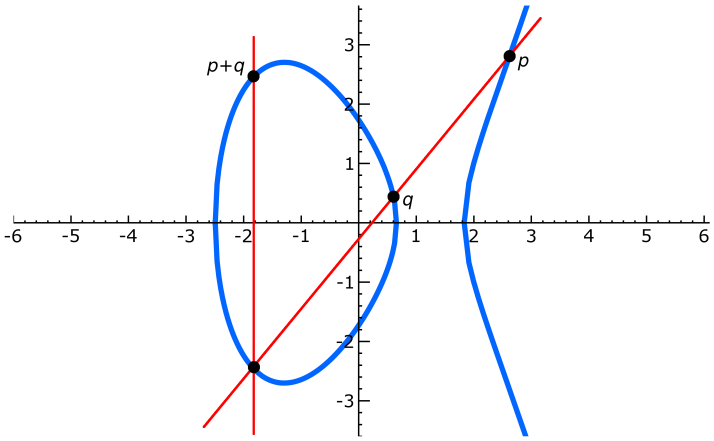


Prof. Dr. Ulrich Görtz
Wintersemester 2021/22

Seminar über
Elliptische Kurven und Kryptographie

1. Organisatorisches

— Siehe auch die Moodle-Seite zum Seminar. —

Vorbesprechung. Donnerstag, 23.9., 14:15 Uhr. Weitere Informationen über die Moodle-Seite. Die Verteilung der Vorträge erfolgt dann kurz nach der Vorbesprechung.

Termin. Dienstags, 14-16 Uhr, S-U-3.01. Beginn: 12.10.

ECTS-Punkte. Das Seminar kann (je nach Vortrag, siehe unten) als Bachelor-Seminar oder als Master-Seminar im Studiengang Lehramt GyGe/BK besucht werden. Für einen erfolgreichen Vortrag erhalten Sie 4 Credit-Punkte. Siehe auch Modulhandbuch Bachelor, S. 40ff.[1] Modulhandbuch Master, S. 23ff.[2].

Kontakt.
Für organisatorische Fragen: `ulrich.goertz@uni-due.de`.
Bei mathematischen Fragen zu Ihrem Vortrag unterstützt Sie Herr Dr. Heer Zhao, `heer.zhao@uni-due.de`.

Das Seminar findet in Präsenz in Seminarraum S-U-3.01 im Mathematik-Gebäude, Thea-Leymann-Str. 9, statt.

Die Seminarvorträge sollen an der Tafel gehalten werden und nicht länger als 80 Minuten dauern. Rechnen Sie bei der Planung mit Fragen der Zuhörer:innen und der Organisatoren. Danach stehen circa 10 Minuten für Fragen und eine Rückmeldung zum Vortrag zur Verfügung.

Im Nachgang eine schriftliche Ausarbeitung Ihres Vortrags abzugeben, ist nicht erforderlich (und kann auch nicht als Ersatz für einen erfolgreichen Vortrag dienen).

[1] `https://www.uni-due.de/imperia/md/content/didmath/lehre/mhb_ba_gyge_190523.pdf`
[2] `https://www.uni-due.de/imperia/md/content/didmath/lehre/mhb_ma_gyge_190523.pdf`

Für das Seminar gilt (moralische) Anwesenheitspflicht; es wird eine *aktive Teilnahme* erwartet. Für den Fall, dass Sie an einem Termin aus wichtigen Gründen verhindert sind, entschuldigen Sie sich bitte vorher bei der/dem Vortragenden und bei mir.

Erforderliche Vorkenntnisse. Gute Kenntnisse der Linearen Algebra, insbesondere:

- Körper, insbesondere die endlichen Körper $\mathbb{F}_p$ für Primzahlen p, siehe (zum Beispiel – Sie können natürlich auch in andere Quellen schauen) [Gö1] Kapitel 4[3], insbesondere die Abschnitte 4.1 und 4.2,
- Gruppen, Gruppenhomomorphismen, Untergruppen, [Gö1] Abschnitt 8.1[4], Ringe, [Gö2] Kapitel 15[5], insbesondere Abschnitte 15.1, 15.2, Abschnitt 18.4[6].
- Polynome über einem Körper, [Gö2] Abschnitt 15.3[7], Abschnitt 15.4.4[8].

2. Anforderungen / Wie halte ich einen guten Seminarvortrag?

- Richten Sie die Vorbereitung auf Ihren Vortrag nach dem Grundsatz aus, dass Ihre Zuhörer möglichst viel dabei lernen und „aus dem Vortrag mitnehmen“ sollen.
- Ihr erstes und wichtigstes Ziel sollte sein, die im Vortrag zu behandelnde Mathematik gründlich zu verstehen. Das wird in der Regel eine ganz Menge Zeit in Anspruch nehmen; beginnen Sie daher frühzeitig mit Vorbereitung!
- Stellen Sie viele Fragen (sich und den anderen Seminarteilnehmer:innen). Seien Sie diszipliniert darin, sich zu fragen, warum (ob) die im zugrundeliegenden Text aufgestellten Behauptungen richtig sind. Was lässt sich vereinfachen? Wenn Sie auf Dinge stoßen, die Sie nicht verstehen, fragen Sie die anderen Seminarteilnehmer:innen (diejenigen, die die Vorträge direkt vor oder nach Ihnen halten, haben sich vielleicht schon genau dieselbe Frage gestellt). Vielleicht ist im Buch ein Fehler? Wenn Sie damit noch nicht weiterkommen, vereinbaren Sie einen Termin mit dem Assistenten, der das Seminar betreut. (Bei diesem Seminar Herr Dr. Heer Zhao, `heer.zhao@uni-due.de`.)
- Wenn Sie die Mathematik verstanden haben, sollten Sie bewusst darüber nachdenken, wie Sie die Inhalte in Ihrem Vortrag darstellen möchten. Oft bietet es sich an, den Aufbau zu ändern, Sachen umzustrukturieren, zusätzliche Beispiele einzubauen, die Notation anzupassen, usw. — schließlich ist ein Vortrag etwas ganz anderes als ein geschriebener Text. Diese Restrukturierung ist Teil der Anforderung an Ihren Vortrag. Es genügt nicht, den Text aus dem Buch an die Tafel zu schreiben!
- Überlegen Sie im Vorfeld, was die Hauptpunkte Ihres Vortrags sind, die jede:r Teilnehmer:in lernen sollte, und berücksichtigen Sie das entsprechend. Sie können nötigenfalls Sachen im Vortrag auslassen (zum Beispiel eine technische Rechnung, die zum Verständnis nicht notwendig ist (schauen Sie sie

[3] `https://math.ug/la1-ws2021/sec-koerper-lgs.html`
[4] `https://math.ug/la1-ws2021/sect0031.html`
[5] `https://math.ug/la2-ss21/ch-ringe.html`
[6] `https://math.ug/la2-ss21/sec-quotient-ring.html`
[7] `https://math.ug/la2-ss21/sec-polynomring.html`
[8] `https://math.ug/la2-ss21/sec-integritaetsringe.html#a0000000200`

sich trotzdem genau an, um gegebenenfalls Fragen beantworten zu können!)). Denken Sie bei der Vortragsplanung darüber nach, was sich zum Weglassen eignet, damit Sie nicht am Ende wegen Zeitmangels gezwungen sind, die interessantesten Teile zu überspringen.

- Denken Sie insbesondere darüber nach, was ein guter Einstieg in den Vortrag ist. Wie fügt er sich ins Seminarprogramm ein? Warum sollte man sich für dieses Thema interessieren? Bereiten Sie auch einen guten Abschluss des Vortrags vor.
- Die Sachen, die Sie in der Vorbereitung besonders viel Zeit gekostet haben, sollten Sie nicht auslassen, denn die anderen Teilnehmer:innen haben vermutlich ähnliche Schwierigkeiten beim Verständnis und können gerade an diesen Stellen viel lernen. Wenn doch einmal noch Fragen bei Ihnen offengeblieben sind, gehen Sie damit ehrlich um und versuchen Sie nicht, Probleme beim Verständnis zu verschleiern.
- Wenn im Text auf eine Übungsaufgabe verwiesen wird, gehört es zur Vorbereitung des Vortrags, diese Aufgabe zu lösen.
- **Aktive Einbindung der Teilnehmer:innen.** Das Seminar lebt von der aktiven Beteiligung aller Teilnehmer:innen an *allen* Vorträgen, nicht nur am eigenen. Die Beteiligung an den anderen Vorträgen ist eine Möglichkeit, Ihre Note im Seminar gegebenenfalls noch zu verbessern.

  Die Beteiligung aller sicherzustellen, ist sowohl eine Aufgabe der Zuhörer:innen als auch der Sprecher:in. Konkret ist daher eine der Anforderungen an einen erfolgreichen Vortrag: Überlegen Sie sich mindestens drei Fragen, die Sie während Ihres Vortrags an das Publikum richten. Es kann sich um offene Fragen oder um Multiple-Choice-Fragen handeln. Wählen Sie Fragen aus, die sich von denjenigen, die dem Vortrag gefolgt sind, relativ schnell beantworten lassen, und die Ihnen ermöglichen, auf einen besonders wichtigen Punkt noch einmal hinzuweisen und/oder helfen zu entscheiden, was Sie vielleicht noch einmal anders/erneut erklären sollten oder worauf Sie im weiteren Verlauf den Fokus legen.

Wenn Sie Ihren Vortrag in den Grundzügen vorbereitet haben, und *spätestens zwei Wochen vor dem Termin Ihres Vortrags* sprechen Sie Ihren Vortrag mit Herrn Zhao durch. Dabei können Sie offene Fragen von Ihrer Seite klären. (Wenn Sie gar keine Fragen haben, sollten Sie noch einmal sehr selbstkritisch hinterfragen, ob Sie die Inhalte des Vortrag mathematisch wirklich hinreichend durchdrungen haben. Es ist für den Verlauf des Vortrag besser und auch für Sie angenehmer, wenn Sie nicht erst bei Nachfragen während des Vortrags feststellen, dass es doch noch Verständnislücken gibt.)

Auch wenn es viel Arbeit sein wird, kann und soll es Spaß machen, an dem Seminar teilzunehmen. Dabei steht im Vordergrund, dass alle Teilnehmer:innen gemeinsam etwas lernen! Daher sollten Sie als Sprecher:in Fragen im Vortrag immer willkommen heißen und als Unterstützung dabei sehen, Ihren Vortrag auf die Bedürfnisse der Teilnehmer:innen auszurichten. Umgekehrt: Geben Sie sich als Zuhörer:in Mühe, den Vorträgen der anderen aktiv zu folgen und stellen Sie dort Fragen, wo Sie etwas nicht verstehen.

Nutzen Sie die Möglichkeit, Ihre eigenen Schwerpunkte zu setzen und überlegen Sie sich, wie Sie Ihren eigenen Vortrag so gestalten können, dass Sie damit zufrieden sind.

3. Literatur

Wir richten uns in erster Linie nach dem Buch [We] von Annette Werner.

Andere Quellen finden Sie im Literaturverzeichnis am Ende (und diese sind gegebenenfalls in den Vortragsbeschreibungen genannt).

4. Vorträge

Ba Bachelor-Seminar-Vortrag.

Ma Master-Seminar-Vortrag.

Ba/Ma Bachelor- oder Master-Seminar-Vortrag. Teils sind im Vortragsprogramm Zusatzanforderungen für den Master-Seminar-Vortrag angegeben; sonst nach Absprache.

– Diesen Vortrag werde ich voraussichtlich selbst übernehmen.

Vortrag 1 (Einführung)**.** **–**
Einführung in das Seminarthema, Grundidee der Public-Key-Kryptographie und der Begriff der elliptischen Kurve.

Vortrag 2 (Erinnerung und Ergänzungen zur Lineare Algebra)**.** **–**
Wir wiederholen kurz einige der Begriffe, die wir aus der Linearen Algebra kennen:

- Gruppen ([Gö1] Abschnitt 8.1[9], eventuell auch [Gö2] Abschnitt 18.3[10]), Ringe ([Gö2] Kapitel 15[11], insbesondere Abschnitte 15.1, 15.2, eventuell auch Abschnitt 18.4[12]),
- Körper, insbesondere die Beispiele $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ (p eine Primzahl), [Gö1] Kapitel 4[13],
- Polynome über einem Körper in einer Variablen, irreduzible Polynome, [Gö2] Abschnitt 15.3[14], Abschnitt 15.4.4[15].

Außerdem benötigen wir die folgenden Ergänzungen.

- Ordnung einer Gruppe, Ordnung eines Gruppenelements
- Die Charakteristik eines Körpers, [Gö1] Abschnitt 4.2.2[16],

[9] https://math.ug/la1-ws2021/sect0031.html
[10] https://math.ug/la2-ss21/sec-quotient-gruppe.html
[11] https://math.ug/la2-ss21/ch-ringe.html
[12] https://math.ug/la2-ss21/sec-quotient-ring.html
[13] https://math.ug/la1-ws2021/sec-koerper-lgs.html
[14] https://math.ug/la2-ss21/sec-polynomring.html
[15] https://math.ug/la2-ss21/sec-integritaetsringe.html#a0000000200
[16] https://math.ug/la1-ws2021/sect0018.html#subsec:charakteristik

- Algebraisch abgeschlossene Körper und der algebraische Abschluss eines Körpers, [Gö2] Abschnitt 15.4.4[17], [Bo] Abschnitt 3.4. Wir belassen es hier dabei, den Satz über die Existenz eines „algebraischen Abschlusses“ ohne Beweis anzugeben.
- Polynome in mehreren (endlich vielen) Variablen, [Bo] Abschnitt 2.5.
- Die formale (partielle) Ableitung eines Polynoms, [Bo] Abschnitt 2.6.
- **Satz.** Ist K ein Körper und ist $G \subseteq K^\times$ eine endliche Untergruppe, dann ist G eine *zyklische Gruppe*, d.h. es existiert $g \in G$ mit $G = \langle g \rangle = \{g^i;\ i \in \mathbb{Z}\}$. (Wenn Zeit bleibt, wäre es schön, etwas zum Beweis zu sagen. Siehe zum Beispiel [Gö1] Ergänzung 8.59[18]. Vergleiche Vortrag 8.)

Vortrag 3 (Affine ebene Kurven)**.** Ba/Ma

Erklären Sie den Inhalt von Abschnitt 2.1 in [We]. Dabei sollten Sie folgende Punkte umsetzen:

- Ersetzen Sie in Definition 2.1.1 die Bedingung $f \neq 0$ dadurch, dass f nicht konstant sei, und ändern Sie den letzten Satz der Definition wie folgt: Wir sagen, durch f sei eine *affine ebene Kurve* gegeben und nennen $C_f(F)$ die Menge der Punkte der zu f gehörigen Kurve (über F).
- Geben Sie zusätzlich zu den im Text genannten Beispielen weitere Beispiele, auch über den reellen und komplexen Zahlen. Erläutern Sie anhand der Beispiele insbesondere: Warum spricht man von einer *affinen ebenen Kurve*? Verschiedene Polynome können über $\mathbb{R}$ dieselben, aber über $\mathbb{C}$ unterschiedliche Nullstellenmengen haben; dies ist ein Grund für unsere Änderung von Definition 2.1.1. Geben Sie jeweils ein Beispiel, in dem $C_f(F) = \emptyset$ und $C_f(F) = F^2$ ist und diskutieren Sie, warum man trotzdem von einer *Kurve* spricht.
- Erklären Sie Definition 2.1.2 „geometrisch“. Wenn der Vortrag „als Master-Seminar-Vortrag“ gehalten wird: Bringen Sie die Definition mit dem Satz über implizite Funktionen[19] aus der Analysis in Verbindung.

Vortrag 4 (Projektive ebene Kurven)**.** Ba/Ma

Erklären Sie den Inhalt von Abschnitt 2.2 bis einschließlich Proposition 2.2.6 in [We].

Ich denke, es ist sinnvoll, mit Definition 2.2.1 zu beginnen und die Diskussion am Anfang des Abschnitts erst danach zu führen. Ändern Sie Definition 2.2.4 analog zu der Änderung von Definition 2.1.1 (siehe Vortrag 1).

Diskutieren Sie als weiteres Beispiel Geraden in der projektiven Ebene, siehe [We], Definition 2.3.4, Lemma 2.3.5.

Vortrag 5 (Weierstraß-Gleichungen)**.** Ba

Diskutieren Sie [We] Definition 2.2.7, Lemma 2.2.8 und Abschnitt 2.3 bis einschließlich Prop. 2.3.3.

[17] `https://math.ug/la2-ss21/sec-integritaetsringe.html#a0000000200`
[18] `https://math.ug/la1-ws2021/sect0034.html#a0000001572`
[19] `https://de.wikipedia.org/wiki/Satz_von_der_impliziten_Funktion`

Wenn Sie möchten, können Sie zu der Nummerierung der Koeffizienten in einer Weierstraß-Gleichung darauf aufmerksam machen, dass für jeden Summanden $a_n X^i Y^j Z^k$ gilt, dass $n + 2i + 3j = 6$ gilt (und natürlich $i + j + k = 3$, weil das betrachtete Polynom homogen vom Grad 3 ist).

Die Beweise von Proposition 2.3.2 und Proposition 2.3.3 müssen Sie geeignet kürzen. Aber erklären Sie so viel, dass alle Teilnehmer:innen in die Lage versetzt werden, den Rest der Beweise selbst zu ergänzen.

Vortrag 6 (Tangenten und Sekanten)**.** **Ma**

Erläutern Sie Definition 2.3.6 bis Korollar 2.3.9 in [We].

Die Beschreibung der Nullstellenordnung durch Verschwinden der Ableitungen auf Seite 36 in [We] ist so zwar über Körpern der Charakteristik 0, aber (warum?) nicht allgemein richtig (betrachten Sie als Beispiel das Polynom $t^2 + t^3$ über $\mathbb{F}_2$). Es ist aber richtig, dass aus $\psi(0) = \psi'(0) = 0$ folgt, dass ψ Nullstellenordnung ≥ 2 bei 0 hat, und das ist alles, was wir in der sich anschließenden Diskussion benötigen.

Planen Sie vorher, wo Sie (gegebenenfalls) kürzen können, aber erklären Sie auf jeden Fall die Ideen, die den Ergebnissen und Beweisen zugrundeliegen.

Ergänzung zu Definition 2.3.7. (Im Vortrag wird dafür nicht genügend Zeit sein.) Für ein Polynom $\psi \in F[t]$ bezeichnen wir mit $v(\psi)$ die Vielfachheit, mit der die Nullstelle 0 in ψ auftritt. Dies ist also die eindeutig bestimmte natürliche Zahl v, für die sich ψ als $\psi = t^v \varphi$ mit einem Polynom $\varphi \in F[t]$ mit $\varphi(0) \neq 0$ schreiben lässt.

Wir betrachten nun die Situation von Definition 2.3.7 im Buch von Werner und das dort definierte Polynom

$$\psi(t) = g(a + ta', b + tb', c + tc') \in F[t].$$

Wir wollen zeigen: $v(\psi)$ ändert sich nicht

(1) wenn wir (a', b', c') durch (ra', rb', rc') für ein $r \in F^\times$ ersetzen,

(2) wenn wir (a, b, c) durch (ra, rb, rc) für ein $r \in F^\times$ ersetzen,

(3) wenn wir (a', b', c') durch einen anderen Punkt auf der Geraden L ersetzen (der von $(a : b : c)$ verschieden ist).

Dafür benutzen wir das folgende Lemma.

Lemma. Sei v wir oben die Abbildung $v\colon F[t] \setminus \{0\} \to \mathbb{N}$, $\varphi \mapsto v(\varphi)$.

(1) Für $\varphi_1, \varphi_2 \in F[t]$ gilt $v(\varphi_2\varphi_2) = v(\varphi_1)v(\varphi_2)$.

(2) Sei

$$F(t) = \left\{ \frac{\varphi_1}{\varphi_2};\ \varphi_1, \varphi_2 \in F[t],\ \varphi_2 \neq 0 \right\}$$

der Körper der *rationalen Funktionen*, also aller Brüche von Polynomen. (Addition und Multiplikation sind durch die „üblichen Bruchrechenregeln“ gegeben.)

Wir können die Abbildung v fortsetzen zu einer Abbildung

$$v\colon F(t)^\times \to \mathbb{Z}, \quad \frac{\varphi_1}{\varphi_2} \mapsto v(\varphi_1) - v(\varphi_2),$$

wir können also über die Nullstellenordnung einer rationalen Funktion bei 0 sprechen (und wenn diese negativ ist, stellen wir uns das als *Polstelle* bei 0 vor). Die Eigenschaft (1) gilt dann für alle Elemente von $F(t)^\times$.

(3) Ist $\lambda \in F(t)$ mit $v(\lambda) = 1$, dann gilt $v(\psi(\lambda(t))) = v(\psi(t))$ für alle $\psi \in F(t)^\times$.

Beweis. Teil (1) kann man leicht nachrechnen, und daraus folgt Teil (2). Für Teil (3) genügt es wegen Eigenschaft (1), den Fall $\psi \in F[t]$ zu behandeln. Man schreibt $\lambda = t\mu$ mit $\mu \in F(t)$, wobei μ als Bruch von Polynomen darstellbar ist, die beide nicht durch t teilbar sind. Die dann notwendige Rechnung ist nicht so schwierig.

Mit dem Lemma beweisen wir die obigen Eigenschaften:

Zu (1). Wir wenden Teil (3) des Lemmas mit $\lambda(t) = rt$ an. Es folgt

$$v(g(a+tra', b+trb', c+trc')) = v(g(a+\lambda(t)a', b+\lambda(t)b', c+\lambda(t)c')) = v(g(a+ta', b+tb', c+tc')).$$

Zu (2). Wir benutzen, dass g homogen ist (sei d der Grad von g), und die gerade bewiesene Eigenschaft (1). Wir haben

$$\begin{aligned} v(g(ra+ta', rb+tb', rc+tc')) &= v(r^d g(a+tr^{-1}a', b+tr^{-1}b', c+tr^{-1}c')) \\ &= v(r)^d v(g(a+ta', b+tb', c+tc')) \\ &= v(g(a+ta', b+tb', c+tc')). \end{aligned}$$

Im letzten Schritt haben wir $v(r) = 0$ benutzt (denn $r \in F^\times$ ist ein konstantes Polynom).

Zu (3). Nach Voraussetzung gilt $(a : b : c) \neq (a' : b' : c')$, also erzeugen die Vektoren $(a, b, c)^t$ und $(a', b', c')^t$ die Lösungsmenge des linearen Gleichungssystems $\alpha X + \beta Y + \gamma Z = 0$ (als Untervektorraum von F^3). Liegt $(a'' : b'' : c'')$ auch auf der Gerade L, so folgt

$$(a'', b'', c'') = r(a, b, c) + s(a', b', c')$$

für geeignete $r, s \in F$. Weil $(a'' : b'' : c'') \neq (a : b : c)$ sein muss, gilt außerdem $s \neq 0$. Wir setzen $\lambda(t) = \frac{st}{1+rt}$. Es gilt dann $v(\lambda) = 1$ und mit Teil (3) des Lemmas erhalten wir

$$\begin{aligned} &v(g(a+ta'', b+tb'', c+tc'')) \\ &= v(g(a+t(ra+sa'), b+t(rb+sb'), c+t(rc+sc'))) \\ &= v(g((1+tr)a+tsa', (1+tr)b+tsb', (1+tr)c+tsc')) \\ &= v(1+tr)^d v(g(a+t(1+tr)^{-1}sa', b+t(1+tr)^{-1}sb', c+t(1+tr)^{-1}sc')) \\ &= v(g(a+\lambda(t)a', b+\lambda(t)b', c+\lambda(t)c')) \\ &= v(g(a+ta', b+tb', c+tc')). \end{aligned}$$

Vortrag 7 (Das Gruppengesetz auf Elliptischen Kurven)**.** Ma
Besprechen Sie [We] Definition 2.3.10 bis zum Ende von 2.3. Die Assoziativität der gegebenen Verknüpfung nehmen wir ohne Beweis hin. Geben Sie die Sätze 2.3.13 und 2.3.14 an. Wir verzichten auf den Beweis von Satz 2.3.13. Arbeiten Sie stattdessen einen direkten Beweis von Satz 2.3.14 aus und erklären Sie ihn; die Rechnungen sind deutlich einfacher als diejenigen für Satz 2.3.13.

Vortrag 8 (Endliche Körper). **Ma**

Die Anwendungen der Theorie der elliptischen Kurven, die wir im Folgenden kennenlernen werden, beruhen darauf, endliche Körper als Grundkörper zu betrachten. In diesem Vortrag stellen wir einige Grundlagen über endliche Körper bereit, die die Ergebnisse aus der Linearen Algebra ergänzen.

Erinnern Sie kurz an die Körper $\mathbb{F}_p$ mit p Elementen, p eine Primzahl.

Erklären Sie dann die folgenden Punkte:

(1) Ist K ein Körper mit endlich vielen Elementen, so ist die Charakteristik von K positiv, also eine Primzahl p, und die Anzahl q der Elemente von K ist eine Potenz $q = p^r$ von K, $r \geq 1$.

In dieser Situation gilt $a^q = a$ für alle $a \in K$.

Siehe [Gö1] Abschnitt 4.2.2[20], Ergänzung 6.57[21]. Die Aussage am Ende folgt aus dem Satz von Lagrange [Gö1] Satz 8.55[22] oder [Gö2] Korollar 18.22[23], angewandt auf die multiplikative Gruppe $K^\times$.

(2) Sei K ein Körper der Charakteristik p. Dann ist die Abbildung $\mathrm{Fr}_p \colon K \to K$, $x \mapsto x^p$, ein injektiver Ringhomomorphismus. (Zu zeigen ist hier insbesondere die Verträglichkeit mit der Addition.)

Ist K endlich, so ist Fr_p sogar ein Isomorphismus, der sogenannte *Frobenius-Automorphismus* von K. Analog hat man für $q = p^r$, $r \geq 1$ den q-Frobenius-Homomorphismus $x \mapsto x^q$.

Siehe [Bo] Abschnitt 3.2, Bem. 3.

(3) Ist L ein algebraischer Abschluss von $\mathbb{F}_p$ und $r \geq 1$, so ist

$$K := \{x \in L;\ x^{p^r} = x\} = \{x \in L;\ \mathrm{Fr}_{p^r}(x) = x\}$$

ein Teilkörper von L mit p^r Elementen. Das lässt sich leicht direkt „nachrechnen“. (Dass die Menge ein Körper ist, folgt daraus, dass Fr_{p^r} ein Ringhomomorphismus ist. Dass sie genau p^r Elemente hat, folgt daraus, dass das Polynom $X^{p^r} - X$ über L vollständig in Linearfaktoren zerfällt und keine doppelten Nullstellen hat.)

(4) Erklären Sie, wie man die Körper $\mathbb{F}_{p^r}$ für $r > 1$ „rechnerisch“ realisieren kann. Sei dazu $f \in \mathbb{F}_p[X]$ ein normiertes irreduzibles Polynom vom Grad $r \geq 1$. (Dass es für jedes $r \geq 1$ ein irreduzibles Polynom vom Grad r gibt, ist nicht ganz offensichtlich und können wir an dieser Stelle nicht beweisen.) Wir schreiben $f = X^r + a_{r-1}X^{r-1} + \cdots + a_1 X + a_0$ mit $a_i \in \mathbb{F}_p$. Dass f irreduzibel ist, bedeutet, dass sich f nicht als Produkt zweier Polynome von kleinerem Grad schreiben lässt.

Wir betrachten

$$K = \left\{b_0 + b_1 x + \cdots + b_{r-1}x^{r-1};\ b_i \in \mathbb{F}_p\right\},$$

[20] https://math.ug/la1-ws2021/sect0018.html#subsec:charakteristik
[21] https://math.ug/la1-ws2021/sect0026.html#erg-kardinalitaet-endlicher-koerper
[22] https://math.ug/la1-ws2021/sect0034.html#stz:lagrange
[23] https://math.ug/la2-ss21/sec-quotient-gruppe.html#a0000000574

wobei wir x als „formales Symbol“ betrachten und damit folgendermaßen rechnen: Die Addition ist gegeben durch

$$(b_0 + b_1x + \cdots + b_{r-1}x^{r-1}) + (c_0 + c_1x + \cdots + c_{r-1}x^{r-1}) =$$
$$(b_0 + c_0) + (b_1 + c_1)x + \cdots + (b_{r-1} + c_{r-1})x^{r-1},$$

und die Multiplikation durch

$$(b_0 + b_1x + \cdots + b_{r-1}x^{r-1}) \cdot (c_0 + c_1x + \cdots + c_{r-1}x^{r-1}) =$$
$$b_0c_0 + (b_0c_1 + b_1c_0)x + \cdots ,$$

das heißt wir multiplizieren erstmal mit dem Distributivgesetz alles aus, *behandeln dann aber x als Nullstelle des Polynoms f*, d.h. für x gilt $x^r = -a_0 - a_1x - \cdots - a_{r-1}x^{r-1}$, und wir ersetzen in dem obigen Ausdruck x^r (und dann induktiv alle Potenzen von x mit Exponent $\geq r$) durch Linearkombinationen von $1, \ldots, x^{r-1}$, also durch Elemente von K in der oben angegebenen Form.

Mit diesen Verknüpfungen ist K ein Ring.

Bemerkung:

- Machen Sie sich die Analogie zur Konstruktion der komplexen Zahlen aus den reellen Zahlen klar. Dort nehmen wir zu $\mathbb{R}$ ein „formales Symbol“ i mit der Eigenschaft $i^2 = -1$ hinzu (also eine Nullstelle des Polynoms $X^2 + 1$) und „rechnen dann einfach damit“.
- Etwas formaler ist K der Ring $\mathbb{F}_p[X]/(f)$, der Quotient des Polynomrings $\mathbb{F}_p[X]$ nach dem Ideal $(f) = \{gf;\ g \in \mathbb{F}_p[X]\}$ aller Vielfachen von f. Dies ist auch die „richtige“ Sichtweise, um zu begründen, dass es sich bei K tatsächlich um einen Ring handelt.
- $\mathbb{F}_p$ ist ein Teilkörper von K, und als $\mathbb{F}_p$-Vektorraum hat K die Dimension $r = \deg(f)$ (denn die Elemente $1, x, \ldots, x^{r-1}$ bilden eine Basis). Daher hat K genau p^r Elemente.

Behauptung. K ist ein Körper.

Begründung. Sei $b \in K \neq \{0\}$, wir schreiben $b = b_0 + b_1x + \cdots + b_{r-1}x^{r-1}$ (nicht alle b_i sind $= 0$) und wollen zeigen, dass ein Element $c \in K$ mit $bc = 1$ existiert. Wir werden dafür benutzen, dass f nach Voraussetzung irreduzibel ist.

Sei $g = b_0 + b_1X + \cdots + b_{r-1}X^{r-1} \in \mathbb{F}_p[X]$, wir machen also aus dem Element b ein Polynom im Polynomring $\mathbb{F}_p[X]$. Weil g Grad $< r$ hat und $\neq 0$ ist, kann f kein Teiler von g sein. Weil f irreduzibel ist, hat f keine echten Teiler und es folgt, dass der (normierte) größte gemeinsame Teiler von f und g gleich 1 ist.

Im Polynomring $\mathbb{F}_p[X]$ steht uns mittels der Polynomdivision der euklidische Algorithmus zur Verfügung, und damit können wir Polynome $u, v \in \mathbb{F}_p[X]$ mit

$$uf + vg = 1$$

finden. Wenn wir in dieser Gleichung in alle Polynome für die Unbestimmte X den Wert $x \in K$ einsetzen, erhalten wir

$$v(x)\, b = v(x)g(x) = u(x)f(x) + v(x)g(x) = 1,$$

denn $f(x) = 0$. Also ist $c := v(x) \in K$ das gesuchte inverse Element zu b.

Beispiel: $p = 2$, $f = X^2 + X + 1$. Dies ist ein irreduzibles Polynom und die obige Prozedur liefert uns einen Körper mit $2^2 = 4$ Elementen.

Vergleiche [We] Abschnitt 6.6.

(5) Wenn Zeit bleibt und es in Vortrag 2 noch nicht geschehen ist, könnte man etwas zum Beweis des Satzes aus Vortrag 2 sagen: **Satz.** Ist K ein Körper und ist $G \subseteq K^\times$ eine endliche Untergruppe, dann ist G eine *zyklische Gruppe*, d.h. es existiert $g \in G$ mit $G = \langle g \rangle = \{g^i;\ i \in \mathbb{Z}\}$. Siehe zum Beispiel [Gö1] Ergänzung 8.59[24].

Vortrag 9 (Elliptische Kurven über endlichen Körpern). **Ma**

Wir besprechen jetzt einige Besonderheiten von elliptischen Kurven über endlichen Körpern. Sie können sich, um Zeit zu sparen, auf den Fall von Weierstraß-Gleichungen mit $a_1 = a_3 = 0$ beschränken.

Diskutieren Sie [We] Abschnitte 3.1 und 3.2 bis Satz 3.2.1. Ergänzen Sie in Abschnitt 3.1, dass $E(F)$ genau die Teilmenge derjenigen Punkte P von $E(\overline{F})$ ist, für die $\phi(P) = P$ gilt. (Das ist nicht schwierig, aber auch nicht ganz offensichtlich, weil wir mit homogenen Koordinaten arbeiten.)

Vortrag 10 (Faktorisieren mit elliptischen Kurven). **Ma**

In diesem Kapitel besprechen wir einen Algorithmus, der die Theorie der elliptischen Kurven benutzt, um große natürliche Zahlen in ihre Primfaktoren zu zerlegen, also zu *faktorisieren*.

Sie können der Darstellung in [ST] Chapter IV, §4, ab Seite 146, letzter Absatz (bzw. in der ersten Auflage: S. 132 Mitte), „Now we are ready to describe Lenstra's idea ...“, folgen.

Alternativ siehe auch [Wa] 7.1.

Vortrag 11 (Grundlagen der Public-Key-Kryptographie). **Ba/Ma**

Erklären Sie die Grundidee der Public-Key-Kryptographie (Kommunikation über einen nicht-abhörsicheren Kanal ohne vorherigen Schlüsselaustausch). Wenn genug Zeit ist, könnten Sie das RSA-Verfahren besprechen, siehe [We] Abschnitte 1.1, 5.2.1, [Bu] Abschnitt 9.3, [Gö1] Bemerkung 8.58[25].

Erläutern Sie das Verfahren zum Schlüsseltausch von Diffie und Hellman (für eine beliebige abelsche Gruppe G, [We] 1.2.1). Erklären Sie, warum sich die additiven Gruppen $\mathbb{F}_q$ nicht dafür eignen.

Diskutieren Sie die Fälle der Gruppen $\mathbb{F}_q^\times$ ([We] 5.2.2) und $E(\mathbb{F}_q)$ für eine elliptische Kurve über $\mathbb{F}_q$.

Gegebenenfalls können Sie noch andere der Verfahren aus [We] Kapitel 1 darstellen.

Siehe auch [Bu] Kapitel 9.

[24] https://math.ug/la1-ws2021/sect0034.html#a0000001572
[25] https://math.ug/la2-ss21/sec-integritaetsringe.html#bem:rsa-2

Vortrag 12 (Backdoor to NIST standard). Ba/Ma

Erklären Sie, was man unter einem Pseudo-Zufallszahlen-Generator versteht und warum so etwas aus kryptographischer Sicht von Bedeutung ist. (Wird der Vortrag als Bachelor-Seminar-Vortrag gehalten, genügt uns eine „naive“ Erklärung dazu; für einen Master-Seminar-Vortrag sollten Sie das etwas weiter unterfüttern.)

Erläutern Sie anhand des Artikels [Ha] von Thomas Hales, wie man mit elliptischen Kurven einen solchen Zufallszahlengenerator konstruieren kann, und warum der 2012 vom US-amerikanischen National Institute for Standards and Technology vorgeschlagene Algorithmus anfällig für eine „Backdoor“ ist. Den letzten Teil (Diffie-Hellman Key Exchange), in dem erklärt wird, wie einen das Schlüsseltauschverfahren nach Diffie und Hellmann auf die Idee bringen könnte, einen solchen Algorithms mit Backdoor zu konstruieren, können Sie gegebenenfalls weglassen.

Siehe auch [Lu] Lecture 1, und/oder [Bu] Kap. 5.

Vortrag 13 (Quantencomputer und der Algorithmus von Shor 1). Ma

Der Vortrag hat zwei Teile, die Reihenfolge können Sie selbst bestimmen, wie es Ihnen passender erscheint:

- Übersicht über den Algorithmus von Shor,
- das Funktionsprinzip eines Quantencomputers.

Der Algorithmus von Shor. Ziel des Algorithmus ist es, einen echten Teiler einer natürlichen Zahl $N \in \mathbb{N}$ zu finden, die keine Primzahl ist (induktiv könnte man dann die Primfaktorzerlegung von N finden). Der naive Ansatz, dafür für alle Zahlen $2, 3, 4, \dots$ die Division (mit Rest) von N durch diese Zahl durchzuführen, ist für große N nicht praktikabel. Man kennt zwar etwas bessere Methoden (eine haben wir in Vortrag 10 kennengelernt; andere sind das sogenannte quadratische Sieb und das Zahlkörpersieb), aber für „große“ Zahlen (mehr als 600 Stellen ist jedenfalls groß) dauern diese Verfahren in schlechten Fällen Jahre (oder vielleicht eher Jahrhunderte).

Die Grundidee des Algorithmus von Shor ist die folgende: Ist x eine zu N teilerfremde Zahl, $1 < x < N-1$, so dass $x^2 \equiv 1 \mod N$ gilt, dann haben wir $N \mid x^2 - 1 = (x-1)(x+1)$, aber $N \nmid x-1$, $N \nmid x+1$, und es folgt, dass $\mathrm{ggT}(N, x-1)$ ein echter Teiler von N ist (und ebenso $\mathrm{ggT}(N, x+1)$).

Um x zu finden, könnte man versuchen, zufällig eine Zahl a zwischen 1 und N zu wählen. Gilt $a^r \equiv 1 \mod N$ für eine *gerade* Zahl r, so wäre $a^{r/2}$ (bzw. genauer der Rest dieser Zahl modulo N) ein Kandidat für x. (Es bleibt allerdings zusätzlich zu prüfen, dass dieser Rest $\neq 1$ und $\neq N-1$ ist.)

Um das noch etwas besser zu formulieren, sei $(\mathbb{Z}/N\mathbb{Z})^\times$ die (multiplikative) Gruppe der Einheiten im Ring $\mathbb{Z}/N\mathbb{Z}$. Sie besteht genau aus den Elementen von $\mathbb{Z}/N\mathbb{Z}$, die Restklassen von Zahlen sind, die teilerfremd zu N sind. Für $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ sei $\mathrm{ord}(a)$ die Ordnung von a als Element von $(\mathbb{Z}/N\mathbb{Z})^\times$, also die kleinste Zahl $m \in \mathbb{N}_{>0}$ mit $a^m = 1$ (in $(\mathbb{Z}/N\mathbb{Z})^\times$). Siehe [Gö2] Beispiel 15.3 (2)[26] und die Verweise dort.

Wir suchen $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, so dass $r := \mathrm{ord}(a)$ gerade ist und $a^{r/2} \neq -1$ (in $(\mathbb{Z}/N\mathbb{Z})^\times$).

[26] `https://math.ug/la2-ss21/sec-ringe-def.html#bsp:ringe`

Das führt auf die folgenden Schritte des Shor-Algorithmus:

Schritt 1. Wähle zufällig eine natürliche Zahl a, $1 < a < N$. Gilt $\mathrm{ggT}(a, N) > 1$, dann ist $\mathrm{ggT}(a, N)$ ein echter Teiler von N und wir haben das Ziel schon erreicht. Sonst sind a und N teilerfremd und die Restklasse von a ist ein Element von $(\mathbb{Z}/N\mathbb{Z})^\times$, das wir wieder mit a bezeichnen.

Schritt 2. Berechne $\mathrm{ord}(a)$. Wenn diese Zahl ungerade ist, müssen wir ein neues a wählen, d.h. wieder zu Schritt 1 zurückspringen.

Schritt 3. Wir haben a gefunden, so dass $r := \mathrm{ord}(a)$ gerade ist. Wenn $a^{r/2} = -1$ (in $(\mathbb{Z}/N\mathbb{Z})^\times$) gilt, müssen wir ein neues a wählen, d.h. wieder zu Schritt 1 zurückspringen. Sonst ist $\mathrm{ggT}(a^{r/2} + 1, N)$ ein echter Teiler von N und wir sind fertig.

Die Hauptprobleme, die bleiben, sind die folgenden:

(1) Der Algorithmus basiert darauf, zufällig ein Element a zu wählen. Damit der Algorithmus in der Praxis sinnvoll anwendbar ist, muss die Wahrscheinlichkeit ein a zu wählen, das die im weiteren Verlauf benötigten Eigenschaften hat, genügend groß sein. (Sonst müsste man eventuell sehr oft zu Schritt 1 zurückspringen und ein neues a wählen ...)

Man kann zeigen, dass diese Wahrscheinlichkeit (mindestens) ungefähr $\frac{1}{2}$ ist, so dass man in aller Regel nach wenigen Versuchen ein geeignetes a finden wird. Diese Abschätzung ist nicht sehr schwierig und auch nicht so interessant, und wir lassen sie deshalb aus. (Referenz, wenn Sie es genau wissen möchten: [Sch] Satz 6.7.)

Außerdem ist wichtig, dass für einen gegebenen Kandidat schnell überprüft werden kann, ob es sich tatsächlich um eine Lösung des gegebenen Problems handelt. Das ist hier der Fall, denn Multiplikation und Potenzieren in Restklassenringen ist „schnell“ möglich, ebenso der Test ob eine gegebene Zahl die Zahl N teilt.

(2) Wie berechnet man in Schritt 2 die Ordnung von a? Es ist nicht klar, wie man das effizient machen kann, genauer ist kein Algorithmus bekannt, der diese Rechnung auf einem „klassischen“ Computer für große N in annehmbarer Zeit durchführt. Der wesentliche Punkt des Algorithmus von Shor ist, dass es auf *Quantencomputern* einen Algorithmus gibt, der dieses Problem „schnell“ lösen kann.

Quantencomputer. Es wird vermutlich nicht überraschen, dass die Darstellung an einigen Punkten etwas vereinfacht werden muss, aber die meisten wesentlichen Punkte lassen sich hoffentlich illustrieren.

Bevor wir beschreiben, was wir unter einem Quantencomputer verstehen, betrachten wir kurz einen „klassischen“ Computer (bzw. ein „mathematisches Modell“ davon). Ein klassischer Computer besteht (für uns) aus seinem Speicher und einem Programm, das der Computer ausführen kann. Alle Daten im Speicher zusammen betrachten wir als ein s-Tupel von Nullen und Einsen, also als ein Element von $\{0, 1\}^s$. Ein solches Tupel gibt den Zustand des Speichers zu einem Zeitpunkt an. Wir sagen, der Computer könne s Bits abspeichern, jedes Bit entspricht einem Eintrag des gegebenen s-Tupels von Nullen und Einsen. Zum Beispiel würden 16GB Speicherplatz gerade $s = 2^{3840}$ Bits entsprechen (eine Zahl mit mehr als 1000 Stellen, also schon eine

ganze Menge). Wir nummerieren diese einzelnen Bits von 0 bis $s-1$ und schreiben $a_i \in \{0,1\}$ für den Inhalt/Zustand des i-ten Bits zu einem gegebenen Zeitpunkt.

Das Programm besteht aus einer Folge von Operationen, wobei die einzelnen erlaubten Schritte die folgenden sind (für $i,j,k \in \{0,\dots,s-1\}$):

- Schreibe eine 0 oder eine 1 in Eintrag i,
- kopiere den Eintrag a_i an die Stelle j,
- ersetze den Inhalt von Bit i durch `NOT` $a_i := 1 - a_i$,
- ersetze den Inhalt von Bit i durch a_j `AND` $a_k := a_j \cdot a_k$,
- ersetze den Inhalt von Bit i durch a_j `OR` $a_k := 1 - (1-a_j)(1-a_k)$.

Entscheidend sind die letzten drei *logischen Operationen*. Auf der rechten Seite sind diese jeweils durch Rechnungen im Körper $\mathbb{F}_2$ ausgedrückt (was aber vielleicht nicht sehr hilfreich ist).

Übung: Schreiben Sie ein Programm (im obigen Sinne), das zwei Zahlen addiert. Sie dürfen annehmen, dass die beiden Zahlen im Binärsystem im Speicher abgelegt sind, dass die erste Zahl zwei Stellen und die zweite Zahl eine Stelle hat. (Zweck dieser Übung ist, glaubhaft zu machen, dass man durch (sehr) viele solcher Schritte auch komplizierte Berechnungen durchführen kann, und zwar alle Rechnungen, die sich auf klassischen Computern eben durchführen lassen.)

Den Computer kann man dann folgendermaßen benutzen: Man kann den Speicher „initialisieren“, also Nullen und Einsen in die Speicherplätze „eintragen“, das Programm ablaufen lassen, und dann den Speicher wieder auslesen.

Ein Quantencomputer hat auch einen „Speicher“ und kann ein „Programm abarbeiten“ und das Ergebnis „auslesen“. Wie wir sehen werden, sind Speicher und Programm wesentlich „besser“ als beim klassischen Computer; das Ergebnis auszulesen, ist aber „problematisch“, insbesondere *verändert das Auslesen das Ergebnisses in der Regel den Inhalt des Speichers*!

Wir benötigen zur Beschreibung (eines Quantencomputers mit s Quantenbits) einen $\mathbb{C}$-Vektorraum V der Dimension 2^s mit einem Skalarprodukt. Wir können (und werden) einfach den Standardvektorraum $V := \mathbb{C}^{2^s}$ mit dem Standardskalarprodukt betrachten. Wir folgen der üblichen Notation und benennen die Standardbasisvektoren $e_1,\dots,e_{2^s}$ folgendermaßen („ket-Notation“ aus der Physik):

$$|x\rangle, \quad x = 0,\dots,2^s-1.$$

Oft schreibt man die natürliche Zahl x an dieser Stelle in Binärdarstellung, also zum Beispiel $111_2 = 7$ und entsprechend $|111_2\rangle$ für den achten Standardbasisvektor. (In der Literatur wird fast immer auch der Index $-_2$ für die Binärdarstellung weggelassen.)

Die möglichen Speicherzustände unseres Quantencomputers sind dann die Vektoren in V der Länge 1. Zum Beispiel sind die Standardbasisvektoren $|x\rangle$ selbst mögliche Zustände („klassische Zustände“, denn diese sind in Bijektion zu den Speicherzuständen eines klassischen Computers mit s Bits), aber eben auch alle Linearkombinationen

$$\sum_{x=0}^{2^s-1} a_x|x\rangle \quad \text{mit} \ \sum_x |a_x|^2 = 1$$

(man spricht von *Überlagerungen* klassischer Zustände). Während ein klassischer Computer mit einem Speicherplatz von s Bits also „nur“ 2^s verschiedene Speicherzustände hat, hat schon ein Quantencomputer mit nur einem einzigen Quantenbit unendlich viele Speicherzustände, nämlich alle Vektoren der Länge 1 in $\mathbb{C}^2$.

Ein Programm des Quantencomputers besteht aus einer Folge von unitären Matrizen $U \in M_{2^s}(\mathbb{C})$. In dem entsprechenden Schritt des Programms wird der Speicherzustand $v \in V$ ersetzt durch Uv. Eine quadratische Matrix U heißt unitär, wenn UU^* die Einheitsmatrix ist (insbesondere ist U dann invertierbar). Hier ist U^* die Matrix, die aus U durch Transponieren und Anwenden der komplexen Konjugation auf alle Einträge entsteht. Für uns wichtig ist die Eigenschaft $\|Uv\| = \|v\|$ für unitäre Matrizen, diese erhalten also die Länge von Vektoren. (Siehe [Gö2] Abschnitt 19.6.2[27].)

Das Analogon zum „Auslesen“ des Speichers ist für den Quantencomputer die „Durchführung einer Messung“. Es ist ein essenzieller Bestandteil der Quantentheorie, dass der Zustand eines Systems eine Angabe von Wahrscheinlichkeiten ist und dass eine Messung den Zustand des Systems verändern kann (weil die Messung ein genaues Ergebnis, nicht nur eine Wahrscheinlichkeit, liefern muss und dadurch den Zustand des Systems auf das gelieferte Ergebnis festlegt).

Konkret: Ist $v = \sum_{x=0}^{2^s-1} a_x|x\rangle$ der aktuelle Zustand unseres Quantencomputers, dann liefert eine Messung zufällig ein Element $y \in \{0, \dots, 2^s - 1\}$, und zwar wird jedes y mit Wahrscheinlichkeit $|a_y|^2$ „gemessen“. (Weil v Länge 1 hat, ist die Summe aller dieser Wahrscheinlichkeiten gleich Eins.) Der Koeffizient a_y ist nicht Teil des Messergebnisses. Danach befindet sich der Computer im Zustand $|y\rangle$ (und das bedeutet in der Regel: ein Großteil der Information über den vorherigen Zustand ist durch die Messung verloren gegangen).

Für den Umgang mit Quantencomputern ist daher ein wesentlicher Aspekt, dass man damit rechnen muss, nur mit einer gewissen Wahrscheinlichkeit ein „brauchbares“ Ergebnis zu erhalten. Wenn man „Pech gehabt“ hat, muss man die Rechnung wiederholen und „hoffen“, dass es beim nächsten Mal klappt. Bei der Entwicklung von Programmen/Algorithmen für Quantencomputer muss man daher sicherstellen, dass die Programme mindestens mit einer hinreichend hohen Wahrscheinlichkeit zum Erfolg führen. Außerdem muss es möglich sein, schnell zu überprüfen, ob das Ergebnis der Quantencomputer-Rechnung tatsächlich eine Lösung des gegebenen Problems liefert. (Das ist ähnlich zu der Wahl von a in Schritt 1 des Algorithmus von Shor oben, wo auch das Risiko besteht, zufällig ein a mit ungerader Ordnung zu wählen, mit dem wir dann im weiteren Verlauf nichts anfangen können.)

Im nächsten Vortrag werden wir der Übersichtlichkeit halber die folgende Variante für die Schreibweise verwenden: Hat man einen Quantencomputer mit $s+t$ Quantenbits, hat der zugehörige unitäre Vektorraum die Dimension $2^{s+t} = 2^s 2^t$. Für die Basisvektoren bedeutet das, dass jeder Vektor in der Form $|x\rangle$ für eine Zahl x geschrieben werden kann, die im Binärsystem $\leq s+t$ Stellen hat. Wir füllen gegebenenfalls vorne mit Nullen auf, so dass wir genau $s+t$ Stellen haben und schreiben dann $|x\rangle = |y\rangle|z\rangle$, wo y durch die linken s Stellen von x und z durch die rechten t Stellen von x (im Binärsystem) gegeben sei. Zwei ket-Symbole nebeneinander zu schreiben, bedeutet also einfach, die beiden Zahlen im Binärsystem mit der vorgegebenen Stellenanzahl zu

[27] `https://math.ug/la2-ss21/sec-normale-endom.html#subsec:isometrien`

schreiben und nebeneinander zu schreiben. Man nennt dann das linke ket-Symbol das *erste Register* und das rechte ket-Symbol das *zweite Register* des Quantencomputers. (Mathematisch kann man diese Konstruktion mit dem Tensorprodukt von (unitären) Vektorräumen beschreiben, aber damit müssen wir uns nicht befassen.)

Wenn Zeit ist, könnten Sie an dieser Stelle Beispiele für unitäre Matrizen erwähnen, die nützlich sein können:

- Jede Permutationsmatrix ist unitär. (Insbesondere lässt sich jede invertierbare Rechnung, die man auf einem klassischen Computer machen kann, auch auf einem Quantencomputer durchführen. Mit einem Trick kann man zeigen, dass das auch für nicht-invertierbare Rechnungen möglich ist.)
- Für jedes $n \in \mathbb{N}$ gibt es eine unitäre Matrix $U \in M_n(\mathbb{C})$, für die alle Einträge der erste Spalten gleich (und zwar $= 1/\sqrt{n}$) sind (zum Beispiel: Hadamard-Matrix[28]). Was ist der Effekt, wenn man U auf den Zustand $|0\rangle$ unseres Quantencomputers anwendet?

Weitere Quellen: [Ak], [Sch], Wikipedia: Quantencomputer[29], Algorithmus von Shor[30] (die englischen Seiten sind noch ausführlicher).

Vortrag 14 (Der Algorithmus von Shor 2)**.** Ma
In diesem Vortrag soll erklärt werden, wie man mit einem Quantencomputer *Schritt 2* des Shor-Algorithmus (siehe den vorherigen Vortrag) durchführen kann.

Die Beschreibung ist ziemlich lang geworden und Sie müssen sicher eine Auswahl treffen, was Sie am Ende im Vortrag präsentieren möchten. Es war mir aber wichtig, einige „Hintergrundinformationen“ zu geben, die Sie zumindest als Vortragende:r haben sollten.

Die Lösung beruht auf der „Quanten-Fouriertransformation“ – keine Angst, das klingt komplizierter, als es ist. Wir haben keine Zeit, in das Thema *Fourieranalysis* wirklich einzusteigen, und begnügen uns mit den folgenden motivierenden Bemerkungen:

- Grundidee der Fouriertransformation ist es, eine Funktion als Summe von „symmetrischeren“ Funktionen auszudrücken. Ein sehr einfaches aber prototypisches Beispiel ist das folgende: Eine Funktion $f\colon \mathbb{R} \to \mathbb{R}$ heißt *gerade*, wenn $f(-x) = f(x)$ für alle $x \in \mathbb{R}$ gilt, und *ungerade*, wenn $f(-x) = -f(x)$ für alle $x \in \mathbb{R}$ gilt. (Was bedeutet das geometrisch für den Funktionsgraphen von f?)

  Ist nun $f\colon \mathbb{R} \to \mathbb{R}$ irgendeine Funktion, dann ist f die Summe der geraden Funktion $f_g\colon \mathbb{R} \to \mathbb{R}$, $f_g(x) = \frac{1}{2}(f(x) + f(-x))$, und der ungeraden Funktion $f_u\colon \mathbb{R} \to \mathbb{R}$, $f_u(x) = \frac{1}{2}(f(x) - f(-x))$. (Rechnen Sie nach, dass f_g gerade, f_u ungerade und $f(x) = f_g(x) + f_u(x)$ für alle $x \in \mathbb{R}$ ist – vielleicht nicht im Vortrag, aber jedenfalls für sich selbst).
- Die Fourierreihe einer periodischen Funktion drückt die Funktion als „Überlagerung“, also als Summe, von trigonometrischen Funktionen aus. Das sollte man sich so vorstellen, dass ein (periodisches) Signal in seine verschiedenen

[28] https://de.wikipedia.org/wiki/Hadamard-Matrix
[29] https://de.wikipedia.org/wiki/Quantencomputer
[30] https://de.wikipedia.org/wiki/Shor-Algorithmus

Frequenzen zerlegt wird. (Eventuell wurde in Ihrer Analysis-Vorlesung das Thema Fourier-Reihen behandelt, sonst siehe gegebenenfalls zum Beispiel [Fo] Kapitel 23. Wir brauchen diese Theorie aber unten nicht, die Bemerkung dient nur dazu, einen Kontext für die Theorie der Quanten-Fouriertransformation herzustellen.)

Insofern ist es plausibel, dass eine Variante der Fouriertransformation dazu dienen kann, die unbekannte Periode einer periodischen Funktion zu ermitteln. Wie das genau geht (und warum es mit einem Quantencomputer „schnell“ durchgeführt werden kann) ist aber nicht offensichtlich und soll nun erklärt werden.

Schritt 2 in Shors Algorithmus. Wir benutzen einen Quantencomputer mit $2q$ Quantenbits, wobei q so gewählt wird, dass für $Q = 2^q$ und die zu faktorisierende Zahl N gilt, dass $N^2 \leq Q < 2N^2$ ist. Für die klassischen Zustände (also die Standardbasisvektoren unseres Vektorraums) benutzen wir die Schreibweise $|x\rangle|y\rangle$ mit $x, y \in \{0, \dots, 2^q - 1\}$, wir teilen also die $2q = q + q$ Quantenbits auf in „zwei Register“ mit jeweils q Quantenbits.

Es sei $a \in (\mathbb{Z}/N)^\times$ eine zu N teilerfremde Zahl und $f\colon \{0, \dots, Q-1\} \to \mathbb{C}$ die Funktion $x \mapsto a^x$. Um die Werte von f als komplexe Zahlen zu betrachten, identifizieren wir $\mathbb{Z}/N = \{0, 1, 2, \dots, N-1\} \subseteq \mathbb{C}$, wir wählen für die Restklasse a^x also immer den eindeutig bestimmten Repräsentanten in $\{0, 1, 2, \dots, N-1\}$. Die Funktion f ist periodisch mit Periode $r := \operatorname{ord}(a)$, d.h. es ist $f(x + r) = f(x)$ für alle $x \in \mathbb{Z}$, für ein uns unbekanntes r, das wir gerne ermitteln möchten.

Vorüberlegung. Sei $\omega = e^{2\pi i/Q} \in \mathbb{C}$. Dies ist eine *primitive Q-te Einheitswurzel*, d.h. es gilt $\omega^Q = 1$, $\omega^s \neq 1$ für alle $0 < s < Q$. In der komplexen Zahlenebene liegt ω auf dem Einheitskreis, und der Winkel zwischen der reellen Achse und der Gerade durch ω ist $\frac{1}{Q}$ des Vollwinkels. Die Potenzen $\omega^0 = 1, \omega, \omega^2, \dots, \omega^{Q-1}$ unterteilen also die Kreislinie des Einheitskreises in Q gleich große Abschnitte. Weil $\omega^Q = 1$ gilt, können wir auch von den Potenzen ω^x für $x \in \mathbb{Z}/Q$ sprechen, denn jeder Repräsentant von x in $\mathbb{Z}$ liefert dasselbe Ergebnis. Es gilt dann für $y \in \mathbb{Z}/Q$ die folgende Gleichung, die fundamental für das Weitere ist:

$$\sum_{x \in \mathbb{Z}/Q} \omega^{xy} = \begin{cases} Q & \text{wenn } y = 0, \\ 0 & \text{sonst.} \end{cases}$$

Der erste Fall ist klar, denn $\omega^0 = 1$. Im zweiten Fall nutzen wir aus, dass die Menge der Summanden invariant ist unter der Drehung um $\frac{y}{Q} \cdot 360°$, also unter der Multiplikation mit ω^y:

$$\omega^y \sum_{x \in \mathbb{Z}/Q} \omega^{xy} = \sum_{x \in \mathbb{Z}/Q} (\omega^y)^{x+1} = \sum_{x \in \mathbb{Z}/Q} (\omega^y)^x.$$

Weil für $y \neq 0$ (in $\mathbb{Z}/Q$) die Potenz $\omega^y \neq 1$ ist, kann diese Gleichung nur gelten, wenn die Summe verschwindet.

(Im einfachsten Fall $Q = 2$ ist $\omega = -1$ und dann sind die obigen Gleichungen einfach $(-1)^0 + (-1)^0 = 2$ und $(-1)^0 + (-1)^1 = 0$. Dieser Fall korrespondiert zu dem Beispiel am Anfang mit geraden und ungeraden Funktionen.)

Wir führen nun auf dem Quantencomputer die folgenden Schritte durch. (An einigen Stellen sind wir etwas ungenau in Hinsicht darauf, wie/ob das so wirklich möglich ist. Wir konzentrieren uns hier auf die „interessanten“ Probleme bei der Berechnung.) Wir schreiben die Standardbasisvektoren von $\mathbb{C}^{2^{2q}}$ als $|x\rangle|y\rangle$, wobei x und y jeweils q Stellen im Binärsystem haben (gegebenenfalls mit führenden Nullen).

(A) Initialisierung des Quantencomputers. Wir initialisieren den Computer im Zustand

$$\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|0\rangle.$$

(B) Berechnung der Potenzen a^x. In diesem Schritt ersetzen wir den Wert 0 im „zweiten Register“ durch den Wert $|f(x)\rangle$. Hier verstehen wir $f(x) \in (\mathbb{Z}/N)^\times \subset \mathbb{Z}/N = \{0, \dots, N-1\} \subset \{0, \dots, Q-1\}$ mit der oben erklärten Identifikation $\mathbb{Z}/N = \{0, \dots, N-1\}$ als Element von $\{0, \dots, Q-1\}$. Wir wenden also eine (unitäre) Abbildung mit $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ (für $x = 0, \dots, Q-1$) an. Diese Vorschrift kann man erhalten durch eine geeignete Permutation aller Basisvektoren der fixierten Standardbasis. Jede Permutationsmatrix ist unitär.

Damit können wir auf dem Quantencomputer gleichzeitig a^x für alle x berechnen (man spricht von Quantenparallelismus). Dadurch wird der Quantencomputer in den Zustand

$$\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|f(x)\rangle$$

versetzt.

(C) Die Quanten-Fouriertransformation. Als nächsten Schritt wenden wir die Quanten-Fouriertransformation auf das erste Register an, das ist die folgende unitäre Abbildung:

$$\mathbb{C}^Q \longrightarrow \mathbb{C}^Q, \quad |x\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} \omega^{xy} |y\rangle.$$

(Dass diese Abbildung unitär ist folgt mit einer Rechnung aus der Vorüberlegung.) Dies wenden wir auf das linke Register im vorherigen Ausdruck an und erhalten

$$\begin{aligned} \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|f(x)\rangle \mapsto & \frac{1}{Q} \sum_{x=0}^{Q-1} \sum_{y=0}^{Q-1} \omega^{xy} |y\rangle|f(x)\rangle \\ = & \frac{1}{Q} \sum_{y=0}^{Q-1} \sum_{z \in \mathrm{Im}(f)} \left(\sum_{x,\ f(x)=z} \omega^{xy} \right) |y\rangle|z\rangle. \end{aligned}$$

(D) Messung. Wir führen nun eine Messung des Zustands unseres Quantencomputers durch und erhalten damit einen Messwert der Form $|y\rangle|z\rangle$, und zwar erhalten wir das Paar $(y, z) \in \{0, \dots, Q-1\} \times \mathrm{Im}(f)$ mit Wahrscheinlichkeit

$$\Pr(y, z) = \left| \frac{1}{Q} \sum_{x,\ f(x)=z} \omega^{xy} \right|^2,$$

(Paare (y, z), für die $z \notin \mathrm{Im}(f)$ ist, können nicht als Messwert auftreten.)

Für den Wert z unserer Messung schreiben wir $z = f(x_0)$ mit minimalem x_0. Dann ist

$$f^{-1}(z) = \{x_0, x_0 + r, \ldots, x_0 + (m-1)r\}$$

für $m = \#f^{-1}(z) = \lfloor \frac{Q - x_0 - 1}{r} \rfloor + 1$. Damit können wir wie folgt weiterrechnen:

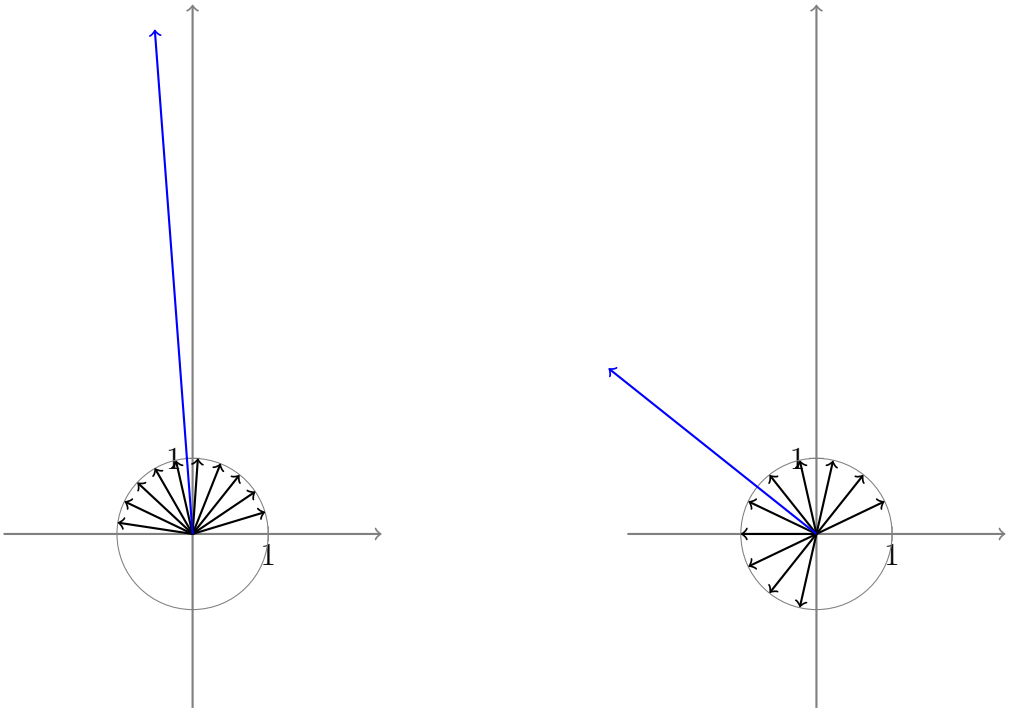
$$\Pr(y, z) = \frac{1}{Q^2} \left| \sum_{b=0}^{m-1} \omega^{(x_0 + br)y} \right|^2 = \frac{1}{Q^2} \left| \sum_{b=0}^{m-1} (\omega^{ry})^b \right|^2 .$$

Wir sehen an dieser Darstellung schon, dass die Quanten-Fouriertransformation dem Standardbasisvektor $|y\rangle|z\rangle$ eine Wahrscheinlichkeit zuordnet, die von ry abhängt. Genauer gilt: Wenn $r \mid Q$ gilt, ist ω^r eine primitive $\frac{Q}{r}$-te Einheitswurzel und die Summe auf der rechten Seite ist von derselben Form wie in der Vorüberlegung, d.h. der Koeffizient von $|y\rangle|z\rangle$ ist genau dann von Null verschieden, wenn y ein Vielfaches von $\frac{Q}{r}$ ist. Durch eine Messung des Quantencomputer-Zustands findet man also als y ein Element der Form cQ/r von $\{0, \ldots, Q-1\}$. Wenn $c = 0$, also $y = 0$ ist, kann man mit dem Ergebnis nichts anfangen und muss erneut ansetzen. Sonst kann man $y/Q = a/r$ als gekürzten Bruch ausrechnen und erhält bestenfalls (wenn a und r teilerfremd sind) die Zahl r als den Nenner, oder andernfalls als Nenner immerhin einen nicht-trivialen Teiler von r. Das genügt normalerweise, um r zu bestimmen. Wir lassen die weiteren Details des Falls $r \mid Q$ aus, weil er weniger interessant und relevant ist als der Fall $r \nmid Q$.

Wir nehmen also nun an, dass $r \nmid Q$ gilt. Dann sind wir nicht genau in der Situation der Vorüberlegung, aber – wie wir sehen werden – noch nah genug an dieser Situation, dass das gemessene Paar (y, z) es mit hoher Wahrscheinlichkeit ermöglicht, r zu berechnen.

Anschaulich können wir das wie folgt beschreiben: Mit hoher Wahrscheinlichkeit wird ein Wert (y, z) gemessen, für den $\Pr(y, z)$ groß ist, also $\left|\sum_{b=0}^{m-1} \omega^{byr}\right|$ groß ist. Damit diese Summe groß ist, müssen alle Summanden ω^{byr} möglichst eng beieinander auf dem Einheitskreis liegen. Das ist gerade dann der Fall, wenn ω^{ry} nahe bei 1 liegt, also ry sich nicht sehr von einem Vielfachen von Q unterscheidet, oder mit anderen Worten: Wenn der Bruch $\frac{yr}{Q}$ nahe an einer ganzen Zahl liegt. Da y und Q bekannt sind, erhalten wir damit Informationen über r. (Wir werden das unten präzisieren.)

Die folgenden Abbildungen illustrieren das. In beiden Fällen werden 10 Einheitswurzeln aufsummiert, die Summe ist durch den blauen Pfeil gegeben. Selbst wenn die Einheitswurzeln nur wenig mehr als einen Halbkreis des Einheitskreises „ausfüllen“ ist die Länge des Summenvektors deutlich kleiner als im anderen Fall. Genau diese Bedingung werden wir weiter unten wiedersehen und rechnerisch begründen.



Wie wir nachrechnen werden, ist $\frac{yr}{Q}$ mit hoher Wahrscheinlichkeit nah genug an einer ganzen Zahl, damit man aus der Kenntnis von y die Zahl r berechnen kann. Dass die Wahrscheinlichkeiten $\Pr(y,z)$ bei wenigen y konzentriert sind, sieht man auch, wenn man die Funktion $y \mapsto \sum_z \Pr(y,z)$ plottet, siehe zum Beispiel [Sh], Abb. 5.1. (Was bei uns y heißt, heißt dort c.)

Wir wollen als nächstes überlegen, wie man aus einem gemessenen Paar (y,z) in gewissen Fällen den gesuchten Wert der Periode r bestimmen kann. Dafür benutzen wir das folgende Lemma.

Lemma. Sei $x \in \mathbb{R}$ eine reelle Zahl und sei $s \in \mathbb{N}$. Dann existiert höchstens eine Zahl $\xi \in \mathbb{Q}$, die sich mit Nenner $\leq s$ schreiben lässt und für die $|x - \xi| < \frac{1}{2s^2}$ gilt.

Beweis. Wenn $\xi_1, \xi_2 \in \mathbb{Q}$ beide die genannten Bedingungen erfüllen, dann folgt $|\xi_1 - \xi_2| < 1/s^2$. Schreiben wir $\xi_i = \frac{a_i}{s_i}$ mit $a_i, s_i \in \mathbb{Z}$, $0 < s_1, s_2 \leq s$, dann haben wir andererseits $|a_1/s_1 - a_2/s_2| = |\frac{a_1 s_2 - a_2 s_1}{s_1 s_2}| \geq 1/s^2$, es sei denn es ist $a_1 s_2 - a_2 s_1 = 0$. Das würde aber gerade $\xi_1 = \xi_2$ bedeuten. □

Mit der Theorie der Kettenbrüche kann man zeigen, dass sich ξ effizient bestimmen lässt, wenn x und s gegeben sind. Dieser Teil des Algorithmus lässt sich wieder auf einem klassischen Computer erledigen. (Siehe gegebenenfalls Wikipedia[31], Wikipedia (Englisch)[32], [Bs] Kap. 5, §3, aber im Vortrag wird dafür wohl keine Zeit bleiben.)

Das Lemma können wir folgendermaßen anwenden: Sei c eine zu r teilerfremde Zahl zwischen 1 und r. Wegen der Teilerfremdheit können wir r bestimmen, sobald wir die rationale Zahl $\frac{c}{r}$ kennen. Wenn $y \in \{0, 1, \ldots, Q-1\}$ so beschaffen ist, dass $\frac{y}{Q}$ nahe an $\frac{c}{r}$ liegt, und zwar so dass $|\frac{y}{Q} - \frac{c}{r}| < \frac{1}{2N^2}$ gilt, dann folgt aus dem Lemma

[31] `https://de.wikipedia.org/wiki/Kettenbruch`
[32] `https://en.wikipedia.org/wiki/Continued_fraction`

(mit $x := \frac{y}{Q}$, $s := N$), dass $\xi := \frac{c}{r}$ die *eindeutig bestimmte* rationale Zahl mit Nenner $\leq N$ ist, die diese Abschätzung erfüllt. Wie oben bemerkt, kann man die Zahl $\frac{c}{r}$ in effizienter Weise aus y, Q und N bestimmen (die uns nach der Messung des Quantencomputer-Zustands alle bekannt sind).

Wir würden also (wenn wir einen Quantencomputer gebaut hätten) so vorgehen: Wir führen die obige Prozedur durch und messen y. Wir nähern y möglichst gut durch eine Bruchzahl mit kleinstem Nenner $r \leq N$ an und überprüfen dann, ob r tatsächlich die Ordnung des betrachteten Elements a ist. Wenn ja, ist Schritt 2 von Shors Algorithmus abgeschlossen. Wenn nein, starten wir einen erneuten Durchlauf des Quantencomputers. (In der Praxis ist es sinnvoll, eventuell noch kleine Vielfache von r daraufhin zu untersuchen, ob sie gleich $\mathrm{ord}(a)$ sind.)

Die verbleibende Frage ist, mit welcher Wahrscheinlichkeit man damit rechnen kann, ein Paar (y, z) zu messen, dessen erster Eintrag y die obige Bedingung erfüllt und folglich das gesuchte r liefert. Wir werden dafür zeigen, dass die Wahrscheinlichkeit, einen Eintrag (y, z) zu messen, so dass

$$\left|\frac{y}{Q} - \frac{c}{r}\right| < \frac{1}{2Q} \quad \text{für ein zu } r \text{ teilerfremdes } c \in \{1, \ldots, r\}$$

gilt, größer als (ungefähr) $1/(6\ln(\ln(N)))$ ist. (Weil nach Wahl von Q gilt, dass $N^2 \leq Q$ ist, erfüllen diese y die obige Bedingung.)

Der Wert $1/(6\ln(\ln(N)))$ erscheint auf den ersten Blick vielleicht zu klein, um nützlich zu sein. Aber da die Funktion $x \mapsto \ln(\ln(x))$ extrem langsam wächst, kann man damit trotzdem arbeiten. Man wird zwar damit rechnen müssen, den Algorithmus mehrfach durchführen zu müssen, aber wenn die Dauer der einzelnen Durchläufe im Sekunden- oder Minutenbereich ist, hat man trotzdem etwas gewonnen (sogar dann noch, wenn jeder Durchlauf wenige Stunden dauert ...). Dazu eine Überschlagsrechnung: Ist N ungefähr von der Größe 10^{1000} (also 1000 Stellen), so ist $\ln(\ln(N))$ etwas kleiner als 8, die Erfolgswahrscheinlichkeit ist also etwas besser als $\frac{1}{50}$. Mit 230 Versuchen hätte man damit schon eine Erfolgswahrscheinlichkeit von über 99%. Mit klassischen Computern würden die besten bekannten Methoden in schwierigen Fällen Jahre für die Faktorisierung einer so großen Zahl benötigen. (Siehe RSA challenge[33] für einige Beispiele dazu.)

In den folgenden Abschnitten leiten wir die genannte Abschätzung her. Wir benutzen das folgende Lemma.

Lemma.

(1) Für alle $\vartheta \in \mathbb{R}$ gilt $|e^{i\vartheta} - 1| = 2|\sin(\vartheta/2)|$.

(2) Für $\vartheta \in [0, \frac{\pi}{2}]$ gilt $\frac{2}{\pi}\vartheta \leq \sin(\vartheta) \leq \vartheta$.

(3) Für $\vartheta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ gilt $\frac{4}{\pi^2}\vartheta^2 \leq \sin(\vartheta)^2 \leq \vartheta^2$.

Beweis. Teil (1) folgt aus der Beziehung zwischen Sinusfunktion und komplexer Exponentialfunktion:

$$\sin(\alpha) = \frac{1}{2i}(e^{i\alpha} - e^{-i\alpha}).$$

[33] `https://de.wikipedia.org/wiki/RSA_Factoring_Challenge`

Mit $\alpha = \vartheta/2$ bekommen wir

$$|\sin(\vartheta/2)| = \left|\frac{1}{2i}(e^{i\alpha} - e^{-i\alpha})\right| = \frac{1}{2}|e^{-i\alpha}(e^{2i\alpha} - 1)| = \frac{1}{2}|e^{i\vartheta} - 1|,$$

weil $|e^{-i\alpha}| = 1$ ist.

Teil (2) besagt, dass der Graph der Sinusfunktion im Intervall $[0, \pi/2]$ zwischen den Geraden mit Steigung $\frac{2}{\pi}$ und mit Steigung 1 liegt. Machen Sie sich das an einer Skizze klar. Welchen „Bezug“ haben diese beiden Geraden zur Sinusfunktion?

Teil (3) folgt direkt aus Teil (2), weil $\sin(-x) = -\sin(x)$ für alle $x \in \mathbb{R}$ gilt. □

Nun formen wir den Ausdruck, den wir für die einzelnen Wahrscheinlichkeiten $\Pr(y, z)$ erhalten haben, etwas weiter um. Mit der endlichen geometrischen Reihe und Teil (1) des Lemmas erhalten wir (wegen $\omega = e^{2\pi i/Q}$):

$$\Pr(y, z) = \frac{1}{Q^2}\left|\sum_{b=0}^{m-1}(\omega^{ry})^b\right|^2 = \frac{1}{Q^2}\frac{|\omega^{mry} - 1|^2}{|\omega^{ry} - 1|^2} = \frac{1}{Q^2}\frac{\sin(m\frac{ry}{Q}\pi)^2}{\sin(\frac{ry}{Q}\pi)^2}.$$

Die Funktion $x \mapsto \sin(x\pi)^2$ ist periodisch mit Periode 1, bei der Zahl $\frac{ry}{Q}$ im letzten Ausdruck kommt es also nur auf den gebrochenen Anteil an. Wir schreiben $\left\{\frac{ry}{Q}\right\}$ für die eindeutig bestimmte Zahl im Intervall $(-\frac{1}{2}, \frac{1}{2}]$, für die $\frac{ry}{Q} - \left\{\frac{ry}{Q}\right\} \in \mathbb{Z}$ gilt. Es gilt dann also

$$\Pr(y, z) = \frac{1}{Q^2}\frac{\sin(m\left\{\frac{ry}{Q}\right\}\pi)^2}{\sin(\left\{\frac{ry}{Q}\right\}\pi)^2}.$$

Für die folgende Rechnung tun wir so, als ob $m = \frac{Q}{r}$ gelten würde. Da der Unterschied zwischen diesen beiden Zahlen sehr klein ist, hat das auf die weitere Rechnung keinen signifikanten Einfluss. Wir schreiben jeweils $\approx$, wenn diese Ersetzung vorgenommen wird, nehmen aber an, dass die entsprechenden Abschätzungen auch danach noch gelten.

Für $\left|\left\{\frac{ry}{Q}\right\}\right| \leq \frac{1}{2m} \approx \frac{r}{2Q}$ erhalten wir mit Teil (3) des Lemmas:

$$\Pr(y, z) \geq \frac{4m^2}{\pi^2 Q^2} \approx \frac{4}{\pi^2 r^2}.$$

(Dies ist genau der Fall, dass in der Summe $\sum_{b=0}^{m-1}(\omega^r)^{by}$ alle Punkte ω^{rby} auf (höchstens) einem Halbkreis des Einheitskreises konzentriert sind.)

Jetzt können wir zusammenfassen: Sei $\varphi(r)$ die Anzahl der zu r teilerfremden Zahlen zwischen 1 und r. (Man nennt φ die Eulersche φ-Funktion[34].) Für jede solche Zahl c existiert (warum?) ein (eindeutig bestimmtes) $y \in \{0, \ldots, Q-1\}$ mit $|\frac{y}{Q} - \frac{c}{r}| \leq \frac{1}{2Q}$. Für dieses y gilt $\left\{\frac{ry}{Q}\right\} \leq \frac{r}{2Q} \approx \frac{1}{2m}$ und damit $\Pr(y, z) \geq \frac{4}{\pi^2 r^2}$ für jedes z von der Form a^x. Es gibt genau r solche Werte für z, die Wahrscheinlichkeit, dieses y

[34] `https://en.wikipedia.org/wiki/Euler%27s_totient_function`

(mit irgendeinem z im zweiten Eintrag) zu messen ist folglich $\geq \frac{4}{\pi^2 r}$. Da es $\varphi(r)$ Möglichkeiten für c gibt, sehen wir, dass wir mit Wahrscheinlichkeit

$$\geq \frac{4}{\pi^2} \cdot \frac{\varphi(r)}{r}$$

ein y messen, „mit dem wir arbeiten können“, d.h. aus dem wir in der oben beschriebenen Weise r bestimmen können.

Ein Satz aus der Zahlentheorie (der allerdings nicht leicht zu beweisen ist – er folgt aus dem *Primzahlsatz* über die Verteilung der Primzahlen) sagt, dass

$$\liminf_{r\to\infty} \frac{\varphi(r)}{r} \cdot \ln(\ln(r)) = e^{-\gamma} \approx 0,56$$

gilt. (Hier ist γ die sogenannte Eulersche γ-Konstante.)

Wenn wir $\frac{4}{\pi^2} \geq \frac{1}{3}$ und mit dem gerade genannten Resultat $\frac{\varphi(r)}{r}$ gegen $\frac{1}{2\ln(\ln(r))}$ (für genügend große r) abschätzen, bekommen wir das gewünschte Ergebnis.

Weitere Quellen: [Ak], [Sch], Wikipedia: Quantencomputer[35], Algorithmus von Shor[36] (die englischen Seiten sind noch ausführlicher).

Literaturverzeichnis

Auf die verlinkten Bücher sollten Sie kostenfrei über Ihren Uni-Account zugreifen können. Sie müssen sich dazu auf der Springer-Seite einloggen (klicken Sie *Login* auf der Springer-Seite und wählen Sie den Login über die Institution, d.h. die Universität Duisburg-Essen). Bitte melden Sie sich gegebenenfalls, wenn Sie Probleme haben, die Literatur, die Sie benötigen, zu beschaffen.

Die Bücher, zu denen kein Link angegeben ist, finden Sie (wenigstens die relevanten Teile) auf der Moodle-Seite. *Diese Dokumente sind nur für den Gebrauch für dieses Seminar bestimmt. Sie dürfen die Dateien nicht an andere weitergeben.*

[Ak] B. Aktas, *Quantum computing und Shor-Algorithms*, Bachelos-Arbeit Univ. Ulm, 2019
https://oparu.uni-ulm.de/xmlui/handle/123456789/26053

[Bo] S. Bosch, *Algebra*, Springer 2009.
https://doi.org/10.1007/978-3-540-92812-6

[Bu] J. Buchmann, *Einführung in die Kryptographie*, 5. Aufl., Springer 2010,
https://doi.org/10.1007/978-3-642-11186-0

[Bs] P. Bundschuh, *Einführung in die Zahlentheorie*, 6. Aufl., Springer 2008.
https://doi.org/10.1007/978-3-540-76491-5

[Fo] O. Forster, *Analysis 1*, 12. Aufl. (oder eine andere Auflage), Springer Spektrum, 2016
https://doi.org/10.1007/978-3-658-11545-6

[Gö1] U. Görtz, *Lineare Algebra 1*, Vorlesungsskript WS 2020/21,
https://math.ug/la1-ws2021/

[Gö2] U. Görtz, *Lineare Algebra 2*, Vorlesungsskript SS 2021,
https://math.ug/la2-ss21/

[Ha] T. Hales, *The NSA Back Door to NIST*, Notices of the A.M.S. **61**, No. 2 (2014), 190–192.
https://www.ams.org/notices/201402/rnoti-p190.pdf

[Lu] M. Luby, *Pseudorandomness and Cryptographic Applications*, Princeton University Press 1996.

[35] https://de.wikipedia.org/wiki/Quantencomputer

[36] https://de.wikipedia.org/wiki/Shor-Algorithmus

[Sch] W. Scherer, *Mathematik der Quanteninformatik*, Springer 2016
https://doi.org/10.1007/978-3-662-49080-8
[Sh] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, https://arxiv.org/pdf/quant-ph/9508027v2.pdf
[ST] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., 2nd ed., Springer 2015.
https://doi.org/10.1007/978-3-319-18588-0
[Wa] L. Washington, *Elliptic Curves*, 2nd ed., CRC Press 2008.
[We] A. Werner, *Elliptische Kurven in der Kryptographie*, Springer 2002.

Bemerkungen. Die Vorträge 10 (Faktorisieren mit elliptischen Kurven) und 14 (Algorithmus von Shor) sind im Vergleich recht schwierig (und umfangreich). Die Vorträge 11 und 12 sind relativ kurz; insbesondere in Vortrag 12 ist „nicht so viel Mathematik enthalten“.