“Algorithmische Zahlentheorie mit Anwendungen in der Kryptographie”

Vorlesung 1
Euklidischer Algorithmus

Der euklidische Algorithmus ist ein Verfahren zur Bestimmung des größten gemeinsamen Teilers (a, b) zweier natürlicher Zahlen a und b. Er ist einer der ältesten bekannten Algorithmen der Welt, benannt nach dem griechischen Mathematiker Euklid, der ihn um 300 v. Chr. in seinem Werk “Die Elemente” angegeben hat. Der Algorithmus kommt ohne die Kenntnis der Primfaktorzerlegung der Zahlen a und b aus.

1.1. Satz (Euklidischer Algorithmus). Seien a und b zwei natürliche Zahlen. Setzen wir $a_0 = a$ und $a_1 = b$ und werden entsprechend das folgende Schema a_i durch a_{i+1} teilen und Reste a_{i+2} finden. Wir stoppen nur dann, wenn wir 0 als Rest bekommen[1].

$$\begin{cases} a_0 = a_1 q_1 + a_2, & 0 < a_2 < a_1, \\ a_1 = a_2 q_2 + a_3, & 0 < a_3 < a_2, \\ \dots & \\ a_{n-2} = a_{n-1} q_{n-1} + a_n, & 0 < a_n < a_{n-1}, \\ a_{n-1} = a_n q_n + \mathbf{0}. & \end{cases}$$

Dann ist $(a, b) = a_n$. Dabei gibt es (insbesondere) zwei ganze Zahlen u, v mit

$$ua + vb = (a, b).$$

Die Zahlen u, v kann man mit Hilfe dieses Schemas bekommen.

1.2. Folgerung. Seien a und n zwei teilerfremde Zahlen. Dann gibt es solche ganze Zahl u, daß $au \equiv 1 \,(\mathrm{mod}\, n)$ gilt.

1.3. Beispiel. Berechnen wir $(50, 22)$:

$$\begin{cases} \mathbf{50} = 2 \cdot \mathbf{22} + \mathbf{6}, \\ \mathbf{22} = 3 \cdot \mathbf{6} + \mathbf{4}, \\ \mathbf{6} = 1 \cdot \mathbf{4} + \mathbf{2}, \\ \mathbf{4} = 2 \cdot \mathbf{2} + \mathbf{0}. \end{cases}$$

So ist $(50, 22) = 2$. Jetzt ermitteln wir nach diesem Schema die ganzen Zahlen u, v so, daß $50u + 22v = (50, 22)$ gilt:

$$\mathbf{2} = \mathbf{6} - 1 \cdot \mathbf{4} = \mathbf{6} - 1 \cdot (\mathbf{22} - 3 \cdot \mathbf{6}) = 4 \cdot \mathbf{6} - 1 \cdot \mathbf{22}$$

[1] **Ausführlich:** Erst teilen wir a_0 durch a_1 und finden den Rest a_2, wobei $0 \leqslant a_2 < a_1$ ist. Wenn $a_2 = 0$ ist, stoppen wir. Wenn $a_2 > 0$ ist, setzen wir fort: wir teilen a_1 durch a_2 und finden den Rest a_3, wobei $0 \leqslant a_3 < a_2$ ist. Und so weiter.

$$= 4 \cdot (\mathbf{50} - 2 \cdot \mathbf{22}) - 1 \cdot \mathbf{22} = 4 \cdot \mathbf{50} - 9 \cdot \mathbf{22}.$$

Also, $u = 4$, $v = -9$.

LAUFZEITANALYSE.

Mit dem euklidischen Algorithmus kann man (a, b) mit verhaltnismaäßig geringem Aufwand (im Vergleich zur Berechnung der Primfaktorzerlegung) die Zahlen a und b berechnen. Bei der Laufzeitanalyse stellt sich interessanterweise heraus, daß der schlimmste Eingabefall zwei aufeinander folgende Fibonacci-Zahlen sind. Die *Fibonacci-Zahlen* definiert man per Induktion: $F_1 = F_2 = 1$, $F_{i+2} = F_{i+1} + F_i$. Hier sind die ersten 10 Fibonacci-Zahlen:

i	1	2	3	4	5	6	7	8	9	10
F_i	1	1	2	3	5	8	13	21	34	55

1.4. Beispiel. Berechnen wir (F_9, F_{10}) mit dem euklidischen Algorithmus:

$$\begin{cases} \mathbf{55} = 1 \cdot \mathbf{34} + \mathbf{21}, \\ \mathbf{34} = 1 \cdot \mathbf{21} + \mathbf{13}, \\ \mathbf{21} = 1 \cdot \mathbf{13} + \mathbf{8}, \\ \mathbf{13} = 1 \cdot \mathbf{8} + \mathbf{5}, \\ \mathbf{8} = 1 \cdot \mathbf{5} + \mathbf{3}, \\ \mathbf{5} = 1 \cdot \mathbf{3} + \mathbf{2}, \\ \mathbf{3} = 1 \cdot \mathbf{2} + \mathbf{1}, \\ \mathbf{1} = 1 \cdot \mathbf{1} + \mathbf{0}. \end{cases}$$

So ist $(F_9, F_{10}) = 1$. Außerdem sehen wir, daß die Zahl der Divisionen in diesem Beispiel zweimal größer ist als die Zahl der Divisionen in dem Beispiel 1.3.

Unser Ziel ist ein Satz von Lamé beweisen, in dem die Zahl der Divisionen in dem euklidischen Algorithmus eingeschätzt ist. Vorher werden wir das folgende Lemma beweisen.

1.5. Lemma. Für $n \geqslant 2$ gilt es $F_{n+5} > 10F_n$.

Beweis. $F_{n+5} = F_{n+4} + F_{n+3} = 2F_{n+3} + F_{n+2} = 3F_{n+2} + 2F_{n+1} = 5F_{n+1} + 3F_n = 8F_n + 5F_{n-1} > 8F_n + 4F_{n-1} \geqslant 8F_n + 2F_n = 10F_n$. Die letzte Ungleichung folgt aus der Formel $2F_{n-1} \geqslant F_{n-1} + F_{n-2} = F_n$. □

1.6. Satz von Lamé. Seien a und b natürliche Zahlen, $a > b > 0$. Dann ist die Zahl der Divisionen in dem euklidischen Algorithmus nicht größer als $5k$, wobei k die Anzahl der Ziffern in dezimaler Darstellung der Zahl b ist.

Beweis. Aus dem Schema des euklidisches Algorithmus folgt es $a_n \geqslant 1 = F_2$ und $a_{n-1} > a_n \geqslant 1$. Dann ist $a_{n-1} \geqslant 2 = F_3$. Folglich ist $a_{n-2} \geqslant a_{n-1}q_{n-1} + a_n \geqslant a_{n-1} + a_n \geqslant F_2 + F_3 = F_4$. Setzen wir so fort und bekommen $b = a_1 \geqslant F_{n+1}$. Angenommen $n > 5k$, bekommen wir $b \geqslant F_{5k+2} > 10^k F_2 = 10^k$ – das ist ein Widerspruch! □

1.7. Aufgabe. 1) Beweisen Sie, daß F_{kl} durch F_k teilbar ist. Aus diesem wird folgen: Ist F_n eine Primzahl, so ist n eine Primzahl oder $n = 4$. Bemerkung: $F_4 = 3$ ist durch $F_2 = 1$ teilbar.

2) Finden Sie die minimale Primzahl $n > 2$ so, daß F_n keine Primzahl ist.

Vorlesung 2
Struktur des Restklassenringes $\mathbb{Z}_m$

2.1. Beispiel. Betrachten wir die Addition und die Multiplikation der minimalen nichtnegativen Reste modulo 4:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Bezeichnen wir $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Nachdem Sie die Definitionen in den folgenden Punkten gelesen haben, ist es nützlich zu verstehen, daß $\mathbb{Z}_4$ bezüglich der Addition eine Gruppe ist, und bezüglich der Multiplikation keine Gruppe ist. Außerdem ist $\mathbb{Z}_4$ mit beiden Verknüpfungen $+$ und $\cdot$ ein Ring.

Sei G eine nichtleere Menge. Eine beliebige Abbildung $\circ : G \times G \to G$ heißt *binäre Verknüpfung auf* G. Mit anderen Worten, $\circ$ ist binäre Verknüpfung auf G, wenn für je zwei Elemente $a, b \in G$ ein Element $a \circ b$ in G erklärt ist. Die binäre Verknüpfung kann man nicht nur mit $\circ$, sondern mit allen anderen Symbolen (zum Beispiel mit $+$ oder mit $\cdot$) bezeichnen. Man schreibt sogar kurz ab statt $a \circ b$.

2.2. Definition der Gruppe. Eine Nichtleere Menge G mit einer binaren Verknüpfung $\circ$ nennt man *Gruppe*, wenn folgende Axiome erfüllt sind:

1) Für alle Elemente $a, b, c \in G$ gilt

$$(a \circ b) \circ c = a \circ (b \circ c)$$

(*Assoziativität*);

2) Existiert ein Element $e \in G$, so daß für alle $a \in G$ gilt

$$a \circ e = e \circ a = a$$

(das Element e heißt *neutrales*);

3) Für jedes Element $a \in G$ existiert ein Element $b \in G$ mit

$$a \circ b = b \circ a = e$$

(das Element b heißt *inverses* zu a und bezeichnet a^{-1}).

Wenn die Verknüpfung als $\cdot$ bezeichnet ist, dann wird das neutrale Element als 1 bezeichnet und das inverse Element zu a wird als a^{-1} bezeichnet. Wenn aber die Verknüpfung als $+$ bezeichnet ist, dann wird das neutrale Element als 0 bezeichnet und das inverse Element zu a wird als $-a$ bezeichnet.

Man kann beweisen, daß jede Gruppe ein einziges neutrales Element hat und für jedes ihrer Elemente gibt es ein einziges inverses Element.

Eine Gruppe heißt *abelsch* oder *kommutativ*, wenn für alle Elemente $a, b \in G$ gilt $ab = ba$.

Zwei Gruppen G und G_1 heißen *isomorph*, wenn ein Isomorphism $\phi : G \to G_1$ existiert. *Isomorphism* von G nach G_1 ist eine biektive Abbildung von G nach G_1 mit der Bedingung, daß für alle zwei Elemente $a, b \in G$ gilt $\phi(ab) = \phi(a)\phi(b)$.

Beispiel. ....

2.3. Definition des Ringes. Eine nichtleere Menge K mit zwei binären Verknüpfungen $+$ und $\cdot$ nennt man *Ring*, wenn folgende Axiome erfüllt sind:

1) K ist eine abelsche Gruppe bezüglich der Verknüpfung $+$:
   a) für alle $a, b, c \in K$ gilt $(a + b) + c = a + (b + c)$;
   b) existiert ein Element $0 \in K$, so daß für alle $a \in G$ gilt $a + 0 = 0 + a = a$;
   c) für jedes Element $a \in K$ existiert ein Element $b \in K$ mit $a + b = b + a = 0$;
   d) $a + b = b + a$;
2) Es gelten linke und rechte Distributivgesetze, d. h. für alle $a, b \in K$ ist:
   e) $a(b + c) = ab + ac$;
   f) $(a + b)c = ab + ac$.

Der Ring heißt *assoziativ*, wenn für alle $a, b, c \in K$ gilt $(ab)c = a(bc)$.

Der Ring heißt *kommutativ*, wenn für alle $a, b \in K$ gilt $ab = ba$.

Ein Element $b \in K$ heißt *Einselelement* von K, wenn für alle $a, b \in K$ gilt $ba = a = ab$. Man kann leicht beweisen, daß K entweder keiner oder nur ein einziges Einselelement enthält. Man bezeichnet das Einselelement als 1.

Sei $(K, +, \cdot)$ ein Ring. Die Gruppe $(K, +)$ heißt *additive Gruppe des Ringes* und wird als K^+ bezeichnet. Das Paar $(K, \cdot)$ ist keine Gruppe[2]. Aber mit zusätzlichen Voraussetzungen kann ein Teil des Ringes K eine Gruppe bezüglich der Verknüpfung $\cdot$ sein.

Sei $(K, +, \cdot)$ ein assoziativer und kommutativer Ring mit Einselelement 1. Bezeichnen wir als K_{inv} die Menge der Elemente aus K, für die inverse Elemente existieren. Dann ist $(K_{inv}, \cdot)$ eine Gruppe. Diese Gruppe heißt *multiplikative Gruppe des Ringes* K und wird als K^* bezeichnet.

Zwei Ringe K und K_1 heißen *isomorph*, wenn ein Isomorphism $\phi : G \to G_1$ existiert. *Isomorphism* von K nach K_1 ist eine biektive Abbildung von K nach K_1 mit der Bedingung, daß für alle zwei Elemente $a, b \in G$ gilt $\phi(a + b) = \phi(a) + \phi(b)$ und $\phi(ab) = \phi(a)\phi(b)$.

Beispiel. ....

2.4. Definition des Restklassenringes $\mathbb{Z}_m$. Seien x und m natürliche Zahlen. Teilen wir x durch m und bekommen einen Rest r, so daß $x = mq + r$, wobei $q, r \in \mathbb{Z}$ und $0 \leqslant r \leqslant m - 1$ ist. Der Rest r wird als $\mathrm{Rest}_m(x)$ bezeichnet. Wenn wir m fixieren und x variieren, bekommen wir die Reste aus der Menge

$$\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}.$$

Definieren wir Addition und Multiplikation auf der Menge mit den folgenden Gesetze:

– die Summe der Elemente i und j ist $\mathrm{Rest}_m(i + j)$;

– das Produkt des Elemente i und j ist $\mathrm{Rest}_m(i \cdot j)$.

[2]Das Element 0 hat kein inverses. Auch andere Elemente können kein inverses haben. Auch die Verknüpfung $\cdot$ kann nicht assoziativ sein.

Es ist leicht nachzuprüfen, daß $\mathbb{Z}_m$ mit der Verknüpfung ein Ring ist. Der Ring heißt *Restklassenring modulo* m. Der Ring ist assoziativ, kommutativ und hat Einselelement 1.

2.5. Definition der kartesischen Summe der Ringe. Seien $K_1, \dots, K_s$ Ringe. Bezeichnen wir

$$K_1 \oplus \dots \oplus K_s = \{(r_1, \dots, r_s) \mid r_i \in K_i \ \forall i\}.$$

Definieren wir auf dieser Menge die Verknüpfungen $+$ und $\cdot$:

$$(r_1, \dots, r_s) + (r'_1, \dots, r'_s) = (r_1 + r'_1, \dots, r_s + r'_s),$$
$$(r_1, \dots, r_s) \cdot (r'_1, \dots, r'_s) = (r_1 \cdot r'_1, \dots, r_s \cdot r'_s).$$

Es ist leicht nachzuprüfen, daß $K_1 \oplus \dots \oplus K_s$ mit diesen Verknüpfungen ein Ring ist. Diesen Ring nennt man *kartesische Summe* der Ringe $K_1, \dots, K_s$.

Sein Neutralelement ist $(0, \dots, 0)$; und sein Einselelement ist $(1, \dots, 1)$, wenn alle K_i das Einselelement haben.

2.6. Satz über die Struktur des Restklassenringes $\mathbb{Z}_m$. Sei $m = m_1 m_2 \dots m_s$, wobei $m_1, m_2, \dots, m_s$ paarweise teilerfremde natürliche Zahlen sind. Dann gilt

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}.$$

Beweis. Sei $0 \leqslant x \leqslant m-1$ ein beliebiges Element von $\mathbb{Z}_m$. Prüfen wir nach, daß die Abbildung $\phi : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$ mit

$$\phi : x \mapsto (\mathrm{Rest}_{m_1}(x), \dots, \mathrm{Rest}_{m_s}(x))$$

ein Isomorphism ist.

1) Prüfen wir nach, daß die Abbildung ϕ injektiv ist. Nehmen wir an, daß es $x, y \in \mathbb{Z}_m$ mit $\mathrm{Rest}_{m_i}(x) = \mathrm{Rest}_{m_i}(y)$ für alle i gibt. Dann ist $x - y$ durch m_i teilbar für alle i. Da die Zahlen $m_1, \dots, m_s$ paarweise teilerfremde sind, ist die Zahl $x - y$ durch ihr Produkt m teilbar. Daher und aus $0 \leqslant x, y \leqslant m-1$ folgt $x = y$.

2) Prüfen wir nach, daß ϕ surjektiv ist. Das folgt aus zwei folgenden Fakten:
- ϕ ist injektiv.
- Die Zahl der Elemente in $\mathbb{Z}_m$ ist gleich der Zahl der Elemente in $\mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$.

3) Prüfen wir nach, daß $\phi(x+y) = \phi(x) + \phi(y)$. Diese Gleichung ist äquivalent dem, daß für alle i gilt

$$\mathrm{Rest}_{m_i}(x+y) = \mathrm{Rest}_{m_i}(\mathrm{Rest}_{m_i}(x) + \mathrm{Rest}_{m_i}(y)).$$

Das gilt, weil

$$(x+y) - (\mathrm{Rest}_{m_i}(x) + \mathrm{Rest}_{m_i}(y))$$

durch m_i teilbar ist.

4) Ähnlich können wir die Gleichung $\phi(xy) = \phi(x)\phi(y)$ nachprüfen. □

Um aus dem Tupel $(x_1, \dots, x_s)$ ein Element x zu konstruieren, wendet man den folgenden Satz an.

2.7. Chinesischer Restklassensatz. Seien $m_1, m_2, \ldots, m_s$ paarweise teilerfremde ganze Zahlen. Dann existiert für jedes Tupel (geordnete Menge) ganzer Zahlen $x_1, x_2, \ldots, x_s$ eine ganze Zahl x, so daß die folgenden Kongruenzen erfüllt sind:

$$\begin{cases} x \equiv x_1 (\bmod m_1), \\ x \equiv x_2 (\bmod m_2), \\ \ldots \\ x \equiv x_s (\bmod m_s). \end{cases}$$

Setzen wir $m = m_1 m_2 \ldots m_s$. Dann findet man eine solche Zahl x mit der Formel:

$$x_0 := \sum_{i=1}^{s} c_i (m/m_i) x_i,$$

wobei c_i ein inverses zu der Zahl m/m_i in dem Restkassenring $\mathbb{Z}_{m_i}$ ist:

$$c_i (m/m_i) \equiv 1 \,(\bmod m_i).$$

Alle anderen x sind diesem x_0 kongruent (mod m).

Beweis. Zuerst bemerken wir, daß für alle verschiedenen Zahlen i und j die Zahl m/m_i durch m_j teilbar ist. Dann haben wir

$$\begin{aligned} c_i (m/m_i) x_i &\equiv 0 \ \ (\bmod m_j) \quad \text{für } \ i \neq j, \\ c_i (m/m_i) x_i &\equiv x_j \,(\bmod m_j) \quad \text{für } \ i = j. \end{aligned}$$

Dann ist es klar, daß gilt

$$\sum_{i=1}^{s} c_i (m/m_i) x_i \equiv x_j \,(\bmod m_j).$$

Also gilt $x_0 \equiv x_j \,(\bmod m_j)$ für jedes $j = 1, \ldots, s$.

Nehmen wir an, daß x eine andere Zahl ist, die die Bedinungen $x_0 \equiv x_j \,(\bmod m_j)$ für jedes $j = 1, \ldots, s$ erfüllt. Dann gilt $x - x_0 \equiv 0 \,(\bmod m_j)$ für alle j. Da die Zahlen $m_1, \ldots, m_s$ paarweise teilerfremd sind, haben wir $x - x_0 \equiv 0 \,(\bmod m)$. □

Beispiel. Gesucht ist eine ganze Zahl x mit der Eigenschaft

$$\begin{cases} x \equiv 2 \,(\bmod 3), \\ x \equiv 3 \,(\bmod 4), \\ x \equiv 2 \,(\bmod 5). \end{cases}$$

Antwort:

$$x \equiv 47 \,(\bmod 60).$$

Vorlesung 3
Grundlagen der Gruppentheorie und der Körpertheorie

Beilage G
Grundlagen der Gruppentheorie

G.1. Definition der zyklischen Gruppe. Sei G eine Gruppe. Die Gruppe heißt *zyklisch*, wenn jedes Element von G eine Potenz von g ist:

$$\forall x \in G \, \exists n \in \mathbb{Z} : x = g^n.$$

In dem Fall schreibt man $G = \langle g \rangle$ und sagt, daß G mit g *erzeugt* ist. Das Element g heißt ein *Erzeugendes* der Gruppe G.

G.2. Beispiel. 1) $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle = \langle 5 \rangle$.

2) $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle = \langle 5 \rangle$.

Betrachten wir dieses Beispiel ausführlich. Wir haben $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, da nur diese Elemente des Restklassenringes $\mathbb{Z}_9$ inverse Elemente haben. Diese Inverse sind $1, 5, 7, 2, 4, 8$ entsprechend. Ausserdem kann man nachprüfen, daß gilt

$$\mathbb{Z}_9^* = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\}.$$

Das ermöglicht, einen Isomorphismus $\mathbb{Z}_6^+ \to \mathbb{Z}_9^*$ mit dem Gesetz $i \mapsto 2^i$ einzustellen.

3) $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$.

Analog können wir einen Isomorphismus $\mathbb{Z}_6^+ \to \mathbb{Z}_7^*$ mit dem Gesetz $i \mapsto 3^i$ einstellen.

4) Die Gruppe $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ ist nicht zyklisch.

G.3. Definition der Ordnung des Elementes. Sei G eine Gruppe mit Einselelement e und sei $g \in G$. Die kleinste natürliche Zahl n mit $g^n = e$ heißt *Ordnung von* g, falls es ein solches n gibt. Wenn $g^n \neq e$ für alle $n \geqslant 1$ ist, dann setzt man die Ordnung gleich ∞. Die Ordnung von g bezeichnet man mit $\mathrm{ord}(g)$.

Insbesondere ist $\mathrm{ord}(e) = 1$. Es ist leicht zu verstehen, daß die Ordnung des Elementes von einer endlichen Gruppe auch endlich ist.

G.4. Beispiel. 1) Sei $\mathbb{Z}^+$ die Gruppe der ganzen Zahlen bezüglich der Addition. Dann sind die Ordnungen ihrer nicht-nullischen Elemente gleich ∞.

2) Seien $\mathbb{Z}_n^+$ und $\mathbb{Z}_n^*$ additive und multiplikative Gruppen des Restklassenringes $\mathbb{Z}_n$. Die Ordnungen der Elemente in Gruppen $\mathbb{Z}_6^+, \mathbb{Z}_9^*$ и $\mathbb{Z}_8^*$ sind folgende:

g	0	1	2	3	4	5
$\mathrm{ord}(g)$	1	6	3	2	3	6

g	1	2	4	5	7	8
$\mathrm{ord}(g)$	1	6	3	6	3	2

g	1	3	5	7
$\mathrm{ord}(g)$	1	2	2	2

G.5. Satz. Sei G eine Gruppe, $g \in G$ und $n = \mathrm{ord}(g) < \infty$. Dann gilt $g^m = e$ nur dann, wenn m durch n teilbar ist.

Beweis. Ist m durch n teilbar, so ist $g^m = (g^n)^{m/n} = e$.

Jetzt nehmen wir an, daß $g^m = e$ ist und beweisen, daß m durch n teilbar ist. Teilen wir m durch n mit einem Rest: $m = qn + r$, wobei $0 \leqslant r < n$ ist. Dann ist $e = g^m = g^{qn+r} = (g^n)^q \cdot g^r = g^r$ und aus der Minimalität von n erhalten wir $r = 0$. □

G.6. Satz. Wenn $G = \langle g \rangle$ eine endliche zyklische Gruppe ist, dann ist $G = \{e, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\}$ und alle diese Elemente sind verschiedene.

Beweis. Zuerst zeigen wir, daß die Elemente verschieden sind. Würde $g^i = g^j$ für $0 \leqslant i < j \leqslant \mathrm{ord}(g) - 1$ gelten, dann hätten wir $g^{j-i} = e$ – ein Widerspruch mit der Minimalität von $\mathrm{ord}(g)$.

Jetzt zeigen wir, daß jedes Element $x \in G$ in der Menge $\{e, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\}$ liegt. Da G mit g erzeugt ist, haben wir $x = g^n$ für einen $n \in \mathbb{Z}$. Teilen wir n durch $\mathrm{ord}(g)$ und erhalten einen Rest: $n = k{\cdot}\mathrm{ord}(g) + r$, wobei $0 \leqslant r < \mathrm{ord}(g)$ ist. Dann gilt $x = (g^{\mathrm{ord}(g)})^k g^r = g^r$. □

G.7. Definition der Untergruppe. Sei G eine Gruppe und $H \subseteq G$ eine nichleere Menge. Die Menge H heißt *Untergruppe* der Gruppe G, wenn folgende Bedingungen erfüllt sind:

1) Für alle $h_1, h_2 \in H$ gilt $h_1 h_2 \in H$.
2) Für alle $h \in H$ gilt $h^{-1} \in H$.

G.8. Beispiel. Alle Untergruppen der Gruppe $\mathbb{Z}_6^+$ sind $\{0\}, \{0, 3\}, \{0, 2, 4\}$ und $\mathbb{Z}_6^+$.

G.9. Aufgabe. Jede Untergruppe der zyklischen Gruppe ist zyklisch.

G.10. Definition der Ordnung der Gruppe. *Die Ordnung der Gruppe* ist die Anzahl der Elemente der Gruppe. Die Ordnung der Gruppe G wird als $|G|$ bezeichnet.

G.11. Satz von Lagrange. Sei G eine endliche Gruppe und sei H ihre Untergruppe. Dann ist die Ordnung von H ein Teiler der Ordnung von G.

Beweis. Sei $H = \{h_1, \ldots, h_n\}$. Wenn $G = H$ ist, sind wir fertig. Wenn H kleiner als G ist, dann nehmen wir ein Element $x \in G \setminus H$ und betrachten die Menge $Hx = \{h_1 x, \ldots, h_n x\}$. Alle Elemente der Menge sind verschiedene und nicht gleich den Elementen von H. In der Tat, aus $h_i x = h_j x$ folgt $h_i = h_j$, und aus $h_i x = h_j$ folgt $x = h_i^{-1} h_j \in H$, was unmöglich ist. Also, haben wir

$$|H| = |Hx| \quad \text{und} \quad H \cap Hx = \emptyset.$$

Wenn $H \cup Hx = G$ ist, dann ist der Satz bewiesen. Wenn $H \cup Hx$ kleiner als G ist, dann nehmen wir ein Element $y \in G \setminus (H \cup Hx)$ und betrachten die Menge $Hy = \{h_1 y, \ldots, h_n y\}$. Analog können wir beweisen, daß diese neuen Elemente verschieden und nicht gleich den Elementen von $H \cup Hx$ sind. Setzen wir so fort, dann erhalten wir eine Zerlegung

$$G = H \cup Hx \cup Hy \cup \cdots \cup Hz,$$

wobei jedes Paar der Mengen $H, Hx, Hy, \ldots, Hz$ kein gemeinsames Element hat und jede der Menge enthält genau n Elemente. Daraus folgt, daß n ein Teiler von $|G|$ ist. □

G.12. Folgerung. Sei G eine endliche Gruppe und sei g ein Element von G. Dann ist die Ordnung von g ein Teiler der Ordnung von G.

Beweis. Es ist klar, daß $\{e, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\}$ eine Untergruppe von G ist. Ihre Ordnung ist gleich $\mathrm{ord}(g)$ und nach dem Satz G.11 ist sie ein Teiler von $|G|$. □

Beilage K

Grundlagen der Körpertheorie

K.1. Definition. Ein *Körper* ist eine nichtleere Menge K mit zwei Verknüpfungen $+$ und $\cdot$, so daß die folgenden Bedingungen erfüllt sind:

(a) K ist eine abelsche Gruppe bezüglich der Addition. Bezeichnen wir ihr neutrales Element als 0.

(b) $K \setminus \{0\}$ ist eine abelsche Gruppe bezüglich der Multiplikation. Bezeichnen wir ihr neutrales Element als 1.

(c) Es gilt Distributivität: $a(b+c) = ab + ac$ für alle $a, b, c \in K$.

Es ist klar, daß $K^* = K \setminus \{0\}$ ist und daß das Produkt von zwei nichtnullischen Elementen von K wieder ein nichtnullisches Element von K ist.

K.2. Beispiel. 1) Rationelle, reelle und komplexe Zahlen sind die Körper.

2) Ein Restklassenring $\mathbb{Z}_n$ ist ein Körper nur dann, wenn n eine Primzahl ist.

K.3. Satz. Sei K ein Körper. Jedes Polynom von x des Grades n mit Koeffizienten aus K hat nicht mehr als n Nullstellen in K.

Der Beweis dieses fundamentalen Satzes können Sie in jedem guten Buch über höhere Algebra finden (siehe z.B. [S. Leng, Algebra]). Folgendes Lemma werden wir im Beweis des Satzes K.5 benutzen.

K.4. Lemma. (1) Sei G eine abelsche Gruppe und seien $a, b \in G$ Elemente mit teilerfremden Ordnungen. Dann gilt $\mathrm{ord}(ab) = \mathrm{ord}(a)\mathrm{ord}(b)$.

(2) Sei G eine endliche abelsche Gruppe und sei a ein Element von G der maximalen Ordnung. Dann ist die Ordnung jedes Elementes von G ein Teiler von $\mathrm{ord}(a)$.

Beweis. (1) Bezeichnen wir $k = \mathrm{ord}(ab)$, $n = \mathrm{ord}(a)$, $m = \mathrm{ord}(b)$. Da G eine abelsche Gruppe ist, haben wir $e = (ab)^{km} = a^{km}(b^m)^k = a^{km}$. Nach dem Satz G.5 ist km durch n teilbar. Da m und n teilerfremd sind, ist k durch n teilbar. Analog ist k durch m teilbar. Daraus folgt, daß k durch nm teilbar ist. Von anderer Seite ist es offensichtlich, daß $(ab)^{nm} = e$ gilt. Da k die minimale Zahl mit der Eigenschaft $(ab)^k = e$ ist, ist $k = nm$.

(2) Sei x ein Element von G. Wenn $\mathrm{ord}(x)$ kein Teiler von $\mathrm{ord}(a)$ ist, dann existiert eine Primzahl q und zwei maximale Zahlen α und β, so daß $q^\alpha | \mathrm{ord}(x)$, $q^\beta | \mathrm{ord}(a)$ und $\alpha > \beta$ ist. Setzen wir $y = x^{\mathrm{ord}(x)/q^\alpha}$ und $b = a^{q^\beta}$. Dann gilt $\mathrm{ord}(y) = q^\alpha$ und $\mathrm{ord}(b) = \mathrm{ord}(a)/q^\beta$. Da $\mathrm{ord}(y)$ und $\mathrm{ord}(b)$ teilerfremd sind und die Gruppe G abelsch ist, haben wir nach dem Punkt (1) $\mathrm{ord}(yb) = \mathrm{ord}(y)\cdot\mathrm{ord}(b) = \mathrm{ord}(a)q^{\alpha-\beta} > \mathrm{ord}(a)$ – ein Widerspruch. □

K.5. Satz. Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.

Beweis. Sei K ein endlicher Körper. Beweisen wir, daß seine multiplikative Gruppe K^* zyklisch ist. Seien $x_1, \ldots, x_n$ alle Elemente der Gruppe K^* und sei $\mathrm{ord}(x_1)$ maximal, $d = \mathrm{ord}(x_1)$. Nach dem Satz G.5 ist $\mathrm{ord}(x_i) | d$ für $i = 1, \ldots, n$. Dann sind alle x_i Nullstellen des Polynomes $x^d - 1 = 0$ in K. Nach dem Satz K.3 haben wir $n \leqslant d$. Und nach der Folgerung G.12 haben wir $d | |K^*|$, also $d | n$. Daraus folgt $d = n$. Das bedeutet, daß $\{x_1, x_1^2, \ldots, x_1^n\} = K^*$ gilt, also x_1 erzeugt K^*. □

K.6. Folgerung. Wenn p eine Primzahl ist, dann ist $\mathbb{Z}_p^*$ die zyklische Gruppe der Ordnung $p - 1$.

Vorlesungen 4

Die Struktur der multiplikativen Gruppe des Ringes $\mathbb{Z}_m$

4.1. Satz über die Zerlegung der multiplikativen Gruppe des Ringes $\mathbb{Z}_m$.
Sei m eine natürliche Zahl und $m = p_1^{e_1} \dots p_s^{e_s}$ die Primzahlzerlegung von m. Dann gilt

$$\mathbb{Z}_m^* \simeq \mathbb{Z}_{p^{e_1}}^* \times \dots \times \mathbb{Z}_{p^{e_s}}^*. \tag{4.1}$$

Beweis. Nach dem Chinesischen Restklassensatz haben wir $\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{e_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{e_s}}$. Daraus folgt

$$\mathbb{Z}_m^* \simeq (\mathbb{Z}_{p_1^{e_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{e_s}})^* = \mathbb{Z}_{p_1^{e_1}}^* \times \dots \times \mathbb{Z}_{p_s^{e_s}}^*.$$

□

Wir werden beweisen, daß die Gruppe $\mathbb{Z}_{p^k}^*$ zyklisch ist, ausgenommen den Fall $p = 2$, $k \geqslant 3$.

Sei $\varphi(m)$ die *Eulersche Funktion* von m, d.h. die Anzahl der Zahlen in der Reihe $1, 2, \dots, m-1$, die m teilerfremd sind.

4.2. Satz über die Ordnung der multiplikativen Gruppe des Ringes $\mathbb{Z}_m$.
1) Die Ordnung der Gruppe $\mathbb{Z}_m^*$ ist gleich $\varphi(m)$:

$$|\mathbb{Z}_m^*| = \varphi(m). \tag{4.2}$$

2) Wenn $m = p_1^{k_1} \dots p_s^{k_s}$ die Primzahlzerlegung von m ist, dann gilt

$$\varphi(m) = \varphi(p_1^{k_1}) \dots \varphi(p_s^{k_s}). \tag{4.3}$$

Außerdem gilt für jede Primzahl p die Formel

$$\varphi(p^k) = p^{k-1}(p-1). \tag{4.4}$$

Beweis. 1) Es ist ausreichend zu verstehen, daß die Gruppe $\mathbb{Z}_m^*$ nur die Zahlen von $1, 2, \dots, m-1$ enthält, die m teilerfremd sind. Nach Definition ist a ein Element von $\mathbb{Z}_m^*$ nur dann, wenn ein b existiert, so daß $ab \equiv 1 \pmod m$ gilt. Dann ist es klar, daß a teilerfremd m ist. Umgekehrt, wenn a teilerfremd m ist, dann existiert nach der Folgerung 1.2 ein b, so daß $ab \equiv 1 \pmod m$ ist. Daraus folgt $a \in \mathbb{Z}_m^*$.
2) Die Formel (4.3) folgt aus den Formeln (4.1) und (4.2). Beweisen wir die Formel (4.4). Sei p eine Primzahl. Dann sind in der Reihe $1, 2, \dots, p^k - 1$ nur die Zahlen $p, 2p, \dots, (p^{k-1}-1)p$ nicht teilerfremd p. Daraus folgt die Formel (4.4). □

4.3. Folgerung (Satz von Euler). Sei a teilerfremd m. Dann gilt

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

Beweis. Da a teilerfremd m ist, können wir annehmen, daß $a \in \mathbb{Z}_m^*$ gilt. Nach der Folgerung G.12 ist die Ordnung des Elementes a ein Teiler der Ordnung der Gruppe $\mathbb{Z}_m^*$. Deshalb ist $\mathrm{ord}(a)$ ein Teiler von $\varphi(m)$. Daraus folgt $a^{\varphi(m)} = 1$ in $\mathbb{Z}_m^*$. □

4.4. Folgerung (Kleiner Fermatischer Satz). Sei p eine Primzahl und sei a eine natürliche Zahl, die nicht durch p teilbar ist. Dann gilt

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\ p).$$

4.5. Satz. Wenn p eine Primzahl ist, dann ist $\mathbb{Z}_p^*$ die zyklische Gruppe der Ordnung $p-1$.

Beweis. Siehe Satz K.5 und Folgerung K.6 in der Beilage K.

4.6. Satz. Wenn $p \geqslant 3$ eine Primzahl ist, dann ist die Gruppe $\mathbb{Z}_{p^n}^*$ zyklisch für alle $n \geqslant 1$.

Beweis. Nach Satz 4.5 existiert eine natürliche Zahl g, so daß folgende Formeln gelten:

$$g^{p-1} \equiv 1 \,(\mathrm{mod}\ p) \quad \text{und} \quad g^l \not\equiv 1 \,(\mathrm{mod}\ p) \quad (1 \leqslant l < p-1). \tag{4.5}$$

Jetzt zeigen wir, daß es möglich ist, ein solches g zu wählen, das die folgende zusätzliche Eigenschaft hat

$$g^{p-1} \not\equiv 1 \ (\mathrm{mod}\ p^2). \tag{4.6}$$

Nehmen wir an, daß $g^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$ gilt. Dann gilt

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + (p-1)g^{p-2}p + p^2(\dots) \\ &\equiv 1 + (p-1)g^{p-2}p \,(\mathrm{mod}\ p^2) \\ &\not\equiv 1 \,(\mathrm{mod}\ p^2).\end{aligned}$$

Ersetzen wir g nach $g+p$, dann werden die Formeln (4.5) und (4.6) gelten. Deshalb können wir annehmen, daß gilt

$$g^{p-1} = 1 + pu$$

für ein u, das nicht durch p teilbar ist. Wir werden beweisen, daß dieses g die Gruppe $\mathbb{Z}_{p^n}^*$ erzeugt. Erst beweisen wir, daß für alle $k \geqslant 0$ eine natürliche Zahl u_k exisiert, so daß u_k teilerfremd p ist und die Formel

$$g^{(p-1)p^k} = 1 + p^{k+1}u_k \tag{4.7}$$

gilt. Nehmen wir an, daß diese Voraussetzung schon für ein $k \geqslant 0$ bewiesen ist. Wir werden sie für $k+1$ beweisen.

$$g^{(p-1)p^{k+1}} = (1 + p^{k+1}u_k)^p = 1 + p^{k+2}u_k + \sum_{i=2}^{p} C_p^i (p^{k+1}u_k)^i.$$

Es ist hinreichend zu beweisen, daß jeder Summand in der Summe durch p^{k+3} teilbar ist. Für $2 \leqslant i < p$ ist der binomiale Koeffizient C_p^i durch p teilbar. Dann ist der Summand $C_p^i(p^{k+1}u_k)^i$ durch $p^{1+i(k+1)}$ teilbar. Da $1 + i(k+1) \geqslant 1 + 2(k+1) \geqslant k+3$ ist, ist der Summand durch p^{k+3} teilbar. Der Summand in der Summe mit $i = p$ ist durch $p^{(k+1)p}$

teilbar. Da $(k+1)p \geqslant 3(k+1) \geqslant k+3$ ist, ist dieser Summand auch durch p^{k+3} teilbar. Die Voraussetzung ist schon bewiesen.

Jetzt kommen wir zur Berechnung der Ordnung des Elements g in der Gruppe $\mathbb{Z}_{p^n}^*$. Diese Ordnung d teilt die Ordnung der Gruppe, also teilt die Zahl $\varphi(p^n) = p^{n-1}(p-1)$. Da $g^d \equiv 1 \,(\mathrm{mod}\, p^n)$ ist, haben wir $g^d \equiv 1 \,(\mathrm{mod}\, p)$ und so $(p-1)|d$. Deshalb hat d die Form $d = (p-1)p^k$ für einen $k \geqslant 0$. Aus der Formel (4.7) folgt, daß k nicht kleiner als $n-1$ ist. Also gilt $d = \varphi(p^n)$. □

Wenn A, B zwei Untermengen der Gruppe G sind, dann bezeichnen wir

$$AB = \{ab \mid a \in A,\, b \in B\}.$$

Wenn G eine abelsche Gruppe ist und A, B zwei ihrer Untergruppen, dann ist es klar, daß AB auch eine Untergruppe von G ist.

4.7. Lemma. Sei G eine abelsche Gruppe und seien A, B zwei ihrer Untergruppen, so daß $A \cap B = \{e\}$ ist. Dann existieren für jedes Element $g \in AB$ einzige Elemente $a \in A$ und $b \in B$ mit $g = ab$. Ausserdem gilt $AB \simeq A \times B$.

Beweis. Nehmen wir an, daß $g = ab = a_1 b_1$ gilt, wobei $a, a_1 \in A$ und $b, b_1 \in B$ ist. Dann gilt $aa_1^{-1} = bb_1^{-1}$. Da $A \cap B = \{e\}$ ist, folgt daraus $a = a_1$, $b = b_1$. Einen Isomorphismus $AB \to A \times B$ stellt man mit dem Gesetz $ab \mapsto (a, b)$ her. □

Bevor wir Satz 4.9 beweisen, betrachten wir ein Beispiel.

4.8. Beispiel. In der Gruppe $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ gibt es zwei Untergruppen:

$$\begin{aligned} \langle -1 \rangle &= \{(-1)^0, (-1)^1\} &&= \{1, 15\}, \\ \langle 5 \rangle &= \{5^0, 5^1, 5^2, 5^3\} &&= \{1, 5, 9, 13\}. \end{aligned}$$

Ihr Produkt ist die ganze Gruppe $\mathbb{Z}_{16}^*$. Ausserdem haben wir nach dem Lemma 4.7 $\mathbb{Z}_{16}^* = \langle -1 \rangle \langle 5 \rangle \simeq \langle -1 \rangle \times \langle 5 \rangle \simeq \mathbb{Z}_2^+ \times \mathbb{Z}_4^+$.

4.9. Satz. 1) Die Gruppen $\mathbb{Z}_2^*$ и $\mathbb{Z}_4^*$ sind zyklisch und haben die Ordnungen 1 und 2 entsprechend.

2) Wenn $k \geqslant 3$ ist, dann gilt $\mathbb{Z}_{2^k}^* \simeq \mathbb{Z}_2^+ \times \mathbb{Z}_{2^{k-2}}^+$. Diese Gruppe ist nicht zyklisch.

Beweis. Die erste Behauptung ist leicht zu beweisen. Beweisen wir die zweite. Erst merken wir an, daß $|\mathbb{Z}_{2^k}^*| = \varphi(2^k) = 2^{k-1}$ gilt. Weiterhin werden wir folgende Punkte beweisen:

(a) Es gilt $-1 \in \mathbb{Z}_{2^k}^*$ und -1 hat die Ordnung 2 in der Gruppe $\mathbb{Z}_{2^k}^*$;

(b) Es gilt $5 \in \mathbb{Z}_{2^k}^*$ und 5 hat die Ordnung 2^{k-2} in der Gruppe $\mathbb{Z}_{2^k}^*$;

(c) Es gilt $\langle -1 \rangle \cap \langle 5 \rangle = \{1\}$.

Nehmen wir an, daß diese Punkte schon bewiesen sind. Dann, nach Lemma 4.7, hat das Produkt der Untergruppen $\langle -1 \rangle$ und $\langle 5 \rangle$ die Ordnung 2^{k-1}. Die Gruppe $\mathbb{Z}_{2^k}^*$ hat dieselbe Ordnung. Deshalb ist $\langle -1 \rangle \cdot \langle 5 \rangle = \mathbb{Z}_{2^k}^*$. Ausserdem gilt nach Lemma 4.7 die Formel $\langle -1 \rangle \cdot \langle 5 \rangle \simeq \mathbb{Z}_2^+ \times \mathbb{Z}_{2^{k-2}}^+$, und so wird der Satz bewiesen.

Es bleiben nur die Punkte (a)–(c) zu beweisen. Der Punkt (a) ist klar. Weiter haben wir $5 \in \mathbb{Z}_{2^k}^*$, da 5 und 2^k teilerfremd sind. Beweisen wir, daß $\mathrm{ord}(5) = 2^{k-2}$ gilt. Es reicht zu beweisen, daß folgende Formeln gelten:

$$5^{2^{k-2}} \equiv 1 \,(\mod 2^k)$$

und

$$5^{2^l} \not\equiv 1 \,(\mod 2^k) \quad \text{für} \quad l = 0, 1, \ldots, k-3.$$

Diese Formeln leiten wir ab aus der folgenden Behauptung.

Behauptung. Für jedes $l \geqslant 0$ existiert eine ungerade Zahl $u = u(l)$, so daß gilt

$$5^{2^l} = 1 + 2^{l+2}u.$$

Beweis. Für $l = 0$ ist die Behauptung ist offensichtlich. Machen wir einen induktiven Schritt von l zu $l+1$:

$$5^{2^{l+1}} = (1 + 2^{l+2}u)^2 = 1 + 2^{l+3}(u + 2^{l+1}u^2).$$

Es bleibt zu bemerken, daß für $l \geqslant 0$ die Zahl in Klammern ungerade ist.

Beweisen wir Punkt (b). Nehmen wir an, daß $-1 \in \langle 5 \rangle$ gilt, also gilt $-1 \equiv 5^s \,(\mathrm{mod}\, 2^k)$ für ein s. Betrachten wir diese Kongruenz modulo 4, dann erhalten wir die Kongruenz $-1 \equiv 1 \,(\mathrm{mod}\, 4)$ – ein Widerspruch. □

Vorlesung 5
Diskrete Logarithmierung und Diffie-Hellman-Schlüsselaustausch

5.1. Problem der diskreten Logarithmierung. Seien q eine Primzahl, $\mathbb{Z}_q$ der Restklassenring modulo q und $\mathbb{Z}_q^*$ die multiplikative Gruppe dieses Ringes. Da q eine Primzahl ist, ist die Gruppe $\mathbb{Z}_q^*$ zyklisch und hat die Ordnung $q-1$.

Seien b ein Erzeugendes von $\mathbb{Z}_q^*$ und a ein beliebiges Element von $\mathbb{Z}_q^*$. Dann existiert eine Zahl x, so daß

$$a \equiv b^x \,(\bmod\, q) \tag{5.1}$$

ist. Diese Zahl ist die einzige modulo $q-1$ und heißt *diskreter Logarithmus von a bezüglich der Basis b in der Gruppe $\mathbb{Z}_q^*$*. Wie man schnell diese Zahl x finden kann?

5.2. Der Pohlig-Hellman-Algorithmus. Sei $q-1 = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}$ die Primzahlzerlegung der Zahl $q-1$. Nehmen wir an, daß alle p_i kleine Zahlen sind[3]. Zum Beispiel $p_i \leqslant 1000$.

Erst werden wir die Reste von x modulo $p_i^{e_i}$ finden: $x = u_i p_i^{e_i} + r_i$, $0 \leqslant r_i < p_i^{e_i}$ $(i = 1, 2, \dots, l)$. Dann können wir x modulo $q-1$ mit Hilfe des Chinesischen Restklassensatzes finden. Bezeichnen wir $A_i = a^{(q-1)/p_i^{e_i}}$ und $B_i = b^{(q-1)/p_i^{e_i}}$. Dann haben wir die Gleichung

$$A_i = B_i^x.$$

Da $\operatorname{ord}(B_i) = p_i^{e_i}$ ist, können wir sie so umschreiben:

$$A_i = B_i^x = B_i^{u_i p_i^{e_i} + r_i} = (B_i^{p_i^{e_i}})^{u_i} \cdot B_i^{r_i} = B_i^{r_i}. \tag{5.2}$$

Nach folgendem Lemma können wir schnell r_i finden. □

5.3. Lemma. Seien $A, B \in \mathbb{Z}_q^*$ und sei $\operatorname{ord}(B) = p^e$, wobei p eine **kleine** Primzahl ist. Wenn eine t mit $A = B^t$ und $0 \leqslant t < p^e$ existiert, dann kann man t schnell finden.

Beweis. Da $0 \leqslant t < p^e$ ist, können wir t in folgender Form darstellen:

$$t = n_0 + n_1 p + \dots + n_{e-1} p^{e-1},$$

wobei $0 \leqslant n_0, n_1, \dots, n_{e-1} < p$ ist. Dann ist

$$A = B^{n_0 + n_1 p + \dots + n_{e-1} p^{e-1}}.$$

<u>*Schritt* 0</u>. Berechnung wir n_0.
Steigern wir diese Gleichung in die Potenz p^{e-1} und benutzen, dass $B^{p^e} = 1$ modulo q ist:

$$\begin{aligned} A^{p^{e-1}} &= B^{n_0 p^{e-1} + p^e(\dots)} \\ &= (B^{p^{e-1}})^{n_0}. \end{aligned}$$

[3]Hier werden wir nicht präzise definieren, was "kleine Zahl" und "schneller Algorithmus" bedeuten.

Mit den Bezeichnungen $D_0 = A^{p^{e-1}}$ und $c = B^{p^{e-1}}$ haben wir die Gleichung

$$D_0 = c^{n_0}. \tag{5.3}$$

Da $0 \leqslant n_0 < p$ und p klein ist, können wir n_0 schnell mit der Probier-Methode finden. Dafür kalkulieren wir die Zahlen $1, c, c^2, \ldots, c^{p-1}$ und vergleichen sie mit D_0 modulo q.

Schritt $i+1$. Berechnen wir n_{i+1}, vorausgesetzt, dass die Zahlen $n_0, \ldots, n_i$ schon berechnet sind. Erst berechnen wir

$$t_i = n_0 + n_1 p + \cdots + n_i p^i.$$

Aus der Gleichung $A = B^t$ leiten wir ab:

$$AB^{-t_i} = B^{t-t_i} = B^{p^{i+1}n_{i+1} + p^{i+2}(\ldots)}.$$

Daraus und mit Hilfe der Gleichung $B^{p^e} = 1$ erhalten wir

$$(AB^{-t_i})^{p^{e-(i+2)}} = B^{p^{e-1}n_{i+1} + p^e(\ldots)} = (B^{p^{e-1}})^{n_{i+1}}.$$

Mit den Bezeichnungen $D_{i+1} = (AB^{-t_i})^{p^{e-(i+2)}}$ und $c = B^{p^{e-1}}$ haben wir

$$D_{i+1} = c^{n_{i+1}}. \tag{5.4}$$

Da $0 \leqslant n_{i+1} < p$ und p klein ist, können wir n_0 schnell mit der Probier-Methode finden. Dafür kalkulieren wir die Zahlen $1, c, c^2, \ldots, c^{p-1}$ und vergleichen sie mit D_{i+1} modulo q. Danach können wir t_{i+1} mit folgender Formel berechnen:

$$t_{i+1} = t_i + n_{i+1} p^{i+1}. \tag{5.5}$$

Am Ende finden wir $t = t_{e-1}$.

□

Also, um $t = t_{e-1}$ zu finden, müssen wir die folgende Tabelle schrittweise ausfüllen. Am Anfang an berechnen wir $D_0 = A^{p^{e-1}}$ und $c = B^{p^{e-1}}$. Demnächst berechnen wir n_0 mit Hilfe der (5.3) und setzen $t_0 = n_0$. Wenn t_i schon bekannt ist, berechnen wir $D_{i+1} = (AB^{-t_i})^{p^{e-(i+2)}}$. Demnächst berechnen wir n_{i+1} mit Hilfe der (5.4) und t_{i+1} mit Hilfe der (5.5).

i	0	1	...	$e-1$
D_i	$*$	$*$	...	$*$
n_i	$*$	$*$	...	$*$
t_i	$*$	$*$	...	t

5.4. Beispiel. Betrachten wir die multiplikative Gruppe $\mathbb{Z}^*_{163}$. Es ist leicht zu beweisen, daß das Element $4 \in \mathbb{Z}^*_{163}$ die Ordnung $81 = 3^4$ hat. Wir werden die Gleichung

$$97 = 4^t$$

in der Gruppe $\mathbb{Z}^*_{163}$ lösen. In der Gruppe haben wir $A = 97$, $B = 4$, $p = 3$, $e = 4$, $c = B^{p^{e-1}} = 4^{3^3} = 104$, $c^2 = 58$.

i	0	1	2	3
D_i	104	58	1	104
n_i	1	2	0	1
t_i	1	7	7	34

Also ist $t = 34$.

5.5. Beispiel. Da 163 eine Primzahl ist, ist die Ordnung der multiplikative Gruppe $\mathbb{Z}_{163}^*$ gleich 162. Man kann beweisen, daß 2 ein Erzeugendes der Gruppe $\mathbb{Z}_{163}^*$ ist. Wir werden die Gleichung

$$74 = 2^x$$

in der Gruppe $\mathbb{Z}_{163}^*$ lösen. Mit den Bezeichnungen der Punkte 5.2 haben wir $a = 74$, $b = 2$, $q = 163$. Zerlegen wir $q - 1$ in Primzahlen: $q - 1 = 2^1 \cdot 3^4$, also ist $p_1 = 2$, $e_1 = 1$ und $p_2 = 3$, $e_2 = 4$.

Weiterhin suchen wir die Reste r_1 und r_2 von x modulo 2^1 und 3^4.

1) Aus (5.2) haben wir $A_1 = B_1^{r_1}$, wobei $A_1 = a^{(q-1)/p_1^{e_1}} = 74^{81} = 1$ und $B_1 = b^{(q-1)/p_1^{e_1}} = 2^{81} = -1$ ist. Deshalb ist $r_1 = 0$.

2) Aus (6.2) haben wir $A_2 = B_2^{r_2}$, wobei $A_2 = a^{(q-1)/p_2^{e_2}} = 74^2 = 97$ und $B_2 = b^{(q-1)/p_2^{e_2}} = 2^2 = 4$ ist. Aus dem Punkt 6.4 haben wir $r_2 = 34$.

3) Mit Hilfe der Chinesicher Restklassensatzes erhalten wir $x = 34 \,(\mathrm{mod}\ 162)$.

5.6. Diffie-Hellman-Schlüsselaustausch.

Alice und Bob kommunizieren nur per Internet. Einige Emails wollen sie mit Hilfe eines gemeinsamen geheimen Schlüssels führen. Unter dem Schlüssel verstehen wir eine Zahl K, die nur Alice und Bob bekannt ist. Am Anfang haben sie kein gemeinsamen geheimen Schlüssel und wollen ihn konstruieren. Wie können sie das machen, wenn Oscar ihre Korrespondenz liesst?

Dafür gibt es das Diffie-Hellman-Verfahren:

Schritt 1. Zuerst einigen sich Alice und Bob auf eine Primzahl p und ein Erzeugendes g der Gruppe $\mathbb{Z}_p^*$. Diese beiden Zahlen können öffentlich bekannt werden.

Schritt 2. Alice wählt dann zufällig eine Zahl $a \in \{0, 1, \ldots, p-2\}$ und berechnet

$$A \equiv g^a \,(\mathrm{mod}\ p).$$

Die Zahl A schickt sie an Bob, aber sie hält den Exponent a geheim bei sich.

Bob auch wählt zufällig eine Zahl $b \in \{0, 1, \ldots, p-2\}$ und berechnet

$$B \equiv g^b \,(\mathrm{mod}\ p).$$

Die Zahl B schickt er an Alice und hält b geheim.

Es gilt nun:

$$B^a \,(\mathrm{mod}\ p) \equiv g^{ab} \,(\mathrm{mod}\ p) \equiv A^b \,(\mathrm{mod}\ p). \tag{5.6}$$

Schritt 3. Alice und Bob berechnen die Zahl $K \equiv g^{ab} \,(\mathrm{mod}\ p)$ und nehmen sie als geheim Schlüssel.

Die Zahl K können sowohl Alice als auch Bob schnell mit Hilfe (5.6) berechnen. Oscar kann das nicht, weil er weiß nur die Zahlen p, g und g^a, g^b. Wenn aber er die Zahlen a und b finden könnte, dann könnte er auch schnell K berechnen. Aber zu Zeit ist kein schneller Algorithmus für disktere Logarithmierung bekannt.

5.7. ElGamal-Kryptosystem. Alice und Bob wollen miteinander geheim per Email kommunizieren. Alice wählt eine Primzahl p, ein Erzeugendes $g \in \mathbb{Z}_p^*$ und einen "privaten Schlüssel" $a \in \mathbb{Z}_p^*$. Den Schlüssel a teilt sie nur Bob mit. Dafür kann sie Diffie-Hellman-Schlüsselaustausch benutzen.

Außerdem veröffentlicht Alice (z.B. im Telefonbuch) drei Zahlen (p, g, A), wobei

$$A \equiv g^a \,(\mathrm{mod}\ p)$$

ist. Diese drei Zahlen nennt man einen "öffentlichen Schlüssel". Den öffentlichen Schlüssel wird Alice beim Chiffrieren ihres Textes benutzen. Unter einem Text verstehen wir eine beliebige Zahl $x \in \mathbb{Z}_p^*$.

Sei $x \in \mathbb{Z}_p^*$ eine Zahl (= ein Text), die Alice Bob mitteilen will. Dafür wählt Alice zufällig eine Zahl $k \in \{0, 1, \ldots, p-2\}$ und schickt an Bob ein Chiffretext – ein Paar der Zahlen (g^k, xA^k).

Nachdem Bob den Chiffretext $(u, v) = (g^k, xA^k)$ erhalten hat, kann er den Klartext x mit folgender Formel restaurieren:

$$x = vu^{-a}.$$

In der Tat ist

$$x = xA^k \cdot A^{-k} = v \cdot (g^a)^{-k} = v \cdot (g^k)^{-a} = vu^{-a}.$$

Oscar könnte auch x berechnen, wäre er in der Lage, a oder k zu finden. Das ist aber sehr schwerig, weil er beide Zahlen nur mit der diskreten Logarithmierung in $\mathbb{Z}_p^*$ finden kann: $a = \log_g A$, $k = \log_g u$.

Vorlesung 6
Diskrete Logarithmierung: Das Geburtstagsparadox und der Pollard-ρ-Algorithmus

Folgendes Paradox hat Anwendungen in vielen Algorithmen, inklusive des Pollard-ρ-Algorithmus.

6.1. Geburtstagsparadox. In einem Saal treffen sich 23 Personen. Dann gibt es mit der Wahrscheinlichkeit $> \frac{1}{2}$ zwei von ihnen, die Geburtstag am selben Tag haben.

Formulieren wir eine allgemeine Frage. Sei n die Anzahl der Tage in einem Jahr ($n = 365$ für die Erde und $n = 669$ für den Mars). Sei k die Anzahl der Personen in einem Saal, $k < n$. Wie groß ist die Wahrscheinlichkeit, dass zwei Personen am selben Tag Geburtstag haben?

Bezeichnen wir diese Wahrscheinlichkeit mit P_1. Sei P_2 die Wahrscheinlichkeit, dass alle die k Personen Geburtstag an unterschiedlichen Tagen haben. Dann ist $P_1 + P_2 = 1$. Außerdem ist

$$P_2 = \frac{n(n-1)\dots(n-(k-1))}{n^k} = \frac{n-1}{n} \cdot \frac{n-2}{n} \cdot \ldots \cdot \frac{n-(k-1)}{n}$$
$$= \Big(1 - \frac{1}{n}\Big)\Big(1 - \frac{2}{n}\Big)\dots\Big(1 - \frac{k-1}{n}\Big).$$

Jetzt benutzen wir eine Formel aus der Analysis: $1 + x < e^x$ für alle reellen $x \neq 0$ ist. Dann erhalten wir

$$P_2 < e^{-\frac{1}{n}} e^{-\frac{2}{n}} \dots e^{-\frac{k-1}{n}} = e^{-\frac{k(k-1)}{2n}}.$$

Daraus folgt

$$P_1 > 1 - e^{-\frac{k(k-1)}{2n}}.$$

Berechnen wir, für welche natürliche k ist die Wahrscheinlichkeit P_1 größer als $\frac{1}{2}$:

$$1 - e^{-\frac{k(k-1)}{2n}} > \frac{1}{2}.$$

Nach der Vereinfachung und Logarithmierung erhalten wir:

$$\frac{k(k-1)}{2n} > \ln 2.$$

Die positive Lösung dieser quadratischen Ungleichung ist

$$k > \frac{1 + \sqrt{1 + 8(\ln 2)n}}{2}.$$

Also, für diese k ist die Wahrscheinlichkeit P_1 größer als $\frac{1}{2}$.

Setzen wir $n = 365$ an, dann erhalten wir $k \geqslant 23$. Das erklärt das Geburtstagparadox.

6.2. Das Problem der diskreten Logarithmierung. Seien q eine Primzahl, g ein Erzeugendes der Gruppe $\mathbb{Z}_q^*$ und a ein beliebiges Element von $\mathbb{Z}_q^*$. Dann existiert eine einzige Zahl x mit $0 \leqslant x < q-1$ und

$$a \equiv g^x \,(\bmod\, q). \tag{6.1}$$

Wie kann man diese Zahl schnell finden?

6.3. Pollard-ρ-Algorithmus. Lenken wir von dem Problem (6.1) für einen Moment ab. Nehmen wir beliebige natürliche Zahlen y, z und betrachen die Zahl $b = g^y a^z$. Mit der Gleichung verbinden wir das Tripel (b, y, z):

$$b = g^y a^z \rightsquigarrow (b, y, z).$$

Wir bekommen gültige Gleichungen, wenn wir diese Gleichung quadrieren, oder mal a oder mal g multiplizieren (diese Berechnungen machen wir modulo q). Daraus können wir neue Tripel erhalten:

$$\begin{array}{lll} b^2 & = g^{2y}a^{2z} & \rightsquigarrow (b^2, 2y, 2z), \\ ba & = g^y a^{z+1} & \rightsquigarrow (ba, y, z+1), \\ bg & = g^{y+1}a^z & \rightsquigarrow (bg, y+1, z). \end{array}$$

Jetzt kehren wir zu unserer Kongruenz (6.1) zurück. Wir werden eine Reihe von Tripel (b_i, y_i, z_i) konstruieren.

1. Starten wir mit der Gleichung $a = g^0 a^1$. Das entsprechende Tripel ist $(a, 0, 1)$. Setzen wir $(b_0, y_0, z_0) = (a, 0, 1)$.

2. Nehmen wir an, daß das Tripel (b_i, y_i, z_i) schon bekannt ist. Wählen wir zufällig eine Zahl $x_i \in \{0, 1, 2\}$. Dann setzen wir

$$(b_{i+1}, y_{i+1}, z_{i+1}) = \begin{cases} (b_i^2, 2y_i, 2z_i) & \text{falls} \quad x_i = 0 \quad \text{ist}, \\ (b_i a, y_i, z_i + 1) & \text{falls} \quad x_i = 1 \quad \text{ist}, \\ (b_i g, y_i + 1, z_i) & \text{falls} \quad x_i = 2 \quad \text{ist}. \end{cases}$$

WICHTIG: die Zahlen b_i werden modulo q berechnet und die Zahlen y_i und z_i werden modulo $q-1$ berechnet.

3. Wir beenden den Prozess nur dann, wenn wir ein Paar von Indexen i, j mit $i < j$ und $b_i = b_j$ erhalten (eine Wiederholung). Dann erhalten wir folgende Gleichungen:

$$g^{y_i} a^{z_i} \equiv b_i = b_j \equiv g^{y_j} a^{z_j} \,(\bmod\, q).$$

Umschreiben wir sie:

$$g^{y_i - y_j} \equiv a^{z_j - z_i} \,(\bmod\, q).$$

Da $a \equiv g^x \,(\bmod\, q)$ ist, haben wir

$$g^{y_i - y_j} \equiv g^{(z_j - z_i)x} \,(\bmod\, q).$$

Daraus folgt

$$y_i - y_j \equiv (z_j - z_i)x \,(\bmod\, q-1). \tag{6.2}$$

Aus dieser Kongruenz können wir x finden, wenn $z_j - z_i$ invertibel modulo $q-1$ ist. Wenn nicht, dann können wir den ganzen Prozess mit anderen zufälligen Zahlen x_i wiederholen und eine neue Gleichung der Form (6.2) erhalten. Es wird erwartet, dass irgendwann $z_j - z_i$ modulo $q-1$ invertibel wird.

6.4. Wie schnell passiert die Wiederholung $b_i = b_j$?

Interpretieren wir die Zahlen $b_0, b_1, \ldots$ als die Tage des "Geburtstages". Da $1 \leqslant b_i \leqslant q-2$ ist, "das Jahr" hat $(q-2)$ Tage. Setzen wir

$$k = \left\lceil \frac{1 + \sqrt{1 + 8(\ln 2)(q-2)}}{2} \right\rceil.$$

Nach dem Punkt 6.1, existiert eine Wiederholung $b_i = b_j$ in der Reihe $b_0, b_1, \ldots b_k$ mit der Wahrscheinlichkeit $> \frac{1}{2}$.

Vorlesung 6 (Vortsetzung)
Diskrete Logarithmierung: der Babystep-Giantstep-Algorithmus von Shanks und Die Index-Calculus-Methode

Wir betrachten das Problem der diskreten Logarithmierung:

Seien q eine Primzahl, g ein Erzeugendes der Gruppe $\mathbb{Z}_q^*$ und a ein beliebiges Element von $\mathbb{Z}_q^*$. Dann existiert eine einzige Zahl x mit $0 \leqslant x < q-1$ und

$$a \equiv g^x \,(\mathrm{mod}\ q). \tag{6.3}$$

Wie kann man diese Zahl schnell finden?

6.5. Babystep-Giantstep-Algorithmus von Shanks. Um x zu finden, werden wir die Kongruenz in eine andere Form umschreiben. Bezeichnen wir $k = \lceil \sqrt{q}\, \rceil$. Zuerst teilen wir x durch k und erhalten einen Rest:

$$x = km + r. \tag{6.4}$$

Lemma. Es gelten $0 \leqslant r < k$ und $0 \leqslant m < k$.

Beweis. Die erste Ungleichung ist offenbar. Beweisen wir die zweite: $m \leqslant x/k < (q-1)/\lceil \sqrt{q} \rceil < \lceil \sqrt{q} \rceil = k$. □

Aus (6.3) und (6.4) folgt

$$ag^{-r} \equiv (g^k)^m \,(\mathrm{mod}\ q).$$

Mit der Bezeichnung $d = g^k$ haben wir

$$ag^{-r} \equiv d^m \,(\mathrm{mod}\ q).$$

Daraus folgt der Giantstep-Babystep-Algorithmus:

1. Berechnen wir $k = \lceil \sqrt{q}\, \rceil$ und $d \equiv g^k \,(\mathrm{mod}\ q)$.

2. (die "Giantstep"): Listen wir alle Paare $(m, d^m \mod q)$ mit $0 \leqslant m < k$.

3. (die "Babystep"): Listen wir alle Paare $(r, ag^{-r} \mod q)$ mit $0 \leqslant r < k$.

4. Finden wir in den beiden Listen zwei Paare mit gleichen zweiten Einträgen. Danach stellen wir ihre ersten Einträge m und r in die Formel (6.4) ein und berechnen x.

6.6. Beispiel. Finden wir x, so daß gilt

$$7^x \equiv 100 \,(\mathrm{mod}\ 601).$$

Hier ist $k = \lceil \sqrt{601}\, \rceil = 25$ und $d \equiv 7^{25} \equiv 295 \,(\mathrm{mod}\ 601)$.

$(0, 1)$	$(1, 295)$	$(2, 481)$	$(3, 59)$	$(4, 577)$
$(5, 132)$	$(6, \mathbf{476})$	$(7, 387)$	$(8, 576)$	$(9, 438)$
$(10, 596)$	$(11, 328)$	$(12, 600)$	$(13, 306)$	$(14, 120)$
$(15, 542)$	$(16, 24)$	$(17, 469)$	$(18, 125)$	$(19, 214)$
$(20, 25)$	$(21, 163)$	$(22, 5)$	$(23, 273)$	$(24, 1)$

Giantstep-Liste

$(0, 100)$	$(1, 186)$	$(2, 370)$	$(3, 568)$	$(4, 167)$
$(5, 539)$	$(6, 77)$	$(7, 11)$	$(8, 345)$	$(9, 221)$
$(10, 375)$	$(11, 397)$	$(12, 486)$	$(13, 327)$	$(14, \mathbf{476})$
$(15, 68)$	$(16, 439)$	$(17, 492)$	$(18, 242)$	$(19, 378)$
$(20, 54)$	$(21, 437)$	$(22, 320)$	$(23, 475)$	$(24, 583)$

Babystep-Liste

Daraus haben wir $x \equiv 25 \cdot 6 + 14 = 164 \,(\bmod\, 600)$.

6.7. Die Index-Calculus-Methode für diskrete Logarithmierung. Diese Methode ist kein Algorithmus, da ihre Schritte nicht präzise beschrieben sind. In der Praxis funktioniert diese Methode etwas schneller als der Pohlig-Hellman-Algorithmus.

Seien q eine Primzahl, g ein Erzeugendes der Gruppe $\mathbb{Z}_q^*$ und a eine Zahl aus $\mathbb{Z}_q^*$. Dann existiert eine natürliche Zahl x mit

$$a \equiv g^x \,(\bmod\, q).$$

Wir wollen diese x modulo $q-1$ finden.

Schritt 1. Wählen wir eine Menge von "kleinen" Primzahlen

$$\mathcal{B} = \{p_1, p_2, \ldots, p_k, \} \quad \text{(die Faktorbasis)}.$$

Schritt 2. Berechnen wir Logarithmen (bezüglich g) aller Elemente p_i aus $\mathcal{B}$ mit folgender Methode.

Wählen wir zufällig einige Zahlen $t_1, \ldots, t_s$ in $\mathbb{Z}_{q-1}$, wobei s etwas größer als k ist. Für jede Zahl t_i entscheiden wir durch Probedivision, ob es möglich ist g^{t_i} auf Primzahlen $p_1, \ldots, p_k$ modulo q zu zerlegen:

$$g^{t_i} \equiv p_1^{e_{i,1}} p_2^{e_{i,2}} \ldots p_k^{e_{i,k}} \,(\bmod\, q).$$

Wenn ja, werden wir folgende Kongruenz haben:

$$t_i \equiv e_{i,1} \log_g(p_1) + e_{i,2} \log_g(p_2) + \cdots + e_{i,k} \log_g(p_k) \,(\bmod\, q-1).$$

Die Zahlen $e_{i,1}, e_{i,2}, \ldots, e_{i,k}$ und t_i sind bekannt. Werden wir viele solche Kongruenzen haben, dann können wir die Unbekannten $\log_g p_1, \ldots, \log_g p_k$ finden.

Schritt 3. Wählen wir zufällig eine Zahl $s \in \mathbb{Z}_{q-1}$ und versuchen, $a \cdot g^s$ auf Primzahlen $p_1, p_2, \ldots, p_k$ modulo q zu zerlegen:

$$a \cdot g^s \equiv p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}.$$

Gelingt das, bekommen wir die Kongruenz

$$\log_g a + s \equiv e_1 \log_g(p_1) + e_2 \log_g(p_2) + \cdots + e_k \log_g(p_k) \,(\bmod\, q-1)$$

und können leicht $\log_g a$ finden. Gelingt das nicht, werden wir noch einmal den Schritt 3 mit einer anderen Zahl s durchführen. Wird das mit vielen s nicht gelingen, müssen wir zu Schritt 1 zurückkehren und die Menge $\mathcal{B}$ vergrößern.

6.8. Beispiel. Wir werden die folgende Kongruenz lösen:

$$17 \equiv 5^x \,(\bmod\, 43)$$

Nehmen wir $\mathcal{B} = \{2, 3, 5\}$. Zuerst wird es $\log_5 2$ und $\log_5 3$ kalkuliert (es ist klar, daß $\log_5 5 \equiv 1 \,(\bmod\, 42)$ ist). Nehmen wir "zufällig" $t_1 = 1$ und $t_2 = 32$ und versuchen, die Zahlen 5^{t_1} und 5^{t_2} über der Faktorbasis $\{2, 3\}$ zu faktorisieren:

$$\begin{aligned} 5^1 &\equiv 5 + 43 = 48 = 2^4 \cdot 3 \,(\bmod\, 43), \\ 5^{32} &\equiv 9 = 3^2 \,(\bmod\, 43). \end{aligned}$$

Logarithmierung bezüglich 5 ergibt die Kongruenzen

$$\begin{cases} 1 \equiv 4\log_5 2 + \log_5 3 \,(\bmod\, 42), \\ 32 \equiv \quad 2\log_5 3 \,(\bmod\, 42). \end{cases}$$

Daher erhalten wir $\log_5 2 \equiv 32 \,(\bmod\, 42)$ und $\log_5 3 \equiv 37 \,(\bmod\, 42)$.

Jetzt finden wir $\log_5 17 \,(\bmod\, 42)$. Wir haben

$$17 \equiv 17 + 43 = 60 = 2^2 \cdot 3 \cdot 5 \,(\bmod\, 43).$$

Daher erhalten wir

$$x = \log_5 17 \equiv 2\log_5 2 + \log_5 3 + \log_5 5 \equiv\ 2 \cdot 33 + 37 + 1 = 104 \equiv 20 \,(\bmod\, 42).$$

Vorlesungen 7–8
Quadratischer Reziprozitätssatz

7.1. Definition. Sei p eine Primzahl. Eine ganze Zahl a, die teilerfremd p ist, heißt *quadratischer Rest modulo* p, wenn die Kongruenz $x^2 \equiv a \,(\mathrm{mod}\, p)$ eine Lösung hat.

7.2. Behauptung. Sei $p \geqslant 3$ eine Primzahl.
1) Nur die Hälfte der Zahlen $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ sind quadratische Reste modulo p.
2) Für $a \in \mathbb{Z}_p^*$ gilt

$$a^{\frac{p-1}{2}} = \begin{cases} 1, & \text{wenn } a \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1, & \text{wenn } a \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Beweis. 1) Nach Satz K.5 in der Gruppe $\mathbb{Z}_p^*$ existiert ein Element z, so daß $\mathbb{Z}_p^* = \{1, z, z^2, \dots, z^{p-2}\}$ gilt. Für die weitere Berechnung ist es bequem, diese Menge in zwei Mengen zu teilen:

$$\mathbb{Z}_p^* = \{1, z, z^2, \dots, z^{\frac{p-3}{2}}\} \cup \{z^{\frac{p-1}{2}}, z^{\frac{p-1}{2}+1}, \dots, z^{\frac{p-1}{2}+\frac{p-3}{2}}\}.$$

Wenn wir alle diese Elemente in Grad 2 heben, dann erhalten wir die Elemente $1, z^2, z^4, \dots, z^{p-3}$. Also nur diese Elemente von $\mathbb{Z}_p^*$ sind quadratische Reste. Die Anzahl dieser Elemente ist $\frac{1}{2}|\mathbb{Z}_p^*|$.

2) Sei a ein quadratischer Rest modulo p, also gilt $a = x^2$ für einen $x \in \mathbb{Z}_p^*$. Dann ist $a^{\frac{p-1}{2}} = x^{p-1} = 1$. Sei a kein quadratischer Rest modulo p. Dann gilt $a = z^k$ für eine ungerade Zahl k. Wir haben $a^{\frac{p-1}{2}} = z^{k\frac{p-1}{2}} \neq 1$, da $k\frac{p-1}{2}$ nicht durch $p-1$ teilbar ist. Da $\left(a^{\frac{p-1}{2}}\right)^2 = 1$ gilt, erhalten wir $a^{\frac{p-1}{2}} = -1$. Hier haben wir benutzt, daß die Gleichung $y^2 = 1$ in dem Körper $\mathbb{Z}_p$ genau 2 Nullstellen hat: 1 und -1.

7.3. Definition des Legendre-Symbols $\left(\frac{a}{p}\right)$. Sei $p \geqslant 3$ eine Primzahl und sei a eine ganze Zahl. Wenn a durch p teilbar ist, setzt man $\left(\frac{a}{p}\right) = 0$. Wenn a nicht durch p teilbar ist, setzt man

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{wenn } a \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1, & \text{wenn } a \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Nach der Behauptung 7.2 haben wir folgende Gleichung in $\mathbb{Z}_p$:

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

7.4. Die Eigenschaften des Legendre-Symbols. Es gelten

1) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ für die b, die teilerfremd p sind.
2) $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.
3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Um die Sätze 7.6 und 7.7 zu beweisen, brauchen wir den folgenden wichtigen Satz.

7.5. Satz über endliche Körper. Für jede Primzahl p und jede natürliche Zahl $n \geqslant 1$ existiert ein einziger (bis zu Isomorphie) Körper mit genau p^n Elementen. Dieser Körper $GF(p^n)$ enthält einen Unterkörper, der $\mathbb{Z}_p$ isomorph ist. Insbesondere ist die Summe von p Eins in $GF(p^n)$ gleich 0. Außerdem ist jeder endliche Körper isomorph dem Körper $GF(p^n)$ für einige p und n.

Beweis. Den Beweis dieses Satzes kann man in jedem guten Buch über höhere Algebra finden. Um den Beweis zu illustrieren, werden wir einen Körper der Ordnung 9 konstruieren. Sei P eine Menge der Polynomen der Form $ax + b$, wobei a, b in $\mathbb{Z}_3$ sind. Die Polynome kann man mit einem natürlichen Weg addieren und multiplizieren. Aber wir werden das modulo Polynom $x^2 + 1$ machen. Zum Beispiel, das übliche Produkt der Polynome $x+2$ und $2x+1$ gleich $2x^2+5x+2$ ist. Aber unser Produkt gleich dem Rest von Division von $2x^2+5x+2$ durch x^2+1 ist. Der Rest gleich $5x$ ist, was modulo 3 gleich $2x$ ist (alle Koeffizienten betrachten wir in $\mathbb{Z}_3$). Beweisen wir, daß jedes nichtnullische Polynom $f(x)$ in P ein Inverses hat. Wenn $f(x) = ax + b$ ist, dann ist $f(x)(ax - b) = -a^2 - b^2$. Es ist leicht zu verstehen, daß für $(a, b) \neq (0, 0)$ das Element $-a^2 - b^2$ von Körper $\mathbb{Z}_3$ ungleich 0 ist, deshalb hat es ein Inverses, sagen wir c. Dann ist $(ax - b)c$ ein inverses Polynom zu $f(x)$. Alle anderen Axiome von Körper können trivial nachgeprüft werden.

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

Beweis. Zuerst merken wir an, daß für jedes ungerade n gilt

$$\frac{n^2-1}{8} = \begin{cases} \text{eine gerade Zahl,} & \text{wenn } n = \pm 1 \,(\bmod 8) \quad \text{ist,} \\ \text{eine ungerade Zahl,} & \text{wenn } n = \pm 5 \,(\bmod 8) \quad \text{ist.} \end{cases}$$

Betrachten wir die Körper $GF(p^2)$. Nach dem Satz K.5 ist ihre multiplikative Gruppe zyklisch. Da diese Gruppe die Ordnung p^2-1 hat, enhält sie ein Element α der Ordnung 8. Dann gilt $\alpha^4 = -1$. Daraus folgt $\alpha^2 + \alpha^{-2} = 0$. Setzen wir $y = \alpha + \alpha^{-1}$. Dann gilt

$$y^2 = 2.$$

Außerdem haben wir nach der binomialen Formel

$$y^p = \alpha^p + \alpha^{-p}.$$

Wenn $p = \pm 1 \,(\bmod 8)$ ist, dann leiten wir daraus $y^p = \alpha + \alpha^{-1} = y$ ab. Dann ist $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = y^{p-1} = 1$.
Wenn $p = \pm 5 \,(\bmod 8)$ ist, dann leiten wir $y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y$ ab. Dann ist $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = y^{p-1} = -1$. □

7.7. Quadratischer Reziprozitätssatz (Gauß). Wenn $p \geqslant 3$ und $q \geqslant 3$ zwei Primzahlen sind, dann gilt

$$\Big(\frac{q}{p}\Big) = \Big(\frac{p}{q}\Big)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}.$$

Beweis. Nehmen wir $p \neq q$ an. Betrachten wir die Körper $GF(p^{q-1})$. Nach dem Satz K.5 ist ihre multiplikative Gruppe zyklisch. Da diese Gruppe die Ordnung $p^{q-1}-1$ hat, enthält sie ein Element der Ordnung $p^{q-1}-1$. Da nach dem Eulerschen Satz $p^{q-1}-1$ durch q teilbar ist, enthält diese Gruppe ein Element der Ordnung q. Bezeichnen wir es als ω. Dann gelten $\omega \neq 1$ und $\omega^q = 1$ in $GF(p^{q-1})$. Jetzt definieren wir *die Summe von Gauß*:

$$y = \sum_{x \in \mathbb{Z}_q} \Big(\frac{x}{q}\Big)\omega^x.$$

Behauptung 1. Es gilt die Gleichung

$$y^2 = (-1)^{\frac{q-1}{2}} q.$$

Beweis. Wir haben

$$y^2 = \sum_{x,z} \Big(\frac{xz}{q}\Big)\omega^{x+z} = \sum_{u \in \mathbb{Z}_q} \omega^u \sum_{x \in \mathbb{Z}_q} \Big(\frac{x(u-x)}{q}\Big).$$

Da $\left(\frac{0}{q}\right) = 0$ ist, kann man annehmen, daß x in der letzten Summe über die Menge $\mathbb{Z}_q \setminus \{0\}$ läuft. Für $x \neq 0$ haben wir

$$\Big(\frac{x(u-x)}{q}\Big) = \Big(\frac{-x^2}{q}\Big)\Big(\frac{1-ux^{-1}}{q}\Big) = (-1)^{\frac{q-1}{2}}\Big(\frac{1-ux^{-1}}{q}\Big).$$

Daraus folgt

$$(-1)^{\frac{q-1}{2}} y^2 = \sum_{u \in \mathbb{Z}_q} C_u \omega^u, \tag{7.1}$$

wobei

$$C_u = \sum_{x \in \mathbb{Z}_q \setminus \{0\}} \Big(\frac{1-ux^{-1}}{q}\Big)$$

ist. Betrachten wir zwei Fälle.

Fall 1. Sei $u = 0$. Dann ist

$$C_0 = \sum_{x \in \mathbb{Z}_q \setminus \{0\}} \Big(\frac{1}{q}\Big) = q - 1. \tag{7.2}$$

Fall 2. Sei $u \neq 0$. Wenn x über die Menge $\mathbb{Z}_q \setminus \{0\}$ läuft, dann läuft $1 - ux^{-1}$ über die Menge $\mathbb{Z}_q \setminus \{1\}$. Deshalb gilt

$$C_u = \sum_{s \in \mathbb{Z}_q \setminus \{1\}} \Big(\frac{s}{q}\Big) = \sum_{s \in \mathbb{Z}_q \setminus \{0\}} \Big(\frac{s}{q}\Big) + \Big(\frac{0}{q}\Big) - \Big(\frac{1}{q}\Big) = -\Big(\frac{1}{q}\Big) = -1, \tag{7.3}$$

weil $\left(\frac{0}{q}\right) = 0$ ist und die Anzahl der quadratischen Reste in $\mathbb{Z}_q \setminus \{0\}$ gleich der Anzahl der nicht-quadratischen Reste in $\mathbb{Z}_q \setminus \{0\}$ ist.

Aus den Formeln (7.1)–(7.3) folgt

$$\begin{aligned}(-1)^{\frac{q-1}{2}} y^2 = \sum_{u\in\mathbb{Z}_q} C_u\omega^u &= (q-1) - \sum_{u\in\mathbb{Z}_q\setminus\{0\}} \omega^u \\ &= q - (1+\omega+\cdots+\omega^{q-1}) \\ &= q - \frac{\omega^q - 1}{\omega - 1} \\ &= q,\end{aligned}$$

weil die Ordnung von ω gleich q ist. Die Behauptung ist bewiesen.

Behauptung 2. Es gilt

$$y^{p-1} = \left(\frac{p}{q}\right).$$

Beweis. Mit der binomialen Formel erhalten wir die Gleichungen:

$$y^p = \sum_{x\in\mathbb{Z}_q} \left(\frac{x}{q}\right)\omega^{xp} = \sum_{z\in\mathbb{Z}_q} \left(\frac{zp^{-1}}{q}\right)\omega^z = \left(\frac{p^{-1}}{q}\right) y = \left(\frac{p}{q}\right) y.$$

Teilen wir sie durch y und erhalten die gewünschte Gleichung. □

Ende des Beweises des Satzes 7.7. Nach den Behauptungen 1 und 2 haben wir

$$\left(\frac{p}{q}\right) = y^{p-1} = \left((-1)^{\frac{q-1}{2}} q\right)^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{q}{p}\right)$$

in dem Körper $GF(p^{q-1})$ und so auch in dem Ring der ganzen Zahlen. □

Vorlesungen 9-10
Fermatischer Primzahlen-Test. Carmichael-Zahlen

Der kleine Fermatische Satz behauptet folgendes. Sei n eine Primzahl. Dann gilt für alle zu n teilerfremden Zahlen a die Kongruenz

$$a^{n-1} \equiv 1 \,(\mathrm{mod}\ n). \tag{9.1}$$

Aber es existieren zusammengesetzten Zahlen n, für die die Behauptung auch gilt. Die kleinste solche Zahl ist $561 = 3 \cdot 11 \cdot 17$.

9.1. Definition der Carmichael-Zahlen. Eine natürliche Zahl n heißt *Carmichael-Zahl*, wenn sie zusammengesetzt ist und für alle zu n teilerfremden Zahlen a die Kongruenz

$$a^{n-1} \equiv 1 \,(\mathrm{mod}\ n)$$

gilt.

9.2. Satz. (1) Eine ungerade Zahl n ist Carmichael-Zahl nur dann, wenn folgende zwei Bedingungen erfüllt sind:

(a) es gilt $n = p_1 p_2 \dots p_r$, wobei p_i verschiedene Primzahlen sind;

(b) die Zahl $n-1$ ist durch $p_i - 1$ teilbar $(i = 1, \dots, r)$.

(2) Jede Carmichael-Zahl ist mindestens in drei Primzahlen zerlegbar.

Beweis. (1) Sei $n = p_1^{e_1} \dots p_r^{e_r}$ die Primzahl-Zerlegung von n. Nach dem Satz 4.1 haben wir ein Isomorphismus von Gruppen

$$\mathbb{Z}_n^* \to \mathbb{Z}_{p_1^{e_1}}^* \times \dots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

Nehmen wir an, daß n eine Carmichael-Zahl ist. Dann gilt für alle $a \in \mathbb{Z}_n^*$ die Gleichung $a^{n-1} = 1$. Deshalb für alle $a_i \in \mathbb{Z}_{p_i^{e_i}}^*$ gilt $a_i^{n-1} = 1$. Nach Satz 4.6 die Gruppe $\mathbb{Z}_{p_i^{e_i}}^*$ ist zyklisch und hat ein Element a_i der Ordnung $|\mathbb{Z}_{p_i^{e_i}}^*| = \phi(p_i^{e_i}) = p_i^{e_i - 1}(p_i - 1)$. Deshalb ist $n-1$ durch diese Ordnung teilbar. Daraus folgen $e_i = 1$ und $(p_i - 1) | (n-1)$, also die Bedingungen (a), (b) erfüllt sind.

Jetzt nehmen wir an, daß die Bedingungen (a), (b) erfüllt sind. Aus (a) folgt, daß wir ein Isomorphismus

$$\mathbb{Z}_n^* \to \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$$

haben. Für alle $a_i \in \mathbb{Z}_{p_i}^*$ gilt $a_i^{p_i - 1} = 1$, dann gilt nach (b) $a_i^{n-1} = 1$. Deshalb für alle $a \in \mathbb{Z}_n^*$ gilt $a^{n-1} = 1$. Also n ist eine Carmichael-Zahl.

(2) Nehmen wir an, daß n eine Carmichaei-Zahl ist und $n = pq$ ist, wobei p, q verschiedene Primzahlen sind. Dann ist $n-1$ durch $p-1$ und $q-1$ teilbar. Wir haben $n - 1 = (p-1)q + (q-1)$. Dann ist $p-1$ durch $q-1$ teilbar. Analog ist $q-1$ durch $p-1$ teilbar. Daraus filgt $p = q$ – ein Widerspruch. □

Sei $C(n)$ die Anzahl der Carmichael-Zahlen, die kleiner als n sind. In 1994 haben Alford, Granvillle und Pomerance bewiesen, daß $C(n) > n^{2/7}$ für alle groß genug n gilt. Insbesondere gibt es unendlich viele Carmichael Zahlen.

Setzen wir

$$B_n = \{a \in \mathbb{Z}_n^* \,|\, a^{n-1} = 1\}.$$

9.3. Satz. Wenn n eine Primzahl ist, dann ist $B_n = \mathbb{Z}_n^*$. Wenn n eine zusammengesetzte Zahl ist, dann ist

$$B_n = \mathbb{Z}_n^* \quad \text{oder} \quad |B_n| \leqslant \frac{1}{2}|\mathbb{Z}_n^*|.$$

Beweis. Die erste Behauptung entspringt dem kleinen Fermatischen Satz. Die zweite Behauptung entspringt den Fakten, daß B_n eine Untergruppe der Gruppe $\mathbb{Z}_n^*$ ist und daß die Ordnung der Untergruppe die Ordnung der Gruppe teilt. □

9.4. Aufgabe. Sei n eine ungerade Zahl und $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, wobei $p_1, p_2, \dots, p_r$ verschiedene Primzahlen sind. Dann gilt

$$|B_n| = \prod_{i=1}^{r} \mathbf{ggT}\,(n-1, p_i - 1).$$

Hinwes. Der Beweis folgt aus dem Beweis des Satzes 9.2 und aus dem Lemma 9.8.

9.5. Die allgemeine Struktur des probablistischen Primzahlentests.
Sei weiterhin n eine ungerade Zahl. Wir wollen wissen, ob die gegebene Zahl n eine Primzahl ist. Einige probablistische Primzahlentests, so wie der Miller-Rabin Test, haben folgende allgemeine Struktur. Nehmen wir an, daß für alle ungeraden Zahlen n eine Untermenge $L_n \subseteq \mathbb{Z}_n^*$ und eine Zahl $0 < c < 1$ so definiert, so daß die folgenden Bedingungen erfüllt sind:

• Es gibt einen effizienten Algorithmus, der nach gegebenen $a \in \mathbb{Z}_n$ bestimmt, ob a in L_n liegt;

• wenn n eine Primzahl ist, ist $L_n = \mathbb{Z}_n^*$;

• wenn n eine zusammengesetzte Zahl ist, dann ist $|L_n| \leqslant c\,\phi(n)$, wobei ϕ die Eulersche Funktion ist.

Wählen wir eine natürliche Zahl s (von der Zahl hängt die Abweichung des Testes ab).

Test. Wählen wir zufällig s Zahlen $a_1, \dots, a_s$ in der Menge $\{1, \dots, n-1\}$. Prüfen wir nach, ob die Zahlen a_i in L_n liegen. Wenn eine von a_i nicht in L_n liegt, wird die Antwort

n ist eine zusammengesetzte Zahl

zurückgegeben. Wenn alle a_i in L_n liegen, wird die Antwort

n ist eine Primzahl mit der Wahrscheinlichkeit $\geqslant 1 - c^s$

zurückgegeben.

Erklärung. Wenn der Test uns die Antwort "n ist eine zusammengesetzte Zahl" zurückgegeben hat, dann ist n wirklich zusammengesetzt. In der Tat, diese Antwort erhalten wir nur in dem Fall, wenn eine a_i ausser L_n liegt. Wäre n eine Primzahl, hätten wir $a_i \in \{1, \ldots, n-1\} = \mathbb{Z}_n^* = L_n$. Deshalb ist n keine Primzahl.

Wenn der Test uns die Antwort "n ist eine Primzahl mit der Wahscheinlichkeit $\geqslant 1 - c^s$" zurückgegeben hat, dann können wir nicht sicher sein, daß n eine Primzahl ist. Wir können nur mit dieser Wahrscheinlichkeit zustimmen. In der Tat, diese Antwort erhalten wir nur in dem Fall, wenn alle a_i in L_n liegen. Wäre n eine zusammengesetzte Zahl, hätten wir das Ereignis, "alle a_i liegen in L_n" mit der Wahrscheinlichkeit $\leqslant c^s$.

Bemerkung. 1) Normalerweise führt man den Test in s Schritten aus. Bei jedem Schritt wählt man nur eine zufällige Zahl in der Menge $\{1, \ldots, n-1\}$. Die Wahlen müssen unabhängig sein.

2) Für $c = 1/4$ und $s = 10$ gilt $1 - c^s > 0,99999904$.

Können wir

$$L_n = \{a \in \mathbb{Z}_n^* \,|\, a^{n-1} = 1\}$$

einsetzen?

Wenn wir zuvor wissen, daß n keine Carmichael-Zahl ist, dann haben wir nach dem Satz 9.3 die Ungleichung $|L_n| \leqslant \phi(n)/2$ und können den Test mit der Konstante $c = 1/2$ anwenden. Wenn n eine Carmichael-Zahl ist, ist $L_n = \mathbb{Z}_n^*$ und so ist $|L_n| = \phi(n)$. Deshalb erfüllt die Menge L_n nicht die Bedingungen, die vor dem Test formuliert sind. Wenn wir den Test doch zu diesem n anwenden werden, dann erhalten wir fast sicher nicht die richtige Antwort, daß n eine Primzahl ist. Es ist ein schwacher Trost, daß man selten Carmichael-Zahlen trifft.

Folgende Verstärkung des kleinen Fermatischen Satzes wird uns helfen, eine neue Menge L_n zu definieren, die den Bedingungen vor dem Test für $c = 1/4$ und alle $n \neq 9$ erfüllt.

9.6. Verstärkung des kleinen Fermatischen Satzes. Sei n eine Primzahl und sei $n - 1 = m2^h$, wobei m eine ungerade Zahl ist. Sei a teilerfremd zu n. Dann gilt

$$a^m \equiv 1 \,(\mathrm{mod}\ n) \quad \text{oder} \quad \exists\, t,\, 0 \leqslant t < h: \;\; a^{m2^t} \equiv -1 \,(\mathrm{mod}\ n).$$

Beweis. Nach der Fermatischer Satz, $a^n - 1$ durch n teilbar. Weiter gilt

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \ldots (a^{2^{h-1}m} + 1).$$

Da n eine Primzahl ist, ist ein von den Faktoren durch n teilbar. □

9.7. Miller-Rabin Test. Sei n eine ungerade Zahl und sei $n - 1 = m2^h$, wobei m eine ungerade Zahl ist und $h \geqslant 1$ ist. Der Test läuft mit dem folgenden L_n:

$$L_n = \{a \in \mathbb{Z}_n \,|\, a^m \equiv 1 \,(\mathrm{mod}\ n) \;\; \text{или} \;\; \exists\, i,\, 0 \leqslant i < h: \;\; a^{m2^i} \equiv -1 \,(\mathrm{mod}\ n)\}.$$

Wir werden beweisen, daß diese L_n für alle $n \neq 9$, die Bedingungen aus dem Punkt 9.5 erfüllt für $c = 1/4$. Vorher beweisen wir folgendes Lemma.

9.8. Lemma. Sei G eine zyklische Gruppe der Ordnung n.
(1) Die Anzahl der Lösungen der Gleichung $x^m = 1$ in G gleich $\mathbf{ggT}\,(n, m)$ ist.
(2) Sei $g \in G$ ein Element. Wenn die Gleichung $x^m = g$ mindestens eine Lösung hat, dann ist die Anzahl aller seiner Lösungen gleich $\mathbf{ggT}\,(n, m)$.

Beweis. Sei a erzeugt G, dann haben wir $\mathrm{ord}(a) = n$. Das Element a^d erfüllt die Gleichung $x^m = 1$ nur dann, wenn dm durch n teilbar ist. Das gilt nur dann, wenn d durch $\frac{n}{\mathbf{ggT}\,(n,m)}$ teilbar ist. Es gibt genau $\mathbf{ggT}\,(n, m)$ solche Zahlen d modulo n.
Bezeichnen wir mit A die Menge der Lösungen der Gleichung $x^m = 1$. Wenn die Gleichung $x^m = g$ eine Lösung x_0 hat, dann ist $x_0 A$ die Menge aller seiner Lösungen. □

9.9. Satz (Monier-Rabin). Sei n eine ungerade Zahl. Wenn n eine Primzahl ist, dann ist $L_n = \mathbb{Z}_n^*$. Wenn n eine zusammengesetzte Zahl ist und $n \neq 9$ ist, dann ist $|L_n| \leqslant \phi(n)/4$.

Beweis. Sei $n - 1 = m2^h$, wobei m eine ungerade Zahl ist und $h \geqslant 1$ ist. Betrachten wir drei Fälle.
Fall 1: n ist eine Primzahl. Dann folgt die Behauptung aus dem Punkt 9.7.

Fall 2: $n = p^e$, wobei p eine Primzahl ist und $e > 1$ ist. Offensichtlich ist $L_n \subseteq \{a \in \mathbb{Z}_n^* \mid a^{m2^h} = 1\}$. Nach Lemma 9.8 (1) ist die Anzahl des Elements der Menge L_n

$$\mathbf{ggT}(|\mathbb{Z}_n^*|, n-1) = \mathbf{ggT}\big(p^{e-1}(p-1), p^e - 1\big) = p - 1 = \frac{\phi(n)}{p^{e-1}} < \frac{\phi(n)}{4}.$$

Fall 3: $n = p_1^{e_1} \dots p_r^{e_r}$ ist die Primzerlegung von n und $r > 1$.
Nach dem Satz 4.1 haben wir einen Isomorphismus von Gruppen

$$\theta : \mathbb{Z}_n^* \to \mathbb{Z}_{p_1^{e_1}}^* \times \dots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

Bezeichnen wir $\theta(a) = (a_1, \dots, a_r)$, $G = \mathbb{Z}_n^*$ und $G_i = \mathbb{Z}_{p_i^{e_i}}^*$.

Sei $\phi(p_i^{e_i}) = m_i 2^{h_i}$, wobei m_i eine ungerade Zahl ist. Nach den Sätzen 4.6 und 4.2 ist die Gruppe G_i zyklisch und hat die Ordnung $m_i 2^{h_i}$. Setzen wir $l = \min\{h, h_1, \dots, h_r\}$. Dann ist $l \geqslant 1$, weil n eine ungerade Zahl ist.

Behauptung. Für alle $a \in L_n$ gilt $a^{m2^l} = 1$ in $\mathbb{Z}_n^*$.

Beweis. Nehmen wir an, daß ein $a \in L_n$ mit $a^{m2^l} \neq 1$ existiert. Aus der Definition von L_n folgt die Gleichnung $a^{m2^h} = 1$. Deshalb ist $l < h$ und es existiert eine solche Zahl j, so daß gilt

$$a^{m2^l} \neq 1, \dots, a^{m2^j} \neq 1,\ a^{m2^{j+1}} = 1, \dots, a^{m2^h} = 1.$$

Dann folgt aus der Definition von L_n, daß $a^{m2^j} = -1$ gilt. Deshalb gilt $a_i^{m2^j} = -1$ für alle $i = 1, \dots, r$. Daraus folgt $\mathrm{ord}(a_i^m) = 2^{j+1}$ in der Gruppe G_i. Da die Ordnung des Elementes ein Teiler der Ordnung der Gruppe ist, haben wir $2^{j+1} | m_i 2^{h_i}$ und so $j+1 \leqslant h_i$. Deshalb gilt $l < j + 1 \leqslant h_i$ für alle i. Da die Ungleichung $l < h$ auch gilt, erhalten wir einen Widerspruch mit der Definition von l. □

Aus der Definition von L_n und aus der Behauptung ergibt sich, daß für alle $a \in L_n$ gilt $a^{m2^{l-1}} = \pm 1$. Nach dem Punkt (2) des Lemmas 9.8 haben wir

$$\begin{aligned} |L_n| &\leqslant |\{a \in G \mid a^{m2^{l-1}} = \pm 1\}| \\ &\leqslant 2|\{a \in G \mid a^{m2^{l-1}} = \quad 1\}|. \end{aligned}$$

Bezeichnen wir $A = \{a \in G \mid a^{m2^{l-1}} = \quad 1\},\ A_i = \{a_i \in G_i \mid a_i^{m2^{l-1}} = \quad 1\},\ i = 1, \ldots, r$. Dann gilt $\theta(A) = A_1 \times \cdots \times A_r$. Nach dem Punkt (1) des Lemmas 9.8 haben wir

$$|A_i| = \mathbf{ggT}\,(|G_i|, m2^{l-1}) = \mathbf{ggT}\,(m_i 2^{h_i}, m2^{l-1}) \leqslant \frac{1}{2}|G_i|,$$

weil $h_i \geqslant l$ gilt. Daraus folgt

$$|L_n| \leqslant 2\prod_{i=1}^{r}|A_i| \leqslant 2\prod_{i=1}^{r}\frac{1}{2}|G_i| = 2^{1-r}|G| = 2^{1-r}\phi(n).$$

Wenn $r \geqslant 3$ ist, dann gilt $|L_n| \leqslant \frac{1}{4}|G|$.

Sei $r = 2$. In diesem Fall ist es notwendig, die Ordnung $|A_i|$ genauer einzuschätzen. Wenn für einen $i = 1, 2$

$$\mathbf{ggT}\,(m_i, m) < m_i \quad \text{oder} \quad h_i > l, \tag{9.2}$$

gilt, dann gilt $|A_i| \leqslant \frac{1}{4}|G_i|$, und wieder haben wir $|L_n| \leqslant \frac{1}{4}|G|$.

Jetzt nehmen wir an, daß für jeweils $i = 1, 2$ die Bedingung (9.2) nicht gilt. Dann ist $m_i | m$ und $h_i = l$ für alle i. Da $h \geqslant l$ ist, ist $m_i 2^{h_i} | m2^h$ für alle i. Dann: Für alle $a_i \in G_i$ haben wir $a_i^{n-1} = a_i^{m2^h} = 1$ und deshalb gilt für alle $a \in G$ die Gleichung $a^{n-1} = 1$. Das bedeutet, daß n eine Carmichael-Zahl ist. Aber für Carmichael-Zahlen ist immer $r \geqslant 3$ nach dem Punkt (2) des Satzes 9.2. Ein Widerspruch. □

Vorlesung 11
Tschebyschow-Funktion

11.1. *Die Tschebyschow-Funktion* θ ist für alle reellen $x > 0$ mit folgender Formel definiert:

$$\theta(x) = \sum_{p \leqslant x} \ln p.$$

Die Summierung in der Formel läuft über alle Primzahlen $p \leqslant x$.

11.2. Lemma. Für $n \geqslant 1$ gelten die Ungleichungen

$$4^n > \binom{2n}{n} \geqslant \frac{4^n}{2\sqrt{n}}.$$

Beweis. Die Ungleichung $4^n > \binom{2n}{n}$ entspringt der Formel

$$2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i}.$$

Die zweite Ungleichung werden wir per Induktion für n beweisen. Für $n = 1$ gilt sie. Nehmen wir an, daß sie gilt für $n = k$ und beweisen sie für $n = k+1$:

$$\binom{2(k+1)}{k+1} = \frac{2(2k+1)}{k+1}\binom{2k}{k} \geqslant \frac{2(2k+1)}{k+1}\frac{4^k}{2\sqrt{k}} > \frac{4^{k+1}}{2\sqrt{k+1}}.$$

□

11.3. Lemma. Für alle reellen x gilt $\theta(x) < (4\ln 2)x$.

Beweis. Die folgenden Ungleichungen sind leicht zu beweisen:

$$4^n > \binom{2n}{n} > \prod_{\substack{n<p<2n \\ p \text{ eine Primzahl}}} p.$$

Nach Logarithmierung erhalten wir $2n\ln 2 > \theta(2n) - \theta(n)$. Daraus folgt

$$\theta(2^m) \leqslant 2\ln 2(1 + 2 + \cdots + 2^{m-1}) < (2\ln 2)2^m.$$

Also für $x = 2^m$ gilt das Lemma. Für $2^{m-1} < x < 2^m$ haben wir

$$\theta(x) \leqslant \theta(2^m) < (2\ln 2)2^m = (4\ln 2)2^{m-1} < (4\ln 2)x. \quad \square$$

11.4. Lemma. Für alle natürlichen $n > 4$ gilt $\theta(n) > n/2$.

Beweis. Sei n eine natürliche Zahl und p eine Primzahl. Bezeichnen wir mit $\nu_p(n)$ die maximale k, so daß p^k ein Teiler von n ist. Schätzen wir $\nu_p(n!)$ ein. In dem Produkt $1 \cdot 2 \cdot \ldots \cdot n$ sind genau $\lfloor \frac{n}{p} \rfloor$ Faktoren durch p teilbar, genau $\lfloor \frac{n}{p^2} \rfloor$ sind durch p^2 teilbar und s.w. Deshalb gilt

$$\nu_p(n!) = \sum_{i \geqslant 1} \Big\lfloor \frac{n}{p^i} \Big\rfloor.$$

Daraus folgt

$$\nu_p(\binom{2n}{n}) = \nu_p\Big(\frac{(2n)!}{(n!)^2}\Big) = \sum_{i \geqslant 1} \Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\sum_{i \geqslant 1} \Big\lfloor \frac{n}{p^i} \Big\rfloor$$

$$= \sum_{i \geqslant 1}^{i \leqslant \log_p(2n)} \Big(\Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \frac{n}{p^i} \Big\rfloor \Big) \leqslant \log_p(2n),$$

weil $\lfloor 2x \rfloor - 2\lfloor x \rfloor \leqslant 1$ für alle x gilt. Weiterhin haben wir

$$\binom{2n}{n} = \prod_{p<2n} p^{\nu_p(\binom{2n}{n})} \leqslant \prod_{p<2n} p^{\lfloor \log_p(2n) \rfloor}$$

$$\leqslant \prod_{p \leqslant \sqrt{2n}} p^{\log_p(2n)} \prod_{\sqrt{2n}<p \leqslant 2n} p^{\lfloor \log_p(2n) \rfloor} \leqslant (2n)^{(\sqrt{2n}+1)/2} \prod_{\sqrt{2n}<p \leqslant 2n} p.$$

Mit Hilfe des Lemmas 11.2 erhalten wir

$$\theta(2n) > \sum_{\sqrt{2n}<p \leqslant 2n} \ln p \geqslant n \ln 4 - \ln 2 - \frac{1}{2} \ln n - \frac{1}{2}(\sqrt{2n} + 1) \ln(2n).$$

Die letzte Funktion ist größer als n für $n \geqslant 134$. (Man kann das nachprüfen zum Beispiel mit dem Mapple). Sei $m \geqslant 268$. Für gerade m haben wir dann $\theta(m) > m/2$. Für ungerade m haben wir $\theta(m) = \theta(m+1) > (m+1)/2 > m/2$. Für $4 < m < 268$ kann man die Ungleichung $\theta(m) > m/2$ auch mit einem Programm nachprüfen. □

11.5. Folgerung. Für alle natürlichen $n > 4$ ist das Produkt aller Primzahlen aus der Interval $[1, n]$ größer als $e^{n/2}$.

11.6. Bemerkung. 1) Sei $\pi(x)$ die Anzahl der Primzahlen, die nicht größer als x sind. Im Jahr 1896 haben Hadamar und Valle-Pussen unabhängig voneinander bewiesen, daß

$$\lim_{n \to +\infty} \frac{\pi(n)}{n/\ln n} = 1$$

gilt. Man kann beweisen, daß diese Formel der Formel $\lim\limits_{n \to +\infty} \frac{\theta(n)}{n} = 1$ äquivalent ist.

2) Es ist bekannt, daß für alle natürlichen $n > 1$ das Produkt der Primzahlen aus der Interval $[n, 2n]$ größer als 2^n ist.

Vorlesungen 12–13
Polynomialer deterministischer Algorithmus von Agrawal-Kayal-Saxena

12.1. Kongruenzen modulo $(h(x), n)$. Fixieren wir ein Polynom $h(x) \in \mathbb{Z}[x]$ mit dem Hauptkoeffizienten gleich 1 und fixieren eine natürliche Zahl n. Sei $f(x)$ ein beliebiges Polynom aus $\mathbb{Z}[x]$. Ein *Rest von $f(x)$ modulo $(h(x), n)$* ist ein Polynom $r(x)$, das in den folgenden zwei Scritten berechnet wird:

1) Teilen wir $f(x)$ durch $h(x)$ und finden die Polynome $q(x)$ und $s(x)$, so daß

$$f(x) = h(x)q(x) + s(x)$$

gilt, wobei $\mathrm{Grad}(s(x)) < \mathrm{Grad}(h(x))$ ist;

2) In dem Polynom $s(x)$ ersetzen wir alle Koeffizienten nach ihre Reste modulo n. Das Resultat bezeichnen wir als $r(x)$.

Man sagt, daß zwei Polynome $f(x), g(x) \in \mathbb{Z}[x]$ modulo $(h(x), n)$ kongruent sind, wenn ihre Reste modulo $(h(x), n)$ gleich sind. In dem Fall schreibt man

$$f(x) \equiv g(x) \mod (h(x), n). \tag{12.1}$$

Zum Beispiel:

$$x^3 + 3x^2 + 4x + 1 \equiv x + 1 \mod (x^2 + x + 1, 2).$$

Aufgabe. Die Kongruenz (12.1) gilt nur dann, wenn ein Polynom $q(x) \in \mathbb{Z}[x]$ existiert, so daß alle Koeffizienten des Polynomes $f(x) - g(x) - h(x)q(x)$ duch n teilbar sind.

12.2. Der Ring $\mathbb{Z}_n[x]/\langle h(x)\rangle$. Sei F die Menge aller möglichen Reste modulo $(h(x), n)$, also die Menge aller Polynomen, dessen Grad kleiner als Grad $h(x)$ ist und dessen Koeffizienten in der Menge $\{0, 1, \ldots, n-1\}$ liegen.

Diese Reste kann man natürlicherweise addieren und multiplizieren. Die Summe der Reste $r_1(x)$ und $r_2(x)$ ist den Rest von $r_1(x) + r_2(x)$ modulo $(h(x), n)$. Analog definiert man das Produkt der Reste $r_1(x)$ und $r_2(x)$.

Die Menge F mit einer so definierten Addition und Multiplikation bildet ein Ring. Bezeichnen wir diesen Ring als $\mathbb{Z}_n[x]/\langle h(x)\rangle$.

Zum Beispiel, der Ring $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ enthält die Reste $0, 1, x, x+1$, die werden mit folgenden Regeln addiert und multipliziert:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

12.3. Kinder binomialer Satz. Sei $n \in \mathbb{N}$, $a \in \mathbb{Z}$ und $\mathbf{ggT}(n, a) = 1$. Die Zahl n ist eine Primzahl genau dann, wenn gilt

$$(x + a)^n \equiv x^n + a \,(\mathrm{mod}\ n). \tag{12.2}$$

Beweis. Nach binom Newton haben wir

$$(x + a)^n - (x^n + a) = \sum_{i=1}^{n-1} \binom{n}{i} x^i a^{n-i} + a^n - a. \tag{12.3}$$

Wenn n eine Primzahl ist, dann ist $\binom{n}{i}$ durch n teilbar für $1 \leqslant i \leqslant n-1$. Ausserdem ist $a^n - a$ durch n teilbar (nach dem kleinen Fermatischen Satz). Deshalb gilt die Kongruenz (12.2) für alle Primzahlen n.

Sei n eine zusammengesetzte Zahl und sei $n = p^e p_1^{e_1} \cdots p_s^{e_s}$ die Primzahlzerlegung von n. Dann ist $\binom{n}{p}$ durch p^{e-1} aber nicht durch p^e teilbar. Deshalb ist der Koeffizient bei x^p in (12.3) nicht durch n teilbar. Also gilt für zusammengesetzte n die Kongruenz (12.2) nicht. □

Seien n und r teilerfremde natürliche Zahlen. Bezeichnen wir als $\mathrm{ord}_r(n)$ die Ordnung des Elementes n modulo r. Mit anderen Worten $\mathrm{ord}_r(n)$ ist die minimale natürliche Zahl $k \geqslant 1$, so daß $n^k \equiv 1 \,(\mathrm{mod}\ r)$ gilt. Des weiteren bedeutet $\log n$ der Logarithmus von n zur Basis 2.

12.4. Lemma. Für jede natürliche Zahl $n > 4$ existiert eine Primzahl $r \leqslant \log^5 n$ mit $r \nmid n$, so daß folgende Ungleichung gilt:

$$\mathrm{ord}_r(n) > \log^2 n.$$

Beweis. Nehmen wir das Entgegengesetzte an: es existiert eine natürliche Zahl $n > 4$, so daß für alle Primzahlen r mit den Bedingungen $r \leqslant \lfloor \log^5 n \rfloor$ und $r \nmid n$ die Ungleichung

$$\mathrm{ord}_r(n) \leqslant \log^2 n$$

gilt. Setzen wir $m = \lfloor \log^5 n \rfloor$. Dann ist jede solche Zahl r (und so ihr Produkt) ein Teiler von $\prod\limits_{1 \leqslant i \leqslant \log^2 n} (n^i - 1)$. Von der anderen Seite ist das Produkt der Primzahlen r mit den Bedingungen $r \,|\, n$ und $r \leqslant m$ nicht größer als n. Daraus und aus der Folgerung 11.5 haben wir

$$2^{(\log e)m/2} = e^{m/2} \leqslant \prod_{\substack{r \leqslant m \\ r - \text{eine Primzahl}}} r \leqslant n \cdot \prod_{1 \leqslant i \leqslant \log^2 n} (n^i - 1) < n^{1+1+2+\cdots+\lfloor \log^2 n \rfloor} \leqslant 2^{(\log^5 n + \log^3 n + 2 \log n)/2}.$$

Daraus folgt

$$(\log e)\lfloor \log^5 n \rfloor < \log^5 n + \log^3 n + 2 \log n,$$

was unmöglich für $n > 4$ ist. Ein Widerspruch. □

12.5. Satz (Agrawal, Kayal, Saxena, 2002). Sei $n > 1$ eine natürliche Zahl und sei r eine Primzahl, so daß folgende Bedingungen erfüllt sind:

(1) n ist nicht durch die Primzahlen, die nicht größer als r sind, teilbar;

(2) $\mathrm{ord}_r(n) > \log^2 n$;

(3) $(x+a)^n \equiv x^n + a \mod (x^r - 1, n)$ für alle $1 \leqslant a \leqslant A$, wobei $A = \sqrt{r} \log n$ ist.

Dann ist n eine Potenz einer Primzahl.

12.6. Deterministischer Primtest von Agrawal-Kayal-Saxena. Sei $n > 1$ eine natürliche Zahl. Bezeichnen wir $m = \lfloor \log^5 n \rfloor$. Für $n < 5690034$ prüfen wir nach, ob n eine Primzahl ist. Dafür benutzen wir eine Liste bekannter kleiner Primzahlen oder Eratosphenus sieb. Für $n > 5690034$ gilt $n > m$. In diesem Fall machen wir folgende Schritte.

(1) Prüfen wir nach, ob n durch eine natürliche Zahl aus dem Interval $[2, m]$ teilbar ist. Wenn ja, dann ist n eine zusammengesetzte Zahl. Wenn nein, dann machen wir Schritt 2.

(2) Nach Lemma 12.4 existiert eine Primzahl $r \leqslant m$ mit $\mathrm{ord}_r(n) > \log^2 n$. Finden wir eine solche Zahl mit Probemethode.

(3) Prüfen wir nach, ob die Kongruenz

$$(x+a)^n \equiv x^n + a \mod (x^r - 1, n)$$

für alle $1 \leqslant a \leqslant \sqrt{r} \log n$ gilt. Wenn nein, dann (nach dem Satz 12.3) ist n eine zusammengesetzte Zahl. Wenn ja, dann (nach dem Satz 12.5) ist n eine Potenz einer Primzahl. In dem Fall machen wir Schritt 4.

(4) Prüfen wir nach, ob existieren natürliche Zahlen q, l mit $n = q^l$, $l \geqslant 2$. Wenn ja, dann ist n eine zusammengesetzte Zahl. Wenn nein, dann ist n eine Primzahl.

12.7. Warum der Primtest von Agrawal-Kayal-Saxena polynomiel ist. Bemerken wir, daß $\log(n)$ ungefähr die Anzahl dar Ziffern in binäre Darstellung von n ist. Man sagt, daß ein Test mit einem Input n polynomiel ist, wenn ein Polynom $P(x)$ existiert, so daß für jede Zahl n erfüllt den Test nicht mehr als $P(\log(n))$ Operationen, um eine Antwort auszugeben.

Der Primtest von Agrawal-Kayal-Saxena polynomiel ist. Die kurze Erklärung dafür ist, daß im Lemma 12.4 und im Satz 12.5 die Potenzen von $\log n$ auftauchen. Dazu muß man verstehen, daß die Reste von $x^n + a$ und $(x+a)^n$ modulo $(x^r - 1, n)$ schnell berechnenbar sind. Der erste Rest gleich $x^s + a$ ist, wobei s ein Rest von n modulo r ist. Der zweite Rest wird mit folgender Bemerkung berechnet.

Seien $f(x)$ und $g(x)$ beliebige Reste modulo $(x^r - 1, n)$. Also $f(x)$ und $g(x)$ sind die Polynome von Grad kleiner als r mit Koeffizienten aus der Menge $\{0, 1, \ldots, n-1\}$. Dann kann der Rest von $f(x)g(x)$ modulo $(x^r - 1, n)$ mit Hilfe nicht mehr als r^2 Multiplikationen und r Additionen modulo n berechnet sein. Nennen wir die Menge dieser Operationen als Block-Schritt. Insbesonder, den Rest von $f(x)^2$ modulo $(x^r - 1, n)$ kann man in einem Block-Schritt berechnen.

Sei $n = 2^l$. Dann wird der Rest von $(x+a)^n$ modulo $(x^r - 1, n)$ in $l = \log n$ Block-Schritten berechnet.

Sei n eine beliebige natürliche Zahl. Stellen wir n in der Form $n = 2^{l_1} + 2^{l_2} + \cdots + 2^{l_k}$ dar, wobei $l_1 > l_2 > \cdots > l_k$ ist. Dann wird der Rest von $(x + a)^n$ modulo $(x^r - 1, n)$ in wenige als in $2\lfloor \log n \rfloor$ Block-Schritten berechnet (prüfen Sie das nach!).

12.8. Bemerkung. Seit Jahr 2002 sind etliche Modifikationen und Verbesserungen des Primestes von Agraval-Kayal-Saxena erschienen. Zu der Zeit ist bewiesen, daß die polynomiale Komlexität dieses Testes ist $O(\log^7 n)$ Bit-Operationen. Im Praxis wird die Zahl r neben der Zahl $\log^2 n$ schnell zu finden sein. Die haupte Komplexität dieses Testes liegt im Schritt (3).

Vorlesung 14

Wie kann man große Primzahlen konstruieren. Mersenne-Zahlen

14.1. Der Ring $\mathbb{Z}_n[\sqrt{q}]$. Sei n eine natürliche Zahl und sei $q = -1$ oder q ein Produkt verschiedener Primzahlen in ersten Potenzen: $q = p_1 \dots p_k$. Betrachten wir die Menge aller Ausdrücke der Form $a + b\sqrt{q}$, wobei a, b über den Restklassenring $\mathbb{Z}_n$ laufen. Diese Ausdrücke kann man natürlicherweise addieren und multiplizieren. Zum Beispiel: für $n = 5, q = 3$ gilt

$$(2 + \sqrt{3}) + (3 + 4\sqrt{3}) = 0 + 0\sqrt{3} \quad \text{und} \quad (2 + \sqrt{3})(3 + 4\sqrt{3}) = 3 + \sqrt{3}.$$

So erhalten wir einen Ring mit dem Nullelement $0 + 0\sqrt{q}$ und mit dem Einzelelement $1 + 0\sqrt{q}$. Der Ring wird als $\mathbb{Z}_n[\sqrt{q}]$ bezeichnet. Definieren wir eine Abbildung

$$N : \mathbb{Z}_n[\sqrt{q}] \to \mathbb{Z}_n$$

mit der Regel: $N(a + b\sqrt{q}) = a^2 - qb^2$. Das Element $N(a + b\sqrt{q})$ des Ringes $\mathbb{Z}_n$ heißt *Norm* des Elementes $a + b\sqrt{q}$.

14.2 Aufgabe. 1) Beweisen Sie, daß die Norm zweier Elemente des Ringes $\mathbb{Z}_n[\sqrt{q}]$ gleich das Produkt ihrer Normen ist.

2) Beweisen Sie, daß ein Element des Ringes $\mathbb{Z}_n[\sqrt{q}]$ ein Inverses nur dann hat, wenn seine Norm ein Inverses in dem Ring $\mathbb{Z}_n$ hat.

3) Finden Sie die Ordnung der multiplikativen Gruppe des Ringes $\mathbb{Z}_5[\sqrt{3}]$.

14.3. Definition der Mersenne-Zahl. Eine Mersenne-Zahl M_n ist die Zahl der Form $2^n - 1$.

Bemerken wir, daß die binare Darstellung der Zahl $2^n - 1$ ist $\underbrace{11\dots1}_{n}$. Es ist leicht zu beweisen: wenn $M_n = 2^n - 1$ eine Primzahl ist, dann ist n auch eine Primzahl. Die entgegengesetzte Behauptung gilt nicht: $2^{11} - 1 = 23 \cdot 89$. Bis zu diesem Moment (Juni 2006) sind 43 Mersenne-Primzahlen bekannt. Die ersten 12 davon sind M_n für $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$ und die waren vor dem Jahr 1887 gefunden. Die nächste, 13-te Mersenne-Primzahl M_{521}, war nur im Jahr 1952 mit Hilfe einer Computer gefunden. Die letzte, $M_{30402457}$, wurde erst im Jahr 2005 mit Hilfe gemeinsamer Kalkulationen vieler Netzcomputer gefunden. Die Zahl ist zur Zeit die grösste bekannte Primzahl.

14.4 Definition der Lucas-Folgen. Für die Untersuchung der Mersenne-Primzahlen definieren wir zwei Lucas-Folgen. Die erste $S_0, S_1, S_2, \dots$ ist mit der Regel

$$S_0 = 2, S_1 = 4,\ S_{n+1} = 4S_n - S_{n-1}$$

definiert. Die zweite $L_1, L_2, \dots$ ist mit der Regel

$$L_1 = 4,\ L_{n+1} = L_n^2 - 2$$

definiert.

14.5. Aufgabe. Sei $u = 2 + \sqrt{3}$, $v = 2 - \sqrt{3}$. Beweisen Sie die Formel

1) $u^{n+1} = 4u^n - u^{n-1}$, $v^{n+1} = 4v^n - v^{n-1}$;
2) $S_n = u^n + v^n$;
3) $L_n = u^{2^{n-1}} + v^{2^{n-1}}$;
4) $L_n = S_{2^{n-1}}$.

14.6. Satz (Lucas-Lehmer). Sei $n > 2$ eine natürliche Zahl. Die Zahl M_n ist eine Primzahl nur dann, wenn L_{n-1} durch M_n teilbar ist.

Beweis. Nach der Aufgabe 14.5 haben wir

$$L_{n-1} = u^{2^{n-2}} + v^{2^{n-2}}.$$

Nehmen wir an, daß L_{n-1} durch M_n teilbar ist. Dann gilt

$$u^{2^{n-2}} + v^{2^{n-2}} = kM_n.$$

Multiplizieren wir die Gleichung mal $u^{2^{n-2}}$, dann erhalten wir

$$u^{2^{n-1}} = kM_n u^{2^{n-2}} - 1.$$

Nehmen wir an, daß M_n eine zusammengesetzte Zahl ist. Dann hat sie einen Primteiler $r \leqslant \sqrt{M_n}$. Betrachten wir die letzte Gleichung als die Gleichung in dem Ring $\mathbb{Z}_r[\sqrt{3}]$. Dann gilt $u^{2^{n-1}} = -1$ in dem Ring. Deshalb ist die Ordnung des Elementes u in der multiplikativen Gruppe dieses Ringes gleich 2^n. Da die Ordnung der Gruppe nicht größer als $r^2 - 1$ ist, erhalten wir

$$2^n \leqslant r^2 - 1 < M_n.$$

Ein Widerspruch.

Nehmen wir an, daß $p = 2^n - 1$ eine Primzahl ist. Jetzt zeigen wir, daß die Kongruenz $S_{2^{n-1}} \equiv -2 \pmod{p}$ gilt. Dann wird $L_n \equiv -2 \pmod{p}$ gelten, also $L_{n-1} \equiv 0 \pmod{p}$. Und das ist genau das, was wir beweisen wollen.

Es gilt die Gleichung

$$2 \pm \sqrt{3} = \Big(\frac{\sqrt{2} \pm \sqrt{6}}{2}\Big)^2.$$

Nach der Aufgabe 14.5 erhalten wir

$$S_{2^{n-1}} = \Big(\frac{\sqrt{2}+\sqrt{6}}{2}\Big)^{p+1} + \Big(\frac{\sqrt{2}-\sqrt{6}}{2}\Big)^{p+1} =$$

$$2^{-p} \sum_{0 \leqslant k \leqslant \frac{p+1}{2}} \binom{p+1}{2k} (\sqrt{2})^{p+1-2k} (\sqrt{6})^{2k} =$$

$$2^{\frac{p+1}{2}-p} \sum_{0 \leqslant k \leqslant \frac{p+1}{2}} \binom{p+1}{2k} \cdot 3^k =$$

$$2^{\frac{1-p}{2}} \sum_{0 \leqslant k \leqslant \frac{p+1}{2}} \binom{p+1}{2k} \cdot 3^k.$$

Da p eine Primzahl ist, ist $\binom{p+1}{2k}$ durch p für alle k, außer $k = 0$ und $k = \frac{p+1}{2}$, teilbar. Daraus folgt

$$2^{\frac{p-1}{2}} S_{2^{n-1}} \equiv 1 + 3^{\frac{p+1}{2}} \,(\mathrm{mod}\ p).$$

Weiter werden wir Legendre-Symbole benutzen. Nach der Voraussetzung ist $p = 2^n - 1$ eine Primzahl und $n > 2$. Deshalb ist n eine ungerade Zahl, also $p \equiv 1 \,(\mathrm{mod}\ 3)$, insbesondere $\left(\frac{p}{3}\right) = 1$. Nach dem quadratischen Reziprozitätssatz von Gauss haben wir

$$3^{\frac{p-1}{2}} \equiv \left(\frac{3}{p}\right) \equiv (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right) \equiv -1 \,(\mathrm{mod}\ p).$$

Deshalb gilt

$$2^{\frac{p-1}{2}} S_{2^{n-1}} \equiv 1 + 3 \cdot (-1) \equiv -2 \,(\mathrm{mod}\ p).$$

Weiterhin gilt $p = 2^n - 1 \equiv -1 \,(\mathrm{mod}\ 8)$. Daraus folgt

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv 1 \,(\mathrm{mod}\ p).$$

Endlich haben wir $S_{2^{n-1}} \equiv -2 \,(\mathrm{mod}\ p)$, und das ist das, was wir beweisen wollten. □

Vorlesung 15
RSA-Kryptosystem

Dieses Kryptosystem haben Rivest, Shamir und Adleman im Jahr 1978 vorgeschlagen. Seitdem hat sie eine grosse theoretische und praktische Bedeutung. Dieses Kryptosystem begründet sich auf folgender Vermutung:

Gegeben eine große natürliche Zahl n, ist es schwer die Eulersche Funktion $\phi(n)$ zu berechnen.

Klar, wenn wir n in Primzahlen faktorisieren können, dann können wir $\phi(n)$ leicht berechnen. Aber das Faktorisierungsproblem ist auch vermutlich sehr schwer.

15.1 Beschreibung der RSA-Kryptosystem. Seien $A, B, \ldots$ verschiedene Abonenten im Internet, die mit Hilfe der RSA-Verfahren miteinander kommunizieren wollen. Jeder Abonent wählt ein Paar große Primzahlen (p, q) und konstruiert seinen geheimen und öffentlichen Schlüssel in 5 Schritten:

1. Die Zahl $n = pq$ wird berechnet.
2. Die Zahl $\phi(n) = (p-1)(q-1)$ wird berechnet.
3. Eine natürliche Zahl e mit $2 \leqslant e < \phi(n)$ und $\mathrm{ggT}(e, \phi(n)) = 1$ wird gewählt. Diese Zahl kann man zufällig wählen.
4. Die Zahl d mit $ed \equiv 1 \,(\mathrm{mod}\ \phi(n))$ wird berechnet.
5. Der öffentliche Schlüssel ist (n, e), der private Schlüssel ist (p, q, d).

Dann setzten die Abonenten ihre öffentlichen Schlüssel in das Telefonbuch ein:

$$\begin{array}{ll} \text{Alice :} & (n_a, e_a) \\ \text{Bob :} & (n_b, e_b) \\ \text{Claudia :} & (n_c, e_c) \\ \ldots\ldots & \end{array}$$

Nehmen wir an, daß Alice einen Klartext, also eine Zahl t, an Bob schicken will. Die notwendigen Voraussetzungen sind:

$$t < n_b \quad \text{und} \quad \mathrm{ggT}(t, n_b) = 1.$$

Alice chiffriert die Zahl t mit Hilfe der öffentlichen Schlüssel von Bob (e_b, n_b). Der Chiffretext ist die Zahl

$$s \equiv t^{e_b} \,(\mathrm{mod}\ n_b). \tag{15.1}$$

Diese Zahl schickt sie an Bob durch den offenen Kanal. Bob dechiffriert diese Zahl mit Hilfe seines privaten Schlüssels d_b:

$$t \equiv s^{d_b} \,(\mathrm{mod}\ n_b). \tag{15.2}$$

Beweisen wir, daß Bob die Zahl t richtig berechnet hat. In dem Beweis werden wir folgende Fakten benutzen:

- Nach dem Schritt 4 existiert eine ganze Zahl k, so daß $e_b d_b \equiv 1 + k\phi(n_b)$ gilt.
- Nach dem kleinen Fermatischen Satz gilt $t^{\phi(n_b)} \equiv 1 (\mathrm{mod}\ n_b)$.

Also gilt

$$s^{d_b} \equiv t^{e_b d_b} = t^{1+k\phi(n_b)} \equiv t \cdot (t^{\phi(n_b)})^k \equiv t \,(\mathrm{mod}\ n_b).$$

15.2. Sicherheit des RSA-Kryptosystems. Nehmen wir an, daß Oscar den Chiffretext s erlauscht hat und will ihn mit Hilfe des öffentlichen Schlüssels von Bob (n, e) dechiffrieren. Dann gibt es zwei Möglichkeiten:

1) Die Zahl t direkt aus der Kongruenz (15.1) zu berechnen.

2) Den privaten Schlüssel (p, q, d) aus dem öffentlichen Schlüssel (n, e) zu rekonstruieren.

Besprechen wir nur die zweite Möglichkeit.

Es ist klar, daß wenn wir die Zahl n faktorisieren können, $n = pq$, dann können wir die Zahl d berechnen. Einige Faktorisierungsmethoden werden in der Vorlesung 16 erklärt.

Zur Verwunderung gibt es einen schnelleren probablistischen Algorithmus, der es ermöglicht, die Zahlen (p, q) aus der Zahl d und aus dem öffentlichen Schlüssel (n, e) zu gewinnen. Der Algorithmus wird uns nützlich, wenn wir in der Vorlesung 16 die Wienner-Attacke auf das RSA-Kryptosystem betrachten.

15.3. Ein probablistischer Algorithmus, der es ermöglicht, die Zahlen (p, q) aus den Zahlen d und (n, e) zu berechnen.

Sei die Zahl d und das Paar (n, e) bekannt. Nach dem Schritt 4 ist die Zahl $ed - 1$ durch $\phi(n)$ teilbar. Stellen wir die Zahl in der folgenden Form dar:

$$ed - 1 = 2^s r,$$

wobei r eine ungerade Zahl ist.

Bezeichnung. Seien a, m teilerfremde natürliche Zahlen. Die Ordnung von a modulo m ist die kleinste Zahl $k > 1$ mit $a^k \equiv 1 \,(\mathrm{mod}\ m)$. Diese Ordnung bezeichnen wir als $\mathrm{ord}_m(a)$.

Lemma a. Sei $a \in \mathbb{Z}_n^*$. Wenn q ein Teiler von n ist, dann ist $\mathrm{ord}_q(a)$ ein Teiler von $\mathrm{ord}_n(a)$.

Beweis. Bezeichnen wir $k = \mathrm{ord}_n(a)$. Dann haben wir $a^k \equiv 1 \,(\mathrm{mod}\ n)$. Daraus folgt $a^k \equiv 1 \,(\mathrm{mod}\ q)$ und so ist $\mathrm{ord}_q(a) | k$. □

Lemma b. Für alle $a \in \mathbb{Z}_n^*$ gilt $\mathrm{ord}_n(a^r) \in \{2^i \mid 0 \leqslant i \leqslant s\}$.

Beweis. Da $ed - 1$ durch $\phi(n)$ teilbar ist, haben wir

$$(a^r)^{2^s} = a^{r2^s} = a^{ed-1} = (a^{\phi(n)})^{\frac{ed-1}{\phi(n)}} \equiv 1 \,(\mathrm{mod}\ n).$$

Deshalb ist die Ordnung von a^r ein Teiler von 2^s. □

Lemma c. Sei $a \in \mathbb{Z}_n^*$ und sei $n = pq$, wobei p, q Primzahlen sind. Wenn die Ordnungen von a^r modulo p und q verschieden sind, dann gibt es ein $t \in \{0, 1, \ldots, s-1\}$ mit

$$1 < \mathrm{ggT}(a^{r2^t} - 1, n) < n.$$

Mit anderen Worten, ist $\mathrm{ggT}(a^{r2^t} - 1, n)$ ein echter Teiler von n.

Beweis. Nehmen wir an, daß $\mathrm{ord}_p(a^r) > \mathrm{ord}_q(a^r)$ ist. Nach Lemmas a und b gilt $\mathrm{ord}_q(a^r) = 2^t$, wobei $0 \leqslant t \leqslant s$ ist. Daraus folgt

$$\begin{cases} a^{r2^t} \equiv 1 \,(\mathrm{mod}\ q), \\ a^{r2^t} \not\equiv 1 \,(\mathrm{mod}\ p). \end{cases}$$

Also, ist $a^{r2^t} - 1$ durch q, aber nicht durch p, teilbar. Deshalb gilt $\mathrm{ggT}(a^{r2^t-1}, n) = q$. □

Lemma d. Sei $n = pq$, wobei p, q verschiedene ungerade Primzahlen sind. Die Anzahl der Zahlen $a \in \mathbb{Z}_n^*$, für die a^r modulo p und modulo q verschiedene Ordnungen hat, ist größer als $|\mathbb{Z}_n^*|/2$. □

Algorithmus. Erinnern wir uns, daß $ed = 2^s r$ gilt, wobei r eine ungerade Zahl ist. Nehmen wir zufällig eine $a \in \mathbb{Z}_n^*$ und berechnen $\mathrm{ggT}(a^{r2^i} - 1, n)$ für $i = s, s-1, \ldots, 0$. Wenn einer von diesen ggT größer als 1 und kleiner als n ist, dann ist dieser ggT ein echter Teiler von n, also p oder q. Wenn alle diese ggT entweder 1 oder n sind, dann, nach dem Lemma c, hat a^r die gleichen Ordnungen modulo p und q. In diesem Fall nehmen wir eine andere $a \in \mathbb{Z}_n^*$ und wiederholen die Prozedur. Nach Lemma d ist die Wahrscheinlichkeit, daß wir s Wiederholungen machen werden, kleiner als 2^{-s}. Also finden wir einen echten Teiler von n sehr schnell.

Vorlesung 16
Wieners-Attacke auf das RSA-Kryptosystem

Nehmen wir an, daß der private Schlüssel (p, q, d) folgende Bedingungen erfüllt:

$$q < p < 2q \quad \text{und} \quad d < \frac{1}{3}n^{1/4}. \tag{16.1}$$

Wir zeigen, wie man diese Information benutzen kann, um den privaten Schlüssel aus dem öffentlichen Schlüssel (e, n) zu rekonstruieren.

16.1. Zwei Sätze über Nährungsbrüche.

16.1.1. Satz von Vahlen. Sei α eine reelle Zahl und $\frac{p_{n-1}}{q_{n-1}}$, $\frac{p_n}{q_n}$ zwei nebeneinander stehende Nährungsbrüche von α. Dann gilt

$$|\alpha - \frac{p_{n-1}}{q_{n-1}}| < \frac{1}{2q_{n-1}^2} \qquad \text{oder} \qquad |\alpha - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}.$$

16.1.2. Satz von Legendre. Seien $p, q \in \mathbb{N}$ und sei $\mathrm{ggT}(p, q) = 1$. Wenn

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$$

gilt, dann ist $\frac{p}{q}$ ein Nährungsbruch von α.

16.2. Satz. Mit den Voraussetzungen (16.1) gilt die Ungleichung

$$\Big|\frac{e}{n} - \frac{k}{d}\Big| < \frac{1}{3d^2}. \tag{16.2}$$

für eine $k \in \mathbb{N}$.

Beweis. Da $n = pq$ und $q < p$ ist, haben wir $q < \sqrt{n}$. Dann gilt

$$n - \phi(n) = pq - (p-1)(q-1) = p + q - 1 < 3q < 3\sqrt{n}.$$

Aus dem Schritt 4 in Punkt 15.1 folgt: es existiert eine natürliche k mit

$$ed - k\phi(n) = 1. \tag{16.3}$$

Daraus folgt

$$\begin{aligned} |ed - kn| &= |ed - k\phi(n) - k(n - \phi(n))| \\ &= |1 - k(n - \phi(n))| \\ &< k(n - \phi(n)) < 3k\sqrt{n}. \end{aligned}$$

Die Gleichung (16.3) und die Bedingung $e < \phi(n)$ des Schrittes 3 implizieren $d \geqslant k$. Also haben wir

$$|ed - kn| < 3d\sqrt{n}.$$

Daraus folgt

$$\Big|\frac{e}{n} - \frac{k}{d}\Big| = \Big|\frac{ed - kn}{dn}\Big| < \frac{3}{\sqrt{n}}.$$

Letzlich benutzen wir die Bedingung $d < \frac{1}{3}n^{1/4}$ und erhalten die Ungleichung (16.2). □

16.3. Folgerung. Seien $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ die Nährungsbrüche von $\frac{e}{n}$. Dann gilt $d \in \{q_1, \ldots, q_m\}$.

Beweis. Nach den Sätzen 16.1.2 und 16.2 ist $\frac{k}{d}$ ein Nährungsbruch von $\frac{e}{n}$ und so gilt $d \in \{q_1, \ldots, q_m\}$. □

16.4. Rekonstruktion des Schlüssels (p, q, d)**.**

Jetzt wissen wir, daß d in der Menge $Q = \{q_1, \ldots, q_m\}$ liegt. Diese Menge ist nicht groß: nach dem Satz von Lamé 1.6 ist $m \leqslant 5(\log_{10} n + 1)$. Einige q_i können wir schnell aus der Menge Q eliminieren, wenn wir die folgende Bemerkung benutzen.

Bemerkung. Nach dem Schritt 4 aus dem Punkt 15.1 gilt $ed \equiv 1 \,(\mathrm{mod}\ \phi(n))$. Deshalb für alle $t \in \mathbb{Z}_n^*$ gilt

$$t^{ed} \equiv t \,(\mathrm{mod}\ n).$$

Wählen wir eine $t \in \mathbb{Z}_n^*$ zufällig. Wenn für einen $q_i \in Q$ gilt

$$t^{eq_i} \not\equiv t \,(\mathrm{mod}\ n),$$

dann ist $d \neq q_i$ und wir können q_i aus der Menge Q eliminieren. Nach solchen Eliminierungen erhalten wir eine Untermenge $\overline{Q} \subseteq Q$, so daß $d \in \overline{Q}$ ist. Für den restlichen $q_i \in \overline{Q}$ müssen wir den Algorithmus aus dem Punkt 15.3 durchführen. Für einen solchen q_i, nämlich für $q_i = d$, wird der Algorithmus die gewünschten Zahlen p, q produzieren.

Vorlesung 17
Elliptische Kurven als Gruppen

Beispiel. Sei α eine reelle Zahl. Betrachten wir die Gleichung

$$X^3 + Y^3 = \alpha.$$

Mit Hilfe der Transformation

$$\begin{aligned} X = &\quad \frac{y + 36\alpha}{6x}, \\ Y = &\quad \frac{36\alpha - y}{6x} \end{aligned}$$

umschreien wir die Gleichung als

$$y^2 = x^3 - 432\alpha^2. \tag{2}$$

Inverse Transformation ist

$$\begin{aligned} x = &\quad \frac{12\alpha}{X + Y}, \\ y = &\quad \frac{36\alpha(X - Y)}{X + Y}. \end{aligned}$$

Deshalb ist die Transformation birational.

Definition. Eine *ebene Kubik* (= ebene kubische Kurve) ist eine Kurve, die mit folgender Formel beschrieben sein kann:

$$AX^3 + BX^2Y + CXY^2 + DY^3 + eX^2 + fXY + gY^2 + hX + iY + j = 0 \tag{3}$$

Satz. Für jede Gleichung (3) existiert eine birationale Transformation

$$\begin{aligned} X = &\quad r_1(x, y), \\ Y = &\quad r_2(x, y), \end{aligned}$$

so dass die Gleichung in der Form

$$y^2 = x^3 + ax^2 + bx + c \tag{4}$$

umgeschrieben sein kann.

Die Graph von $y^2 = f(x)$, wobei $f(x) = x^3 + ax^2 + bx + c$ ist.

Fall 1. $f(x)$ hat nur 1 reelle Nullstelle α.

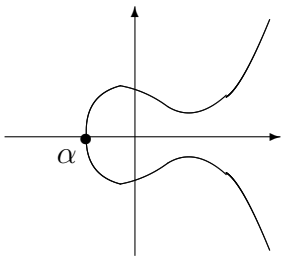
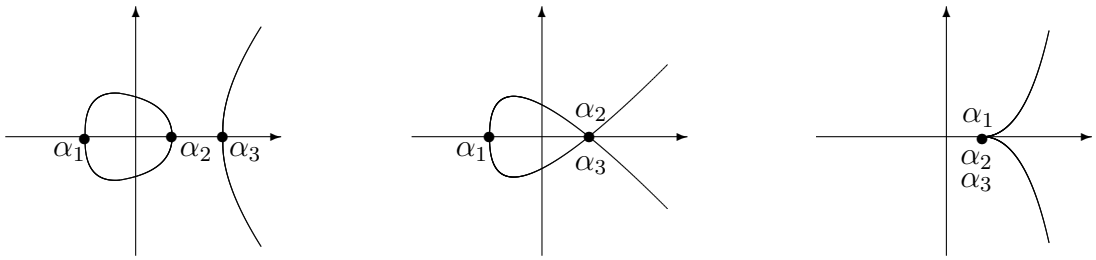


Bild 1

Fall 2. $f(x)$ hat 3 reelle Nullstellen $\alpha_1, \alpha_2, \alpha_3$. Der Fall zerfällt in 3 Unterfälle:



(a) $\alpha_1 \neq \alpha_2 \neq \alpha_3$ (b) $\alpha_1 \neq \alpha_2 = \alpha_3$ (c) $\alpha_1 = \alpha_2 = \alpha_3$

Bild 2

Die Kurven in den Fällen 2(a) und 2(b) sind singular.

Definition. Eine ebene Kubic (3) heißt *elliptisch*, wenn nach einer birationalen Transformation die Gleichung (3) in der Form

$$y^2 = x^3 + ax^2 + bx + c \tag{5}$$

umgeschrieben sein kann, wobei das Polynom $f(x) = x^3 + ax^2 + bx + c$ entweder nur 1 reelle Nullstelle oder 3 verschiede reelle Nulstellen hat.

Also, elliptische Kurven in der Form (5) fallen entweder im Fall 1 oder im Fall 2(a).

Punkte addieren. Sei C eine elliptische Kurve. Wählen wir einen Punkt $\mathcal{O} \in C$. Definieren wir die Addition von Punkten auf C.

Seien P und Q zwei Punkte auf C. Legen wir eine Gerade durch P und Q. Der dritte Schnittpunkt dieser Gerade mit C bezeichnen wir als $P*Q$. Danach legen wir eine Gerade durch $\mathcal{O}$ und $P*Q$. Der dritte Schnittpunkt dieser Gerade mit C bezeichnen wir als $P+Q$.

Wenn $P = Q$ ist, dann wird die erste Gerade als die Tangente an C im Punkte P gemeint.

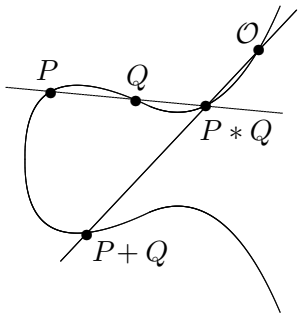


Bild 3

Jetzt zeigen wir, dass C mit dieser Addition eine kommutative Gruppe mit dem neutralen Element $\mathcal{O}$ ist. Die Kommutativität ist klar. Bild 4 zeigt, dass $\mathcal{O}$ ein neutrales Element ist. Bild 5 zeigt, wie kann man inverse Elemente konstruieren.

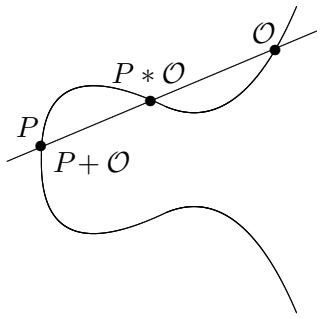


Bild 4

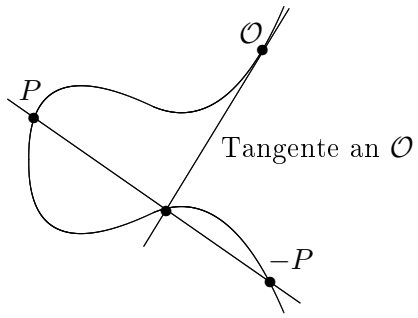


Bild 5

Bild 6 illustriert die Assoziativität: $(P + Q) + R = P + (Q + R)$. Um das streng zu beweisen, muss man exakte Formel für die Addition aufschreiben.

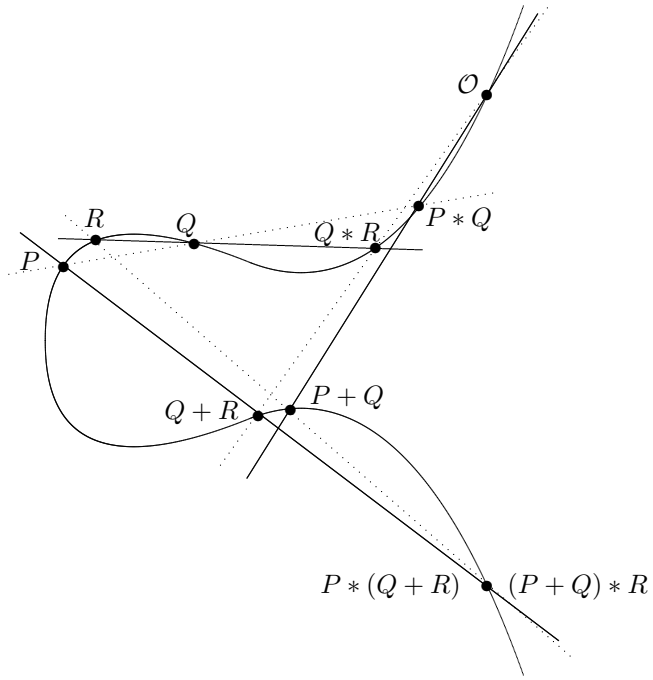


Bild 6

Exakte Berechnung von $P_1 + P_2$.

Sei C eine elliptische Kurve: $y^2 = x^3 + ax + bx + c$. Zur Vereinfachung nehmen wir an, dass $\mathcal{O} = \infty$ ist und dass die Gerade durch ∞ und einen beliebigen Punkt vertikal ist.

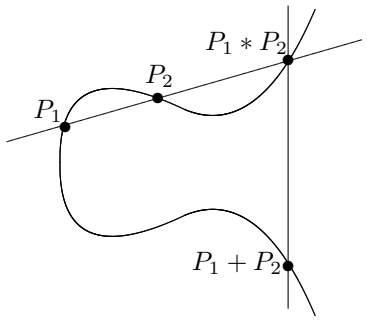


Bild 7

1. Seien $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ zwei Punkte auf der Kurve C, wobei $x_1 \neq x_2$ ist. Sei $P_1 * P_2 = (x_3, y_3)$. Dann ist $P_1 + P_2 = (x_3, -y_3)$. Berechnen wir x_3 und y_3.

Die Gerade L durch P_1 und P_2 hat die Gleichung $y = \lambda x + \nu$, wobei $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ und $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$ ist. Dann erfüllen die x-Koordinaten der Schnittpunkte L und C die Gleichung

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c.$$

Daraus folgt

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0.$$

Da sind x_1, x_2, x_3 die Lösungen der Gleichung, haben wir

$$\lambda^2 - a = x_1 + x_2 + x_3.$$

Also, ist

$$\begin{aligned} x_3 &= \lambda^2 - a - x_1 - x_2, \\ y_3 &= \lambda x_3 + \nu. \end{aligned}$$

2. Berechnen wir $P + P$, wobei $P = (x_1, y_1) \in C$ ist. In dem Fall ist L die Tangente an P. Die Tangente hat die Gleichung $y = \lambda x + \nu$, wobei

$$\lambda = \Big(\frac{dy}{dx}\Big)_{x=x_1} = \Big(\frac{f'(x)}{2y}\Big)_{\substack{x=x_1 \\ y=y_1}} = \Big(\frac{3x^2 + 2ax + b}{2\sqrt{x^3 + ax^2 + bx + c}}\Big)_{x=x_1}$$

ist. Änlich wie oben kann man berechnen, dass x-Koordinate von $P + P$ gleich

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)}$$

ist. Diese Formel heißt die *Duplikations-Formel*.

3. Falls $P_1 = (x, y)$ und $P_2 = (x, -y)$, definiert man $P_1 + P_2 = \mathcal{O}$.

Vorlesung 18

Von Gauß zu Hasse

Sei p eine Primzahl. Betrachten wir zwei Gleichungen über dem Körper $\mathbb{F}_p$:

$$x^3 + y^3 = 1 \tag{1}$$

und

$$x^3 + y^3 + z^3 = 0. \tag{2}$$

Wenn (x_1, y_1, z_1) eine Lösung von (2) ist, dann ist (ax_1, ay_1, az_1) auch eine für alle $a \in \mathbb{F}_p^*$. Zwei Lösungen (x_1, y_1, z_1) und (x_2, y_2, z_2) heißen *äquivalent*, wenn eine $a \in \mathbb{F}_p^*$ mit $(x_2, y_2, z_2) = (ax_1, ay_1, az_1)$ existiert. Eine *projektive Lösung* von (2) ist eine Äquivalenzklasse

$$[(x_1, y_1, z_1)] = \{(ax_1, ay_1, az_1) \,|\, a \in \mathbb{F}_p^*\},$$

wobei (x_1, y_1, z_1) eine nichtnullische Lösung von (2) ist.

Behauptung. Sei C die Anzahl der Lösungen von (1) und sei D die Anzahl der projektiven Lösungen von (2). Dann ist $C = D - 1$ oder $C = D - 3$.

Satz (Gauß). Sei p eine Primzahl und sei M_p die Anzahl der projektiven Lösungen der Gleichung $x^3 + y^3 + z^3 = 0$ in $\mathbb{F}_p$.

Fall 1: $p \not\equiv 1 \mod 3$. Dann gilt $M_p = p + 1$.

Fall 2: $p \equiv 1 \mod 3$. Dann existiert ein einziges Paar der ganzen Zahlen A, B, so dass $4p = A^2 + 27B^2$ und $A \equiv 1 \,(\mod 3)$, $B > 0$ gelten. Außerdem ist $M_p = p + 1 + A$.

Beweis. Wir beweisen den Satz nur im Fall 1. Im Fall 2 ist der Beweis zu kompliziert.

Definieren wir eine Abbildung $\phi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ mit der Formel $\phi(x) = x^3$. Dann ist ϕ ein Homomorphismus.

Fall 1. Sei $p \not\equiv 1 \mod 3$. Dann ist $3 \nmid (p-1) = \mathbb{F}_p^* \cong \mathbb{Z}_{p-1}$. Deshalb enthält $\mathbb{Z}_p^*$ keine Elemente der Ordnung 3. Deshalb ist $\mathrm{Ker}(\phi) = 1$ und ϕ ist ein Isomorphismus. Also hat jedes Element von $\mathbb{F}_p^*$ eine einzige Wurzel des Grades 3. Dann ist die Anzahl der projektiven Lösungen von $x^3 + y^3 + z^3 = 0$ in $\mathbb{Z}_p^*$ gleich der Anzahl der projektiven Lösungen von $x + y + z = 0$ in $\mathbb{Z}_p^*$, also gleich $p + 1$.

Folgerung. $|M_p - (p+1)| < 2\sqrt{p}$.

Definition. Sei p eine Primzahl. Eine Kurve $y^2 = x^3 + ax^2 + bx + c$ mit Koeffizienten aus $\mathbb{F}_p$ heißt elliptisch, wenn das Polynom $f(x) = x^3 + ax^2 + bx + c$ nur einfache Nullstellen hat.

Wir definieren die Addition auf dieser Kurve E mit der Formel aus der Vorlesung 17. Dann ist E eine Gruppe. Die Anzahl der Elemente auf der E bezeichnen wir als $|E|$.

Satz (Hasse). Sei $p \geqslant 3$ eine Primzahl und sei E eine elliptische Kurve über dem Körper $\mathbb{F}_p$. Dann gilt

$$||E| - (p+1)| < 2\sqrt{p}.$$

Beispiel. Betrachten wir die Kurve $E: \; y^2 = x^3 + x - 1$ über dem Körper $\mathbb{F}_5$. Dann ist $|E| = 9$ (wir zählen $\mathcal{O}$ dazu).

Vorlesung 19

Satz von Nagell – Lutz

Diskriminant. Sei $f(x) = x^n + a_{n-1}x^n + \cdots + a_0$ ein Polynom und seien $\alpha_1, \ldots, \alpha_n$ seine Nullstellen. *Diskriminant von* $f(x)$ ist

$$\mathbf{Dis}(f(x)) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Da $\mathbf{Dis}(f(x))$ eine symmetrische Funktion von $\alpha_1, \ldots, \alpha_n$ ist, können wir $\mathbf{Dis}(f(x))$ als eine Funktion von $\sigma_1, \ldots, \sigma_n$ und letztlich als eine Funktion von $a_{n-1}, \ldots, a_0$ aufschreiben.

Beispiele. 1) Sei $f(x) = x^2 + bx + c$. Dann gilt

$$\mathbf{Dis}(f(x)) = b^2 - 4c.$$

2) Sei $f(x) = x^3 + bx + c$. Dann gilt

$$\mathbf{Dis}(f(x)) = -4b^3 - 27c^2.$$

3) Sei $f(x) = x^3 + ax^2 + bx + c$. Dann gilt

$$\mathbf{Dis}(f(x)) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Lemma. Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom mit dem Hauptkoeffizienten 1. Dann existieren Polynome $r(x), s(x) \in \mathbb{Z}[x]$, so dass gilt

$$\mathbf{Dis}(f(x)) = r(x)f(x) + s(x)f'(x).$$

Satz (Nagell – Lutz). Sei $y^2 = f(x) = x^3 + ax^2 + bx + c$ eine elliptische Kurve mit ganzen Koeffizienten a, b, c. Sei $P = (x, y)$ ein rationaler Punkt auf C der endlichen Ordnung. Dann ist $x, y \in \mathbb{Z}$. Zudem ist es entweder $y = 0$ oder $y | \mathbf{Dis}(f(x))$. Im Fall $y = 0$ ist $2P = 0$.

Beweis. Der schwierigste Teil dieses Beweises ist zu zeigen: alle rationalen Punkte auf C der endlichen Ordnung sind ganz. Nehmen wir an, dass das schon bewiesen ist. Dann sind die rationalen Punkte $P = (x, y)$ und $2P = (X, Y)$ ganz. Aus der Vorlesung 17 haben wir im Fall $y \neq 0$ zwei Formeln:

$$2x + X = \lambda^2 - a,$$

$$\lambda = \frac{f'(x)}{2y}.$$

Daraus folgt, dass λ eine ganze Zahl und $y | f'(x)$ ist. Da $y | f(x)$ ist, haben wir $y | \mathbf{Dis}(f)$.

Folgerung. Sei $y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve mit ganzen Koeffizienten a, b, c. Man kann algorithmisch alle rationalen Punkte der endlichen Ordnung auf der Kurve finden.

Vorlesung 20

Elliptische Kurven Algorithmus von Lenstra[4]

20.1. Reduktion von Kurven Modulo p. Sei C eine elliptische Kurve, gegeben mit der Gleichung

$$y^2 = x^3 + ax^2 + bx + c,$$

wobei a, b, c ganze Zahlen sind. Sei $p \geqslant 3$ eine Primzahl, so dass $p \nmid \mathrm{Dis}(x^3 + ax^2 + bx + c)$ ist. Betrachten wir zwei neue Kurven $C(\mathbb{Q})$ und $C(\mathbb{F}_p)$. Die erste Kurve ist die Kurve über $\mathbb{Q}$ und enthält nur rationale Punkte der Kurve C. Die zweite ist die Kurve über $\mathbb{F}_p$ und ist mit der Gleichung

$$y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}$$

gegeben, wobei $\overline{m}$ den Rest von m modulo p bezeichnet. Bezeichnen wir das neutrale Element dieser Kurve als $\widetilde{\mathcal{O}}$.

Merken wir an, dass beide Kurven nichtsingular sind, deshalb können wir sie als Gruppen betrachten. Jetzt definieren wir eine Abbildung $\phi : C(\mathbb{Q}) \to C(\mathbb{F}_p)$ mit der Regel:

$$\phi\Big(\frac{a}{b}, \frac{c}{d}\Big) = \begin{cases} (\overline{a}\,\overline{b}^{-1},\ \overline{c}\,\overline{d}^{-1}) & \text{falls } p \nmid b \text{ und } p \nmid d \text{ ist,} \\ \widetilde{\mathcal{O}} & \text{sonst,} \end{cases}$$

$$\phi(\mathcal{O}) = \widetilde{\mathcal{O}}.$$

Die Abbildung $\phi : C(\mathbb{Q}) \to C(\mathbb{F}_p)$ heißt *Reduktion der Kurve C Modulo p.* Bezeichnen wir $\phi(P) = \widetilde{P}$.

20.2. Satz. Die Abbildung $\phi : C(\mathbb{Q}) \to C(\mathbb{F}_p)$ ist ein Homomorphismus. Wenn H eine endliche Untergruppe von $C(\mathbb{Q})$ ist, ist $\phi|_H : H \to \phi(H)$ ein Isomorphismus.

Beweis. Die erste Aussage prüft man unmittelbar nach. Beweisen wir die zweite. Sei P ein Element der endlichen Ordnung auf $C(\mathbb{Q})$ und sei $P \neq \mathcal{O}$. Dann hat P die Form $P = (x, y)$. Nach dem Nagel-Lutz Satz sind x, y ganze Zahlen. Deshalb ist $\phi(P) \neq \widetilde{\mathcal{O}}$.

20.3. Satz. Sei (x, y) einen rationalen Punkt auf der elliptischen Kurve $y^2 = x^3 + ax^2 + bx + c$ mit $a, b, c \in \mathbb{Z}$. Dann hat er die Form

$$(x, y) = \Big(\frac{n}{d^2}, \frac{m}{d^3}\Big),$$

wobei n, m, d ganze Zahlen sind und $\mathbf{ggT}(n, d) = \mathbf{ggT}(m, d) = 1$ ist.

[4]H.W. Lenstra, Jr., *Factoring integers with elliptic curves*, Annals of Math., **126** (1987), 649-673.

20.4. Elliptische Kurven Algorithmus von Lenstra.
Sei $n \geqslant 2$ eine zusammengesetzte Zahl. Wir wollen einen Faktor von n finden.

Schritt 1. Prüfen wir nach, ob $\mathbf{ggT}(n, 6) = 1$ ist und ob $n \neq m^r$ für einen $r \geqslant 2$ ist.

Schritt 2 (Wahl der kubischen Kurve C und der Punkte $P \in C$).

(a) Wählen wir natürliche Zahlen b, x_1, y_1 zufällig in dem Intervall $[1, n]$.

(b) Berechnen wir $c = y_1^2 - x_1^3 - bx_1 \pmod{n}$. Sei C die Kurve

$$y^2 = x^3 + bx + c$$

und sei $P = (x_1, y_1) \in C$.

Schritt 3 (Nichtsingularität von $C(\mathbb{F}_p)$).
Prüfen wir nach, ob $\mathbf{ggT}(4b^3 + 27c^2, n) = 1$ ist. (Wenn $\mathbf{ggT} = n$ ist, dann wählen wir andere b. Wenn $1 < \mathbf{ggT} < n$ ist, dann ist dieser $\mathbf{ggT}$ ein echter Faktor von n.)

Schritt 4. Berechnen wir $A = \sqrt{n} + 1 + 2n^{1/4}$. Wählen wir eine "kleine" Zahl B (empfohlen ist $B := e^{\sqrt{(\ln n)(\ln\ln n)/4}}$) und setzen wir

$$k = \prod_{\substack{q \leqslant B \\ q \in \mathrm{Prim}}} q^{a_q},$$

wobei $a_q = \lfloor \log_q A \rfloor$ ist.

Schritt 5. Berechnen wir

$$kP = \left(\frac{a_k}{d_k^2}, \frac{b_k}{d_k^3}\right) \mod n.$$

Schritt 6. Berechnen wir $D = \mathbf{ggT}(d_k, n)$. Wenn $1 < D < n$ ist, dann ist D ein echter Faktor von n. Wenn $D = 1$ ist, dann kehren wir zu Schritt 2 zurück und wählen eine neue Kurve oder wir kehren zu Schritt 4 zurück und vergrößern B. Wenn $D = n$ ist, dann kehren wir zu Schritt 2 zurück und wählen eine neue Kurve oder wir kehren zu Schritt 4 zurück und verkleinern B.

Erklärung 1. Sei p ein Primteiler von n (wir kennen p noch nicht). Nehmen wir an, dass wir bei der Auswahl des Punktes P, der Kurve C und der Zahl k Glück hatten, dass die Ordnung von $\widetilde{P}$ in der Kurve $C(\mathbb{F}_p)$ nur durch "kleine" Primzahlen q teilbar ist, die im Schritt 4 auftauchen. Dann ist

$$\widetilde{kP} = k\widetilde{P} = \widetilde{\mathcal{O}}.$$

Also ist $p | d_k$ und so ist $p | \mathbf{ggT}(d_k, n)$. Wenn $n \nmid d_k$ ist, dann ist $\mathbf{ggT}(d_k, n)$ ein echter Teiler von n.

Modulo einer Vermutung, hat Lenstra bewiesen:

Mit dem festgelegten $B = e^{\sqrt{(\ln n)(\ln\ln n)/4}}$ werden wir das Glück mit der Wahl von P und C im Schnitt einmal pro B Iterationen haben. Das impliziert, dass die erwartete Laufzeit des Algorithmus

$$O\Big(e^{\sqrt{(1+o(1))(\ln n)(\ln\ln n)}}\Big)$$

ist. Die Vermutung von Lenstra wird in dem Punkt 20.5 formuliert. In dem Punkt befindet sich auch die Erklärung 2.

Wie berechnet man schnell kP.

(1) Man soll die Primzahlzerlegung von k und die binale Darstellung von Zahlen benutzen.

(2) Seien $Q_1 = (x_1, y_1)$ und $Q_2 = (x_2, y_2)$ zwei verschiedene Punkte auf C. Dann wird $Q_3 = Q_1 + Q_2 = (x_3, y_3)$ mit folgenden Formeln berechnet:

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = -\lambda x_3 - (y_1 - \lambda x_1),$$

wobei

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

ist.

(3) Sei $Q = (x, y)$. Dann wird $2Q = (x_3, y_3)$ mit folgenden Formeln berechnet:

$$x_3 = \lambda^2 - 2x, \qquad y_3 = -\lambda x_3 - (y - \lambda x),$$

wobei

$$\lambda = \frac{f'(x)}{2y} = \frac{3x^2 + 2ax + b}{4y^2}$$

ist.

(4) Da wir $D = \mathbf{ggT}(d_k, n)$ berechnen wollen, können wir alle Berechnungen modulo n führen. Das Problem ist bei der Berechnung von λ, da dort durch $x_2 - x_1$ oder durch y geteilt wird. Zeigen wir, zum Beispiel für die erste Variante, dass das kein großes Problem ist.

Fall 1. $\mathbf{ggT}(x_2 - x_1, n) = 1$. Dann können wir $x_2 - x_1$ in dem Ring $\mathbb{Z}_n$ invertieren.

Fall 2. $1 < \mathbf{ggT}(x_2 - x_1, n) < n$. Dann ist $\mathbf{ggT}(x_2 - x_1, n)$ ein echter Faktor von n.

Fall 3. $\mathbf{ggT}(x_2 - x_1, n) = n$. Dann ist die beste Lösung, eine andere Kurve zu wählen.

Fall 3 passiert selten.

20.5. Warum der Algorithmus von Lenstra schnell läuft

Satz (Hasse). Sei $p \geqslant 3$ eine Primzahl und sei E eine elliptische Kurve über dem Körper $\mathbb{F}_p$. Dann gilt

$$||E| - (p+1)| < 2\sqrt{p}.$$

Definition. Für jede reelle $x > e$ definieren wir eine Funktion

$$L(x) = e^{\sqrt{(\ln x)(\ln\ln x)}}.$$

Satz (Canfeld, Erdös, Pomerance). Sei $\alpha > 0$ eine reelle Zahl (Parameter). Sei s eine zufällig ausgewählte natürliche Zahl in dem Intervall $[1, x]$. Dann sind alle Primfaktoren von s kleiner als $L(x)^\alpha$ mit der Wahrscheinlichkeit

$$\frac{1}{L(x)^{1/2\alpha - o(1)}}.$$

Vermutung von Lenstra. Desselbe gilt, wenn wir den Intervall $[1, x]$ nach dem Intervall

$$[x + 1 - 2\sqrt{x},\ x + 1 + 2\sqrt{x}]$$

ersetzen.

Erklärung 2. Sei p ein fixierter echter Teiler von n. Wenn wir C mit Hilfe der Parameter b oder P variieren, dann variieren wir die Kurve $E = C(\mathbb{F}_p)$. Die Abhängigkeit der Kurve E von Parameter b und P bezeichnen wir als $E(b, P)$. Nach dem Satz von Hasse liegt $|E(b, P)|$ in dem Intervall $[p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$. Außerdem ist die Verteilung von $|E(b, P)|$ in dem Intervall gleichmäßig. Nach der Vermutung von Lenstra können wir erwarten, dass für viele Parameter b und P die Ordnung $|E(b, P)|$ nur "kleine" Primteiler hat. Dann ist k durch $|E(b, P)|$ teilbar (siehe Schritt 4). Diese Eigenschaft haben wir in der Erklärung 1 benutzt.

Vorlesung 21

Diskrete Fouriersche Transformation

Seien $f(x)$ und $g(x)$ zwei Polynome mit ganzen Koeffizienten des Grades n und m. Wie kann man schnell diese Polynome multiplizieren? Ihr Produkt ist ein Polynom $h(x)$ des Grades $n+m$. Nehmen wir $n+m+1$ verschiedene Zahlen $x_0, \ldots, x_{n+m}$ und berechnen wir die Werte $h(x_i) = f(x_i)g(x_i)$. Das können wir mit dem Hornerschen Schema berechnen. Danach rekonstruieren wir $h(x)$ aus diesen Werten mit Hilfe der Interpolations-Formel von Lagrange. Das nimmt aber sehr viel Zeit. Folgende Prozedur reduziert die Zeit wesentlich.

1) Man nimmt eine spezifische Zahl ω und berechnet $h(\omega^i) = f(\omega^i)g(\omega^i)$ für $i = 0, 1, \ldots, n+m$. Dafür benutzt man die (gerade) diskrete Fouriersche Transformation.

2) Um $h(x)$ aus den Werten zu rekonstruieren, benutzt man die inverse diskrete Fouriersche Transformation.

Gerade und inverse diskrete Fouriersche Tranformationen sind änlich. Man berechnet sie schnell mit Hilfe der Technik "teile und herrsche" (es wird im Punkt 22.2 erklärt).

In dieser Vorlesung definieren wir ein primitives Element des Grades n und gerade und inverse diskrete Fouriersche Transformationen. In der Vorlesung 22 wird es gezeigt, wie man schnell die Transformationen und das Produkt zweier Polynomen berechnen kann.

Sei K ein kommutativer Ring mit Einselelement und sei $n > 1$ eine natürliche Zahl, die nicht gleich 0 im K ist.

21.1. Definition. Ein Element $\omega \in K$ heißt ein *primitives Element des Grades* n in dem Ring K, wenn für jedes $1 \leqslant j \leqslant n-1$ die folgende Bedingung erfüllt ist:

(1) $\sum\limits_{i=0}^{n-1} \omega^{ij} = 0.$

Bemerkung. Aus der Bedingung folgt:

(2) Das Element ω hat die Ordnung n.

(3) Es gilt $\sum\limits_{i=0}^{n-1} \omega^{ij} = 0$ für jedes $j \not\equiv 0 \,(\mathrm{mod}\ n)$ und

es gilt $\sum\limits_{i=0}^{n-1} \omega^{ij} = n$ für jedes $j \equiv 0 \,(\mathrm{mod}\ n)$.

Beweis. (2) Zeigen wir, daß $\omega^n = 1$ ist. Aus (1) folgt $1 + \omega + \cdots + \omega^{n-1} = 0$. Da die Gleichung $\omega^n - 1 = (\omega - 1)(1 + \omega + \cdots + \omega^{n-1})$ gilt, haben wir auch $\omega^n = 1$.

Zeigen wir, daß $\omega^j \neq 1$ für $j = 1, 2, \ldots, n-1$ ist. Nehmen wir an, daß für einen solchen j gilt $\omega^j = 1$. Dann erhalten wir aus (1), daß $n = 0$ in K ist. Ein Wiederspruch.

(3) Sei $j = j_0 + kn$, wobei $1 \leqslant j_0 \leqslant n-1$ und $k \in \mathbb{N}$ ist. Dann folgt aus (1) und (2)

$$\sum_{i=0}^{n-1} \omega^{ij} = \sum_{i=0}^{n-1} \omega^{i(j_0+kn)} = \sum_{i=0}^{n-1} \omega^{ij_0} = 0.$$

□

21.2. Beispiel. In dem Restklassenring $\mathbb{Z}_7$ ist $\omega = 2$ ein primitives Element des Grades $n = 3$. In der Tat, in dem Ring gelten

$$\begin{array}{ll} 1 + \omega + \omega^2 = 0 & \text{für} \quad j = 1, \\ 1 + \omega^2 + \omega^4 = 0 & \text{für} \quad j = 2. \end{array}$$

21.3. Definition. Sei ω ein *primitives Element des Grades* n in dem Ring K.

Diskrete Fouriersche Tranformation ist die Abbildung $K^n \to K^n$, die jedem Tupel $(a_0, \dots, a_{n-1})$ aus K^n ein Tupel $(b_0, \dots, b_{n-1})$ aus K^n stellt, so daß für jedes $0 \leqslant i \leqslant n-1$ gilt

$$b_i = \sum_{j=0}^{n-1} a_j \omega^{ij}. \tag{21.1}$$

Mit dem Tupel $(a_0, \dots, a_{n-1})$ verbinden wir das Polynom $f(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$. Dann ist es klar, daß man auch mit der folgenden Formel die Fouriersche Transformation angeben kann:

$$(a_0, a_1, \dots, a_{n-1}) \mapsto \big(f(1), f(\omega), \dots, f(\omega^{n-1})\big). \tag{21.2}$$

21.4. Satz. Für jedes k mit $0 \leqslant k \leqslant n-1$ gilt

$$a_k = \frac{1}{n} \sum_{i=0}^{n-1} b_i \omega^{-ik}. \tag{21.3}$$

Beweis. Beweisen wir, daß die Summe in (21.3) gleich na_k ist.

$$\sum_{i=0}^{n-1} b_i \omega^{-ik} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_j \omega^{ij}\omega^{-ik} = \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_j \omega^{ij}\omega^{-ik} = \sum_{j=0}^{n-1} a_j \sum_{i=0}^{n-1} \omega^{i(j-k)}. \tag{21.4}$$

Für $j \neq k$ haben wir

$$\sum_{i=0}^{n-1} \omega^{i(j-k)} = 0,$$

und für $j = k$ haben wir

$$\sum_{i=0}^{n-1} \omega^{i(j-k)} = n.$$

Deshalb ist die Summe in (21.4) gleich na_k. □

21.5. Definition. *Inverse diskrete Fouriersche Tranformation* ist die Abbildung $K^n \to K^n$, die jedem Tupel $(b_0, \dots, b_{n-1})$ aus K^n ein Tupel $(a_0, \dots, a_{n-1})$ aus K^n stellt, so daß für jedes $0 \leqslant k \leqslant n-1$ die Formel (21.3) gilt.

Mit dem Tupel $(b_0, \dots, b_{n-1})$ verbinden wir das Polynom $F(x) = b_0 + b_1 x + \dots + b_{n-1}x^{n-1}$. Dann ist es klar, daß man auch mit der folgenden Formel die inverse Fouriersche Transformation angeben kann:

$$(b_0, b_1, \dots, b_{n-1}) \mapsto \frac{1}{n}\big(F(1), F(\omega^{-1}), \dots, F(\omega^{-(n-1)})\big).$$

Da $\omega^n = 1$ ist, können wir die Formel so umschreiben:

$$(b_0, b_1, \ldots, b_{n-1}) \mapsto \frac{1}{n}\big(F(1), F(\omega^{n-1}), \ldots, F(\omega)\big). \tag{21.5}$$

21.6. Lemma. Sei K ein kommutativer Ring mit Einselelement. Dann gilt für jedes Element $a \in K$ und jede Zahl $n = 2^k$

$$\sum_{i=0}^{n-1} a^i = \prod_{t=0}^{k-1} (1 + a^{2^t}).$$

Beweis. Induktion per k. Für $k = 1$ ist die Gleichung offenbar. Nehmen wir an, daß die Gleichung für $k-1$ erfüllt ist. Dann erhalten wir für k

$$\begin{aligned}
\sum_{i=0}^{n-1} a^i &= (1+a) \sum_{i=0}^{\frac{n}{2}-1} a^{2i} && \text{(offenbar)} \\
&= (1+a) \prod_{t=0}^{k-2} (1 + (a^2)^{2^t}) && \text{(nach induktiver Voraussetzung)} \\
&= (1+a) \prod_{t=1}^{k-1} (1 + a^{2^t}) && = \prod_{t=0}^{k-1} (1 + a^{2^t}).
\end{aligned}$$

□

21.7. Satz. Seien $n = 2^k$, ω eine gerade Zahl und $M = \omega^{n/2} + 1$. Dann ist ω ein primitives Element des Grades n in dem Ring $\mathbb{Z}_M$.

Beweis. Das Element n hat inverses in dem Ring $\mathbb{Z}_M$, da n und M teilerfremde Zahlen sind. Beweisen wir, daß die Bedingung (1) aus Definition 21.1 erfüllt ist:

$$\sum_{i=0}^{n-1} \omega^{ij} \equiv 0 \,(\bmod\, M).$$

Nach Lemma 21.6 haben wir

$$\sum_{i=0}^{n-1} (\omega^j)^i = \prod_{t=0}^{k-1} (1 + \omega^{j2^t}).$$

Deshalb ist hinreichend zu beweisen, daß ein t mit $0 \leqslant t \leqslant k-1$ existiert, so daß gilt

$$1 + \omega^{j2^t} \equiv 0 \,(\bmod\, M).$$

Sei $j = 2^s l$, wobei l eine ungerade Zahl ist. Dann gilt für $t = k - 1 - s$

$$1 + \omega^{j2^t} = 1 + \omega^{2^{k-1} l} = 1 + (\omega^{n/2})^l \equiv 1 + (-1)^l \equiv 0 \,(\bmod\, M).$$

□

Vorlesung 22

Schnelle Berechnungen mit Hilfe der diskreten Fourierschen Transformation

Hier setzen wir $n = 2^k$, $\omega = 2^s$ und werden die Berechnungen in dem Restklassenring $K = \mathbb{Z}_M$ führen, wobei $M = \omega^{n/2} + 1$ ist. Gerade diskrete Fouriersche Transformation von K^n nach K^n wird als $\mathcal{F}$ und inverse als $\mathcal{F}^{-1}$ bezeichnet.

22.1. Zerlegung des Polynomes x^n-1 in dem Ring K. In weiteren Berechnungen müssen wir einige Polynomen durch das Polynom $x^n - 1$ und seine Faktoren teilen. In dem Punkt wird gezeigt, wie man das Polynom $x^n - 1$ auf kleinere Polynome zerlegen kann. Erst zerlegen wir es in zwei Faktoren, danach in vier, und so weiter, und am Ende in n lineare Polynomen. In dem Prozess werden wir immer $+1$ nach $-\omega^{n/2}$ und $+\omega^t$ nach $-\omega^{t+n/2}$ ersetzen. Das können wir machen, weil $\omega^{n/2} + 1 = 0$ in dem Ring K ist.

$x^n - 1 =$

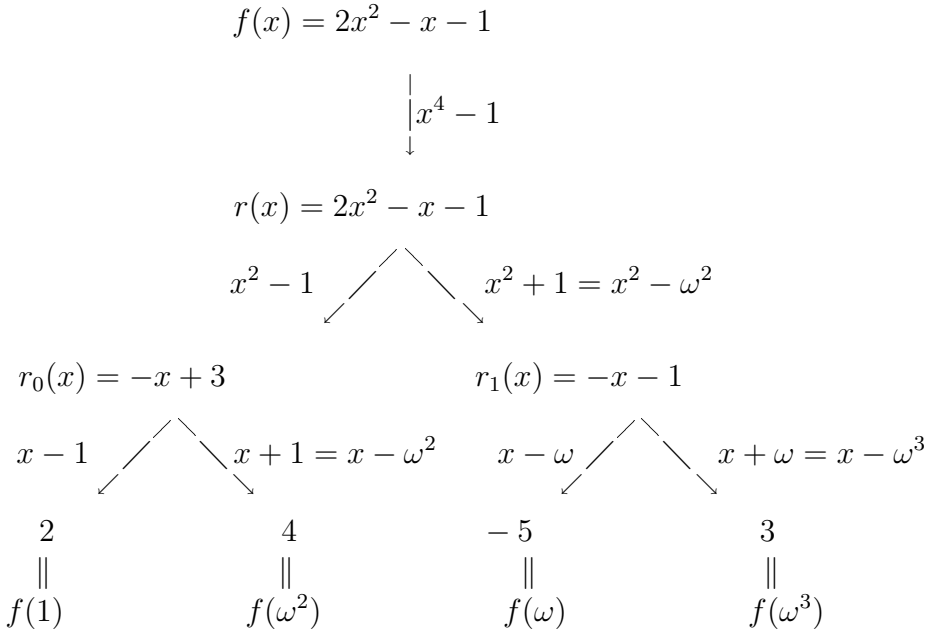
$(x^{n/2} - 1)(x^{n/2} + 1) = (x^{n/2} - 1)(x^{n/2} - \omega^{n/2}) =$

$(x^{n/4}-1)(x^{n/4}+1)(x^{n/4}-\omega^{n/4})(x^{n/4}+\omega^{n/4}) = (x^{n/4}-1)(x^{n/4}-\omega^{n/2})(x^{n/4}-\omega^{n/4})(x^{n/4}-\omega^{3n/4}).$

Setzen wir so fort und bekommen die Zerlegung

$$x^n - 1 = (x - 1)(x - \omega)(x - \omega^2) \dots (x - \omega^{n-1}).$$

22.2. Wie man schnell die diskrete Fouriersche Transformation eines Vektors berechnen kann: ein Beispiel. Sei $n = 4$, $\omega = 4$ und $K = \mathbb{Z}_{17}$. In diesem Punkt berechnen wir die diskrete Fouriersche Transformation $\mathcal{F}$ von Vektor $(1, -1, 2, 0)$. Mit diesem Vektor verbinden wir das Polynom $1 - x + 2x^2$. Nach Formel (21.2) müssen wir die Reste von $f(x)$ modulo $x - 1$, $x - \omega$, $x - \omega^2$ und $x - \omega^3$ berechnen. Zeichnen wir den Prozess mit Hilfe des folgenden Baumes:



So erhalten wir $\mathcal{F}\big((1,-1,2,0)\big) = (2,-5,4,3)$.

Erklärung. Auf erstem Niveau teilen wir $f(x)$ durch x^4-1 und erhalten den Rest $r = f(x)$. Danach splitten wir x^4-1 auf zwei Faktoren: $x^4-1 = (x^2-1)(x^2+1) = (x^2-1)(x^2-\omega^2)$. Auf zweitem Niveau teilen wir r durch x^2-1 und x^2+1 und erhalten die Reste $r_0 = -x+3$ und $r_1 = -x-1$. Danach splitten wir die Faktoren weiter: $x^2-1 = (x-1)(x+1) = (x-1)(x-\omega^2)$ und $x^2-\omega^2 = (x-\omega)(x-\omega^3)$. Auf drittem Niveau teilen wir r_0 durch $x-1$ und $x-\omega^2$, und auch r_1 auf $x-\omega$ und auf $x-\omega^3$ und erhalten die Reste $r_{00}=2, r_{01}=4, r_{10}=-5$ und $r_{11}=3$.

Betrachten wir zum Beispiel den linken Zweig. Aus dem Zweig ziehen wir folgende Gleichungen:

$$\begin{aligned} f(x) &= q(x)(x^4-1)+r(x)\\ r(x) &= q_0(x^2-1)+r_0(x)\\ r_0(x) &= q_{00}(x-1)+r_{00} \end{aligned}$$

Da $x-1$ ein Teiler von x^2-1 ist und x^2-1 ein Teiler von x^4-1 ist, führen wir aus, daß der Rest von $f(x)$ modulo $(x-1)$ gleich r_{00} ist.

Warum die Berechnung schnell läuft?

1) Es ist leicht $f(x)$ durch x^4-1 zu teilen: um den Rest $r(x)$ zu erhalten, muss man im $f(x)$ nur x^{i+4k} nach x^i ersetzen $(i=0,1,2,3)$. Auf jedem weiterem Niveau teilt man ein Polynom mit der Form $r_{i\dots}$ durch Polynom mit der Form $x^t-\omega^s$, wobei $\operatorname{Grad} r_{i\dots}(x) < 2t$ ist. Der Faktor 2 erleichtet die Berechnung wesentlich.

2) Wir berechnen die Reste r_{00}, r_{01}, r_{10} und r_{11} nicht separat: bis zu einem bestimmten Moment gehen die Zweige zusammen. Also berechnen wir die Reste gleichzeitig.

22.3. Schnelle Berechnung des Produktes zweier Polynomen: ein Algorithmus.

Seien $f(x) = a_0 + a_1x + \dots + a_kx^k$ und $g(x) = c_0 + c_1x + \dots + c_lx^l$ zwei Polynomen mit Koeffizienten aus dem Ring K. Wir möchten schnell ihr Produkt $h(x) = d_0 + d_1x + \dots + d_{n-1}x^{n-1}$ berechnen. Nehmen wir an, daß ein primitives Element ω des Grades n in dem Ring K existiert.

Schritt 0. Setzen wir $a_{k+1} = \dots = a_{n-1} = 0$ und $d_{l+1} = \dots = d_{n-1} = 0$. Dann können wir so schreiben:

$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}, \qquad g(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}.$$

Schritt 1. Berechnen wir die Bilder von Tupeln $(a_0, a_1, \dots, a_{n-1})$ und $(c_0, c_1, \dots, c_{n-1})$ bezüglich der Fourierschen Transformation:

$$(a_0, a_1, \dots, a_{n-1}) \mapsto (f(1), f(\omega), \dots, f(\omega^{n-1})),$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto (g(1), g(\omega), \dots, g(\omega^{n-1})).$$

Schritt 2. Für $i = 0, \dots, n-1$ multiplizieren wir die Zahlen $f(\omega^i)$ und $g(\omega^i)$. Dann erhalten wir das Tupel

$$\big(h(1), h(\omega), \dots, h(\omega^{n-1})\big).$$

Schritt 3. Wenden wir inverse diskrete Fouriersche Transformation an dem Tupel an, dann erhalten wir das Tupel des Koeffizienten des Polynoms $h(x)$:

$$(d_0, d_1, \dots, d_{n-1}) \leftarrow \big(h(1), h(\omega), \dots, h(\omega^{n-1})\big).$$

Dafür werden wir Bezeichnungen und die Formel (21.5) aus dem Punkt 21.5 benutzen. Bezeichnen wir $\big(h(1), h(\omega), \dots, h(\omega^{n-1})\big)$ als $(b_0, b_1, \dots, b_{n-1})$ und betrachten das Polynom $F(x) = b_0 + b_1 x + \dots + b_{n-1}x^{n-1}$. Dann gilt

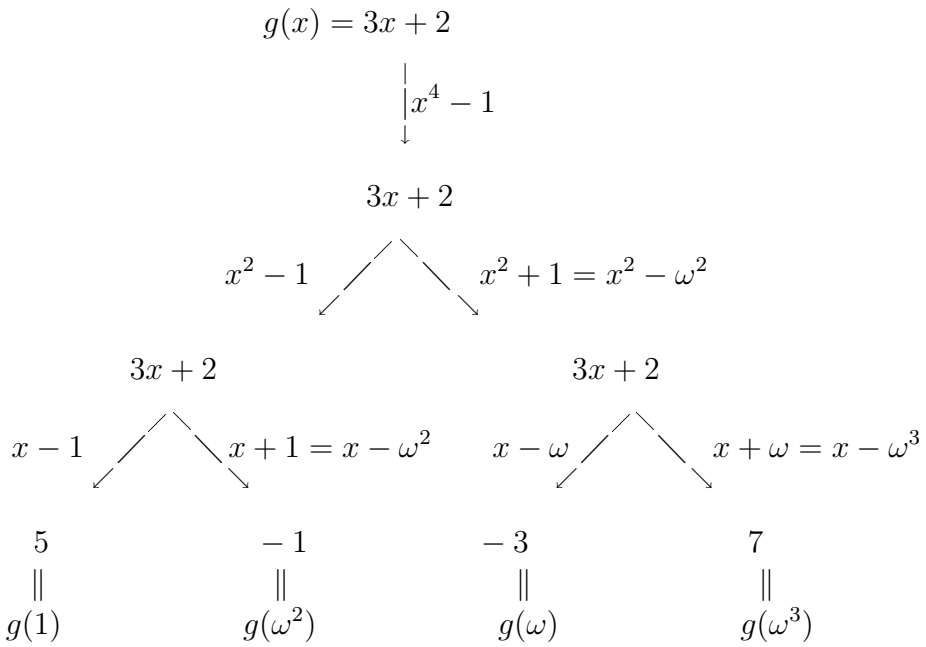
$$(d_0, d_1, \dots, d_{n-1}) = \frac{1}{n}\big(F(1), F(\omega^{n-1}), \dots, F(\omega)\big)$$

und $h(x) = d_0 + d_1 x + \dots + d_{n-1}x^{n-1}$.

22.4. Beispiel. Es wird gezeigt, wie man die Polynomen $f(x) = 2x^2 - x + 1$ und $g(x) = 3x + 2$ in dem Ring $\mathbb{Z}_{17}$ mit Hilfe der diskreten Fourierschen Transformation berechnen kann. Wir können $n = 4$ und $\omega = 4$ nehmen.

Schritt 0. Den Polynomen entsprechen zwei Tupeln: $(1, -1, 2, 0)$ und $(2, 3, 0, 0)$.

Schritt 1. Im Punkt 22.2 haben wir schon berechnet, daß $\mathcal{F}\big((1, -1, 2, 0)\big) = (2, -5, 4, 3)$ ist. Mit dem folgenden Baum erhalten wir, daß $\mathcal{F}\big((2, 3, 0, 0)\big) = (5, -3, -1, 7)$ ist.

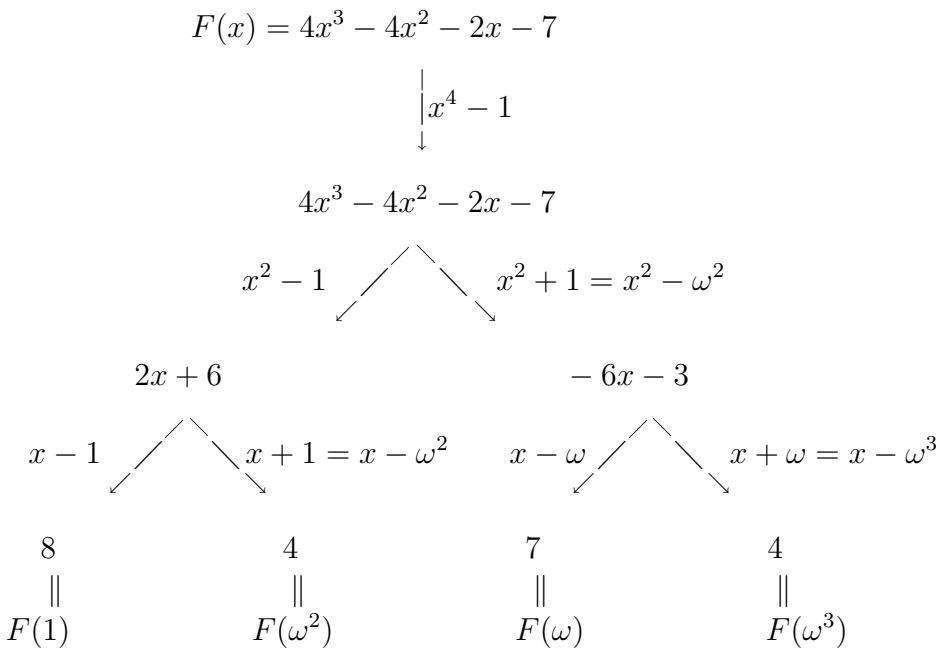


Schritt 2. $(2, -5, 4, 3) \cdot (5, -3, -1, 7) = (10, 15, -4, 21) = (-7, -2, -4, 4)$.

Schritt 3. Aus dem Schritt 2 haben wir das Polynom $F(x) = 4x^3 - 4x^2 - 2x - 7$. Mit Hilfe des folgenden Baumes erhalten wir

$$(d_0, d_1, d_2, d_3) = \frac{1}{4}\big(F(1), F(\omega^3), F(\omega^2), F(\omega)\big) = \frac{1}{4}(8, 4, 4, 7) = (2, 1, 1, 6).$$

Also, $h(x) = 6x^3 + x^2 + x + 2$ ist das Produkt von $f(x)$ und $g(x)$.


$F(x) = 4x^3 - 4x^2 - 2x - 7$
$\big|x^4 - 1$
$4x^3 - 4x^2 - 2x - 7$
$x^2 - 1$
$x^2 + 1 = x^2 - \omega^2$
$2x + 6$
$-6x - 3$
$x - 1$
$x + 1 = x - \omega^2$
$x - \omega$
$x + \omega = x - \omega^3$
8
4
7
4
$F(1)$
$F(\omega^2)$
$F(\omega)$
$F(\omega^3)$

Vorlesung 23
Turingmaschinen

1. Sprachen

Sei Σ ein *Alphabet* (= eine endliche Menge). Seine Elemente heißen *Buchstaben*. Ein Wort über Σ ist eine endliche Folge von Buchstaben. Die leere Folge ist auch ein Wort. Die *Länge* des Wortes $w = \sigma_1\sigma_2\ldots\sigma_k$ mit $\sigma_1, \ldots, \sigma_k \in \Sigma$ ist k und wird als $|w|$ bezeichnet. Bezeichnen wir als Σ^* die Menge aller Wörter über Σ. Eine *Sprache* über Σ ist eine beliebige Untermenge von Σ^*.

2. Informelle Beschreibung von Turingmaschinen

Die Turingmaschine besteht aus

• einem unendlich langen Speicherband mit unendlich vielen sequentiell angeordneten Feldern. In jedem dieser Felder kann genau ein Zeichen gespeichert werden.

• einem programmgesteuerten Lese-und Schreibkopf, der sich auf dem Speicherband feldweise bewegen und die Zeichen verändern kann.

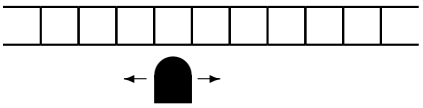


Bild 10

Eine Turingmaschine modifiziert die Eingabe auf dem Band nach einem gegebenen Programm. Ist die Berechnung beendet, so befindet sich das Ergebnis auf dem Band. Es wird somit jedem Eingabewert ein Ausgabewert zugeordnet. Eine Turingmaschine muss aber nicht für alle Eingaben stoppen. In diesem Fall ist die Funktion für die Eingabe nicht definiert.

3. Formale Beschreibung

3.1. Deterministische Turingmaschine

Eine deterministische Turingmaschine ist ein 7-Tupel $M = (Q, \Sigma, \Gamma, \delta, q_0, \square, F)$, wobei gelten:

- Q ist die endliche Zustandsmenge;
- Σ ist das endliche Eingabealphabet;
- $\Gamma \supset \Sigma$ ist das endliche Bandalphabet;
- $\delta : (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{L, S, R\}$ ist die Überführungsfunktion;
- $q_0 \in Q$ ist der Anfangszustand;
- $\square \in \Gamma \setminus \Sigma$ steht für das leere Feld;
- $F \subseteq Q$ ist die Menge der End- bzw. akzeptierenden Zustände.

Die Turingmaschine führt eine Berechnung aus, indem sie schrittweise eine Eingabe in eine Ausgabe umwandelt.

Zu Beginn steht ein Wort als Eingabe auf dem Band (pro Bandfeld ein Zeichen des Eingabewortes), der Rest des Bandes ist mit dem leeren Feld "formatiert". Der Schreib-/Lese-Kopf steht auf dem ersten Zeichen der Eingabe, und die Turingmaschine befindet sich im Startzustand q_0.

Die Überführungsfunktion gibt an, wie die Turingmaschine schrittweise den Bandinhalt, ihren Zustand und die Position des Schreib-/Lese-Kopfes ändert. Diese Funktion nimmt als Argument den aktuellen Zustand und das Zeichen, das sich im aktuellen Schritt unter dem Schreib-/Lese-Kopf befindet. Als Ergebnis liefert sie dann genau ein Zeichen (dieses wird dann der Nachfolgezustand der Turingmaschine), ein Zeichen (mit diesem Zeichen wird dann der Inhalt des Feldes, auf das der Schreib-/Lese-Kopf weist, überschrieben) und eines der Zeichen L, R, S (dann bewegt er sich ein Feld nach links, oder nach rechts, oder verharrt auf dem selben Feld). Damit hat die Turingmaschine einen Schritt ihres Arbeitszyklus durchlaufen und steht für einen weiteren bereit.

Erreicht die Turingmaschine einen Endzustand, also einen Zustand der Menge F, ist die Berechnung beendet. Die Ausgabe ist dann der Inhalt des Bandes (wobei die Felder, die mit Symbolen aus $\Gamma \setminus \Sigma$ gefüllt sind, insbesondere dem Symbol $\square$, nicht berücksichtigt werden).

3.2. Nichtdeterministische Turingmaschine

Für eine beliebige Menge X bezeichnen wir die Menge aller ihrer Untermengen als $P(X)$. Bei der nichtdeterministischen Turingmaschine ändert sich die Überführungsfunktion zu

$$\delta : (Q \setminus F) \times \Gamma \to P(Q \times \Gamma \times \{L, S, R\}).$$

Durch diese Überführungsrelation ist der Folgezustand, der sich aus dem aktuellen Bandzeichen und dem aktuellen Zustand ergibt, nicht mehr eindeutig bestimmt. Die Turingmaschine muss also im Allgemeinen zu jedem Berechnungszeitpunkt einen Folgezustand aus bestimmten potentiellen Folgezuständen wählen, wodurch verschiedene nicht eindeutig vorbestimmte Rechenwege möglich sind.

Mit anderen Worten: Bei jeder erneuten Inbetriebnahme einer nichtdeterministischen Turingmaschine mit der gleichen Eingabe kann diese jedes Mal eine andere Ausgabe liefern.

4. Sprachen und Turingmaschinen

4.1. Sprachen, die eine deterministische Turingmaschine akzeptiert

Sei M eine deterministische Turingmaschine mit einem Eingabealphabet Σ und einem Bandalphabet Γ, so dass $\{0, 1\} \subseteq \Gamma$ ist. Wir sagen, dass die Turingmaschine M ein Wort $w \in \Sigma^*$ *akzeptiert*, wenn sie bei der Eingabe w nach endlich vielen Schritten in einen der Endzustände übergeht und die Ausgabe 1 ergibt.

Wir sagen, dass die Turingmaschine M das Wort $w \in \Sigma^*$ *nicht akzeptiert*, wenn sie bei der Eingabe w entweder gar nicht hält, oder nach endlich vielen Schritten in einen der Endzustände übergeht und die Ausgabe ungleich 1 ergibt.

Die Menge aller Wörter, die die Turingmaschine M akzeptiert, wird als $L(M)$ bezeichnet. Sei $S \subseteq \Sigma^*$ eine Sprache. Wir sagen, dass *die Turingmaschine M die Sprache S akzeptiert*, wenn $S = L(M)$ ist.

Eine Sprache $S \subseteq \Sigma^*$ heißt *rekursiv aufzählbar* (**RA**), wenn eine deterministische Turingmaschine M mit $S = L(M)$ existiert, also wenn M die Sprache S akzeptiert.

Mit anderen Worten:

Definition 1. Eine Sprache $S \subseteq \Sigma^*$ heißt *rekursiv aufzählbar* (**RA**), wenn eine deterministische Turingmaschine M existiert, die

(a) bei der Eingabe w aus S nach endlich vielen Schritten in einen der Endzustände übergeht und die Ausgabe 1 ergibt,

(b) bei der Eingabe w aus $\Sigma^* \backslash S$ entweder nicht hält, oder nach endlich vielen Schritten in einen der Endzustände übergeht und die Ausgabe ungleich 1 ergibt.

Definition 2. Eine Sprache $S \subseteq \Sigma^*$ heißt *rekursiv entscheidbar* (**RE**), wenn eine deterministische Turingmaschine M existiert, die

(a) bei der Eingabe w aus S hält und nach endlich vielen Schritten in einen der Endzustände übergeht und die Ausgabe 1 ergibt,

(b) bei der Eingabe w aus S hält und nach endlich vielen Schritten in einen der Endzustände übergeht und die Ausgabe 0 ergibt.

Es ist klar, dass jede **RE**-Sprache gleichzeitig **RA**-Sprache ist. Es gibt aber **RA**-Sprachen, die nicht **RE**-Sprachen sind. Beispiel: Codieren wir (nach einer Methode) alle Turingmaschinen mit Wörtern aus $\Sigma^* = \{0,1\}^*$, so dass verschiedene Turingmaschinen verschiedene Codes haben. So erhalten wir die Menge $S \subseteq \Sigma^*$ aller Codes. Sei S' die Untermenge von S, die die Codes nur der Machinen enthält, die für jede Eingabe terminieren. Man kann beweisen, dass S' rekursiv aufzählbar, aber nicht rekursiv entscheidbar ist.

Definition 3. Das *Entscheidungs-Problem für* $S \subseteq \Sigma^*$: gegeben $w \in \Sigma^*$, entscheiden, ob w in S liegt.

Für eine rekursiv entscheidbare Menge kann man dieses Problem algorithmisch lösen. Für eine rekursiv aufzählbare Menge kann man im allgemein dieses Problem nicht algorithmisch lösen. Man kann aber alle Elemente dieser Menge S in unendlicher Zeit aufschreiben:

Numerieren wir alle Elemente von Σ^* mit natürlichen Zahlen. Sei M die Turingmaschine, die in der Definition 1 auftaucht. In dem Moment 1 lassen wir eine Kopie von M mit dem ersten Wort aus Σ^* als Eingabe laufen. In dem Moment 2 lassen wir eine Kopie von M mit dem zweiten Wort aus Σ^* als Eingabe laufen u.s.w. In jedem Moment wird also nur eine endliche Anzahl von Kopien von M laufen. Sobald eine der Turingmaschinen stoppt, schreiben wir ihr Ergebnis auf. So werden alle Elemente von S aufgeschrieben sein.

4.1. Sprachen, die eine nichtdeterministische Turingmaschine akzeptiert

Sei M eine nichtdeterministische Turingmaschine mit einem Eingabealphabet Σ und einem Bandalphabet Γ, so dass $\{0,1\} \subseteq \Gamma$ ist.

Wir sagen, dass die Turingmaschine M ein Wort $w \in \Sigma^*$ *akzeptiert*, wenn eine Berechnung der Turingmaschine auf der Eingabe w existiert, so dass die Turingmaschine nach endlich vielen Schritten in einen der Endzustände übergeht und die Ausgabe 1 ergibt.

Die Menge aller Wörter, die die Turingmaschine M akzeptiert, wird als $L(M)$ bezeichnet. Sei $S \subseteq \Sigma^*$ eine Sprache. Wir sagen, dass *die Turingmaschine M die Sprache S akzeptiert*, wenn $S = L(M)$ ist.

Satz. Sei S eine Sprache. Wenn eine nichtdeterministische Turingmaschine diese Sprache akzeptiert, dann existiert eine deterministische Turingmaschine, die auch diese Sprache akzeptiert.

Wir können vermuten, dass die nichtdeterministische Turingmaschine die Sprache S schneller als die deterministische Turingmaschine akzeptiert.

Vorlesungen 24

Komplexitätstheorie

1. Klassen P und NP

Bezeichnung 1. Sei M eine deterministische Turingmaschine und sei $w \in \Sigma^*$ ein Wort, das diese Turingmaschine akzeptiert. Bezeichnen wir als $\text{Zeit}_M(w)$ die Anzahl von Schritten, die diese Turingmaschine mit der Eingabe w läuft.

Bezeichnung 2. Sei M eine nichtdeterministische Turingmaschine und sei $w \in \Sigma^*$ ein Wort, das diese Turingmaschine akzeptiert. Bezeichnen wir als $\text{Zeit}_M(w)$ die minimale Anzahl von Schritten für alle Berechnungen von M mit der Eingabe w und der Ausgabe 1.

Sei M eine (nicht)deterministische Turingmaschine, sei S eine Sprache und sei $p : \mathbb{N} \to \mathbb{N}$ eine Funktion. Wir sagen, dass M *die Sprache* S *in der Zeit* $p(n)$ *akzeptiert*, wenn $S = L(M)$ ist und für alle $w \in S$ gilt

$$\text{Zeit}_M(w) \leqslant p(|w|).$$

Die Sprache S liegt in der Klasse **P** (polynomial), wenn eine deterministische Turingmaschine M und ein Polynom $p(n)$ existieren, so dass M die Sprache S in der Zeit $p(n)$ akzeptiert.

Die Sprache S liegt in der Klasse **NP** (nichtdeterministisch polynomial), wenn eine nichtdeterministische Turingmaschine M und ein Polynom $p(n)$ existieren, so dass M die Sprache S in der Zeit $p(n)$ akzeptiert.

Klar, dass **P**$\subseteq$ **NP** ist. Man weiß aber nicht, ob diese Klassen ungleich sind.
Problem. Ob **P** $\neq$ **NP** ist?

Behauptung. Wenn S in der Klasse **NP** liegt, dann existiert eine deterministische Turingmaschine, die S in einer (Exponent von einem Polynom)-Zeit akzeptiert.

2. NP-vollständige Probleme

Definition 1. Eine Funktion $f : \Sigma^* \to \Sigma^*$ heißt *polynomiell berechenbar*, wenn eine deterministische Turingmaschine und ein Polynom $p(n)$ existieren, so dass die Turingmaschine bei der Eingabe $w \in \Sigma^*$ die Ausgabe $f(x)$ nach weniger als $p(|w|)$ Schritten berechnet.

Definition 2. Seien $L_1, L_2 \subseteq \Sigma^*$ zwei Sprachen. Man sagt, dass L_1 *polynomiell reduzierbar auf* L_2 ist, wenn eine polynomiell berechenbare Funktion $f : \Sigma^* \to \Sigma^*$ existiert, so dass gilt

$$w \in L_1 \Longleftrightarrow f(w) \in L_2.$$

Definition 3. Eine Sprache $L \subseteq \Sigma^*$ heißt **NP**-*vollständig*, wenn L in der Klasse **NP** liegt und alle anderen Sprachen, die in der Klasse **NP** liegen, auf L polynomiell reduzierbar sind.

Viele mathematische Probleme können als Entscheidungsprobleme für eine Sprache umformuliert sein. Wenn die entsprechende Sprache **NP**-vollständig ist, sagt man, dass das Problem **NP**-vollständig ist. Beschreiben wir ein Problem, das **NP**-vollständig ist.

Das Problem **Erfüllbarkeit der Aussagenlogik** (oft mit **SAT** vom Englischen *satisfiability* notiert) fragt, ob eine aussagenlogische Formel erfüllbar ist. Zum Beispiel die Formel

$$x \wedge \neg(y \vee z)$$

ist erfüllbar (mit $x = 1, y = z = 0$). Die Formel

$$x \wedge \neg x$$

ist nicht erfüllbar.

Man kann dieses Problem als Entscheidungsproblem für eine Sprache folgendermaßen umformulieren. Setzen wir $\Sigma = \{x, 0, 1, \wedge, \vee, \neg, (,)\}$. Jede aussagenlogische Formel ergibt dann ein Wort in dem Alphabet Σ. Zum Beispiel die Formel $x \wedge \neg(y \vee z)$ ergibt das Wort $x1 \wedge \neg(x10 \vee x11)$. Sei $S_{\mathbf{SAT}}$ die Menge aller Wörter in Σ^*, die die erfüllbaren aussagenlogischen Formeln ergeben.

Satz (Cook, 1971). Die **SAT** ist eines der **NP**-vollständigen Probleme.
(In dem Sinn, dass die Sprache $S_{\mathbf{SAT}}$ **NP**-vollständig ist.)

Vorlesung 25

Pollard-ρ-Methode für die Faktorizierung

Vorlesung 26

Quadratisches Sieb für die Faktorizierung