Protokoll zur Vorlesung Kryptographie
SS 2023

W. Bley

14. Juli 2023

1 Algebraische Grundlagen

1.1 Teilbarkeit in Integritätsbereichen

Definition 1.1.1 Sei R ein kommutativer Ring mit 1.

(a) R heißt nullteilerfrei, falls für alle $x, y \in R$ gilt:

$$xy = 0 \implies x = 0 \text{ oder } y = 0.$$

Man nennt dann R auch einen Integritätsbereich.

(b) $u \in R$ heißt Einheit, falls es ein $v \in R$ mit $uv = 1$ gibt. Mit $R^\times$ bezeichnen wir die Menge der Einheiten.

(c) Zwei Elemente $x, y \in R$ heißen assoziiert, falls es eine Einheit $u \in R^\times$ mit $x = uy$ gibt. Wir schreiben dann $x \sim y$.

Satz 1.1.2 *Sei R ein Integritätsbereich und $x, y \in R \setminus \{0\}$. Dann gilt:*

$$x \mid y \text{ und } y \mid x \iff x \sim y.$$

Definition 1.1.3 Sei R ein Integritätsbereich und $x_1, \ldots, x_n \in R$.

1. Ein Element $d \in R$ heißt ggT von $x_1, \ldots, x_n$, falls gilt:
   (a) $d \mid x_i$ für $i = 1, \ldots, n$.
   (b) Für jedes Element $d' \in R$ mit $d' \mid x_i$ für $i = 1, \ldots, n$ gilt $d' \mid d$.

Remark 1.1.4 Zwei ggT sind zueinander assoziiert.

Definition 1.1.5 Ein Integritätsbereich heißt euklidischer Ring, falls es eine Funktion

$$\beta \colon R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

gibt, so daß gilt: Für je zwei Elemente $x, y \in R$, $y \neq 0$, gibt es Elemente $q, r \in R$ so daß

$$x = qy + r \text{ mit } r = 0 \text{ oder } \beta(r) < \beta(y).$$

Satz 1.1.6 *In einem euklidischen Ring R existieren größte gemeinsame Teiler.*

Definition 1.1.7 Eine nicht-leere Teilmenge I eines kommutativen Rings R heißt Ideal, falls gilt:

1. I ist eine additive Untergruppe.

2. Für alle $x \in I, a \in R$ gilt $ax \in I$.

Definition 1.1.8 1. Seien $x_1, \ldots, x_n \in R$. Dann nennt man

$$(x_1, \ldots, x_n) := Rx_1 + \ldots Rx_n = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in R \right\}$$

das von $x_1, \ldots, x_n$ erzeugte Ideal. Für $x \in R$ nennt man (x) das von x erzeugte Hauptideal.

2. Ein Hauptidealring ist ein nullteilerfreier Ring, in dem jedes Ideal ein Hauptideal ist.

Satz 1.1.9 *Jeder euklidische Ring ist ein Hauptidealring.*

Satz 1.1.10 *Sei R ein Integritätsbereich.*

1. *Für $x, y \in R$ gilt:*
$$x \mid y \iff (y) \subseteq (x).$$
2. *$x, y \in R \setminus \{0\}$ sind genau dann assoziiert, wenn $(x) = (y)$ gilt.*
3. *Für $u \in R$ gilt:*
$$u \in R^\times \iff (u) = R.$$

Satz 1.1.11 *Sei R ein Hauptidealring und seien $x_1, \ldots, x_n \in R \setminus \{0\}$. Sei $(x_1, \ldots, x_n) = (d)$. Dann ist d ein ggT von $x_1, \ldots, x_n$. Insbesondere existieren größte gemeinsame Teiler in Hauptidealringen.*

1.2 Primfaktorzerlegung

Definition 1.2.1 Sei R ein Integritätsbereich.

1. Ein Element $a \in R \setminus (R^\times \cup \{0\})$ heißt irreduzibel, falls es keine Zerlegung $a = xy$ mit $x, y \in R \setminus R^\times$ gibt.
2. Ein Element $a \in R \setminus (R^\times \cup \{0\})$ heißt prim, falls für alle $a, b \in R$ gilt:
$$p \mid ab \implies p \mid a \text{ oder } p \mid b.$$

Satz 1.2.2 *Sei R ein Integritätsbereich. Dann gilt:*

1. *Jedes Primelement ist irreduzibel.*
2. *Im HIR gilt auch die Umkehrung.*

Satz 1.2.3 *Sei R ein HIR und $a_1, a_2, a_3, \ldots \in R$ erfülle $a_{i+1} \mid a_i$ für alle $i \geq 1$. Dann gibt es ein i_0, so daß $a_i \sim a_{i_0}$ für alle $i \geq i_0$ gilt. Wir sagen, die Kette wird stationär.*

Satz 1.2.4 *Im HIR ist jede Nicht-Einheit $a \neq 0$ Produkt von endlich vielen Primelementen. Die Zerlegung ist bis auf Reihenfolge und Assoziiertheit eindeutig.*

Wir wählen nun in jeder Klasse von assoziierten Primelementen einen Vertreter p und bezeichnen diese Menge mit $\mathbb{P}$. Dann kann man jedes $a \in R \setminus \{0\}$ eindeutig in der Form

$$a = u \cdot \prod_{p \in \mathbb{P}} p^{v_p(a)}$$

mit $u \in R^\times$ und $v_p(a) \in \mathbb{N}_0$ schreiben. Es gilt dabei $v_p(a) = 0$ für fast alle p.

1.3 Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$

Definition 1.3.1 Sei R ein Integritätsring und $I \subseteq R$ ein Ideal. Zwei Zahlen $x, y \in R$ heißen kongruent modulo I (in Zeichen: $x \equiv y \pmod{I}$), falls $x - y \in I$. Die Menge der Äquivalenzklassen bezeichnen wir mit R/I.

Für $R = \mathbb{Z}$ und $I = m\mathbb{Z}$ ist ein Vertretersystem gegeben durch die Menge $\{0, 1, 2, \ldots, m-1\}$. Es gilt:

$$x \equiv y \pmod{I} \iff x \text{ und } y \text{ lassen bei Teilung durch } m \text{ den gleichen Rest.}$$

Wir schreiben auch $\bar{x}$ für die Restklasse von x modulo I, d.h. $\bar{x} = x + I$. Die Menge der Äquivalenzklassen R/I wird durch

$$\bar{x} + \bar{y} := \overline{x + y}, \quad \bar{x} \cdot \bar{y} := \overline{x \cdot y}$$

zu einem kommutativen Ring.

Satz 1.3.2 *1.* $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{x} \mid \mathrm{ggT}(x, m) = 1\}$.

2. Falls $\mathrm{ggT}(x, m) > 1$ *gilt, so ist* $\bar{x}$ *ein Nullteiler in* $\mathbb{Z}/m\mathbb{Z}$.

Man beachte, daß man mit dem erweiterten euklidischen Algorithmus entscheiden kann, ob $x \in \mathbb{Z}$ modulo m invertierbar ist, und gegebenenfalls kann man dann auch $\bar{x}^{-1}$ berechnen.

Folgerung 1.3.3 *$\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

Satz 1.3.4 *(Chinesischer Restsatz) Sei $m > 1$ und $m = m_1 \cdots m_r$ mit paarweise teilerfremden ganzen Zahlen $m_i > 1$. Dann ist die kanonische Abbildung*

$$\begin{aligned} \phi\colon \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}, \\ x + m\mathbb{Z} &\mapsto (x + m_1\mathbb{Z}, \ldots, x + m_r\mathbb{Z}), \end{aligned}$$

ein Ringisomorphismus.

Mit Hilfe des erweiterten euklidischen Algorithmus läßt sich die Umkehrabbildung zu ϕ berechnen.

Folgerung 1.3.5 *Sei $m \in \mathbb{Z}_{>0}$ und*

$$m = p_1^{k_1} \cdots p_s^{k_s}$$

die Primzahlzerlegung von m. Dann gilt

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\simeq \prod_{i=1}^{s} \mathbb{Z}/p_i^{k_i}\mathbb{Z}, \\ (\mathbb{Z}/m\mathbb{Z})^\times &\simeq \prod_{i=1}^{s} \left(\mathbb{Z}/p_i^{k_i}\mathbb{Z}\right)^\times. \end{aligned}$$

Definition 1.3.6 Für $m \in \mathbb{Z}_{>0}$ setzt man

$$\varphi(m) := |\{k \mid 0 < k < m, \mathrm{ggT}(m, k) = 1\}| = |\,(\mathbb{Z}/m\mathbb{Z})^\times\,|.$$

Man nennt φ die Eulersche φ-Funktion.

Satz 1.3.7 *1. Seien $m, n \in \mathbb{N}$ zueinander teilerfremde natürliche Zahlen. Dann gilt:*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

2. Sei $m = p^k$ eine Primzahlpotenz. Dann gilt:

$$\varphi(p^k) = (p-1)p^{k-1}.$$

3. Sei $m = p_1^{k_1} \cdots p_s^{k_s}$ die Primzahlzerlegung von m. Dann gilt:

$$\varphi(m) = \prod_{i=1}^{s} (p_i - 1)p_i^{k_i - 1}.$$

1.4 Abelsche Gruppen und einfache Anwendungen

Wir erinnern an einige grundlegende Definitionen und Resultate. Sei G eine Gruppe. Dann bezeichnet für $g \in G$

$$\mathrm{ord}(g) := \min\{k \in \mathbb{N} \mid g^k = e\} \in \mathbb{N} \cup \{\infty\}$$

die Ordnung des Elements g. Es ist dann $\mathrm{ord}(g)$ die Kardinalität der von g erzeugten zyklischen Untergruppe

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

Ferner gilt für jede natürliche Zahl n

$$g^n = e \iff \mathrm{ord}(g) \mid n.$$

Sei $\mathrm{ord}(g) = n < \infty$. Dann gilt:

$$\mathrm{Aut}(\langle g \rangle) \simeq (\mathbb{Z}/n\mathbb{Z})^\times.$$

Insbesondere also

$$\langle g \rangle = \langle g^k \rangle \iff \mathrm{ggT}(k, n) = 1.$$

Satz 1.4.1 *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Dann ist $|H|$ ein Teiler von $|G|$.*

Folgerung 1.4.2 *(Satz von Lagrange) Sei G eine endliche Gruppe und $g \in G$. Dann ist $ord(g)$ ein Teiler von $|G|$. Insbesondere gilt für alle $g \in G$*

$$g^{|G|} = e.$$

Folgerung 1.4.3 *(Kleiner Satz von Fermat) Sei p eine Primzahl. Dann gilt für alle $a \in \mathbb{Z}$ mit* $\mathrm{ggT}(a, p) = 1$

$$a^{p-1} \equiv 1 \pmod{p\mathbb{Z}}.$$

Für alle $a \in \mathbb{Z}$ gilt demnach $a^p \equiv a \pmod{p\mathbb{Z}}$.

Folgerung 1.4.4 *Sei $m \in \mathbb{Z}_{\geq 2}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann gilt:*

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

Der "kleine Satz von Fermat" liefert einen probabilistischen Primzahltest. Für gegebenes $N \in \mathbb{N}$ wollen wir entscheiden, ob N eine Primzahl ist. Dazu testen wir für "viele" $a \in \{1, \ldots, N-1\}$, ob die Kongruenz

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

erfüllt ist. Falls wir ein a finden, so dass die Kongruenz nicht erfüllt ist, so ist N mit Sicherheit keine Primzahl. Andernfalls können wir eigentlich keine Aussage treffen, außer dass N mit einer gewissen Wahrscheinlichkeit eine Primzahl ist. Der interessierte Leser informiere sich in der Literatur über die sogenannten Carmichael-Zahlen.
Für diesen Fermat-Primzahltest brauchen wir einen schnellen Algorithmus zur Berechnung von $a^{N-1} \bmod N$. Einen solchen haben wir (am Beispiel) kennen gelernt.

1.5 Die Struktur von $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$

Satz 1.5.1 *Sei $p \neq 2$ eine Primzahl und $k \in \mathbb{N}$. Dann ist $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ zyklisch. Für $p = 2$ gilt:*

$$\begin{aligned} (\mathbb{Z}/4\mathbb{Z})^\times &= \langle \overline{-1} \rangle, \\ \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times &= \langle \overline{-1} \rangle \times \langle \overline{5} \rangle, \quad k \geq 3 \end{aligned}$$

Folgerung 1.5.2 *Für jede Primzahl p ist $\mathbb{F}_p^\times$ zyklisch.*

Falls $\mathbb{F}_p^\times = \langle \omega \rangle$, so nennen wir ω eine Primitivwurzel modulo p. Die Menge der Primitivwurzel ist dann gegeben durch $\{\omega^k \mid 1 \leq k \leq p-1, \mathrm{ggT}(k, p-1) = 1\}$.

2 Kryptographie

2.1 Definitionen und einfachste Beispiele

Definition 2.1.1 Ein Kryptosystem oder Verschlüsselungsverfahren ist ein Fünftupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ mit

1. $\mathcal{P}$ ist eine Menge und heißt Klartextraum (englisch "plain text").
2. $\mathcal{C}$ ist eine Menge und heißt Chiffrenraum (englisch "cypher text").
3. $\mathcal{K}$ ist eine Menge und heißt Schlüsselraum (englisch "keys"). (Oftmals gibt es auch zwei Schlüsselräume, wenn die Schlüssel zum Verschlüsseln verschieden von den Schlüsseln zum Entschlüsseln sind.)
4. $\mathcal{E} = \{E_k \colon k \in \mathcal{K}\}$ ist eine Menge von Funktionen
$$E_k \colon \mathcal{P} \longrightarrow \mathcal{C}.$$
Dies sind die Verschlüsselungsfunktionen (englisch "encypher").
5. $\mathcal{D} = \{D_k \colon k \in \mathcal{K}\}$ ist eine Menge von Funktionen
$$E_k \colon \mathcal{C} \longrightarrow \mathcal{P}.$$
Dies sind die Entschlüsselungsfunktionen (englisch "decypher").
6. Zu jedem $e \in \mathcal{K}$ gibt es eine $d \in \mathcal{K}$, so dass für alle $p \in \mathcal{P}$ gilt:
$$D_d(E_e(p)) = p.$$

Ein Kryptosystem nennen wir symmetrisch, falls die Kenntnis des Schlüssels $e \in \mathcal{K}$ zum Verschlüsseln äquivalent zur Kenntnis des Schlüssels $d \in \mathcal{K}$ zum Entschlüsseln ist.
Ein Kryptosystem nennen wir asymmetrisch, falls sich d nicht in "vertretbarer Zeit" aus e berechnen läßt. Man kann dann e veröffentlichen und bezeichnet daher diese Verfahren auch als "Public-Key-Verfahren".
Als einfache Beispiele haben wir affine Chiffren besprochen.

3 RSA (Rivest-Shamir-Adleman 1978)

1. Man wähle zwei große Primzahlen p, q und berechne $N = pq$.
2. Man wähle eine Zahl $e \in \mathbb{N}$ mit
$$1 < e < \varphi(N) = (p-1)(q-1) \text{ und } \mathrm{ggT}(e, \varphi(N)) = 1.$$
3. Man berechne $d \in \mathbb{N}$ mit $ed \equiv 1 \pmod{\varphi(N)}$ und $1 < d < \varphi(N)$.
4. Veröffentliche das Paar (N, e) und halte d geheim.
5. Verschlüsselung: $\mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}, \quad x \mapsto x^e$.
6. Entschlüsselung: $\mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}, \quad y \mapsto y^d$.

Die Sicherheit von RSA beruht auf dem Faktorisierungsproblem für ganze Zahlen. Offensichtlich kann man RSA knacken, wenn man N faktorisieren kann. Umgekehrt werden wir zeigen, dass man aus der Kenntnis von N, e, d die Faktorisierung von N berechnen kann.

Satz 3.0.1 *Es seien N, e, d wie im RSA-Verfahren. Es sei $s := \max\{t \in \mathbb{N} \mid 2^t \text{ teilt } (ed-1)\}$ und $k := (ed-1)/2^s$.*
(a) Für $a \in \mathbb{N}$ mit $1 < a < N$ und $\mathrm{ggT}(a, N) = 1$ gelte

$$ord(a^k \pmod p) \neq ord(a^k \pmod q). \tag{1}$$

Dann gibt es ein $t \in \{0, \ldots, s-1\}$, so dass

$$1 < \mathrm{ggT}(a^{2^t k} - 1, N) < N$$

gilt. Mit anderen Worten: $\mathrm{ggT}(a^{2^t k} - 1, N) \in \{p, q\}$ ist ein echter Teiler von N.
(b) Die Anzahl der zu N teilerfremden Zahlen $a \in \{1, \ldots, N-1\}$, die (1) erfüllen, ist größer gleich $(p-1)(q-1)/2$.

Falls also d bekannt ist, so hat man nach Wahl von r verschiedenen Zahlen a die Zahl N mit einer Wahrscheinlichkeit größer gelich $1 - \frac{1}{2^r}$ faktorisiert.
Prinzipiell könnte man jedoch RSA-Schlüsseltexte auch entschlüsseln, ohne d zu berechnen. Ob dies möglich ist, ist ein offenes Problem.

3.1 Diskrete Logarithmen, Schlüsselaustausch und ElGamal-Verfahren

3.1.1 Diskrete Logarithmen

Definition 3.1.1 Sei $G = \langle a \rangle$ eine zyklische Gruppe und sei $b = a^s$. Dann heißt $\log_a(b) := s$ diskreter Logarithmus von b zur Basis a. Die Berechnung von $\log_a(b)$ nennt man das diskrete Logarithmenproblem (kurz DL-Problem).

Für Anwendungen in der Kryptographie brauchen wir zyklische Gruppen G mit einfacher Gruppenoperation und schwerem DL-Problem. Kandidaten hierfür sind zum Beispiel Untergruppen von $\mathbb{F}_p^\times$ oder Untergruppen von rationalen Punkten auf elliptischen Kurven über endlichen Körpern.

3.1.2 Diffie-Hellman-Schlüsselaustausch

Alice und Bob wollen einen gemeinsamen Schlüssel generieren, den Sie dann für ein symmetrisches Verfahren verwenden wollen. Sie einigen sich dazu auf eine zyklische Gruppe G und einen Erzeuger g von G. Sei $n = \mathrm{ord}(g)$. G und g werden veröffentlicht.
Dann wählt Alice einen Exponenten $a \in \{0, \ldots, n-1\}$, berechnet $A = g^a$ und übermittelt A über den öffentlichen Kanal. Bob wählte einen Exponenten $b \in \{0, \ldots, n-1\}$, berechnet $B = g^b$ und übermittelt B. Die Exponenten a und b bleiben geheim.
Der gemeinsame Schlüssel ist dann gegeben durch $B^a = g^{ab} = A^b$.
Falls $G = \mathbb{F}_p^\times$, so lautet das Diffie-Hellman-Problem: Kann man aus der Kenntnis von p, der Primitivwurzel g und den Elementen A und B den gemeinsamen Schlüssel g^{ab} berechnen?
Offensichtlich kann man das Diffie-Hellman-Problem lösen, wenn man das DL-Problem lösen in $\mathbb{F}_p^\times$ kann. Offen ist, ob man das Diffie-Hellman-Problem lösen kann, ohne das DL-Problem zu lösen.

3.1.3 ElGamal-Verfahren

Dies ist ein weiteres asymmetrisches Verfahren. Während RSA auf dem Faktorisierungsproblem beruht, beruhen ElGamal-Verfahren auf dem DL-Problem. Die Sicherheit hängt hier entscheidend von der Wahl der Gruppe G ab.

1. Es sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n < \infty$.
2. Man wähle eine Zahl $a \in \{0, \ldots, n-1\}$ und berechne $A = g^a$.

3. Veröffentliche (G, g, A) und halte a geheim.

4. Verschlüsselung: Es sei $m \in G$ ein Klartext, den wir verschlüsseln wollen. Man wähle dazu $b \in \{0, \ldots, n-1\}$ und berechne $B = g^b$ und $c = A^b m$. Der Cyphertext ist dann das Paar (B, c).

5. Entschlüsselung: Aus dem Paar (B, c) berechne man c/B^a.

Offensichtlich kann man ein ElGamal-Verfahren knacken, wenn man das DL-Problem in G lösen kann.

4 Faktorisierungsmethoden

Wir erinnern an die "groß O" Notation. Seien $f(x)$ und $g(x)$ Funktionen von $x \in \mathbb{R}$ mit Werten in $\mathbb{R}_{>0}$. Dann schreibt man $f = O(g)$, falls es Konstanten $c, C \in \mathbb{R}_{>0}$ gibt mit

$$f(x) \leq cg(x) \text{ für alle } x \geq C.$$

Die Probedivision ist ein Verfahren mit Laufzeit $O(\sqrt{N})$, falls N die zu faktorisierende Zahl ist. Man beachte das dies eine exponentielle Laufzeit in der Länge der Eingangsdaten ist, die ein $O(\log(N))$ sind.

4.1 Pollards rho-Methode

Anhand Pollards ρ-Methode wollen wir exemplarisch die Laufzeit eines Verfahrens analysieren. Sei N gegeben und es sei bekannt, dass N zusammengesetzt ist.
Man wähle nun eine polynomiale Abbildung

$$f \colon \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z},$$

etwa $f(x) = x^2 + 1$. Weiter wähle man $x_0 \in \mathbb{Z}/N\mathbb{Z}$ und berechne iterativ $x_1, x_2, \ldots$ mittels der Vorschrift $x_{j+1} = f(x_j)$. Nach jedem Schritt berechne man $\mathrm{ggT}(x_j - x_k, N)$ für $k = 0, \ldots, j-1$, in der Hoffnung einen nicht-trivialen Teiler zu finden.
Sei r ein nicht-trivialer Teiler von N. In den folgenden Sätzen wird die Zeit abgeschätzt, bis wir mit "großer Wahrscheinlichkeit" den Teiler r von N gefunden haben.

Satz 4.1.1 *Sei S eine r-elementige Menge. Sei $f \colon S \longrightarrow S$ eine Funktion, $x_0 \in S$, $x_{j+1} = f(x_j)$, $j \geq 0$. Sei $\lambda \in \mathbb{R}_{>0}$ und $l := 1 + [\sqrt{2\lambda r}]$. Dann ist die Anzahl der Paare (f, x_0), so dass $x_0, \ldots, x_l$ paarweise verschieden sind, kleiner* $\exp(-\lambda)$.

Satz 4.1.2 *Sei N eine zusammengesetzte Zahl und r ein nicht-trivialer Teiler von N. Dann findet die ρ-Methode den Faktor r in $O(\sqrt[4]{N}(\log(N))^3)$ Bit-Operationen mit großer Wahrscheinlichkeit. Genauer: Es gibt eine Konstante C, so dass für jedes $\lambda \in \mathbb{R}_{>0}$ die Wahrscheinlichkeit, dass die ρ-Methode keinen echten Teiler in $C\sqrt{\lambda}\sqrt[4]{N}\log(N)^3$ Bit-Operationen findet, kleiner als* $\exp(-\lambda)$ *ist.*

4.2 Fermatfaktorisierung und Faktorbasen

Satz 4.2.1 *Sei N eine ungerade natürliche Zahl. Dann gibt es eine $1-1$-Korrespondenz zwischen den Faktorisierungen $N = ab$ mit $a \geq b \geq 0$ und Darstellungen von N von der Form $N = t^2 - s^2$ mit $s, t \geq 0$. Die Korrespondenz ist gegeben durch*

$$t = \frac{a+b}{2}, s = \frac{a-b}{2}, \qquad a = t + s, b = t - s.$$

Man kann also folgende Strategie versuchen. Für $t \geq [\sqrt{N}]$ teste man, ob $t^2 - N$ ein Quadrat ist. Falls ja, so setze $s := \sqrt{t^2 - N}$. Man erhält die Teiler $a = t + s$ und $b = t - s$.
Wir betrachten die folgende Verallgemeinerung. Es gelten für $s, t \in \mathbb{Z}$ die Kongruenzen

$$t^2 \equiv s^2 \pmod{N}, \qquad t \not\equiv \pm s \pmod{N}. \tag{2}$$

Dann gilt $\mathrm{ggT}(t+s, N) > 1$ oder $\mathrm{ggT}(t-s, N) > 1$. Beide ggT's sind ungleich N. Wir finden also einen echten Teiler.
Die besten Faktorisierungsmethoden beruhen darauf, Zahlen s und t mit (2) zu konstruieren.

Definition 4.2.2 Eine Faktorbasis ist eine Menge $B = \{p_1, p_2, \ldots, p_h\}$ von Primzahlen, mit der Ausnahme, dass wir auch $p_1 = -1$ erlauben. Eine Zahl $b \in \mathbb{Z}$ heißt B-glatte Zahl, falls $b^2 \equiv z \pmod{N}$ mit einer ganzen Zahl z, die über B faktorisiert, d.h.

$$z = \prod_{p \in B} p^{\alpha_p}, \quad \alpha_p \in \mathbb{N}_0.$$

Seien nun $b_1, \ldots, b_m$ B-glatte Zahlen. Falls $b_i^2 \equiv \prod_{j=1}^{h} p_j^{\alpha_{ij}} =: a_i$, so ordnen wir b_i den Zeilenvektor $\epsilon_i := (\alpha_{ij} \pmod 2)_{j=1,\ldots,h} \in \mathbb{F}_2^h$ zu. Falls nun für geeignete Zeilen $i \in I$ die Beziehung

$$\sum_{i \in I} \epsilon_i = 0$$

gilt, so gilt nach Konstruktion

$$\left(\prod_{i \in I} b_i\right)^2 \equiv \left(\prod_{j=1}^{h} p_j^{\sum_{i \in I} \alpha_{ij}/2}\right)^2 \pmod{N}.$$

Wir setzen daher

$$s := \prod_{i \in I} b_i \text{ und } t := \prod_{j=1}^{h} p_j^{\sum_{i \in I} \alpha_{ij}/2}.$$

Natürlich kann es passieren, dass $t \equiv s \pmod{N}$ oder $t \equiv -s \pmod{N}$ gilt. Andernfalls finden wir einen echten Teiler durch Berechnung von $\mathrm{ggT}(s \pm t, N)$.
Wir verfogen also die folgende Strategie: Finde viele B-glatte Zahlen, löse dann das resultierende lineare Gleichungssystem über $\mathbb{F}_2$. Jede nicht-triviale Lösung liefert Zahlen s und t, und damit eventuell einen Teiler von N.
Im Weiteren wollen wir Verfahren kennen lernen, mit denen man effizient viele B-glatte Zahlen produzieren kann.

4.3 Das quadratische Sieb

Definition 4.3.1 Sei p eine Primzahl. Dann definiert man für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, p) = 1$ das Legendresymbol $\left(\frac{a}{p}\right)$ durch

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } a \text{ ein Quadrat modulo } p \text{ ist,} \\ -1, & \text{sonst.} \end{cases}$$

Sei nun $P \in \mathbb{N}$ eine geeignete Schranke und

$$B = \left\{ p \text{ Pz.} \mid p < P, \left(\frac{a}{p}\right) = +1 \right\}$$

eine fixierte Faktorbasis. Wir suchen nun für geeignetes $A \in \mathbb{N}$ in der Menge

$$S = \{t^2 - N \mid [\sqrt{N}] + 1 \leq t \leq [\sqrt{N}] + A\}$$

nach B-glatten Zahlen. Dabei werden wir spaltenweise vorgehen.

Lemma 4.3.2 *Sei $p \neq 2$ eine Primzahl und für $a \in \mathbb{Z}$ gelte* $\mathrm{ggT}(a, p) = 1$ *und* $\left(\frac{a}{p}\right) = +1$. *Dann hat die Kongruenz*

$$x^2 \equiv a \pmod{p^\alpha}$$

für alle $\alpha > 0$ genau zwei Lösungen. Diese lassen sich induktiv berechnen.

Das Lemma stellt einen Spezialfall des Henselschen Lemmas dar.
Im Rahmen der Vorlesung wurde das quadratische Sieb anhand eines Beispiels vorgestellt.

4.4 Die $(p-1)$-Faktorisierungsmethode

Sei p ein Primteiler von N und $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Wir wollen $k \in \mathbb{N}$ konstruieren, so dass gilt

$$a^k \equiv 1 \pmod{p}, \quad a^k \not\equiv 1 \pmod{N}.$$

Dann liefert $\mathrm{ggT}(a^k - 1, N)$ einen nicht-trivialen Teiler von N.
Aufgrund des kleinen Satzes von Fermat muss k die Bedingung $(p-1) \mid k$ erfüllen. Falls also $p - 1 = \prod_{i=1} q_i^{e_i}$ die Primzahlzerlegung von $p-1$ ist, so muss k durch jedes $q_i^{e_i}$ teilbar sein. Das legt folgende Vorgehensweise nahe. Wähle eine Schranke B. Sei $\alpha(q, B) \in \mathbb{N}$ maximal, so dass $q^{\alpha(q,B)} \leq B$ gilt. Setze dann

$$k := \prod_{q<B} q^{\alpha(q,B)}.$$

Falls alle Primpotenzfaktoren von $p-1$ kleiner gleich B sind, so folgt $p - 1 \mid k$.

4.5 Die $(p+1)$-Faktorisierungsmethode

Satz 4.5.1 *Sei K ein Körper und $D \in K^\times \setminus (K^\times)^2$. Dann ist*

$$K(\sqrt{D}) := \{a + b\sqrt{D} \mid a, b \in K\}$$

ein Körper vom Grad 2 über K.

Für $K = \mathbb{F}_p$ ist $\mathbb{F}_p(\sqrt{D})$ unabhängig von der Wahl von $D \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2$. Wir schreiben $\mathbb{F}_{p^2}$ für diesen eindeutig bestimmten Körper.

Satz 4.5.2 *Sei p eine ungerade Primzahl. Dann ist*

$$\sigma_p \colon \mathbb{F}_{p^2} \longrightarrow \mathbb{F}_{p^2}, \quad \alpha \mapsto \alpha^p$$

ein Körperisomorphismus mit $\sigma_p^2 = \mathrm{id}$. Ferner gilt:

$$(a) \qquad \sigma_p(a + b\sqrt{D}) = a - b\sqrt{D}.$$
$$(b) \qquad \sigma_p(\alpha) = \alpha \iff \alpha \in \mathbb{F}_p.$$

Wir betrachten nun die Normabbildung

$$N \colon \mathbb{F}_{p^2} \longrightarrow \mathbb{F}_p, \quad \alpha \mapsto \alpha\sigma_p(\alpha) = \alpha^{p+1}.$$

Es gilt $N(\alpha\beta) = N(\alpha)N(\beta)$ und $N(a + b\sqrt{D}) = a^2 - b^2 D$.

Satz 4.5.3 *Sei $p \neq 2$ eine Primzahl. Dann ist der Gruppenhomomorphismus $N : \mathbb{F}_{p^2}^\times \longrightarrow \mathbb{F}_p^\times$ surjektiv und*

$$\ker(N) = \{\alpha \in \mathbb{F}_{p^2}^\times \mid N(\alpha) = 1\}$$

ist eine zyklische Untergruppe von $\mathbb{F}_{p^2}^\times$ der Ordnung $p+1$.

Für die $(p+1)$-Faktorisierungsmethode sei D eine zu N teilerfremde natürliche Zahl und p ein Teiler von N. Wir betrachten wir nun den Ring

$$R_{N,D} := \mathbb{Z}/N\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}/N\mathbb{Z}\}.$$

Sei $U_1(R_{N,D})$ die Untergruppe von $R_{N,D}^\times$ der Elemente der Norm 1, d.h.

$$U_1(R_{N,D}) := \{a + b\sqrt{D} \mid a^2 - b^2 D \equiv 1 \pmod{N}\}.$$

Man beachte: In dieser Notation gilt $R_{p,D} = \mathbb{F}_{p^2}$ für alle $D \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2$.
Wir haben nun einen kanonischen Gruppenhomomorphismus

$$\pi_p \colon U_1(R_{N,D}) \longrightarrow U_1(R_{p,D})$$

und wir suchen im Folgenden $k \in \mathbb{N}$ und $\xi \in U_1(R_{N,D})$ mit den Eigenschaften

$$\xi^k \neq 1 \text{ und } \pi_p(\xi^k) = 1.$$

Dann folgt mit $\xi^k = a + b\sqrt{D}$, $a, b \in \mathbb{Z}/N\mathbb{Z}$,

$$a \not\equiv 1 \pmod{N}, \quad a \equiv 1 \pmod{p}.$$

Also ist $\mathrm{ggT}(a-1, N)$ ein nicht-trivialer Teiler von N.
Zur Wahl von k: Für $D \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2$ hat $U_1(R_{p,D})$ nach Satz 4.5.3 die Ordnung $p+1$. Sei also $p+1 = \prod_{i=1}^r q_i^{e_i}$ die Primzahlzerlegung von $p+1$. Wir gehen dann wie in der $(p-1)$-Methode vor.

Zur Wahl von ξ: Wir setzen für $1 \leq a < N$ mit $\mathrm{ggT}(a, N) = 1$

$$D := a^2 - 1, \quad \xi := a + \sqrt{D}.$$

Dann gilt: $N(\xi) = a^2 - D = 1$. Ferner gilt mit Wahrscheinlichkeit $1/2$, das D kein Quadrat modulo p ist.

4.6 Kettenbrüche

Definition 4.6.1 Für $x_1, \ldots, x_n \in \mathbb{R}_{>0}$ setzen wir

$$[x_1, ..., x_n] \coloneqq x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\ddots \cfrac{1}{x_{n-1} + \cfrac{1}{x_n}}}}}$$

So ist zum Beispiel

$$[1, 2, 3] = 1 + \frac{1}{2 + \frac{1}{3}} = \frac{10}{7}.$$

Satz 4.6.2 *Eine Zahl $x \in \mathbb{R}_{>0}$ hat genau dann eine endliche Kettenbruchentwicklung, wenn x rational ist.*

Ab jetzt sei $x \in \mathbb{R}_{>0} \setminus \mathbb{Q}$. Wir wollen eine Folge $(a_i)_{i=1,2,\dots}$ mit $a_i \in \mathbb{N}$ konstruieren, so dass gilt:

$$x = \lim_{n\to\infty} [a_1, \dots, a_n].$$

Setze dazu: $a_1 := [x], x_1 := x$ und bestimme x_2, so dass gilt $x = x_1 = a_1 + \frac{1}{x_2}$. Wir definieren die a_i induktiv. Seien

$$a_1, \dots, a_{n-1}, x_1, \dots, x_n$$

bereits gefunden. Dann setzen wir $a_n := [x_n]$ und bestimmen x_{n+1}, so dass $x = [a_1, \dots, a_n, x_{n+1}]$, d.h. $x_n = a_n + \frac{1}{x_{n+1}}$.

Definition 4.6.3 Die Folge der Zahlen $(a_i)_{i=1,2,\dots}$ heißt Kettenbruchentwicklung von x. Die rationale Zahl $r_n := [a_1, \dots, a_n]$ heißt n-ter Näherungsbruch von x.

Satz 4.6.4 $\lim_{n\to\infty} r_n = x$.

Im Beweis definieren wir rekursiv Folgen natürlicher Zahlen (p_i) und (q_i):

$$p_0 := 1, p_1 := a_1, p_i := a_i p_{i-1} + p_{i-2} \text{ für } 2 \le i,$$
$$q_0 := 0, q_1 := 1, q_i := a_i q_{i-1} + q_{i-2} \text{ für } 2 \le i,$$

Beide Folgen sind streng monoton wachsend und für $n \ge 1$ gelten die folgenden Aussagen.

$$(a) \qquad r_n = \frac{p_n}{q_n},$$
$$(b) \qquad x = \frac{p_n x_{n+1} + p_{n-1}}{q_n x_{n+1} + q_{n-1}},$$
$$(c) \qquad \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2},$$
$$(d) \qquad q_n p_{n-1} - q_{n-1} p_n = (-1)^{n+1},$$
$$(e) \qquad r_{2n} < x < r_{2n+1},$$
$$(f) \qquad \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^n}{q_n q_{n-1}}.$$

Umgekehrt konvergiert jeder Kettenbruch natürlicher Zahlen gegen eine reelle Zahl $x > 0$. Genauer:

Satz 4.6.5 *Sei $(a_i)_{i\in\mathbb{N}}$ eine Folge natürlicher Zahlen. Dann konvergiert die Folge $r_n := [a_1, \dots, a_n]$ gegen eine reelle Zahl $x > 0$.*

Definition 4.6.6 Sei $x = \lim_{n\to\infty}[a_1, \dots, a_n]$ eine Kettenbruchentwicklung. Dann heißt die Kettenbruchentwicklung periodisch, falls es ein $n_0 \in \mathbb{N}$ und ein $k \in \mathbb{N}$ gibt, so dass für alle $n \ge n_0$ gilt:

$$a_{n+k} = a_n.$$

Die Kettenbruchentwicklung heißt rein periodisch, wenn man $n_0 = 1$ wählen kann.

Definition 4.6.7 Eine Zahl $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ heißt quadratische Irrationalzahl, falls es ein Polynom

$$f(x) = ax^2 - bx - c \in \mathbb{Z}[x] \text{ mit } \mathrm{ggT}(a, b, c) = 1, a > 0,$$

mit $f(\alpha) = 0$ gibt. Die Zahl $D := b^2 + 4ac$ nennt man die Diskriminante von α.

Die Diskriminante D ist durch α eindeutig bestimmt. Ferner ist $D > 0$ und kein Quadrat in $\mathbb{Q}$. Den folgenden Satz werden wir in der Vorlesung nicht beweisen, er sei jedoch der Vollständigkeit halber hier aufgeführt.

Satz 4.6.8 *Eine Zahl $x \in \mathbb{R}_{>1} \setminus \mathbb{Q}$ hat genau dann eine priodische Kettenbruchentwicklung, wenn x eine quadratische Irrationalzahl ist.*

4.7 Bestmögliche Approxination durch Kettenbrüche

Satz 4.7.1 *Sei $x \in \mathbb{R}_{>1} \setminus \mathbb{Q}$ und $n > 1$. Es seien $p, q \in \mathbb{N}$ teilerfremd und es gelte*

$$0 < q \leq q_n, \quad \frac{p}{q} \neq \frac{p_n}{q_n}.$$

Dann gilt: $|p_n - xq_n| < |p - xq|$.

Folgerung 4.7.2 *Mit den Voraussetzungen von Satz 4.7.1 gilt:*

$$\left|\frac{p_n}{q_n} - x\right| < \left|\frac{p}{q} - x\right|.$$

4.8 Der Kettenbruch-Faktorisierungsalgorithmus

Zur Erinnerung: Sei B eine Faktorbasis und N eine zu faktorisierende Zahl. Dann suchen wir B-glatte Zahlen b, d.h. ganze Zahlen b, so dass $b^2 \bmod N$ über der Faktorbasis B faktorisiert. Grundlage für den Kettenbruch-Faktorisierungsalgorithmus sind der folgende Satz und sein Korollar.

Satz 4.8.1 *Sei $x \in \mathbb{R}_{>1} \setminus \mathbb{Q}$. Dann gilt für $n \geq 1$*

$$\left|p_n^2 - x^2 q_n^2\right| < 2x.$$

Folgerung 4.8.2 *Sei $N \in \mathbb{N}$. Dann gilt für alle $k \in \mathbb{N}$, so dass auch kN kein Quadrat ist,*

$$\left|p_n^2 \bmod N\right| < 2\sqrt{kN}.$$

Wir berechnen also für $k = 1, 2, 3, \ldots$ die Kettenbruchentwicklung $[a_1, a_2, \ldots, a_n]$ von $\sqrt{kN}$ für $n \leq$ einer geeigneten Schranke und suchen unter den p_n nach B-glatten Zahlen. Man beachte, das man bei der berechnung der p_n gemäß der Rekursionsformel $p_{n+1} = a_{n+1}p_n + p_{n-1}$ stets modulo N rechnen kann.

5 Diskrete Logarithmen

Sei $G = \langle\gamma\rangle$ eine endliche zyklische Gruppe der Ordnung $n = \mathrm{ord}(\gamma)$. Sei $\alpha \in G$. Dann gibt es genau eine ganze Zahl x mit $0 \leq x < n$ mit $\alpha = \gamma^x$. Wir setzen $\log_\gamma(\alpha) := x$ und wollen im Folgenden diesen diskreten Logarithmus berechen.

5.1 Shanks Baby-Step-Giant-Step-Algorithmus

Setze $m := \lceil\sqrt{n}\rceil$ und schreibe

$$x = qm + r \text{ mit } 0 \leq r < m.$$

Berechne dann zunächst die Baby-Steps

$$B = \{(\alpha\gamma^{-r} \mid 0 \leq r < m\}.$$

Falls es ein Paar $(1, r)$ in B gibt, so ist $x = r$. Andernfalls setzt man $\delta := \gamma^m$ und testet für $q = 1, 2, \ldots$, ob es ein r mit $(\delta^q, r) \in B$ gibt. Dazu muss man B abspeichern und braucht für jedes q $O(m)$ Vergleiche. Falls wir ein Tupel $(\delta^q, r) \in B$ finden, so ist $x = mq + r$.
Die Berechnung der δ^q nennt man die Giant-Steps.
Das Problem bei Shanks Baby-Step-Giant-Step-Algortihmus ist der hohe Speicherbedarf und die größe Anzahl von Vergleichen. Beides ist von der Größenordnung $O(\sqrt{n})$.

5.2 Pollards ρ-Methode

Wir schreiben

$$G = G_1 \cup G_2 \cup G_3$$

mit paarweise disjunkten, nicht-leeren Teilmengen G_i von G. Wir definieren eine Funktion $f\colon G \longrightarrow G$ durch

$$f(\beta) := \begin{cases} \gamma\beta, & \text{falls } \beta \in G_1, \\ \beta^2, & \text{falls } \beta \in G_2, \\ \alpha\beta, & \text{falls } \beta \in G_3. \end{cases}$$

Wähle sodann $x_0 \in \{1, \ldots, n\}$ und setze $\beta_0 := \gamma^{x_0}$. Wir berechnen nun rekursiv eine Folge $(\beta_i)_{i \in \mathbb{N}_0}$ gemäß

$$\beta_{i+1} := f(\beta_i).$$

Schreibe jeweils $\beta_i = \gamma^{x_i}\alpha^{y_i}$, wobei wir die Exponenten stets modulo n reduzieren. Für $i = 0$ ist also x_0 der gewählte Startwert und $y_0 = 0$. Wir erhalten

$$x_{i+1} = \begin{cases} x_i + 1, & \text{falls } \beta_i \in G_1, \\ 2x_i, & \text{falls } \beta_i \in G_2, \\ x_i, & \text{falls } \beta_i \in G_3, \end{cases}$$

und

$$y_{i+1} = \begin{cases} y_i, & \text{falls } \beta_i \in G_1, \\ 2y_i, & \text{falls } \beta_i \in G_2, \\ y_i + 1, & \text{falls } \beta_i \in G_3. \end{cases}$$

Da G endlich ist, gibt es $i \neq j$ mit $\beta_i = \beta_j$. Dies liefert die Kongruenz

$$x_i - x_j \equiv x(y_j - y_i) \pmod{n}.$$

Diese Kongruenz wird im Allgemeinen mehrere Lösungen haben. Aus diesen hoffentlich wenigen Lösungen kann man den gesuchten diskreten Logarithmus durch Ausprobieren isolieren.
Wir nehme im Folgenden an, dass sich die Folge der β_i wie eine zufällig gewählte Folge verhält. Dann zeigt das Geburtstagsparadox, dass man $O(\sqrt{n})$ Folgenglieder β_i berechnen muss, um mit Wahrscheinlichkeit größer als $1/2$ Indizes $i \neq j$ mit $\beta_i = \beta_j$ zu finden.
In der bislang beschriebenen Form braucht der Algorithmus Speicher für $O(\sqrt{n})$ Tripel der Form (β_i, x_i, y_i). Tatsächlich genügt es jedoch ein Tripel zu speichern. Zu Beginn speichert man dazu (β_1, x_1, y_1). Wir gehen dann induktiv vor und nehmen an, dass gerade das Tripel (β_i, x_i, y_i) im Speicher ist. Dann berechnen wir für $j = i{+}1, i{+}2, \ldots$ jeweils das Tripel (β_j, x_j, y_j) bis wir entweder ein j mit $\beta_i = \beta_j$ finden oder $j = 2i$ ist. In diesem Fall speichern wir das Tripel $(\beta_{2i}, x_{2i}, y_{2i})$ ab und beginnen von neuem.

5.3 Der Pohlig-Hellman-Algorithmus

Sei

$$n = |G| = \prod_{p|n} p^{e_p}$$

die Primzahlzerlegung der Gruppenordnung. Wir setzen

$$n_p := n/p^{e_p}, \quad \gamma_p := \gamma^{n_p}, \quad , \alpha_p := \alpha^{n_p}.$$

Dann hat γ_p die Ordnung p^{e_p} und es gilt $\alpha_p = \gamma_p^x$ für $x = \log_\gamma(\alpha)$.

Satz 5.3.1 *Sei $x_p = \log_{\gamma_p}(\alpha_p)$. Sei x eine Lösung der simultanen Kongruenzen*

$$x \equiv x_p \pmod{p^{e_p}}, \forall p \mid n.$$

Dann gilt $\gamma^x = \alpha$, d.h. $x = \log_\gamma(\alpha)$.

Das offensichtliche Problem hierbei ist, dass die Gruppenordnung faktorisiert werden muss.
Wir haben also nun das allgemeine DL-Problem auf DL-Probleme in Gruppen von Primzahlpotenzordnung zurückgeführt. Als nächstes verfolgen wir das Ziel, die Berechnung dieser diskreten Logarithmen auf die Berechnung in diskreter Logarithmen in Gruppen von Primzahlordnung zurückzuführen.
Sei dazu $|G| = p^e$ mit einer Primzahl p. Zu $\alpha \in G$ wollen wir x mit $\gamma^x = \alpha$ und $0 \leq x < p^e$ bestimmen. Dazu schreiben wir

$$x = x_0 + x_1 p + \ldots + x_{e-1} p^{e-1} \text{ mit } 0 \leq x_i < p.$$

Zur Bestimmung von x_0 löse man das DL-Problem $\alpha^{p^{e-1}} = \left(\gamma^{p^{e-1}}\right)^{x_0}$. Dies ist ein DL-Problem in der Gruppe $\langle \gamma^{p^{e-1}} \rangle$, welche von der Ordnung p ist.
Wir bestimmen nun induktiv die weiteren x_i. Seien $x_0, \ldots, x_{i-1}$ bereits berechnet. Löse dann in $\langle \gamma^{p^{e-1}} \rangle$ das DL-Problem $\alpha_i = \left(\gamma^{p^{e-1}}\right)^{x_i}$ mit

$$\alpha_i := \alpha^{p^{e-i-1}} \gamma^{-(x_0 + \ldots + x_{i-1} p^{i-1}) p^{e-i-1}}.$$

Satz 5.3.2 *Der Pohlig-Hellman-Algorithmus berechnet das diskrete Logarithmenproblem unter Verwendung von*

$$O\left(\sum_{p|n} e_p(\log|G| + \sqrt{p}) + (\log|G|)^2\right)$$

Gruppenoperationen.

Falls also der größte Primteiler von $|G|$ klein ist, so bietet der Pohlig-Hellman-Algorithmus eine relative gute Möglichkeit zur Lösung des diskreten Logarithmenproblems.

5.4 Index-Calculus

Sei $G = \mathbb{F}_p^\times$ mit einer Primzahl p. Sei g eine Primitivwurzel, also $\mathbb{F}_p^\times = \langle g \rangle$. Für $a \in \mathbb{Z}$ mit $p \nmid a$ suchen wir eine eine Lösung x der Kongruenz $g^x \equiv a \pmod{p}$.
Sei dazu $S \in \mathbb{N}$ geeignet und

$$B = \{q \mid q \text{ Primzahl}, q \leq S\}$$

eine Faktorbasis. Wir gehen nun in zwei Schritten vor.

Schritt 1: Löse für alle $q \in B$ das diskrete Logarithmenproblem

$$g^{x_q} \equiv q \pmod{p}.$$

Schritt 2: Finde $y \in \{1, \ldots, p-1\}$, so dass ag^y über B faktorisiert, d.h.

$$ag^y \equiv \prod_{q \in B} q^{e_q}.$$

Dann folgt $x \equiv \left(\sum_{q \in B} x_q e_q\right) - y \pmod{p-1}$.
Um den ersten Schritt zu bewerkstelligen, sucht man genügend viele Relationen der Form

$$g^z \equiv \prod_{q \in B} q^{f(q,z)} \pmod{p}$$

mit $z \in \{1, \ldots, p-1\}$. Dann folgt

$$z \equiv \sum_{q \in B} f(q,z) x_q \pmod{p}.$$

Jede Relation liefert also eine Kongruenz und die gesuchten x_q sind die Lösung eines linearen Gleichungssystems modulo $p-1$.

Hinweis: Die Teile der letzten Vorlesung zur $p \pm 1$ Faktorisierung sind in den Abschnitt über Faktorisierungsalgorithmen eingefügt.