffren und lineare Komplexität

Wir betrachten eine als $(0, 1)$ -Folge (Bitfolge) dargestellte Nachricht m_0, m_1, \dots . Ein *Stromchiffre* verschlüsselt jedes Bit m_j der Nachricht mit dem Element x_j einer binären Schlüsselfolge x_0, x_1, \dots durch

$$c_j = m_j + x_j \pmod{2}.$$

Der verschlüsselte Text c_0, c_1, \dots kann durch erneutes Addieren der Schlüsselfolge zurück erhalten werden: $m_j = c_j + x_j \pmod{2}$.

Die Sicherheit eines Stromchiffres hängt von der 'Zufälligkeit' der Schlüsselfolge, insbesondere von ihrer Vorhersagbarkeit, ab.

Definition 15 Die Legendre-Folge (l_n) ist definiert durch

$$l_n := \begin{cases} 1, & \left(\frac{n}{p}\right) = -1, \\ 0, & \text{sonst,} \end{cases} \quad n = 0, 1, \dots$$

und hat Periode p .

Definition 16 Sei (s_n) eine Bitfolge. Für $N \geq 1$ ist die lineare Komplexität von (s_n) bei N die kleinste nichtnegative ganze Zahl $L = L(s_n, N)$, so dass es $c_0, \dots, c_{L-1} \in \{0, 1\}$ gibt mit

$$s_{n+L} + c_{L-1}s_{n+L-1} + \dots + c_0s_n \equiv 0 \pmod{2}, \quad n = 0, 1, \dots, N - L - 1.$$

Die lineare Komplexität ist ein Maß für die Unvorhersagbarkeit einer Folge.

Satz 11 Für die lineare Komplexität der Legendre-Folge (l_n) bei $1 \leq N \leq p$ gilt:

$$L(l_n, N) > \frac{N}{9p^{1/2} + 1} - 1.$$

Beweis: Sei $L := L(l_n, N)$ und gelte

$$l_{n+L} + c_{L-1}l_{n+L-1} + \dots + c_0l_n \equiv 0 \pmod{2}, \quad 1 \leq n \leq N - L - 1.$$

Da die Aussage anderenfalls trivial ist, dürfen wir annehmen, dass $L \leq p^{1/2}$ und $N \geq p^{1/2} + L + 1$ ist.

Wegen $(-1)^{l_n} = \left(\frac{n}{p}\right)$, $1 \leq n \leq p - 1$, gilt mit $c_L := 1$:

$$1 = (-1)^{\sum_{j=0}^L c_j l_{n+j}} = \left(\frac{\prod_{j=0}^L (n+j)^{c_j}}{p} \right)$$

und daher

$$N - L - 1 = \sum_{n=1}^{N-L-1} \left(\frac{\prod_{j=0}^L (n+j)^{c_j}}{p} \right) =: S.$$

Andererseits gilt nach Satz 8

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

woraus die Behauptung folgt. □

Aufgabe

Bestimme die Legendre Folge für $p = 11$ und berechne $L(l_n, N)$ für alle $1 \leq N \leq 8$.

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:

B 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 B ist (n, e) , der private ist d .

RSA-Verschlüsselung:

A macht folgendes:

1. Hole den öffentlichen Schlüssel (n, e) von B .
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 B .

B 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*).

Aufgaben

1. Zeige, dass $m^{\varphi(pq)+1} \equiv m \pmod{pq}$ gilt.
2. a) Verschlüssele die Nachrichten $m = 5$ und $m = 7$ mit RSA und dem öffentlichen Schlüssel $(n, e) = (35, 5)$.
b) Berechne den privaten Schlüssel d .

3.3 Diskreter Logarithmus und Diffie-Hellman Schlüsselaustausch

Definition 17 Sei $b \in \mathbb{Z}/p\mathbb{Z}^*$ und $a \equiv b^x \pmod{p}$ mit $0 \leq x \leq \text{ord}_p(b) - 1$. 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 $a^x \pmod{p}$.
 B wählt einen persönlichen Schlüssel y und veröffentlicht $a^y \pmod{p}$.
3. A berechnet den Schlüssel $K \equiv (a^y)^x \pmod{p}$.
 B berechnet den Schlüssel $K \equiv (a^x)^y \pmod{p}$.

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

$$y \equiv x + K \pmod{26}$$

mit Schlüssel K .

Aufgabe

Sei $p = 53$, $a = 2$, $x = 29$ und $y = 19$. Beschreibe den Diffie-Hellman Schlüsselaustausch. Wie berechnen A und B jeweils den öffentlichen Schlüssel K ?

Kapitel 4

Faktorisierungsalgorithmen

In diesem Abschnitt werden Algorithmen beschrieben und analysiert, die natürliche Zahlen der Form $n = pq$ mit (unbekannten) Primzahlen p und q , $p < q$, faktorisieren, d.h. p und q bestimmen.

4.1 Sieb des Eratosthenes

Für $t = 2, 3, 5, 7, 11 \dots$ teste, ob n durch t teilbar ist.

Lemma 25 *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.

Aufgabe

Versuche die Zahlen 7721 und 11413 mit dem Sieb des Eratosthenes zu faktorisieren.

4.2 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 nah bei einander liegen.

Aufgabe

Versuche die Zahlen 7721 und 11413 und 200819 mit der Fermat-Faktorisierung zu faktorisieren.

4.3 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 26 Sei $\lambda > 0$ und $l = 1 + \lfloor \sqrt{2\lambda n} \rfloor$. 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: Wir dürfen $l < n$ annehmen. 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 $0 < x < 1$:

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

und somit $h(n, l) < e^{-\lambda}$. □

Lemma 27 (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.

Aufgabe

Faktorisiere 1927 mit Pollards ρ -Methode.

4.4 Quadratwurzelfaktorisierung

Lemma 28 *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 29 *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 $v_i \equiv (e_{i1}, \dots, e_{it}) \pmod 2$, $1 \leq i \leq t+1$, 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 .

Aufgabe

Faktorisiere 17111 mit der Quadratwurzelfaktorisierung.

4.5 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. Ein Algorithmus heißt *subexponential*, falls er $O(p^\varepsilon)$ Bitoperationen für alle $\varepsilon > 0$ benötigt. (Z.B. $2^{(\log p)^{1/2}} = O(p^\varepsilon)$, $\varepsilon > 0$). Bei geeigneter Wahl von t ist das quadratische Sieb subexponential.
2. Ist n kein quadratischer Rest modulo p_j , so kann p_j nicht b_i teilen. (Anderenfalls hätten wir $n \equiv (x + m)^2 \pmod{p_j}$.) Daher kann man in 1. die Primzahlen mit $\left(\frac{n}{p_j}\right) = -1$ weglassen.

Kapitel 5

Algorithmen zur Berechnung des diskreten Logarithmus

In diesem Kapitel werden Algorithmen beschrieben, die zu einer primitiven Wurzel g modulo p (ein Element der Ordnung $p - 1$) und einem Element $a \in \mathbb{Z}/p\mathbb{Z}^*$ den diskreten Logarithmus $x = \text{ind}_g(a)$ berechnen.

5.1 Direkte Suche

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

Lemma 30 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 12 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.

□

Aufgabe

Berechne den diskreten Logarithmus modulo 113 von $a = 57$ zur Basis 3 mit dem Baby-Step Giant-Step Algorithmus.

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

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

Falls dies gelingt, logarithmiere beide Seiten:

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

- (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 $\text{ind}_g(p_i)$, $1 \leq i \leq t$, 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:

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

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. Der Index-Calculus Algorithmus gehört zur Klasse der subexponentialen Algorithmen.

Aufgabe

Berechne den diskreten Logarithmus modulo 229 von 13 zur Basis 6 mit Index-Calculus. (Wähle für S die Menge der ersten 5 Primzahlen.)

Kapitel 6

Interpolationspolynome

6.1 Interpolation der Diffie-Hellman Abbildung

Definition 18 Sei $g \in \mathbb{Z}/p\mathbb{Z}^*$ eine 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 13 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 $S \subseteq \{0, \dots, p-2\}$ 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

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

□

6.2 Interpolation des diskreten Logarithmus

Satz 14 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

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

□

6.3 Interpolation der RSA-Abbildung

RSA Problem: Gegeben sei eine natürliche Zahl n , die Produkt zweier ungerader Primzahlen $p < q$ ist, eine natürliche Zahl e mit $\text{ggT}(e, \varphi(n)) = 1$ und eine ganze Zahl c . Finde eine ganze Zahl m mit $m^e \equiv c \pmod{n}$. In anderen Worten: Ist d eine (unbekannte) ganze Zahl mit $ed \equiv 1 \pmod{\varphi(n)}$, dann müssen wir die Abbildung $f(x) = x^d$ in c auswerten. Das folgende Ergebnis schließt die Existenz eines sehr einfachen Interpolationspolynoms aus, falls der öffentliche Exponent e klein ist.

Satz 15 Sei $n = pq$ das Produkt zweier ungerader Primzahlen $p < q$. Wähle ganze Zahlen $d, e > 1$ mit $ed \equiv 1 \pmod{\varphi(n)}$. Sei $S \subseteq \mathbb{Z}/n\mathbb{Z}^*$ eine Menge mit $s \geq 2$ Elementen. Ist $f(X) = \sum_{i=0}^m a_i X^i \in \mathbb{Z}[X]$ ein Polynom vom Grad $m < (q-1)/e$ und $\text{ggT}(a_0, \dots, a_m, n) = 1$ mit

$$f(x) \equiv x^d \pmod{n} \quad \text{für alle } x \in S,$$

so gilt

$$\text{grad}(f) \geq \max\left(\frac{s}{e(p-1)}, \frac{s^{1/2}}{e}\right).$$

Beweis. Sei $F(X) = f(X)^e - X$. Wegen $s \geq 2$ und $e > 1$ ist das Interpolationspolynomial $f(X)$ nicht konstant und es gilt

$$\text{grad}(F) = e \cdot \text{grad}(f).$$

Für $k \geq 1$ sei $Z_k(F)$ die Anzahl der verschiedenen Nullstellen von $F \pmod{k}$, die in $\mathbb{Z}/\mathbb{Z}_k^*$ liegen. Nach dem Chinesischen Restsatz gilt $Z_{pq}(F) = Z_p(F)Z_q(F)$. Aus den Bedingungen an f folgt $\text{grad}(F) < q-1$. Daher gilt

$$s \leq Z_p(F)Z_q(F) \leq (p-1)Z_q(F) \leq (p-1)\text{grad}(F) = e(p-1)\text{grad}(f).$$

Falls $s < (p-1)^2$ ist, so dürfen wir $\text{grad}(F) = e \cdot \text{grad}(f) < p-1$ annehmen und erhalten

$$s \leq Z_p(F)Z_q(F) \leq (\text{grad}(F))^2 = (e \cdot \text{grad}(f))^2.$$

□

Bemerkung: Ist e groß, so ist die untere Schranke sehr schwach. In diesem Fall gibt es aber erfolgreiche Angriffe auf RSA.

6.4 Interpolation einiger faktorisierender Funktionen

Die Eulersche φ -Funktion $\varphi(n) = (p-1)(q-1)$ für eine ganze Zahl $n = pq$ mit unbekanntem Primzahlen p und q kann zur Bestimmung von p und q benutzt

werden, indem man die quadratische Gleichung

$$X^2 + (\varphi(n) - n - 1)X + n = (X - p)(X - q) = 0$$

löst.

Könnte man φ durch ein Polynom kleinen Grades interpolieren, so könnte man effizient faktorisieren. Daher ist es wichtig untere Schranken für den Grad solcher Interpolationspolynome zu beweisen.

Satz 16 Für $M \geq 3$ sei

$$p_1 < p_2 < \dots < p_M$$

eine Menge geordneter Primzahlen. Sei $f(X) \in \mathbb{R}[X]$ ein Polynom mit

$$f(p_i p_j) = \varphi(p_i p_j), \quad 1 \leq i < j \leq M.$$

Dann gilt

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

Beweis. Das Polynom

$$F(X) = f(p_M X) - (X - 1)(p_M - 1)$$

is nicht identisch dem Nullpolynom, da für $i < j < M$

$$\begin{aligned} F(p_i p_j / p_M) &= f(p_i p_j) - (p_i p_j / p_M - 1)(p_M - 1) = p_M + p_i p_j / p_M - p_i - p_j \\ &= (p_M - p_i)(p_M - p_j) / p_M > 0 \end{aligned}$$

gilt. Andererseits hat F die Nullstellen p_1, \dots, p_{M-1} . Somit gilt $\text{grad}(f) = \text{grad}(F) \geq M - 1$. □

Aufgaben

1. Zeige, dass man die Teilersummenfunktion $\sigma(n) = \sum_{d|n} d$ zum Faktorisieren einer Zahl $n = pq$ mit Primzahlen $p < q$ benutzen kann.
2. Beweise analoge Ergebnisse zu Satz 16 für die Teilersummenfunktion σ und für die Funktion $f(pq) = p$ mit Primzahlen $p < q$.

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 19 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 20 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

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 $1 - (1/2)^t$.

Aufgabe

Zeige, dass $n = 561$ eine Carmichael-Zahl ist.

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 21 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

Algorithmus:

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

- (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.

Aufgabe

Zeige, dass 91 eine Pseudoprimzahl aber keine Euler-Pseudoprimzahl zur Basis 3 ist.

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 22 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. □

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 $y := a^r \bmod n$.
 - (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 $y^2 \bmod n$.
 - 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.

Aufgabe

1. Für $n \equiv 3 \pmod 4$ zeige, dass $\left(\frac{-1}{n}\right) = -1$.
2. Bestimme alle $1 \leq a \leq 64$ mit $\text{ggT}(a, 65) = 1$ für die 65
 - a) Pseudoprimzahl,
 - b) Euler-Pseudoprimzahl,
 - c) strenge Pseudoprimzahlzur Basis a ist.

7.2 Primzahltests

7.2.1 Lucas-Lehmer Test

Definition 23 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 $q^2 - 1 < n < 2^{s+1}$. \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 existiert, 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 Der AKS-Test

Man kann zeigen, dass der in diesem Abschnitt beschriebene Test von Agrawal, Kayal und Saxena (AKS) polynomiale Laufzeit hat.

Lemma 39 Seien a und n ganze Zahl mit $n \geq 2$ und $\text{ggT}(a, n) = 1$. Dann ist n genau dann eine Primzahl, wenn

$$(X + a)^n \equiv X^n + a \pmod{n}.$$

Beweis: Ist n eine Primzahl, so gilt die obige Polynomgleichung nach Lemma 13. Sei n zusammengesetzt, q ein Primteiler von n und k der größte Exponent mit $q^k | n$. Dann sind $n - 1, n - 2, \dots, n - q + 1$ nicht durch q teilbar und somit $\binom{n}{q}$ nicht durch q^k und daher auch nicht durch n teilbar. Also ist $(X + a)^n - X^n - a \equiv \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} X^i \pmod{n}$ nicht identisch Null. \square

Bemerkung: Ein Algorithmus, der direkt auf Lemma 39 basiert, muss die $n - 1$ Koeffizienten von $(X + a)^n - X^n - a \pmod{n}$ bestimmen und ist daher ineffizient. Die Anzahl der zu bestimmenden Koeffizienten verringert sich, wenn man $(X + a)^n - X^n - a \pmod{(X^r - 1, n)}$ mit einem geeigneten kleinen r betrachtet. Allerdings könnte jetzt $(X + a)^n - X^n - a \equiv 0 \pmod{(X^r - 1, n)}$ auch für zusammengesetztes n gelten. Man kann aber zeigen, dass die Anzahl der a mit dieser Eigenschaft klein ist.

Aufgaben

1. Zeige mit Hilfe von Lemma 37, dass $2^7 - 1$ eine Primzahl ist und dass $2^{11} - 1$ zusammengesetzt ist.
2. Formuliere basierend auf Korollar 7 ein Primzahlkriterium für die *Fermatzahlen* $n = 2^{2^k} + 1$, $k \geq 0$.
3. Zeige, dass $(X + a)^{129} - X^{129} - a \pmod{129}$ für kein a mit $\text{ggT}(a, 129) = 1$ das Nullpolynom ist, ohne 129 zu faktorisieren.

Kapitel 8

Elliptische Kurven in der Kryptographie

8.1 Definition und Gruppenstruktur

Definition 24 Eine elliptische Kurve E über einem Körper \mathbb{K} der Charakteristik ungleich 2 oder 3 ist die Menge der Lösungen $(x, y) \in \mathbb{K}^2$ einer kubischen Polynomialgleichung der Form

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K}, \quad 4a^3 + 27b^2 \neq 0, \quad (8.1)$$

zusammen mit einem Punkt O , genannt Punkt im Unendlichen.

Definition 25 ($\mathbb{K} = \mathbb{R}$)

Sei E eine elliptische Kurve über den reellen Zahlen und P, Q auf E . Wir definieren $-P$ und $P + Q$ in folgender Weise:

1. $P = O$: $-O = O$, $O + Q = Q$.
2. $P = (x, y) \neq O$: $-P = (x, -y)$.
3. $P = (x_1, y_1), Q = (x_2, y_2) \neq O$ mit $x_1 \neq x_2$: Die Gerade durch P und Q schneidet die Kurve in genau einem dritten Punkt R und wir setzen $P + Q = -R$.
4. $Q = -P \neq O$: $P + Q = O$.
5. $P = Q \neq O$: Die Tangente an E in P schneidet E in genau einem weiteren Punkt R und wir setzen $P + P = -R$.

Satz 17 Sei E eine elliptische Kurve über den reellen Zahlen definiert durch (8.1) und $P = (x_1, y_1), Q = (x_2, y_2) \neq O$ auf E mit $x_1 \neq x_2$. Dann gilt für

$P + Q = (x_3, y_3)$:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2, \quad (8.2)$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3), \quad (8.3)$$

und für $P + P = (x_4, y_4)$ mit $y_1 \neq 0$:

$$x_4 = \left(\frac{3x_1^2 + a}{2y_1} \right) - 2x_1, \quad (8.4)$$

$$y_4 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_4). \quad (8.5)$$

Beweis: $P \neq Q$, (d.h. $x_1 \neq x_2$):

Sei $y = \alpha x + \beta$ die Gerade durch P und Q , d.h.

$$\begin{aligned} y_1 &= \alpha x_1 + \beta \\ y_2 &= \alpha x_2 + \beta \end{aligned} \Rightarrow \alpha = \frac{y_2 - y_1}{x_2 - x_1}, \beta = y_1 - \alpha x_1.$$

$-(P + Q) = (x_3, -y_3)$ ist der dritte Schnittpunkt der Geraden $y = \alpha x + \beta$ mit E . Einsetzen der Geradengleichung in die Gleichung der elliptischen Kurve liefert:

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0 = (x - x_1)(x - x_2)(x - x_3).$$

Der Koeffizient von x^2 ist $-(x_1 + x_2 + x_3) = -\alpha^2$ und somit

$$x_3 = \alpha^2 - x_1 - x_2 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2.$$

Die zweite Koordinate von $P + Q$ ist

$$y_3 = -(\alpha x_3 + \beta) = -y_1 + \alpha(x_1 - x_3) = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3).$$

$P = Q \neq -P$, (d.h. $y_1 \neq 0$)

Sei $y = \alpha x + \beta$ die Tangente an E im Punkt P , d.h. $\alpha = \frac{dy}{dx}$ in x_1 . Implizites Ableiten von $y^2 = x^3 + ax + b$ ergibt $2y y' = 3x^2 + a$, somit $y' = \frac{3x^2 + a}{2y}$ und daher $\alpha = \frac{3x_1^2 + a}{2y_1}$ und $\beta = y_1 - \alpha x_1$.

Sei $-2P = (x_4, -y_4)$ der zweite Schnittpunkt der Tangente $y = \alpha x + \beta$ mit E . Einsetzen der Geradengleichung liefert

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0 = (x - x_1)^2(x - x_4)$$

also

$$x_4 = \alpha^2 - 2x_1 = \left(\frac{3x_1^2 + a}{2y} \right)^2 - 2x_1$$

und

$$y_4 = -(\alpha x_4 + \beta) = -y_1 + \left(\frac{3x_1^2 + a}{2y} \right) (x_1 - x_4).$$

□

Definition 26 ($\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$)

Sei E eine elliptische Kurve über $\mathbb{Z}/p\mathbb{Z}$, $p > 3$, definiert durch (8.1), so definieren wir $O + Q = Q$ und $P + Q$ durch (8.2) – (8.5) für $P, Q \in E \setminus \{O\}$.

Satz 18 Sei E eine elliptische Kurve über $\mathbb{Z}/p\mathbb{Z}$ und $+$ die oben definierte Punktaddition auf E . Dann ist $(E, +)$ eine abelsche Gruppe.

ohne Beweis

□

8.2 Der Diffie-Hellman Schlüsselaustausch mit elliptischen Kurven

1. A und B einigen sich auf einen Punkt P großer Ordnung auf einer elliptischen Kurve E über $\mathbb{Z}/p\mathbb{Z}$, d. h. (P, E) ist öffentlich.
2. A wählt einen persönlichen Schlüssel x und veröffentlicht $xP \in E$.
 B wählt einen persönlichen Schlüssel y und veröffentlicht $yP \in G$.
3. A berechnet den Schlüssel $K = x(yP) \in E$.
 B berechnet den Schlüssel $K = y(xP) \in E$.

8.3 Primzahltest und Faktorisierung mit elliptischen Kurven

Analog zu elliptischen Kurven über Körpern kann man auch elliptische Kurven über $\mathbb{Z}/n\mathbb{Z}$ definieren:

$$E = \{(x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\} \cup O$$

mit $a, b \in \mathbb{Z}/n\mathbb{Z}$. Weiterhin lassen sich die Formeln (4.8) – (4.11) anwenden, sofern die dort auftretenden Nenner teilerfremd zu n sind. Ist das nicht der Fall, so ist n zusammengesetzt und der größte gemeinsame Teiler von diesem Nenner und n ist ein nichttrivialer Teiler von n . Wir betrachten daher nur den Fall, dass alle im Folgenden auftretenden Nenner zu n teilerfremd sind.

Lemma 40 Sei p ein Teiler von n , E' die Kurve über $\mathbb{Z}/p\mathbb{Z}$ definiert durch dieselbe Gleichung wie E über $\mathbb{Z}/n\mathbb{Z}$, $O \neq P = (x_1, y_1) \in E$ und $O \neq P' = (x'_1, y'_1) \in E'$ mit $x_1 \equiv x'_1 \pmod{p}$ und $y_1 \equiv y'_1 \pmod{p}$. Dann gilt:

$$lP = O \iff lP' = O.$$

Beweis: Da nach Voraussetzung bei der Berechnung von jP , $2 \leq j \leq l-1$, die Nenner teilerfremd zu n sind, erhält man $jP' \equiv jP \pmod{p}$. Sei $(l-1)P = (x_2, y_2)$ und $(l-1)P' = (x'_2, y'_2) \equiv (l-1)P \pmod{p}$.

Die Gleichung $lP = O$ ist äquivalent mit $x_1 \equiv x_2 \pmod{n}$ und $y_1 \equiv -y_2 \pmod{n}$. Hieraus folgt $x'_1 \equiv x_1 \equiv x_2 \equiv x'_2 \pmod{p}$ und $y'_1 \equiv y_1 \equiv -y_2 \equiv -y'_2 \pmod{p}$, was gleichwertig mit $lP' = O$ ist.

Sei umgekehrt $lP' = O$, also $x_1 \equiv x_2 \pmod{p}$ und $y_1 \equiv -y_2 \pmod{p}$. Wegen $\text{ggT}(x_2 - x_1, n) = 1$ oder $\text{ggT}(x_2 - x_1, n) = n$ folgt daraus $x_1 \equiv x_2 \pmod{n}$ und somit $lP = O$. \square

8.3.1 Primzahltest

Lemma 41 Sei n eine natürliche Zahl und E eine elliptische Kurve über $\mathbb{Z}/n\mathbb{Z}$ definiert durch die Gleichung $y^2 = x^3 + ax + b$. Sei l eine ganze Zahl und q ein Primteiler von l mit $q > (n^{1/4} + 1)^2$. Falls es einen Punkt P auf E mit

$$(1) \ lP = O \quad \text{und} \quad (2) \ l/qP \neq O$$

gibt, so ist n prim.

Beweis: Falls n nicht prim wäre, so würde eine Primzahl $p \leq \sqrt{n}$ existieren, die n teilt. Sei E' die elliptische Kurve definiert durch dieselbe Gleichung wie E aber über $\mathbb{Z}/p\mathbb{Z}$ und l' die Ordnung der Gruppe E' . Nach Hasse-Weil gilt

$$l' \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \leq (n^{1/4} + 1)^2 < q$$

und daher $\text{ggT}(q, l') = 1$, weshalb eine ganze Zahl u mit $uq \equiv 1 \pmod{l'}$ existiert. Sei P' auf E' der Punkt P modulo p betrachtet. Dann gilt auf E'

$$l/qP' = uql/qP' = ulP' = O$$

nach (1) im Widerspruch zu (2) und Lemma 40. \square

Algorithmus:

1. Wähle zufällig $a, x, y \in \mathbb{Z}/n\mathbb{Z}$ und setze $b = y^2 - x^3 - ax \in \mathbb{Z}/n\mathbb{Z}$. (Dann liegt $P = (x, y)$ auf der durch $y^2 = x^3 + ax + b$ definierten Kurve E .)
2. Bestimme die Anzahl l der Punkte auf E (z.B. mit Schoofs Algorithmus).

3. Ist l nicht von der Form $l = kq$ mit kleinem k und einem q , das 'wahrscheinlich' prim ist, gehe zu 1.
4. Berechne lP und $kP = l/qP$.
5. Ist $lP \neq O$, so ist n zusammengesetzt.
6. Ist $lP = O$ und $kP = O$, so gehe zu 1.
7. Ist $lP = O$ und $kP \neq O$, so ist n 'wahrscheinlich' prim.
8. Wende den Algorithmus auf q statt n an.

Bemerkung: Der Algorithmus führt den Primzahltest für n sukzessive auf Primzahltests für Zahlen $n_1 = q \leq n/2$, $n_2 \leq n/4$, usw. zurück. Stellt man nach $t \leq \log(n)$ Durchläufen fest, dass n_t eine Primzahl ist, so auch n_{t-1}, \dots, n_1 und n .

8.3.2 Faktorisierung

Der folgende Algorithmus von Lenstra berechnet einen nichttrivialen Teiler d einer zusammengesetzten Zahl n .

1. Wähle eine elliptische Kurve über \mathbb{Z} :

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

und einen Punkt $P = (x, y)$ auf E .

2. Berechne $t = \text{ggT}(4a^3 + 27b^2, n)$.
Falls $1 < t < n$ setze $d = t$. Stopp
Falls $t = n$ gehe zu 1.

3. Wähle Konstanten B und C und setze

$$k = \prod_{\substack{l \leq B \\ l \text{ prim}}} l^{\alpha_l} \quad \text{mit } \alpha_l = \left\lfloor \frac{\log(C)}{\log(l)} \right\rfloor.$$

(Die Zahl k ist das Produkt aller Primzahlpotenzen l^{α_l} mit Primzahlen $l \leq B$ und $l^{\alpha_l} \leq C$.)

4. Versuche kP über $\mathbb{Z}/n\mathbb{Z}$ zu berechnen. Taucht bei den Additionsformeln ein Nenner u mit $d = \text{ggT}(u, n) > 1$ auf, dann stopp.

Bemerkungen:

1. Man kann zeigen, dass für $t = 1$ und zusammengesetztes n mit hoher Wahrscheinlichkeit im letzten Schritt des Algorithmus ein $d > 1$ auftaucht.
2. Die Laufzeit des Algorithmus hängt von der Wahl der Konstanten B und C ab.

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.