DIPLOMARBEIT

Kryptographie mittels elliptischer Kurven im Mathematikunterricht

ausgeführt am Institut für

Diskrete Mathematik und Geometrie

der Technischen Universität Wien

unter der Anleitung von

Univ.Prof. Dr.phil. Dietmar Dorninger

durch

JOHANNES HASIBEDER

Costagasse 9/16

1150 Wien

Wien, am 19. März 2010

Danksagungen

Ich möchte an dieser Stelle meiner Familie für die Geduld und ihr Vertrauen danken. Es ist eine große Unterstützung, zu wissen, dass man sich während der Ausbildung auf diesen starken Rückhalt verlassen kann. Dank gebührt im speziellen meinen Eltern *Otto* und *Maria Hasibeder*, die mir Selbstvertrauen und Eigenständigkeit mitgegeben und mir damit (nicht zuletzt auch finanziell) dieses Studium ermöglicht haben. Danke auch meinen Geschwistern *Magdalena* und *Georg* für ihre herausfordernde und direkte Art, die ein herzlicher aber auch kritischer Begleiter war.

Herzlichen Dank an meine Studienkollegen, mit denen gemeinsames Lernen oft motivierend gewirkt und natürlich auch Spaß gemacht hat. Konkret möchte ich mich bei meinem Kollegen *Paul Kircher* bedanken, mit dem ich die Schwierigkeiten des (Mathematik-)Studiums gemeinsam meistern konnte.

Herrn *Univ. Prof. Dr. Phil. Dietmar Dorninger* danke ich für die sehr detaillierte Auseinandersetzung mit dieser Arbeit und für die schnelle und unkomplizierte Hilfe bei der Umsetzung meiner Ideen.

Johannes Hasibeder

Inhaltsverzeichnis

Danksagungen **iii**

Inhaltsverzeichnis **vii**

Einleitung **1**

1 Mathematische Grundlagen - Lehrerteil **3**

1.1 Grundlagen . . . 3

1.1.1 Kongruenzen auf $\mathbb{Z}$ . . . 3

1.1.2 Quadratische Reste . . . 4

1.1.3 Das Problem des diskreten Logarithmus . . . 5

1.1.4 Einwegfunktionen . . . 6

1.2 Kryptographische Verfahren . . . 6

1.2.1 Einführung . . . 6

1.2.2 Codierung . . . 7

1.2.3 Symmetrische - asymmetrische Chiffrierverfahren . . . 7

1.2.4 Das ElGamal- System . . . 9

1.3 Elliptische Kurven . . . 9

1.3.1 Warum verwenden wir Elliptische Kurven? . . . 9

1.3.2 Wie wird eine Elliptische Kurve über einem Körper K zu einer (abelschen) Gruppe? . . . 10

1.3.3 Punktaddition im Fall $K = \mathbb{R}$: . . . 12

1.3.4 Multiplikation mit einem Skalar . . . 14

1.4 Elliptische Kurven über einem endlichen Körper . . . 14

1.4.1 Anzahl der Elemente von E . . . 15

1.5 Elliptische Kurven in der Kryptographie . . . 16

1.5.1 Diffie Hellman- Schlüsselaustausch mittels elliptischer Kurven 16
1.5.2 ElGamal- Verschlüsselung mittels elliptischer Kurven 16
1.5.3 Vor- und Nachteile der EC-Verschlüsselung 17
1.5.4 Sicherheit 18

2 Schülerteil **19**

2.1 Vorüberlegungen 19
2.2 Vorraussetzung: Rechnen in Restklassen 21
2.2.1 Rechnen in $\mathbb{Z}_m$ 22
2.2.2 Zusammenfassung wichtiger Rechenregeln 23
2.2.3 Inverse berechnen 24
2.3 Der Gruppenbegriff 24
2.3.1 Operationen 25
2.3.2 Das Kommutativgesetz 25
2.3.3 Das Assoziativitätsgesetz 26
2.3.4 Das neutrale Element 27
2.3.5 Das inverse Element 27
2.3.6 Die Gruppe 27
2.3.7 Der Körper 28
2.4 ElGamal über endlichen Körpern 28
2.5 Geometrie 30
2.5.1 Einschub: Kurvendiskussion 32
2.6 Operationen auf der elliptischen Kurve 36
2.6.1 Die Addition 36
2.6.2 Eine Multiplikation 39
2.6.3 Zusammenfassung zu einer Formel 41
2.6.4 Übungsbeispiele 41
2.7 Elliptische Kurven über $\mathbb{Z}_p$ 46
2.7.1 Grundsätzliches 46
2.7.2 Rechnen mit Punkten einer Elliptischen Kurve E 48
2.7.3 Einsatz von Derive 50
2.8 ElGamal über Elliptischen Kurven 55
2.8.1 Codierung 56

2.8.2 Ein ausführliches Beispiel 57

Abbildungsverzeichnis **61**

Literatur **63**

Erklärung **65**

Einleitung

Diese Arbeit hat zum Ziel, elliptische Kurven für den Schulunterricht aufzubereiten. Sie ist in zwei große Kapitel gegliedert, einen Lehrerteil und einen Schülerteil.

Im *Lehrerteil* sind die mathematischen Grundlagen zu dem Thema zusammengestellt; es werden in mathematischer Strenge und ohne didaktische Umsetzung in den Schulunterricht die wichtigsten Sachverhalte beschrieben. Der Lehrer soll vor allem die Möglichkeit haben, eventuell auftretende Fragen der Schüler exakt beantworten und sich kurzfristig mit dem Thema auseinandersetzen zu können. Fachlich orientiert sich dieses Kapitel an [1].

Im *Schülerteil* wird versucht, Chiffrierverfahren mittels elliptischer Kurven für Schüler aufzubereiten. Das Anspruchsniveau erstreckt sich dabei von pädagogisch- didaktischen Anforderungen an Lehrer bis hin zur konkreten Vermittlung des Stoffs in verschiedenen Schulstufen.

Diese Arbeit ist zum Einen für engagierte Lehrer gedacht, die Freude daran haben, über den Tellerrand des Regelunterrichts hinauszublicken; zum Anderen für Schüler der siebenten oder achten Klasse (11. oder 12. Schulstufe), die ein selbstständiges, gewolltes Interesse im Fach Mathematik an den Tag legen. Die Idee dabei ist, Material für vertiefenden Unterricht bereitzustellen, in dem zwar abstrakte mathematische Anforderungen gestellt werden, welches aber auch einen konkreten Realitätsbezug hat. Die Unterlagen eignen sich zum Beispiel für eine Sequenz in einer zusätzlichen Mathematikförderstunde für sehr motivierte Schüler. Weiters bietet sie Stoff für eine Fachbereichsarbeit bei der Matura.

Bei der elliptischen Kurven- Methode handelt es sich um eine der modernsten Arten, Daten zu verschlüsseln. Die Forschung im Bereich der elliptischen Kurven wird seit ca. 150 Jahren betrieben. Seit ungefähr 1985 ist bekannt, dass das elliptische Kurvenproblem für die Kryptographie genutzt werden kann. Es wurde bis heute keine bemerkenswerte Schwachstelle entdeckt.

Das Verfahren wird zurzeit von Institutionen eingesetzt, die hohe Sicherheitsanforderungen stellen, wie zum Beispiel Banken. Die Sicherheit ist jedoch nur ein Aspekt, warum dieser Algorithmus bevorzugt verwendet wird. Ein weiterer großer Vorteil ist die Kürze der verwen-

deten Schlüssel. Diese spart eine Menge Speicherplatz und Datentransfer und macht somit den Einsatz in mobilen Geräten wie z.B. Handys oder Smartphones möglich und wirtschaftlich. Das drückt sich in folgenden Zahlen aus: Um die gleiche Sicherheit wie bei dem (mittlerweile etwas veralteten) RSA-Algorithmus mit 2048 Bit Schlüssellänge zu erhalten, braucht man bei Elliptic-Curves-Cryptography (ECC) nur einen 210 Bit Schlüssel. Die Gesamtmenge der zu übermittelnden Daten bei einer Nachricht von 100 Bit beträgt bei RSA 1024 Bit und bei ECC 321 Bit . In Summe gilt ECC etwa um den Faktor 10 schneller als RSA (siehe [4]).

Durch die Allgegenwärtigkeit der Übermittlung und Verschlüsselung von Daten liegt es nahe, sich mit diesem Thema im Schulunterricht zu befassen.

Kapitel 1

Mathematische Grundlagen - Lehrerteil

1.1 Grundlagen

1.1.1 Kongruenzen auf $\mathbb{Z}$

Definition: $a, b \in \mathbb{Z}, m \in \mathbb{N}^* := \mathbb{N}\{0\}$
a ist kongruent zu b mod m ($a \equiv b \bmod m$) $\Leftrightarrow m|a-b$

Satz: $a, b \in \mathbb{Z}$, Kongruenz $ax \equiv b \bmod m$ ist lösbar $\Leftrightarrow \text{ggT}(a,m)|b$. Es gibt dann $\text{ggT}(a,m)$ inkongruente Lösungen mod m.

Beweis: Sei $d :=\text{ggT}(a,m)$.
„$\Rightarrow$“: Ist $u \in \mathbb{Z}$ Lösung von $ax \equiv b \bmod m$, so $\exists v \in \mathbb{Z} : au + vm = b$, woraus $d|b$ folgt.
„$\Leftarrow$“: Sei nun umgekehrt $d|b$ erfüllt und $d = ra + sm$ mit $r, s \in \mathbb{Z}$, dann gilt:

$$ra + sm = d \Rightarrow r\frac{b}{d}a + s\frac{b}{d}m = b \Rightarrow \frac{rb}{d} = a \equiv b \bmod m \Rightarrow x = \frac{rb}{d}$$

Definition: Die *Eulersche φ- Funktion* $\varphi(m)$ gibt die Anzahl aller ganzen a mit $1 \leq a \leq m$ an, für die gilt: $\text{ggT}(a,m) = 1$. Ist m prim, dann ist $\varphi(m) = m - 1$

Definition: sei $a \in \mathbb{Z}$, $\text{ggt}(a,m) = 1$
Die *Ordnung* von a mod m ($\text{ord}_m(a)$) ist das kleinste Element $e \in \mathbb{N}^*$ mit $a^e \equiv 1 \bmod m$.

Definition: Die Restklassen mod m bilden bezüglich der Operationen + und $\cdot$ einen kommutativen Ring $\mathbb{Z}_m$ mit Einselement. (Seien $\overline{a}$ und $\overline{b}$ die Klassen von a bzw. b mod m, so ist

$\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a}.\overline{b} = \overline{a.b}$ wohldefiniert.
Für $ord_m(a) = \varphi(m)$ heißt *a Primitivwurzel* und die Gruppe der primen Restklasse $\mathbb{Z}_m^*$ ist zyklisch.
Der Restklassenring $\mathbb{Z}_m$ ist genau dann ein Körper, wenn m eine Primzahl ist. Allgemein gilt:

Satz: Die Ordnung jedes endlichen Körpers ist eine Primzahlpotenz p^n (p prim, $n \in \mathbb{N}^*$), und umgekehrt gibt es zu jeder Primzahlpotenz p^n bis auf Isomorphie genau einen Körper mit p^n Elementen, das Galoisfeld GF(p^n).
Dabei heißen zwei algebraische Strukturen A und B isomorph, in Zeichen A $\cong$ B, wenn es einen bijektiven Homomorphismus von A auf B gibt, und f heißt Homomorphismus von A in B, falls für alle n-stelligen Operationen $\circ$ von A gilt $f(\circ(a_1, ..., a_n)) = \circ(f(a_1, ..., a_n))$ für alle $(a_1, ..., a_n) \in A^n$ (Die Operationen in B haben wir hier gleich bezeichnet wie in A).

1.1.2 Quadratische Reste

Definition: Für jede ungerade Primzahl p und jede nicht durch p teilbare ganze Zahl a ist das Legendresymbol $(\frac{a}{p})$ definiert durch

$$(\frac{a}{p}) = \begin{cases} +1 & \text{wenn } x^2 \equiv a \bmod p \text{ lösbar ist} \\ -1 & \text{wenn } x^2 \equiv a \bmod p \text{ unlösbar ist} \end{cases}$$

Im ersten Fall sagt man auch „a ist quadratischer Rest mod p“, im zweiten „a ist quadratischer Nichtrest mod p.“Ferner sei $(\frac{a}{p}) = 0$, falls $p|a$.

Im folgenden Satz sind einige wichtige Eigenschaften des Legendresymbols zusammengefaßt, welche fast unmittelbar aus dessen Definition, sowie der Existenz einer Primitivwurzel mod p folgen.
Die Menge der Primzahlen bezeichnen wir mit **P**:

Satz: Seien $p \in \mathbf{P}\backslash\{2\}$ und $a, b \in \mathbb{Z}$ beliebig. Dann gilt:

1. $a \equiv b \bmod p \Rightarrow (\frac{a}{b}) = (\frac{b}{p})$
2. Ist g eine Primitivwurzel mod p, so sind genau die Zahlen $g^2, g^4, ..., g^{p-1}$ die mod p inkongruenten quadratischen Reste und die Zahlen $g, g^3, ..., g^{p-2}$ die mod p inkongruenten quadr. Nichtreste. Insbesondere gibt es gleich viele quadratische Reste wie quadratische Nichtreste, nämlich je $\frac{(p-1)}{2}$.

3. $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$ (Eulersches Kriterium).

4. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. (Insbesondere ist also $(\frac{a^2b}{p}) = (\frac{b}{p})$.

Ist $(\frac{a}{p}) = 1$ für eine ungerade Primzahl p, so kann man sich die Frage stellen, wie man die Lösungen von $x^2 \equiv a \bmod p$ dann tatsächlich berechnen kann. Für $p \equiv 3 \bmod 4$ ist sie ganz leicht zu beantworten. Nach dem Eulerschen Kriterium gilt nämlich

$$a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) = 1 \bmod p$$

und damit weiter

$$(a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a \equiv a \bmod p$$

was beweist, dass $\pm a^{\frac{p+1}{4}}$ die beiden Wurzeln aus a mod p sind.

1.1.3 Das Problem des diskreten Logarithmus

In der Kryptographie spielt das folgende Problem eine wesentliche Rolle:
Sei $\langle G, \circ \rangle$ eine endliche Gruppe, $\alpha \in G$ und $H = \{\alpha^i | i \geq 0\}$. Dabei ist α so zu wählen, dass es praktisch unmöglich ist, a aus $\beta = \alpha^a$ zu finden, wenn β und α bekannt sind.

Die Schwierigkeit, diskrete Logarithmen in H zu berechnen, hängt dabei wesentlich davon ab, welche Darstellung für G gewählt ist. Angenommen es ist $\langle H, \circ \rangle \cong \langle \mathbb{Z}_n, + \rangle$ mit $ggT(\alpha, n) = 1$. Dann erzeugt α additiv $\mathbb{Z}_n$, und die Berechnung von β bedeutet $\underbrace{\alpha + \alpha + ... + \alpha}_{a \, Summanden} \bmod n \equiv a\alpha \bmod n$ zu berechnen. Da $ggT(\alpha, n) = 1$ hat α ein multiplikatives Inverses α^{-1}, welches leicht zu berechnen ist, und man erhält $a \equiv log_\alpha \beta = \beta\alpha^{-1} \bmod n$.

Wir betrachten folgenden Spezialfall: sei $\mathbb{Z}_p^*$ die multiplikative Gruppe des Körpers $\mathbb{Z}_p$ (also alle Elemente von $\mathbb{Z}_p$ ohne die 0; $\mathbb{Z}_p^*$ ist zyklisch). Man weiß: $\left\langle \mathbb{Z}_p^*, \cdot \right\rangle \cong \langle \mathbb{Z}_{p-1}, + \rangle$. Wir bezeichnen diesen Isomorphismus mit Φ. Kann man Φ ausnutzen, um den diskreten Logarithmus in $\mathbb{Z}_p^*$ zu berechnen?

$$\begin{aligned} \Phi(xy \bmod p) &\equiv (\Phi(x) + \Phi(y)) \bmod p - 1 \Rightarrow \\ \Phi(\alpha^a \bmod p) &\equiv a \cdot \Phi(\alpha) \bmod p - 1 \end{aligned}$$

Also folgt

$$\beta \equiv \alpha^a \bmod p \qquad \Leftrightarrow \qquad \Phi(\alpha) \equiv \Phi(\beta) \bmod p-1$$

und damit

$$a = log_\alpha \beta \equiv \Phi(\beta)(\Phi(\alpha))^{-1} \bmod p-1.$$

Die Antwort ist ja, sofern man Φ kennt. Dies ist aber für große Zahlen so gut wie unmöglich.

1.1.4 Einwegfunktionen

Definition: Eine injektive Funktion $f : X \to Y$ heißt Einwegfunktion (engl. *one-way function*), wenn

1. $\forall x \in X$ der Funktionswert $f(x)$ effizient berechenbar ist und
2. wenn es kein effizientes Verfahren gibt, um aus einem Bild $y = f(x)$ das Urbild x zu berechnen.

Die Einwegeigenschaft einer Funktion basiert wesentlich auf Aussagen über die Effizienz entwickelter Algorithmen zur Berechnung der Funktionswerte sowie deren Umkehrabbildung. Da bei den bekannten Verfahren Komplexitätsaussagen fehlen, ist es oft schwer schwer zu beweisen, dass eine Einwegfunktion vorliegt. Man begnügt sich meist mit Kandidaten, für die man die Eigenschaft zwar noch nicht formal bewiesen hat, für die es aber zur Zeit noch keine effizienten Verfahren zur Berechnung der Umkehrabbildung gibt.

1.2 Kryptographische Verfahren

1.2.1 Einführung

- Kryptographie (Chiffrierung) ist die Wissenschaft von den Methoden der Verschlüsselung von Nachrichten zum Zwecke der Geheimhaltung.
- Kryptoanalyse ist die Wissenschaft von Methoden zur unbefugten Entschlüsselung von Nachrichten zur Rückgewinnung der ursprünglichen Informationen. Ziel der Kryptoanalyse ist die Bewertung der kryptographischen Stärke eines Chiffrierverfahrens.

- Kryptographie und Kryptoanalyse werden gemeinsam als Kryptologie bezeichnet.

1.2.2 Codierung

Nachrichten werden quellencodiert über einem Eingabealphabet A, Wörter haben die Länge n ($n > 1$- Blöcke; $n = 1$- Folge von Buchstaben); das Ausgabealphabet B ist zumeist identisch mit A. Die Codierung "übersetzt" die Nachricht in die Menge von Symbolen, auf der die Verschlüsselungsfunktion definiert wird.

1.2.3 Symmetrische - asymmetrische Chiffrierverfahren

Symmetrische Chiffrierverfahren: Sender und Empfänger haben den gleichen Schlüssel zum Chiffrieren und zum Dechiffrieren. Das Problem dabei ist der Schlüsselaustausch. Gerät dieser in fremde Hände, kann der gesamte Informationsaustausch ohne Probleme mitverfolgt werden. Außerdem kann sich keiner ohne Schlüssel „von außen" in die sichere Verbindung einschalten. Die Verfahren sind sehr einfach konstruiert und die meisten daher eher unsicher. Man unterscheidet:

- Transpositionssysteme: Blockchiffren der Länge n; auf jedes Wort wird eine feste Permutation $\Pi \in S_n$ angewendet.
- Substitutionssysteme:
  - monoalphabetisch: jedes $a \in A$ wird auf die gleiche Weise ersetzt
  - polyalphabetisch: jedes a wird an verschiedenen Stellen auf verschiedene Weise ersetzt.

Beispiel für monoalphabetische Substitution: DES (Data Encryption Standard)
$A = \langle \mathbb{Z}_2^{64}, + \rangle$; $S = s \in A$, s besteht aus 56 Bits + 8 Kontrollbits
$a \in A$, Verschlüsselung von a mit dem Schlüssel s: a wird zunächst durch eine Permutation $\Pi \in S_{64}$ verändert; dann werden 16 Schleifen durchlaufen, bei denen der Permutationsblock in 2 Blöcke der Länge 32 aufgeteilt wird und diese Blöcke in Abhängigkeit von s umgeordnet werden. Abschließend wird Π^{-1} angewendet.

Öffentliche Chiffrierverfahren: Bei öffentlichen Chiffrierverfahren ist der Schlüssel zum Chiffrieren öffentlich bekannt und ungleich dem Schlüssel zum Dechiffrieren, der geheim ist. Es hat

dabei jeder Teilnehmer einen öffentlichen Schlüssel s_x und einen geheimen, privaten Schlüssel t_x, und es muss praktisch unmöglich sein, t_x aus s_x zu berechnen (Verwendung von Einwegfunktionen (siehe Kapitel 1.1.4).

Vorteile der öffentlichen Chiffrierverfahren:

- Kein Schlüsselaustausch notwendig.
- Jeder kann in das System einsteigen.

Der Nachteil ist die deutlich geringere Geschwindigkeit der Ver- und Entschlüsselung gegenüber symmetrischen Verfahren.

Beispiel: Diffie - Hellman Schlüsselaustausch
Will Teilnehmer A mit Teilnehmer B verschlüsselt mittels eines symmetrischen Verfahrens (z.B. DES) kommunizieren, müssen sie vorher den Schlüssel austauschen.

Jeder Teilnehmer X wählt zufällig ein t_x aus dem Galoisfeld GF(q) mit $2 \leq t_x \leq q-2$ und bildet in GF(q): $s_x = \alpha^{t_x}$, wo α ein primitives Element von GF(q) ist. s_x ist öffentlich, t_x geheim. Der gemeinsame Schlüssel von zwei Teilnehmern X und Y, der nirgends aufscheint, ist dann $s_{xy} = \alpha^{t_x t_y} = s_x^{t_y} = s_y^{t_x}$. Will X an Y eine Nachricht senden, so sucht X aus dem öffentlichen Verzeichnis s_y und bildet $s_y^{t_x} = s_{xy}$.

Beispiel

- GF(41)$\cong \mathbb{Z}_{41}$
- $\alpha = 6, \alpha$ ist primitives Element von $\mathbb{Z}_{41}$
- $t_x = 15$, der öffentliche Schlüssel von X ist also $6^{15} \bmod 41 = 3$
- $t_y = 31$, der öffentliche Schlüssel von Y ist $6^{31} \bmod 41 = 13$

Damit ergibt sich als gemeinsamer Schlüssel s_{xy} : $3^{31} = 13^{15} = 14 \mod 41$.
Eine 3. Person, die den Datenaustausch abfängt, steht vor dem Problem, dass sie die Gleichungen $6^a = 10$ oder $6^b = 8$ in GF(41) lösen muss, um den gemeinsamen Schlüssel zu ermitteln. Dieses Problem nennt man Diffie- Hellman- Problem, und es läuft auf das Problem des diskreten Logarithmus (siehe Kapitel 1.1.3) hinaus.

1.2.4 Das ElGamal- System

Sei $\mathbb{Z}_q^*$ (wie oben) die multiplikative Gruppe von GF(q), q prim, α primitives Element von GF(q), $f(x) = \alpha^x, \beta = \alpha^a \mod q$.

Protokoll ElGamal: Teilnehmer A:

- öffentlicher Schlüssel(q, α, β)
- geheimer Schlüssel a

B $\xrightarrow{x}$ A, Nachricht $x \in \mathbb{Z}_q^*$
B wählt zufällig ein $k \in \mathbb{Z}_{q-1}$, bildet $y_1 = \alpha^k \mod q, y_2 = x.\beta^k \mod q$
B $\xrightarrow{(y_1,y_2)}$ A

A dechiffriert: $x = y_2(y_1^a)^{-1} \mod q$, denn $y_2(y_1^a)^{-1} = x.\beta^k\alpha^{-ka} = x.\alpha^{ak}.\alpha^{-ak} = x$

B maskiert x mit β^k; Die Wahl eines zufälligen k ist erforderlich, weil für $k = 1$ aus der Kenntnis von β und p mittels $\beta.\beta^{-1} \equiv 1 \bmod p$ der Wert β^{-1} berechenbar ist und damit aus $y_2 = x\beta$ die Nachricht x erhalten werden kann!

Verallgemeinerung: Statt $\mathbb{Z}_p^*$ nimmt man eine beliebige zyklische Untergruppe H einer Gruppe $\langle G, \circ\rangle$. Erzeugendes Element von H sei α mit der Eigenschaft, dass in G $\log_\alpha \beta$ nicht berechenbar ist.

1.3 Elliptische Kurven

1.3.1 Warum verwenden wir Elliptische Kurven?

Wie weiter oben ausgeführt steht die Sicherheit mancher öffentlicher Chiffrierverfahren in unmittelbarem Zusammenhang mit der Unlösbarkeit des Problems des diskreten Logarithmus. Dieses wiederum beinhaltet das Problem der schwierigen Berechnung des Isomorphismus von $\langle H, \circ\rangle$ auf $\langle \mathbb{Z}_n, +\rangle$. Bei der Verallgemeinerung des ElGamal-Systems ist man auf der Suche nach geeigneten Gruppen. Bislang kennt man im Wesentlichen nur zwei Klassen von solchen Gruppen, nämlich:

- die multiplikativen Gruppen von Galoisfeldern GF(a)
- Gruppen von Punkten elliptischer Kurven

Wir wenden uns nun elliptischen Kurven zu:

Definition: Eine elliptische Kurve E über einem Körper K ist die Menge der Punkte $(x, y) \in K \times K$, welche eine Gleichung der Form

$$y^2 + a_4xy + a_3y = x^3 + a_2x^2 + a_1x + a$$

erfüllen, wobei das rechtsstehende Polynom keine mehrfachen Nullstellen in K besitzt, zusammen mit einem sogenannten *unendlich fernen Punkt* $\mathcal{O}$. Für char$K \neq 2, 3$ kann man durch lineare Transformation obige Gleichung reduzieren auf

$$y^2 = x^3 + ax + b$$

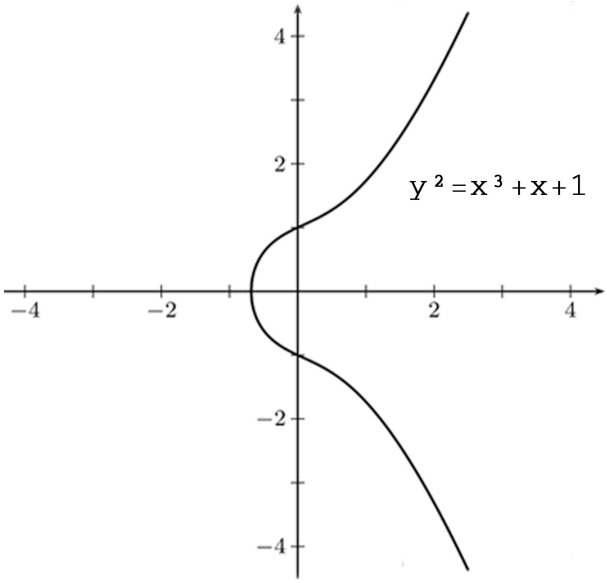
Die Abbildung auf Seite 11 zeigt mögliche Erscheinungsformen einer Elliptischen Kurve.

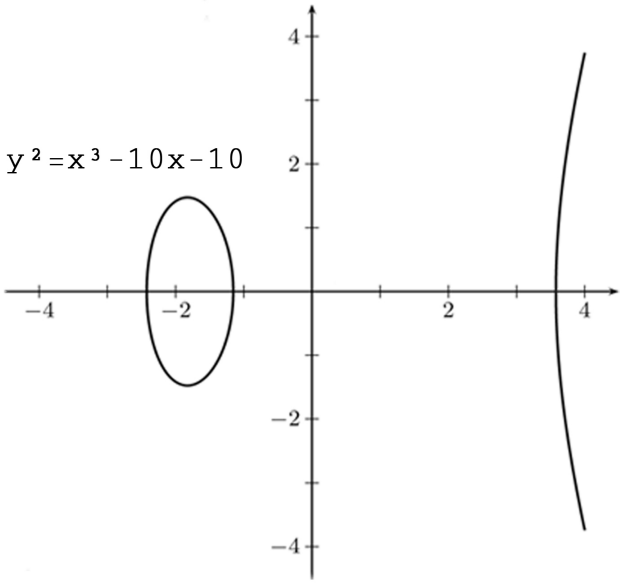
1.3.2 Wie wird eine Elliptische Kurve über einem Körper K zu einer (abelschen) Gruppe?

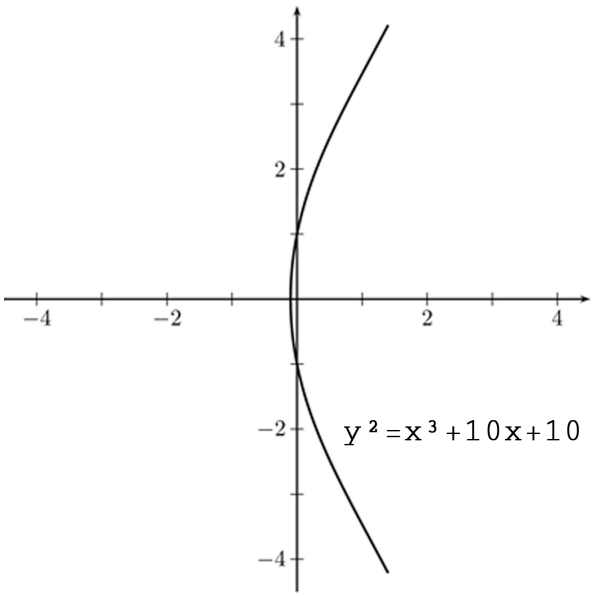
Um eine Gruppe zu bekommen, brauchen wir eine geeignete Operation. Wir definieren folgende Punktaddition:

Definition: Geg.: 2 Punkte $P = (x_1, y_1)$ und $Q(x_2, y_2) \in E$.

- Ist $x_1 = x_2$ und $y_2 = -y_1$, dann sei $P + Q = O$.
- andernfalls sei $P + Q = (x_3, y_3)$ mit $x_3 = \lambda^2 - x_1 - x_2$ und $y_3 = \lambda(x_1 - x_3) - y_1$, wobei
  $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ für $P \neq Q$ bzw.
  $\lambda = \frac{3x_1^2 + a}{2y_1}$ für $P = Q$
- Weiters sei $P + O = O + P = P, \quad \forall P \in E$

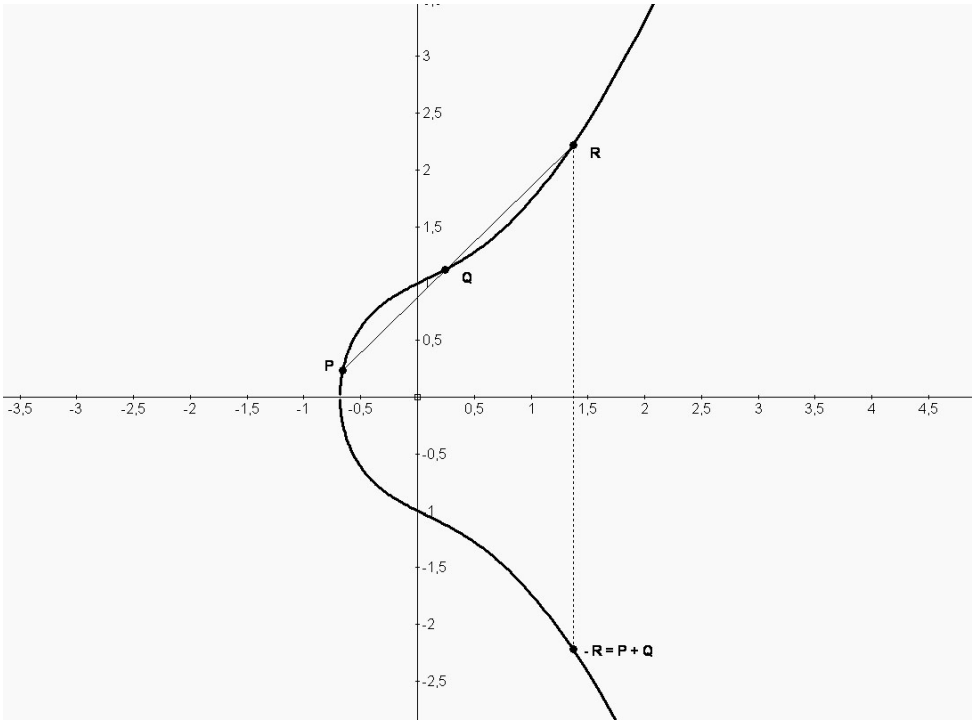






Es ist etwas aufwändig, nachzuprüfen, dass tatsächlich eine Gruppe vorliegt. Das neutrale Element und das Inverse sind mitdefiniert. Der Nachweis der Assoziativität würde den Rahmen dieser Arbeit sprengen.

1.3.3 Punktaddition im Fall $K = \mathbb{R}$:



Wir werden nachweisen: Im Fall $K = \mathbb{R}$ erhält man $P + Q$ auf geometrischem Weg, indem man die Gerade durch P und Q mit der Kurve schneidet und den gewonnenen Schnittpunkt an der x-Achse spiegelt. Das rechnen wir jetzt und motivieren auf diese Weise die allgemeine Definition der Addition.
Die Gerade durch P und Q kat die Steigung

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

und sieht somit wie folgt aus:

$$\begin{aligned} (x_2 - x_1)\lambda &= y_2 - y_1 \\ \Rightarrow y &= (x - x_1)\lambda + y_1 \end{aligned}$$

Diese Gerade durch P und Q schneiden wir jetzt mit der Kurve E:

$$\begin{aligned}(y_1 + (x - x_1)\lambda)^2 &= x^3 + ax + b \\ y_1^2 + 2y_1\lambda(x - x_1) + \lambda^2(x^2 - 2xx_1 + x_1) &= x^3 + ax + b\end{aligned}$$

Nach dem Satz von Vieta gilt:

$$\begin{aligned}-\lambda^2 &= -(x_1 + x_2 + x_3) \\ \Rightarrow x_3 &= \lambda^2 - x_1 - x_2 \\ \Rightarrow x_3 &= (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2\end{aligned}$$

Durch Einsetzen von x_3 in die Geradengleichung lässt sich y_3 ausrechnen. Dieses muss dann mit negativem Vorzeichen versehen werden (Spiegelung des Punktes um die x-Achse)!
Wenn $P = Q$ wird die Gerade durch P und Q zu einer Tangente mit Steigung λ. Um λ zu berechnen, müssen wir die partiellen Ableitungen der Gleichung

$$\Phi(x, y) = y^2 - x^3 - ax - b = 0$$

nach x und nach y ausrechnen.

$$\frac{\delta\Phi}{\delta x} = -3x^2 - a \qquad \frac{\delta\Phi}{\delta x} = 2y$$

Die Tangente hat nun folgende Steigung

$$\frac{\delta y}{\delta x} = -\frac{\frac{\delta\Phi}{\delta x}}{\frac{\delta\Phi}{\delta y}} = \frac{3x_1^2 + a}{2y_1} =: \lambda$$

und diese Formel:

$$y = y_1 + \lambda.(x - x_1)$$

Um die Tangente mit der Ellipse zu schneiden, setzen wir in die Ellipsengleichung ein:

$$\begin{aligned}(y_1 + \lambda(x - x_1))^2 &= x^3 + ax + b \\ S.v.Vieta \Rightarrow -\lambda^2 &= -(x_1 + x_2 + x_3)\end{aligned}$$

und wegen $x_1 = x_2$

$$\Rightarrow \lambda^2 = 2x_1 + x_3$$

$$\begin{aligned} \Rightarrow x_3 &= \lambda^2 - 2x_1 \\ y_3 &= y_1 + \lambda.(x_3 - x_1) \end{aligned}$$

1.3.4 Multiplikation mit einem Skalar

Wir wissen also jetzt, wie $P + P =: 2P$ zu berechnen sind. Wie bekommen wir $23P$?

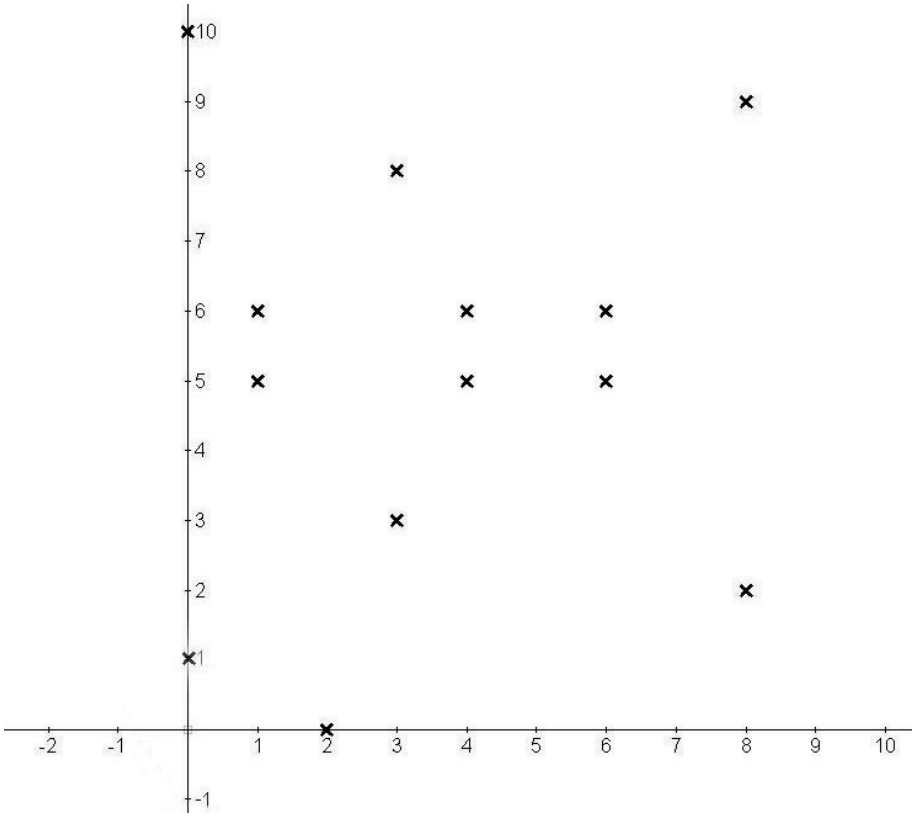
$$23P = P + 2(11P) = P + 2(P + 2(5P)) = P + 2(P + 2(P + 2(2P)))$$

1.4 Elliptische Kurven über einem endlichen Körper

Wir beschränken uns auf $K = \mathbb{Z}_p$, p prim, sowie $p \geq 4$. Eine hinreichende Bedingung dafür, dass $x^3 + ax + b$ keine mehrfachen Nullstellen in $\mathbb{Z}_p$ besitzt, ist $4a^3 + 27b^2 \neq 0$ mod p, was wir stets voraussetzen wollen.
Gegeben sei die elliptische Kurve $y^2 = x^3 + x + 1$ über $\mathbb{Z}_{11}$. Um die Punkte der Kurve zu berechnen, lassen wir x $\mathbb{Z}_{11}$ durchlaufen. Sei $z := x^3 + x + 1$. Wir bestimmen die quadratischen Reste und berechnen dann y aus $y^2 \equiv z$ mod 11 (aus $11 \equiv -1 \bmod 4 \Rightarrow y = \pm z^{\frac{p+1}{4}} \equiv z^3$ mod 11, siehe Kapitel 1.1.2)

x	0	1	2	3	4	5	6	7	8	9	10
$\frac{z}{11}$	1	1	0	1	1	-1	1	-1	1	-1	-1
y	1	5	0	3	5		5		2		
	10	6	0	8	6		6		9		

Die Punkte der Kurve sind dann:



Beispiel: Berechnung der Punkte mit der x-Koordinate 3 auf der Kurve $y^2 = x^3 + x + 1$:

$$\begin{aligned} y^2 &\equiv 3^3 + 3 + 1 \mod 11 \\ y^2 &\equiv 31 \equiv 9 \mod 11 \\ y &\equiv \pm 3 \mod 11 \\ y_1 &= 3 \\ y_2 &= -3 \equiv 8 \mod 11 \end{aligned}$$

1.4.1 Anzahl der Elemente von E

Gegeben sei die elliptische Kurve E über $\mathbb{Z}_p$. Die Anzahl ihrer Elemente ist abzuschätzbar durch

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$$

1.5 Elliptische Kurven in der Kryptographie

1.5.1 Diffie Hellman- Schlüsselaustausch mittels elliptischer Kurven

Nun nehmen wir beim Diffie-Hellman Schlüsselaustausch statt der Gruppe GF(α)* eine zyklische Untergruppe H einer elliptische Kurve $\langle E, + \rangle$
Allgemein bekannt seien:

- die elliptische Kurve E über dem Körper K und ein erzeugendes Element P der zyklischen Untergruppe H von E
- *wir wählen als Beispiel* $y^2 = x^3 + x + 1$ über $\mathbb{Z}_{11}$ und $P = (1, 5)$

Teilnehmer X wählt z.B. $t_x = 5$ (das ist kleiner als $|E|$) und berechnet damit seinen öffentlichen Schlüssel $s_x := P.5 = (4, 6)$. Diesen schickt er an Teilnehmer Y.

Y wählt auch seinen privaten Schlüssel $t_y = 7 (\leq |E|)$, berechnet $s_y = P.7$ und schickt diesen an Teilnehmer X.

Beide berechnen jetzt mithilfe des öffentlichen Schlüssels des Gegenübers sowie mit den jeweiligen privaten Schlüsseln den gemeinsamen Schlüssel $s_y.t_x = s_x.t_y = t_x.t_y.P$, ohne dass die privaten Schlüssel ausgetauscht wurden.

1.5.2 ElGamal- Verschlüsselung mittels elliptischer Kurven

Statt der Gruppe $(\mathbb{Z}_p, .)$ nehmen wir nun wieder eine zyklische Untergruppe H einer additiven Gruppe E (Schreibweise: die Großbuchstaben stellen Punkte der Kurve, die Kleinbuchstaben Skalare dar). Allgemein bekannt seien:

- E: $y^2 = x^3 + u.x + v$ über $\mathbb{Z}_p$ mit einem
- $P \in E$ (welcher die zyklische Untergruppe H erzeugt)

1. Teilnehmer A wählt ein zufälliges $a \in (1, ..., p-1)$ und bildet damit $Q = P.a$. Dieses Q gibt er nun als seinen öffentlichen Schlüssel bekannt, während a als sein privater Schlüssel geheim bleibt.

   öffentlicher Schlüssel von Teilnehmer A: (p, P, Q)

2. Teilnehmer B will an A nun die Nachricht X schicken (die Nachricht wird codiert und ist somit auch ein Punkt der Kurve).

   Er wählt dazu ein beliebiges zufälliges $b \in (1, ..., p-1)$ und berechnet daraus $Y_1 = P.b$ und $Y_2 = X + Q.b \ \ (= X + P.a.b)$

   (Y_1, Y_2) bilden das Chiffrat, das er an A schickt.

3. Um die Nachricht zu entschlüsseln bildet A $S := a.Y_1 = a.P.b$ und das Inverse davon ($S^{-1} = -a.P.b$). Die Nachricht erhält A nun mit $Y_2 + S^{-1}$.

1.5.3 Vor- und Nachteile der EC-Verschlüsselung

Der Nachteil liegt in der Länge der verschlüsselten Nachricht. Diese ist doppelt so lang wie die ursprüngliche. Außerdem können Probleme bei der Wahl der Kurve auftauchen, weil nicht alle Kurven zum Verschlüsseln geeignet sind.

Der Vorteil beim Einsatz in Kryptosystemen mit elliptischen Kurven liegt in der schnellen Verschlüsselung und der größeren Flexibilität. Ohne Abstriche hinsichtlich der Sicherheit in Kauf zu nehmen, kommt man mit deutlich geringeren Parameterlängen aus. (siehe Abbildung 1.1).Dies wirkt sich besonders beim Einsatz in Situationen aus, wo Speicher- oder Rechenkapazität knapp sind, wie z.B. bei Smartcards und anderen Small Devices.

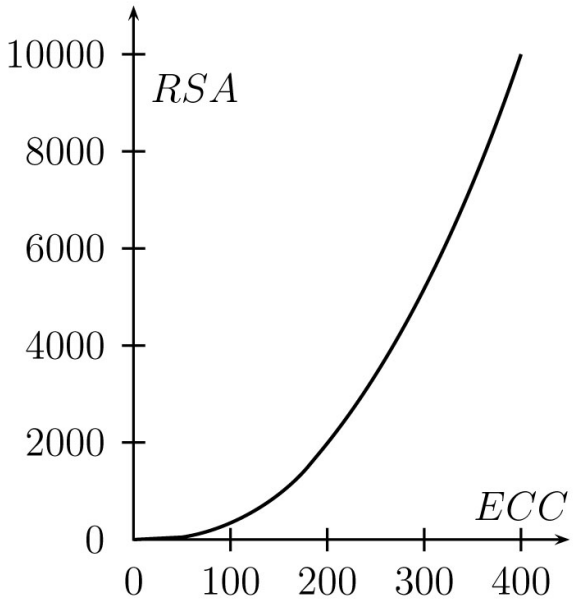


Abbildung 1.1: Vergleich der nötigen Bit-Länge zwischen RSA und ECC

1.5.4 Sicherheit

Die Forschung im Bereich der elliptischen Kurven wird seit ca. 150 Jahren betrieben. Seit ungefähr 1985 ist bekannt, dass das elliptische Kurvenproblem für die Kryptographie genutzt werden kann. Kein führender Mathematiker hat bis heute eine bemerkenswerte Schwachstelle entdeckt.

Es muss jedoch bemerkt werden, dass es Klassen von Kurven gibt, sogenannte supersinguläre Kurven wie auch sogenannte anomale Kurven, die nicht nicht zur Verschlüsselung geeignet sind. Die Attacken darauf wurden unabhängig von einander von Semaev, Smart, Satoh und Araki, und für den allgemeinen Fall von Rück gefunden.

Auszug aus der Homepage des Standardsetzers IEEE (siehe [9]): Standard Specifications For Public-Key Cryptography, Traditional Public-Key Cryptography (1363-2000 and 1363a-2004) This includes digital signature and key establishment schemes based on the following problems:

* The integer factorization (IF) problem (e.g. RSA).

* The discrete logarithm (DL) problem (e.g. Diffie-Hellman, DSA).

* The elliptic curve discrete logarithm (EC) problem (e.g. MQV).

Auf dieser Homepage gibt es auch einen Link zu einem Zahlenbeispiel (siehe [10]).

Kapitel 2

Schülerteil

2.1 Vorüberlegungen

Lehrplanbezug (siehe [8])

Im Lehrplan für Mathematik *Zur Vertiefung und Erweiterung des Bildungsinhaltes von Pflichtgegenständen* finden sich folgende Zeilen:

> Lehrstoff: Wie Lehrplan des Pflichtgegenstandes Mathematik. [...]
> Im Zuge der Erweiterung sind folgende zusätzliche Bereiche möglich: Klassische Probleme der Mathematik; geometrische Probleme; Kongruenzen und Teilbarkeit; zahlentheoretische Probleme; Kryptologie, Codierung; numerische Methoden;

Mathematische Voraussetzungen

Für dieses Thema werden viele Werkzeuge benötigt, die vorher im Regelunterricht gelernt wurden (Die Klassenangaben beziehen sich auf den Lehrplan 2009/10 für Mathematik an der AHS-Oberstufe (siehe [8])).

- Grundrechnungsarten: Die SchülerInnen wissen, wie Addieren und Multiplizieren funktioniert und kennen abzählbare und überabzählbare Zahlenbereiche wie $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$ (zusammenfassend am Anfang der 5. Klasse). In dieser Arbeit wird von diesen Strukturen der Gruppen- und Körperbegriff abstrahiert.

  Ein essentieller Teil der Kryptographie allgemein ist das Rechnen in endlichen Körpern. Da dieses Thema im Regelunterricht ausgespart bleibt, beginnt der Schülerteil damit.

- Geometrie: Die SchülerInnen können bereits mit Objekten in der Ebene operieren, Punkte addieren und multiplizieren (auf 2 Arten), Geraden aufstellen und mit anderen Objekten schneiden, Tangenten berechnen und geometrische Objekte um eine Achse spiegeln (5. und 6. Klasse). Diese Fähigkeiten werden in einem Geometrieschwerpunkt benötigt und eingesetzt. Mit Hilfe des Computerprogramms *DynaGeo* werden Kurven anschaulich gemacht.

- Analysis: Die Schüler beherrschen die Differentialrechnung und kennen den Zusammenhang zwischen erster Ableitung und Tangentensteigung (7. Klasse). Die Herleitung der Rechenoperationen passiert über $\mathbb{R}$, zum Teil auch mit analytischen Methoden. Danach werden sie auf $\mathbb{Z}_p$ übertragen.

- Computereinsatz: Die Rechnungen werden in *Derive* durchgeführt und erklärt. Vorwissen in diesem Programm ist von Vorteil. Die speziellen Derive-Programme können vom Lehrenden vorprogrammiert werden, die Anwendung sollte den Schülern jedoch geläufig sein. Ein Auszug aus dem Lehrplan:

  > Mathematiknahe Technologien wie Computeralgebra-Systeme, dynamische Geometrie-Software oder Tabellenkalkulationsprogramme sind im heutigen Mathematikunterricht unverzichtbar. Sachgerechtes und sinnvolles Nutzen der Programme durch geplantes Vorgehen ist sicherzustellen.[...]

Die SchülerInnen haben schon viel Erfahrung im Umgang mit Kurven und Funktionen. Die elliptischen Kurven über den reellen Zahlen ordnen sich in das bereits Gelernte ein, eine Kurvendiskussion ist für sie Routine. Daher ist der Einstieg in das Thema *Elliptische Kurven* (siehe Kapitel 2.5) auch bewusst über $\mathbb{R}$ gewählt. Hier werden die neuen Rechnungsarten eingeführt, die Kurven diskutiert und deren Eigenschaften beobachtet. Der Schritt von den reellen Zahlen zu einem endlichen Körper ist der Kern zum Verständnis der kryptographischen Verfahren. Die SchülerInnen werden feststellen, dass die Rechnungsarten und Operationen hier genauso funktionieren.

2.2 Vorraussetzung: Rechnen in Restklassen

Dieser Einstieg ist ein möglicher Anfang für das Rechnen in Restklassen. Er orientiert sich (in gekürzter Version) an dem Skriptum der Vorlesung „Arithmetik und Algebra“ des Flensburger Professors Alfred Schreiber (siehe [5]). Klarerweise kann dieses Thema als eigenständige Unterrichtssequenz herangezogen werden, wegen des großen Umfangs wird hier auf nähere Ausführungen verzichtet.

Definition: Sei $m \geq 2$ ganz. Zwei Zahlen heißen kongruent modulo m, wenn sie bei Divisionen durch m den selben nicht negativen Rest haben. Man schreibt dafür kurz: $a \equiv b \bmod m$ oder auch nur $a \equiv b$, wenn der Modul aus dem Zusammenhang hervorgeht.

Beispiel

- $23 \equiv 3 \bmod 5$
- $-1 \equiv 12 \bmod 13$
- $17 \equiv 21 \equiv 1 \bmod 2$

Satz: Für alle $a, b \in \mathbb{Z}$ gilt: $a \equiv b \bmod m \Leftrightarrow m|a-b$

Beweis: (auch geeignet für Schüler höherer Klassen):

- „$\Rightarrow$“: Nach Voraussetzung haben die beiden Zahlen a und b bei der Division durch m den gleichen Rest, also ist $a = q_1 m + r$ und $b = q_2 m + r$. Daraus folgt: $a - b = (q_1 - q_2)m$. ($a - b$ ist eine ganzzahliges Vielfaches von m)
- „$\Leftarrow$“: Nach Voraussetzung gibt es ein $q \in \mathbb{Z}$ mit $a - b = qm$. Nun dividieren wir a und b durch m: $a = q_1 m + r_1, b = q_2 m + r_2$, wobei $0 \leq r_1, r_2 \leq m$. Durch Einsetzen in $a - b = qm$ ergibt sich:

$$q_1 m + r_1 - q_2 m - r_2 = qm$$
$$-(q_1 - q_2 - q)m = r_1 - r_2$$

m ist Teiler der Differenz $r_1 - r_2$, und wegen $0 \leq |r_1 - r_2| < m$ folgt $r_1 = r_2$.

Es erweist sich, dass man mit Kongruenzen zum selben Modul so rechnen kann wie bei gewöhnlichen Gleichungen. Genauer: Aus gültigen Kongruenzen, z.B. $10 \equiv 1 \bmod 3$ und $-7 \equiv 5 \bmod 3$, gewinnt man durch Addieren und multiplizieren jeweils der linken und rechten Seiten neue gültige Kongruenzen, hier $3 \equiv 6 \bmod 3$ bzw. $-70 \equiv 5 \bmod 3$.

Definition: Sei $a \in \mathbb{Z}, m \geq 2$ ganz. Die Menge aller zu a modulo m kongruenten ganzen Zahlen heißt *Restklasse (modulo m) von a*. Die Restklasse modulo m von a beinhaltet somit alle ganzen Zahlen, die bei der Division durch m den gleichen nicht negativen Rest ergeben. Die Menge aller Restklassen modulo m bezeichnen wir mit $\mathbb{Z}_m$. Als Repräsentant eines Elementes a von $\mathbb{Z}_m$ nimmt man günstigerweise zumeist den kleinsten nicht negativen Rest bei Divisionen durch m.

2.2.1 Rechnen in $\mathbb{Z}_m$

Definition: Für $a, b \in \mathbb{Z}_m$ wird festgelegt:

- $a \oplus b := (a + b) \bmod m$
- $a \odot b := (a \cdot b) \bmod m$

$\oplus$ heißt Restklassenaddition, $\odot$ Restklassenmultiplikation. Es gelten insbesondere folgende Gesetze:

- $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
- $a \odot (b\odot) = (a \odot b) \odot c$
- $a \oplus b = b \oplus a$
- $a \odot b = b \odot a$
- $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
- $a \oplus 0 = a$
- $a \odot 1 = a$

Potenzieren in $\mathbb{Z}_m$: Zu $a \in \mathbb{Z}_m$ und ganzem $k \geq 0$ werden Potenzen a^k ebenso gebildet wie bei gewöhnlichen Zahlen: $a^2 = a \odot a$, $a^3 = a^2 \odot a$, usw.; ferner: $a^1 = a$ und $a^0 = 1$. Es gelten die vertrauten Rechenregeln für Potenzen: $a^r a^s = a^{r+s}$ sowie $(a^r)^s = a^{rs}$ und $(ab)^r = a^r b^r$.

a^k als Element von $\mathbb{Z}_m$ ist nach der Definition der Rest a^k mod m. Um ihn rechnerisch zu bestimmen (z.B. bei größeren Werten von k), zerlegt man den Exponenten in eine Summe: $k = n_1 + n_2 + ...$ Man erhält mit der ersten der oben genannten Potenzrechenregeln: $a^k = a^{n_1+n_2+\cdots} = a^{n_1} a^{n_2}$... mod m und hat so die Aufgabe darauf reduziert, zunächst Reste a^{n_1} mod m, a^{n_2} mod m, usw. mit kleineren Exponenten auszuwerten.

2.2.2 Zusammenfassung wichtiger Rechenregeln

Wenn $a \equiv a'$ mod n und $b \equiv b'$ mod n, dann ist
$a + b \equiv a' + b'$ mod n,
$a \cdot b \equiv a' \cdot b'$ mod n und
$a^x \equiv a'^x$ mod n.
Dabei sind a und b beliebige Zahlen aus $\mathbb{Z}$, $x \in \mathbb{N}$ und der Modul $n \geq 2$.

Bemerkung: Wir setzen $n \geq 2$ voraus. Wäre der Modul nämlich 1, hätten wir nur eine einzige Restklasse, nämlich 0, was zum Rechnen wenig Sinn ergibt.

Aufgaben:

1. Berechne den Rest modulo 7 von $2^4, 2^7, 2^{10}, 2^{16}$.

2. Berechne den Rest modulo 5 von $2^3, 2^{14}, 3^7, 3^{257}$.

3. Beweise die Behauptung: "Die Zahl 3^{20} hat die Endziffer 1 oder 6."

   Lösung: Die Endziffer ist jene Zahl, die bei der Division durch 10 als Rest übrigbleibt. Wir befinden uns also in $\mathbb{Z}_{10}$.

$$3^3 = 27 \equiv 7 \text{ mod } 10$$
$$3^4 \equiv 3 \cdot 7 = 21 \equiv 1 \text{ mod } 10$$
$$3^{20} = (3^4)^5 \equiv 1^5 = 1 \text{ mod } 10$$

4. Berechne die Endziffern von $3^{30}, 3^{50}, 3^{2005}$.

Lösung: laut letztem Beispiel ist

$$3^5 = 3^4 \cdot 3 \equiv 1 \cdot 3 \bmod 10$$
$$3^{2005} = (3^5)^{400} \cdot 3 \equiv 3^{400} \cdot 3 = (3^5)^{80} \cdot 3 \equiv 3^{80} \cdot 3 =$$
$$= (3^5)^{16} \cdot 3 \equiv 3^{4 \cdot 4} \cdot 3 \equiv 1^3 \cdot 3 \equiv 3 \bmod 10$$

2.2.3 Inverse berechnen

Wie lautet die Lösungsmenge folgender Gleichung: $3 \cdot x \equiv 5 \bmod 11$?

Wenn wir uns in $\mathbb{Q}$ befinden würden, wäre die Antwort leicht: $x = \frac{5}{3}$. In $\mathbb{Z}_{11}$ gibt es jedoch keine Brüche. Wir müssen jene Zahl $\alpha \in \mathbb{Z}_{11}$ finden, mit der wir 3 multiplizieren müssen, damit 1 herauskommt. Also $3.\alpha \equiv 1 \bmod 11$. So ein α wird, falls es existiert, das Inverse Element von 3 in $\mathbb{Z}_{11}$ genannt (siehe Abschnitt 2.3.5). Bei so kleinen Moduln kann man einfach probieren. Wir finden eine Lösung mit $\alpha = 4$ ($3 \cdot 4 = 12 \equiv 1 \bmod 11$). Wenn wir also beide Seiten mit 4 multiplizieren, ist unsere Gleichung gelöst: $\underbrace{4 \cdot 3}_{=1} \cdot x = 4 \cdot 5 = 20 \equiv 9 \bmod 11$. Die Lösungsmenge ist $L = \{x \in \mathbb{Z} | x = 9 + k \cdot 11, k \in \mathbb{Z}\}$.

Es kann jedoch vorkommen, dass eine Gleichung der Gestalt $a \cdot \alpha \equiv 1 \bmod m$ mit $a < m$ keine ganzzahlige Lösung α hat, d.h. es existiert kei Inverses zu a modulo m. Man sieht das zum Beispiel anhand der Aufgabe $4 \cdot x \equiv 1 \bmod 8$.

Man kann zeigen: Ist der Modul eine Primzahl p, dann gibt es stets ein Inverses und sein Repräsentant in der Menge $\{0, ..., p-1\}$ ist eindeutig bestimmt. Das ist der Grund, warum in der Kryptographie und hier ab jetzt Primzahlmoduln verwendet werden!

Beispiele

- $3 + 2x \equiv 1 \bmod 17$
- $6^7 x \equiv 5 \bmod 13$
- $5 - 4x \equiv 14 \bmod 11$

2.3 Der Gruppenbegriff

Wie am Anfang dieses Kapitels erwähnt haben die SchülerInnen ausführlich gelernt, wie Addieren und Multiplizieren mit Zahlen funktioniert und kennen abzählbare und überabzählbare

Zahlenbereiche wie $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$. Zusätzlich haben wir den Bereich der Restklassen modulo m eingeführt. Wir wollen nun eine Ebene höher treten und die Begriffe „Operation“, „Inversenbildung“sowie die Eigenschaften „kommutativ“und „assoziativ“abstrahieren und im Gruppenbegriff vereinen.

2.3.1 Operationen

Eine Abbildung $f : M \times M \to M$ heißt *zweistellige Operation* auf M, und das geordnete Paar (M, f) heißt dann ein **Gruppoid** (siehe [2]). Wir kennen schon Operationen wie „+“ oder „·“ Als Platzhalter für Operationen wird häufig ein Ring $(\circ)$ verwendet. Um zum Beispiel unser altbekanntes „+“darzustellen, würden wir definieren: $a \circ b := a + b$. Wir können beliebige Definitionen für unseren $\circ$ angeben, wie zum Beispiel in $\mathbb{Q}$ oder $\mathbb{R}$:

1. $a \circ b := a + b - 1$
2. $a \circ b := a^b$
3. $a \circ b := \frac{a+b}{5a+1}$ ist z.B. keine Operation in $\mathbb{Q}$ oder $\mathbb{R}$, da $a \circ b$ nicht für alle Paare a, b definiert ist.

2.3.2 Das Kommutativgesetz

Wenn dieses Gesetz für eine Operation $\circ$ für alle(!) $a, b \in M$ gilt, heißt $\circ$ *kommutativ*:

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

Wir kennen bereits kommutative Operationen wie z.B. “+“in $\mathbb{Z}$, da $a + b = b + a \ \ \forall a, b \in \mathbb{Z}$ ist. Eine nicht kommutative Operation wäre in $\mathbb{Z}$

$$a \circ b = a - b,$$

weil $a - b \neq b - a$ für alle Paare $\{a, b \in \mathbb{Z} | a \neq b\}$.

Aufgaben

Überprüfe, ob die Operationen aus 2.3.1 über $\mathbb{Z}$ kommutativ sind.

2.3.3 Das Assoziativitätsgesetz

Bei einer *assoziativen* Operation gilt wieder für alle Elemente a, b, c in einer Menge M die Gleichung:

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

Unser bekanntes „$\cdot$“ in $\mathbb{R}$ ist zum Beispiel assoziativ, denn

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in \mathbb{R}$$

Aufgaben

Überprüfe, ob die Operationen aus 2.3.1 über $\mathbb{Z}$ assoziativ sind.

- ad 1.: $a \circ b := a + b - 1$
  zu zeigen: $a \circ (b \circ c) = (a \circ b) \circ c$

  $$a \circ (b + c - 1) = (a + b - 1) \circ c$$
  $$a + b + c - 1 - 1 = a + b - 1 + c - 1$$
  $$a + b + c - 2 = a + b + c - 2$$

  $\Rightarrow$ Diese Operation ist assoziativ.

- ad 2.: $a \circ b := a^b$
  zu zeigen: $a \circ (b \circ c) = (a \circ b) \circ c$

  $$a \circ b^c = a^b \circ c$$
  $$a^{(b^c)} = (a^b)^c$$
  $$a^{(b^c)} = a^{b.c} \quad \text{Widerspruch, gilt nicht für alle } a, b, c \in \mathbb{Z}$$

  $\Rightarrow$ Diese Operation ist nicht assoziativ.

Der Nachweis des Assoziativgesetzes kann sehr aufwändig sein. Das ist auch der Grund, warum wir später im Kapitel 2.6.3 bei elliptischen Kurven das Assoziativgesetz nicht beweisen werden.

2.3.4 Das neutrale Element

Das neutrale Element hat die Eigenschaft, dass es, wenn es mit einem beliebigen anderen Element verknüpft wird, dieses andere Element nicht verändert. Bei unserem „+“ in $\mathbb{Z}$ ist das die 0, denn $\forall a \in \mathbb{Z} : a + 0 = a$.
Bei Bsp. 1 aus 2.3.1 in $\mathbb{Z}$ wäre das neutrale Element die 1, denn $a + 1 - 1 = a, \forall a \in \mathbb{Z}$.

2.3.5 Das inverse Element

Das inverse Element eines Elements $a \in M$ hat die Eigenschaft, dass das Ergebnis, wenn es mit a verknüpft wird, das neutrale Element ist. Bei unserem „+“ in $\mathbb{Z}$ ist das jeweils $-a$, denn $\forall a \in \mathbb{Z} : a + (-a) = 0$.
Bei Bsp. 1 aus 2.3.1 in $\mathbb{Z}$ wäre das inverse Element $-a + 2$, denn $a + (-a + 2) - 1 = 1, \forall a \in \mathbb{Z}$.

2.3.6 Die Gruppe

Ein Gruppoid $(M, \circ)$ (lt. 2.3.1) heißt eine *Gruppe*, wenn folgende Eigenschaften für die Operation $\circ : (a, b) \in M \times M \mapsto \circ(a, b) := a \circ b \in M$ auf M zutreffen:

1. $\circ$ erfüllt das Assoziativgesetz
2. es existiert ein neutrales Element $e \in M$
3. $\forall a \in M$ existiert ein Inverses $\bar{a}$ in M, sodass $a \circ \bar{a} = \bar{a} \circ a = e$

Beispiele:

- Die ganzen Zahlen $\mathbb{Z}$ mit unserem „+“ sind eine Gruppe, denn das neutrale Element ist 0, das inverse ist $-a$ und es gilt $a + (b + c) = (a + b) + c$, d.h. + assoziativ.
- Die natürlichen Zahlen mit 0 ($\mathbb{N}_0$) mit unserem „+“ sind keine Gruppe, denn das neutrale Element ist zwar 0, aber die inversen (wäre wieder $-a$) sind nicht in unserer Zahlenmenge $\mathbb{N}_0$ enthalten.

Aufgaben: Überprüfe, ob es sich um Gruppen handelt:

- $\mathbb{Z}$ mit dem bekannten „$\cdot$“, also $(\mathbb{Z}, \cdot)$
- Q mit dem bekannten „$\cdot$“, also $(\mathbb{Q}, \cdot)$
- $a \otimes b := \frac{a \cdot b}{2}$; $\qquad (\mathbb{Q} \backslash \{0\}, \otimes)$

Bemerkung: Wie wir gesehen haben, können Mengen von Zahlen Gruppen bilden, in denen das Kommutativgesetz nicht gilt. Dies ist natürlich für das Rechnen nicht vorteilhaft. Wenn eine Gruppe zusätzlich kommutativ ist, wird sie *kommutative Gruppe* genannt.

2.3.7 Der Körper

Wir betrachten nun Mengen, in denen es zwei Operationen $\oplus$ und $\otimes$ gibt. Eine mindestens zweielementige Menge K, bei der K mit $\oplus$ und K, ohne das neutrale Element gegenüber $\oplus$, mit $\otimes$ jeweils eine kommutative Gruppe bildet und bei der für alle $a, b, c \in K$ gilt $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ heißt ein *Körper*. Wir schreiben dafür kurz $(K, \oplus, \otimes)$. In Körpern können wir genauso rechnen, wie wir es mit „+“ und „·“ von reellen Zahlen gewohnt sind.

Beispiele:

1. $(\mathbb{R}, +, \cdot)$

2. $(\mathbb{Z}_p, +, \cdot)$, $p \in \mathbb{P}$
   Wie schon in 2.2.3 erwähnt gibt es beim Restklassenrechnen modulo einer Primzahl p ein eindeutig bestimmtes Inverses aus $\{1, ..., p-1\}$. Mit dieser Zusatzbedingung wird der Zahlenbereich $\mathbb{Z}_p$ mit „+“ und „·“ zu einem Körper, genannt *Restklassenkörper* $\mathbb{Z}_p$. Er ist im Unterschied zu $(\mathbb{R}, +, \cdot)$ ein endlicher Körper, weil die Anzahl seiner Elemente endlich ist.

2.4 ElGamal über endlichen Körpern

Bis jetzt haben wir in Restklassen rechnen gelernt und Gruppen und Körper kennengelernt. Jetzt können wir uns bereits Verschlüsselungsalgorithmen ansehen. Ähnlich wie im Lehrerteil kann man das ElGamal - System erklären.
Allgemein bekannt seien eine Primzahl p und ein Element g von $\mathbb{Z}_p$.

1. Alice wählt zufällig ein $a \in \{1, ..., p-1\}$ aus und bildet damit $q = g^a \bmod p$. Dieses q gibt Alice nun als ihren öffentlichen Schlüssel bekannt, während a als ihr privater Schlüssel geheim bleibt.

2. Bob will Alice nun die Nachricht m schicken.

Er wählt dazu ein beliebiges zufälliges $b \in \{1, ..., p-1\}$ und berechnet daraus $c_1 = g^b$ und $c_2 = m \cdot q^b$

3. (c_1, c_2) bilden das Chiffrat, das er an Alice schickt.

4. Diese bildet $\frac{c_2}{c_1^a} = \frac{m \cdot q^b}{g^{ab}} = \frac{m \cdot g^{ab}}{g^{ab}} = m$

Es sei hier noch erwähnt, dass die Sicherheit dieser Verschlüsselung auf dem diskreten Logarithmusproblem beruht (siehe Kapitel 1.1.3). Ein unbefugter Mithörer des Datenaustausches steht nämlich vor folgender Aufgabe, wenn er die Nachricht lesen will: Er kennt g und auch q und er weiß, dass a der Schlüssel ist. Er muss versuchen, a aus den anderen beiden Zahlen zu berechnen:

$$q = g^a$$
$$a = log_g q$$

In $\mathbb{R}$ ist dieser Logarithmus leicht zu berechnen, in einem endlichen Körper dauert das jedoch mehrere Millionen Jahre, wenn geeignet große Zahlen zur Verschlüsselung verwendet werden. Verwendet man zum Beispiel bei ECC einen 210 Bit Schlüssel, braucht die Entschlüsselung so viele Rechenschritte, dass ein moderner Computer dafür etwa 10^{20} Jahre (siehe [4], S.122f) benötigt. In Worten sind das einhundert Trillionen Jahre. Man sieht schnell ein, dass das Knacken des Schlüssels mit der so genannte *Brute Force*- Methode, d.h. alle möglichen Zahlen nach der Reihe auszuprobieren, wenig Sinn hat.

Im folgenden Kapitel beschäftigen wir uns mit elliptischen Kurven für den Schulunterricht. Die Annäherung an dieses Thema wird in vier Schritten erfolgen:

- Geometrie der Kurven, Kurven zeichnen, grundsätzliches Verständnis
- Eigenschaften der Kurven, Steigungen der Tangenten ausrechnen, Rechenoperationen
- Elliptische Kurven über endlichen Körpern
- Verschlüsselung mittels elliptischer Kurven

2.5 Geometrie

Ziel dieses Abschnittes ist das Kennenlernen und das anschauliche Begreifen elliptischer Kurven über $\mathbb{R}$ sowie deren Eigenschaften. Die SchülerInnen sollten bereits mit Objekten in der Ebene operieren, Punkte addieren und multiplizieren (auf 2 Arten), Geraden aufstellen und mit anderen Objekten schneiden, Tangenten berechnen und geometrische Objekte um eine Achse spiegeln (5. und 6. Klasse) können.

Zuerst sollte man erklären, dass es sich bei elliptischen Kurven nicht um Ellipsen handelt. Dieser Unterschied ist wichtig und wird nicht nur von Schülern des öfteren vergessen. In der eine Ellipse darstellenden Polynomfunktion treten höchstens Potenzen zweiten Grades auf, bei einer elliptischen Kurve jedoch Potenzen dritten Grades. Ihre Formel lautet wie folgt (über $\mathbb{R}$ und $\mathbb{Z}_p$, p prim $\neq 2, 3$):

$$y^2 = x^3 + ax + b,$$

wobei die Funktion $x^3 + ax + b$ keine mehrfachen Nullstellen haben darf, was durch die Bedingung $4a^3 + 27b^2 \neq 0$ garantiert wird.

Es ist nicht nötig, die allgemeinere Formel $y^2 + a_4xy + a_3y = x^3 + a_2x^2 + a_1x + a_0$, welche über $\mathbb{R}$ durch eine Transformation stets auf die Form $y^2 = x^3 + ax + b$ gebracht werden kann, zu erklären. Viel wichtiger ist es, sich schon zu Beginn ein Bild von dieser Kurve zu machen. Wir zeichnen einige Punkte der Kurve, indem wir x- Werte annehmen und die y-Werte ausrechnen. Für a und b wählen wir 1. Damit hat die Kurve nur eine Nullstelle, wie wir nachfolgend zeigen werden, und ist dadurch leichter zu zeichnen.
Wir gehen von der allgemeinen Gleichung

$$y^2 = x^3 + x + 1$$

aus und berechnen als erstes die Nullstelle(n) der Kurve mittels der Formel von Cardano. (Diese Berechnung ist nur für den Lehrenden, falls die Formel bzw. das Ziehen der dritten Wurzel aus negativen Zahlen- Moivresche Formel- nicht im Unterricht besprochen wird bzw. vorangehend nicht besprochen worden ist.)

$$0 = x^3 + x + 1$$
$$D = (\frac{1}{2})^2 + (\frac{1}{3})^3 = \frac{31}{108}$$

$$u = \sqrt[3]{-\frac{1}{2} + \sqrt{D}}$$
$$v = \sqrt[3]{-\frac{1}{2} - \sqrt{D}}$$
$$x = u + v = \sqrt[3]{-\frac{1}{2} + \sqrt{D}} + \sqrt[3]{-\frac{1}{2} - \sqrt{D}}$$
$$x \cong -0,68$$

Mit diesen Informationen können wir folgende Tabelle erstellen und die Kurve wie in Abbildung 2.1 zeichnen.

x	y
$-0,68$	0
0	± 1
1	$\pm\sqrt{3}$
2	$\pm\sqrt{11}$
3	$\pm\sqrt{31}$
-1	$\sqrt{-1}$
-2	$\sqrt{-9}$

Um ein Bild von den verschiedenen möglichen Erscheinungsformen einer elliptischen Kurve zu bekommen, wollen wir sie mit dem Programm „Euklid DynaGeo“ zeichnen. Wir nehmen also jetzt den allgemeinen Fall an, dass eine Kurve $y^2 + ax + b$ vorliegt. Mit dem eben genannten Programm kann man die Parameter der Kurve mit einem Schieberegler verändern, was sehr hilfreich ist, um die Eigenschaften der Kurve zu verstehen:

- Zuerst die beiden Schieberegler installieren (Messen&Rechnen/Zahlenobjekt erstellen - durch doppelklicken umbenennen auf a und b)
- Mit `rechte Maustaste auf Schieberegler/Bereich editieren` kann man die Grenzen von a und b einstellen (Vorschlag: $-200 \leq a, b \leq 200$).
- Kurve konstruieren (`Kurven/Funktionsschaubild : f(x)= sqrt (x^3+a*x+b)` und `f(x)= -sqrt(x^3+a*x+b)`)

Nun kann man mit Hilfe der Schieberegler die Entwicklung der Kurve beobachten (vgl. Abbildung 2.2). Einige Beobachtungen (die jeweils andere Variable halten wir bei 1 fest):

- Wenn a sehr groß wird „legt“ sich die Kurve an die y-Achse (siehe Abbildung 2.3a).

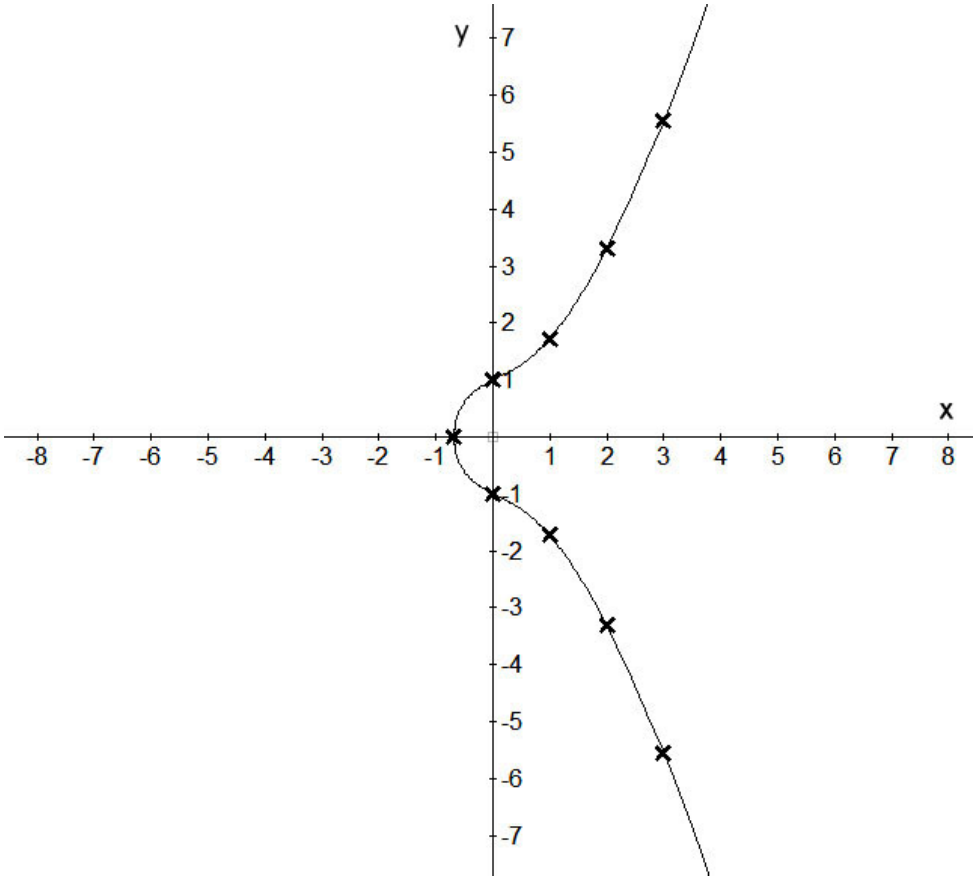


Abbildung 2.1: $y^2 = x^3 + x + 1$

- Wenn a klein wird, teilt sich die Kurve in einen geschlossenen, eiförmigen Teil links und einen parabelähnlichen Teil rechts (siehe Abbildung 2.3b).
- Wenn b groß wird, wird der „Bauch“ größer (siehe Abbildung 2.3c).
- Wenn b klein wird, wird der Bauch zu einem Oval, das kleiner wird bis es verschwindet und der parabelähnliche Teil übrig bleibt (siehe Abbildung 2.3d).

Diese Beobachtungen sind wichtig, um eine beliebige Kurve schnell klassifizieren zu können, in dem Sinn: „Diese Kurve hat wahrscheinlich drei Nullstellen“ oder „Diese Kurve hat keine lokalen Extremstellen“.

2.5.1 Einschub: Kurvendiskussion

Man kann elliptische Kurven mit analytischen Methoden diskutieren. Mittels Differentialrechnung kann man Hoch- und Tiefpunkte berechnen. Zuerst muss jedoch die Sinnhaftigkeit dieser

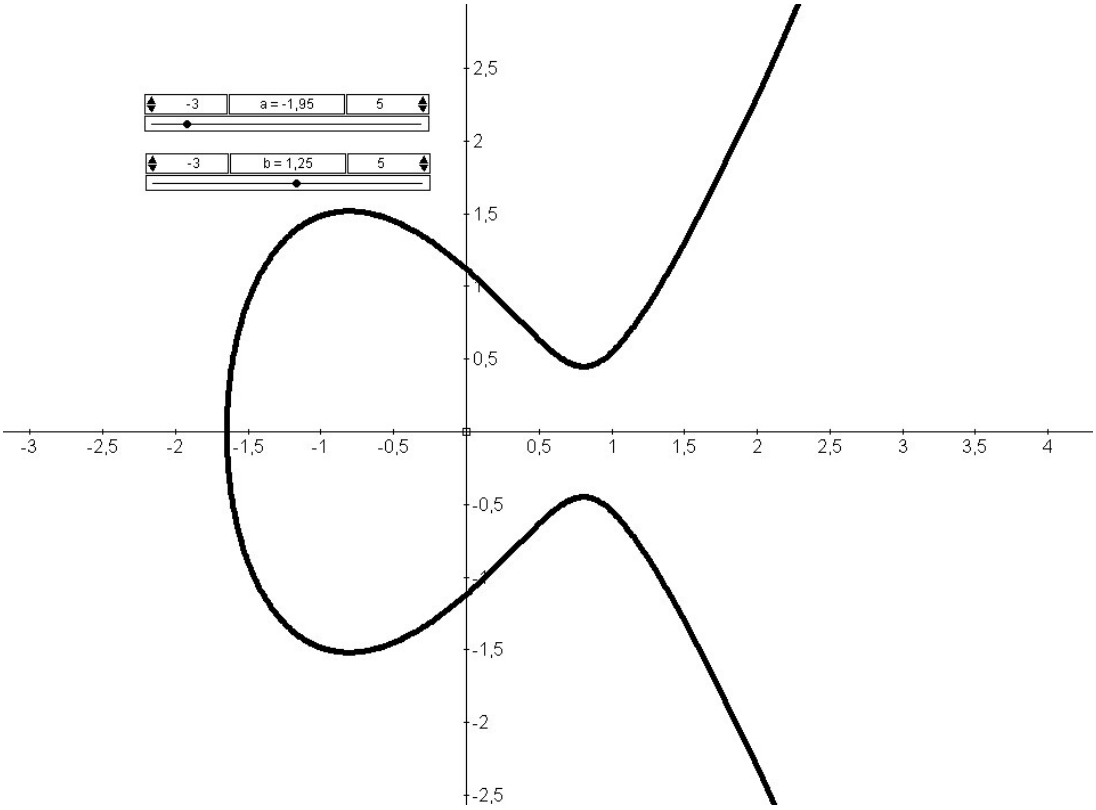


Abbildung 2.2: Dynamisch Darstellung einer elliptischen Kurve mit Hilfe von Schiebereglern in dem Programm *DynaGeo*.

Rechnungen überlegt werden. Wie im folgenden Beispiel zu sehen ist, kommen hier Fragestellungen vor, die Schüler zum Nachdenken und Interpretieren herausfordern können. Die Schwierigkeit dabei ist, dass die Lösungen, wenn sie existieren, aufgrund der Wurzeln immer doppelt vorkommen.

Beispiel: Sei $y^2 = x^3 - 50x + 200, x, y \in \mathbb{R}$. Untersuche die Kurve auf Hoch-und Tiefpunkte, Wendestellen und Nullstellen. Als Lehrer weiß man, dass die kubische Gleichung $x^3 + 3px + 2q = 0$ für $D = p^3 + q^2 > 0$ genau eine reelle Lösung besitzt, was hier der Fall ist. Ist diese Aussage Schülern nicht (oder noch nicht) bekannt, wird man dies als Erklärung anfügen.

Nullstelle(n): Die Nullstelle kann man dann entweder wieder mit der Formel von Cardano (soferne diese zur Verfügung steht) berechnen, oder man hat ein CAS zu Verfügung. Das Ergebnis ist $x = -8,56$. Wir werden den Wert später brauchen.

Extremwerte: Umformen auf $f(x) = \pm\sqrt{x^3 - 50x + 200}$. Diese Rechnungen werden auch vermehrt mit dem Computer durchgeführt, die erste Ableitung ist jedoch auch leicht mittels

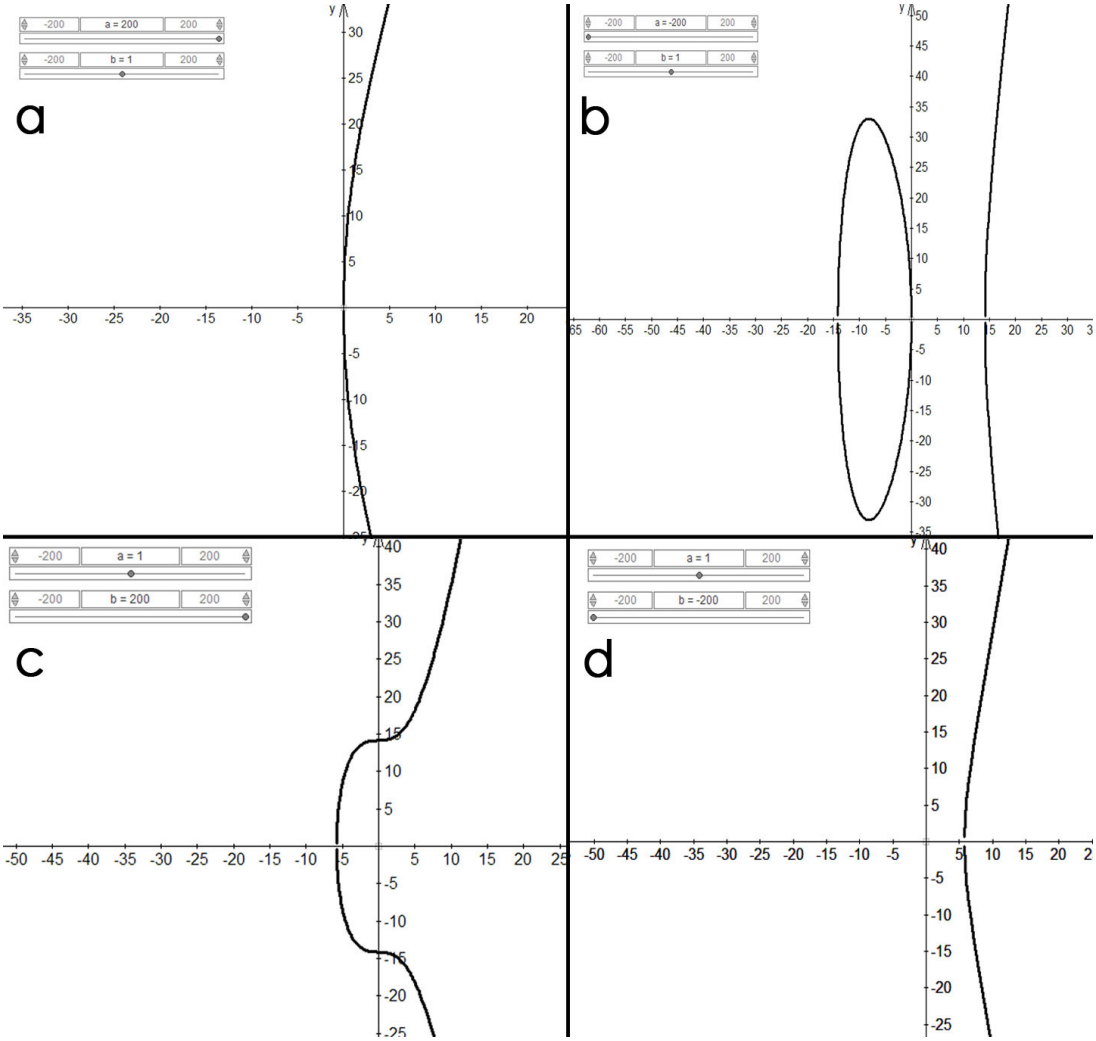


Abbildung 2.3: Charakteristische Erscheinungsformen von $y^2 = x^3 + ax + b$

der Kettenregel zu berechnen. Wir erhalten

$$f'(x) = \frac{3x^2-50}{2\sqrt{x^3-50x+200}} = 0$$

Fragestellung: Dürfen wir mit dem Nenner multiplizieren? Ja, weil er nur eine Lösung liefern würde, wenn x gegen ∞ geht.

$$3x^2 - 50 = 0 \qquad \Rightarrow$$
$$x_{1,2} = \pm\frac{5\sqrt{6}}{3}$$

Für x_1 und x_2 erhalten wir jeweils zwei y-Werte:

$$y_{1,2} \cong \pm 18,33$$
$$y_{3,4} \cong \pm 8$$

Wir haben also vier Kandidaten für Extremwerte, für die wir mittels zweiter Ableitung die Krümmung bestimmen:
$P_1 = \begin{pmatrix} \frac{5\sqrt{6}}{3} \\ 8 \end{pmatrix}, P_2 = \begin{pmatrix} \frac{5\sqrt{6}}{3} \\ -8 \end{pmatrix}, P_3 = \begin{pmatrix} -\frac{5\sqrt{6}}{3} \\ 18{,}33 \end{pmatrix}, P_4 = \begin{pmatrix} -\frac{5\sqrt{6}}{3} \\ -18{,}33 \end{pmatrix}$.

$$f''(x) = \frac{3x^4 - 300x^2 + 2400x - 2500}{\pm 4(x^3 - 50x + 200)^{\frac{3}{2}}}$$
$$f''(-\frac{5\sqrt{6}}{3}) = \pm 0,66$$
$$f''(\frac{5\sqrt{6}}{3}) = \pm 1,53$$

Wir haben jetzt eine Menge Punkte und Zahlen, die es zu interpretieren gilt: vier Punkte, die als Extremstellen in Frage kommen und vier dazugehörige zweite Ableitungen ($\neq 0$). Welche gehören zusammen?

- P_3 : Zwischen dem x-Wert von P_3 und dem x-Wert der Nullstelle liegen keine weiteren Kandidaten für einen Extremwert, also muss P_3, nachdem die Kurve stetig ist und der y-Wert von $P_3 > 0$, ein Hochpunkt sein.

- P_4 : Zwischen dem x-Wert von P_3 und dem x-Wert von P_4 liegen wieder keine weiteren Kandidaten für einen Extremwert, also folgt, weil P_3 ein Hochpunkt ist, dass P_4 ein Tiefpunkt ist.

- P_1 und P_2: Wegen der Symmetrie um die x-Achse trivial.

Mit Hilfe dieser die Kurve charakterisierenden Punkte kann man sie zeichnen (siehe Abbildung 2.4).
Man sieht, dass eine Kurvendiskussion nicht mit Formeln alleine zu bewältigen ist, sondern dass man sich sehr wohl überlegen muss, wie die Ergebnisse zusammenpassen. In diesem Beispiel hatte die Kurve eine Nullstelle und je zwei (lokale) Extremstellen auf jeder Seite der x-Achse. Man kann auch Beispiele im Unterricht bringen, wo drei reelle Nullstellen vorkommen, wie zum Beispiel $y^2 = x^3 - 11x + 1$, oder (mit Hilfe der Formel von Cardano) Beispiele konstruieren, die nur zwei Nullstellen haben, z.B. $y^2 = x^3 - 6x + 2\sqrt{8}$. Dafür muss in der Formel

$$y^2 = x^3 + 3px + 2q$$

die Gleichung $q^2 = -p^3$ gelten.

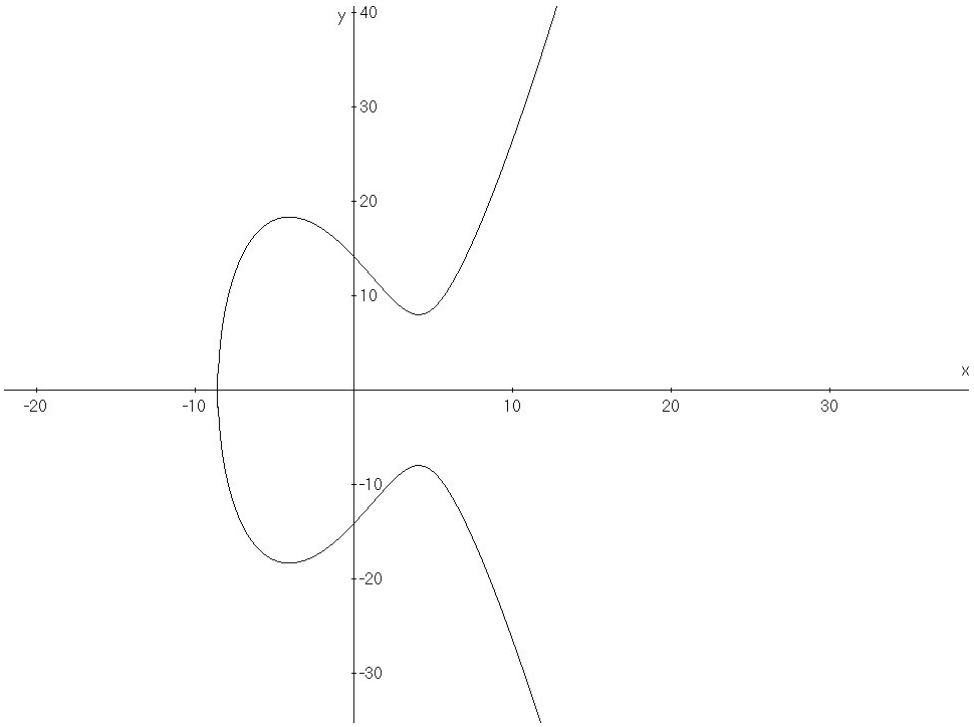


Abbildung 2.4: $y^2 = x^3 - 50x + 200$

2.6 Operationen auf der elliptischen Kurve

2.6.1 Die Addition

Motivation

Es stellt sich die Frage, warum wir von Addition reden, wenn wir mit einer elliptischen Kurve, einem geometrischen Objekt, hantieren. SchülerInnen kennen die Addition von Punkten in der euklidischen Ebene und es muss besprochen werden, dass diese neue Addition nichts mit der schon bekannten zu tun hat, außer dass man mit zwei Punkten rechnet und als Ergebnis einen dritten erhält.

Der Mathematiker gestaltet die Addition auf elliptischen Kurven so, dass sie auf der Menge der Punkte der elliptischen Kurve eine Gruppe ergeben. Die zugrunde liegende Menge ist nun die Menge der Punkte, die die elliptische Kurvengleichung erfüllen. Die Operation, welche zu einer Gruppe führt, werden wir jetzt motivieren.

Addition: geometrisch

Als erstes wollen wir die Addition geometrisch erklären: Man addiert zwei Punkte $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ mit $x_1 \neq x_2$ einer elliptischen Kurve E, indem man eine Gerade durch P und Q legt und diese anschließend ein drittes mal mit E schneidet. Diesen dritten Schnittpunkt spiegelt man an der x- Achse (siehe Abbildung 2.5).

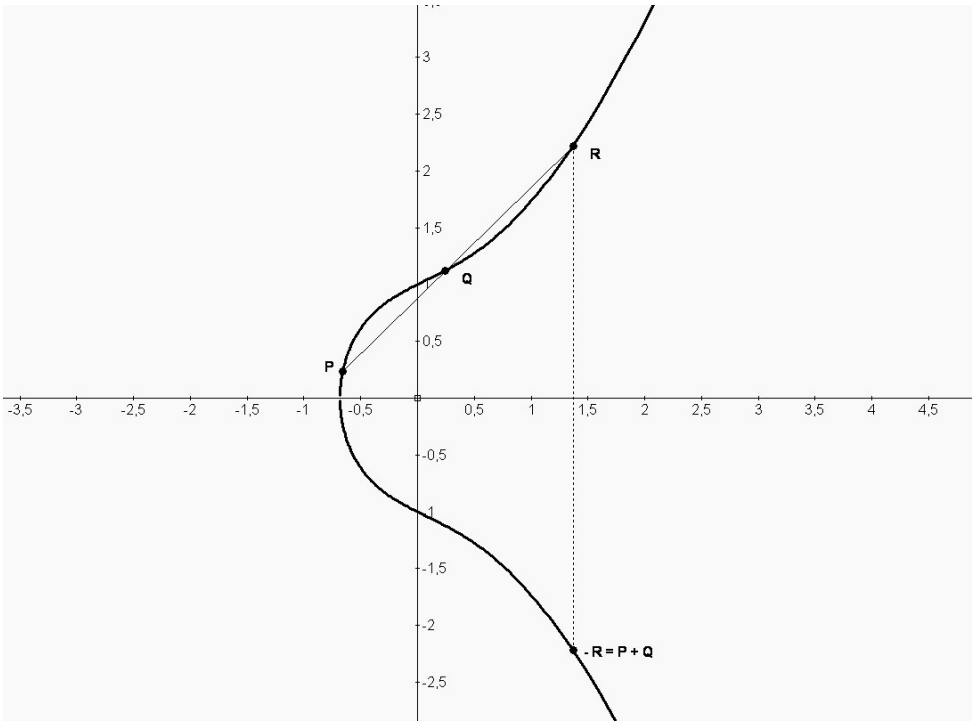


Abbildung 2.5: Addition geometrisch

Addition: rechnerisch

Diesen Punkt kann man folgendermaßen berechnen: Dazu stellen wir als erstes die Gleichung der Geraden durch P und Q auf. Ihre Steigung λ beträgt

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

Die Geradengleichung ist dann $g = P + k\begin{pmatrix} 1 \\ \lambda \end{pmatrix}, k \in \mathbb{R}$ oder $y = (x - x_1)\lambda + y_1$. Der folgende Umrechnungsschritt ist dem Lehrerteil zu entnehmen, als Koordinaten für die „Summe“

$-R = P + Q$ ergeben sich

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

Dabei stellen sich folgende Fragen:

1. Gibt es immer einen dritten Punkt?
2. Was passiert, wenn es keinen dritten Punkt gibt?

Es ist eine spannende Aufgabe, die Schüler soweit zu bringen, diese Fragen selbst zu stellen. Natürlich muss man die Antworten bereit halten:

1. Wenn ich eine Gerade mit der elliptischen Kurve schneide, d.h zum Beispiel die Gerade auf die Form $y = kx + d$ bringe und anschließend in die Kurvengleichung einzusetze, dann entsteht eine Gleichung dritten Grades $(kx + d)^2 = x^3 + ax + b$ bzw. $0 = x^3 - k^2x^2 + (a - 2kd)x + (b - d^2)$. Die möglichen Lösungen über $\mathbb{R}$ dieser Gleichung, welche die x-Koordinaten des Schnittpunktes der Geraden mit der elliptischen Kurve sind, sind in der Abbildung 2.6 anschaulich gemacht.

   Wir werden uns vorerst mit dem oben angenommenen Fall beschäftigen, zwei in den

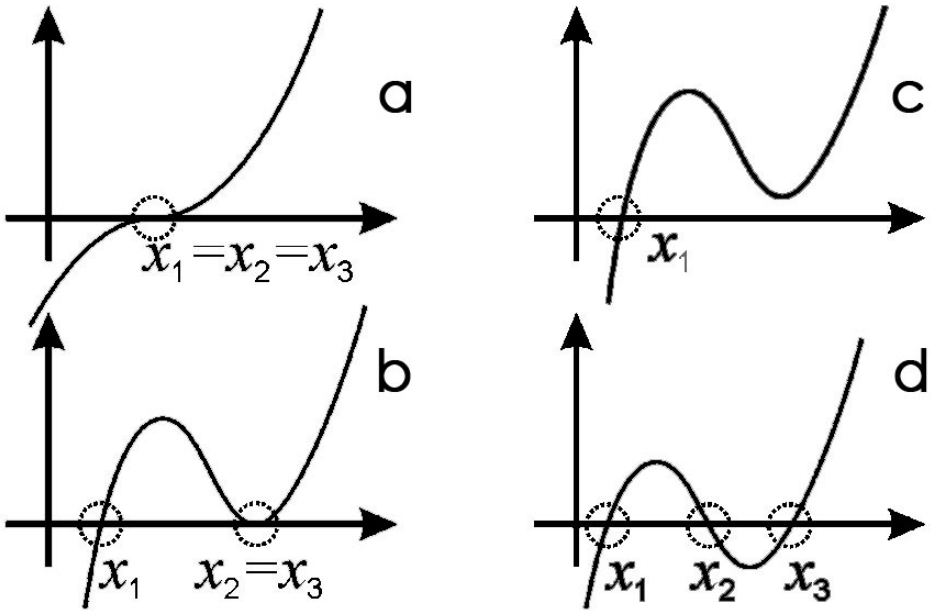


Abbildung 2.6: mögliche Lösungen einer kubischen Gleichung

x-Koordinaten *verschiedene* Punkte der Kurve zu addieren (Zwei Punkte können auch

verschieden sein, wenn $x_1 = x_2$ ist!). Wir studieren nun die Situation für die Koordinate x_3 des Schnittpunktes:

(a) Dieser Fall der Grafik kommt dann nicht in Frage.

(b) Der zweite Fall tritt ein, wenn die Gerade durch P und Q die elliptische Kurve in einem der beiden Punkte tangiert. Dieser Punkt ist dann ein doppelter Schnittpunkt und sein Spiegelbild ist die Lösung.

(c) Der dritte Fall kann auch nicht eintreten, weil wir annehmen, dass wir zwei Punkte mit $x_1 \neq x_2$ addieren, hier aber nur eine reelle Nullstelle vorkommt.

(d) Im vierten Fall hat die Gleichung dritten Grades drei verschiedene reelle Lösungen.

Zusammenfassend kann man sagen, dass die Gleichung, wenn man schon zwei verschiedene reelle Lösungen kennt (wie das der Fall ist beim Addieren von zwei Punkten mit $x_1 \neq x_2$), dann muss es auch eine dritte Lösung in $\mathbb{R}$ geben. Es kann nur der Fall eintreten, dass einer der beiden Punkte doppelt vorkommt, weil er ein Tangentialpunkt ist.

2. Wenn die beiden Punkte den gleichen x-Wert $v \in \mathbb{R}$ haben, ist die entstehende Gerade parallel zur y-Achse und hat die Form $x = v$. Wenn wir diese Geradengleichung nun in die Kurvengleichung von E einsetzen, hat diese die Form

$$y^2 = v^3 + a \cdot v + b$$

Sie wird also zu einer quadratischen Gleichung, die nur zwei Lösungen hat. Hierfür haben die Mathematiker den unendlich entfernten Punkt „erfunden“, der in diesem Fall als Lösung angenommen wird. Man kann eventuell die Vorstellung heranziehen, dass sich zwei parallele Geraden im Unendlichen schneiden- ebenso schneidet die elliptische Kurve im Unendlichen die y-Achse und somit auch jede zur y-Achse parallele Gerade. Diesen unendlich weit entfernten Punkt taufen wir $\mathcal{O}$.

Im nächsten Abschnitt wenden wir uns dem noch ausstehenden Fall zu, dass die Punkte P und Q gleich sind.

2.6.2 Eine Multiplikation

Schüler kennen schon Operatoren, um Punkte zu „multiplizieren“, wie das Skalarprodunkt oder das Kreuzprodukt. Sie kennen also schon zwei verschiedene Multiplikationsarten und

sind daher auf diesem Gebiet sensibilisiert. Im Falle der Multiplikation von Punkten auf einer elliptischen Kurve helfen wir uns mit einem Trick: Wir berechnen nicht $2P$, sondern $P + P$ und nennen es im Anschluss $2P$. Was das für unsere Gerade bedeutet, können die Schüler selbst herausfinden. Wir müssen jetzt also die Gleichung der Tangente im Punkt P an E berechnen (siehe Abbildung 2.7). Um die Steigung der Tangente zu berechnen, werden die Schüler auf

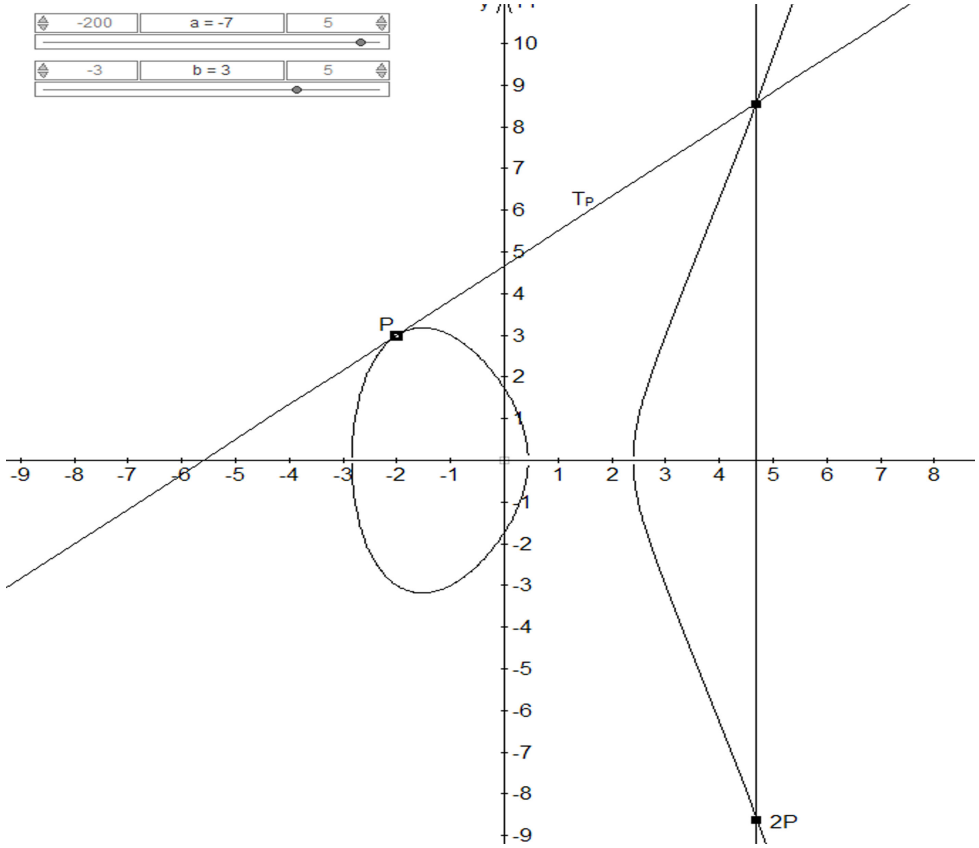


Abbildung 2.7: Multiplikation auf einer elliptischen Kurve, grafisch

die Idee kommen, im Punkt P zu differenzieren. Das funktioniert wie folgt:

$$f(x) = \pm\sqrt{x^3 - 7x + 3}$$
$$f'(x) = \pm\frac{3x^2 - 7}{2\sqrt{x^3 - 7x + 3}}$$

Wir sehen, dass unter dem Bruchstrich des Ergebnisses $2 \cdot f(x)$ steht. Wenn wir nun also die Steigung λ der Tangente im Punkt $P = (x_1, y_1)$ wissen wollen, setzen wir

$$\lambda = \frac{3x_1^2 - 7}{2y_1}.$$

Somit müssen wir auch nicht mehr überlegen, ob wir die positive oder negative Wurzel verwenden sollen. Nun können wir die Gerade mit dem soeben berechneten λ aufstellen. Die Gleichung lautet $g = P + k\left(\begin{smallmatrix}1\\ \lambda\end{smallmatrix}\right), k \in \mathbb{R}$, und wir erhalten wieder einen dritten Schnittpunkt.

Bemerkung: Wäre P eine Nullstelle von E, dann würde wegen der Symmetrie von E um die x- Achse die Tangente parallel zur y- Achse stehen und das Ergebnis ist $\mathcal{O}$. Diesen Fall haben wir aber bereits oben behandelt und daher ausgeschlossen.

Multiplikation mit einem Skalar

Wir wissen jetzt, wie $2P := P + P$ zu berechnen sind. Wie bekommen wir $23P$? Einfach durch Iteration:

$$23P = P + 2(11P) = P + 2(P + 2(5P)) = P + 2(P + 2(P + 2(2P)))$$

2.6.3 Zusammenfassung zu einer Formel

Wir definieren die Punktaddition wie im Lehrerteil:
Geg.: 2 Punkte $P = (x_1, y_1)$ und $Q(x_2, y_2) \in E$.

- Ist $x_1 = x_2$ und $y_2 = -y_1$, dann sei $P + Q = \mathcal{O}$.
- andernfalls sei $P + Q = (x_3, y_3)$ mit $x_3 = \lambda^2 - x_1 - x_2$ und $y_3 = \lambda(x_1 - x_3) - y_1$, wobei

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{für} \quad P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{für} \quad P = Q \end{cases}$$

Weiters sei $P + \mathcal{O} = \mathcal{O} + P = P, \quad \forall P \in E$

2.6.4 Übungsbeispiele

Es ist wegen der Beschaffenheit der Formel für elliptische Kurven nicht einfach, Beispiele mit so genannten „schönen“Zahlen zu konstruieren. Man kann die Kurven zwar auf einzelnen ganzzahligen Punkten aufbauen, aber sobald Rechenoperationen ins Spiel kommen, befindet man sich in den meisten Fällen im irrationalen Zahlenbereich. Dabei ist es hilfreich, vorher über *sinnvolles Runden* zu sprechen.

Beispiel 1: Sei $E : y^2 = x^3 - 70x + 4$ sowie $P = \begin{pmatrix} -2 \\ \sqrt{136} \end{pmatrix}$ und $Q = \begin{pmatrix} -1 \\ \sqrt{73} \end{pmatrix}$ gegeben. Zeige, dass P und Q auf E liegen, fertige eine Skizze (siehe Abbildung 2.8) und berechne P+Q, $2 \cdot P$ und $2 \cdot Q$.

- $P + Q$:

$$x_3 = (\frac{\sqrt{73} - \sqrt{136}}{-1+2})^2 + 2 + 1 \cong 12,73$$
$$y_3 = (\frac{\sqrt{73} - \sqrt{136}}{-1+2})(-2 - 12,73) - \sqrt{136} \cong 34,24$$

$$\underline{P + Q = \begin{pmatrix} 12,73 \\ 34,24 \end{pmatrix}}$$

- $2 \cdot P$:

$$x_3 = (\frac{3 \cdot 4 - 70}{2\sqrt{136}})^2 + 2 + 2 \cong 10,18$$
$$y_3 = (\frac{3 \cdot 4 - 70}{2\sqrt{136}})(-2 - 10,18) - \sqrt{136} \cong 18,36$$

$$\underline{2 \cdot P = \begin{pmatrix} 10,18 \\ 18,36 \end{pmatrix}}$$

- $2 \cdot Q$:

$$x_3 = (\frac{3 \cdot 1 - 70}{2\sqrt{73}})^2 + 1 + 1 \cong 17,37$$
$$y_3 = (\frac{3 \cdot 1 - 70}{2\sqrt{73}})(-1 - 17,37) - \sqrt{73} \cong 63,5$$

$$\underline{2 \cdot Q = \begin{pmatrix} 17,37 \\ 63,5 \end{pmatrix}}$$

In diesem Beispiel wurden die Punkte so gewählt, dass die Ergebnispunkte nicht zu weit vom Mittelpunkt entfernt sind, um eine Zeichnung ohne lange Maßstabsüberlegungen zu ermöglichen. Im nächsten Beispiel werden wir sehen, dass sich die Punkte schnell sehr weit vom Ursprung entfernen können:

Beispiel 2: Sei $E : y^2 = x^3 - 50x + 200$ sowie $P = \begin{pmatrix} -8 \\ y>0 \end{pmatrix}$ und $Q = \begin{pmatrix} 0 \\ y>0 \end{pmatrix}$ gegeben. Berechne P+Q, $2 \cdot P$ und $2 \cdot Q$ und fertige eine Skizze an (siehe Abbildungen 2.9 und 2.10).

- $P + Q$:

$$x_3 = (\frac{\sqrt{200} - \sqrt{88}}{-8})^2 + 8 \cong 8,35$$
$$y_3 = (\frac{\sqrt{200} - \sqrt{88}}{-8})(-8 - 8,35) - \sqrt{88} \cong -19,11$$

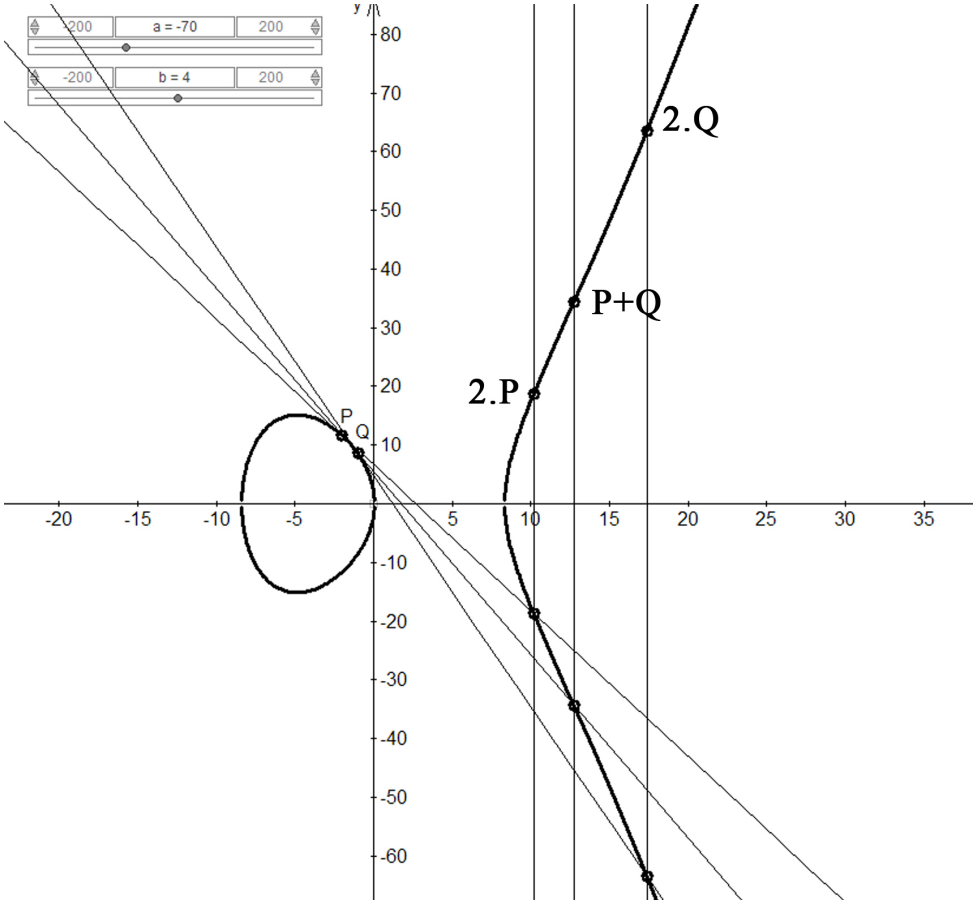


Abbildung 2.8: Skizze Beispiel 1

$$\underline{P + Q = \begin{pmatrix} 8{,}35 \\ -19{,}11 \end{pmatrix}}$$

- $2 \cdot P$:

$$x_3 = (\frac{3 \cdot 64 - 50}{2\sqrt{88}})^2 + 8 + 8 \cong 73{,}28$$
$$y_3 = (\frac{3 \cdot 64 - 50}{2\sqrt{88}})(-8 - 73{,}28) - \sqrt{88} \cong -624{,}59$$

$$\underline{2 \cdot P = \begin{pmatrix} 73{,}28 \\ -624{,}59 \end{pmatrix}}$$

- $2 \cdot Q$:

$$x_3 = (\frac{-50}{2\sqrt{200}})^2 \cong 3{,}125$$
$$y_3 = (\frac{-50}{2\sqrt{200}})(-3{,}125) - \sqrt{200} \cong -8{,}62$$

$$\underline{2 \cdot Q = \begin{pmatrix} 3{,}125 \\ -8{,}62 \end{pmatrix}}$$

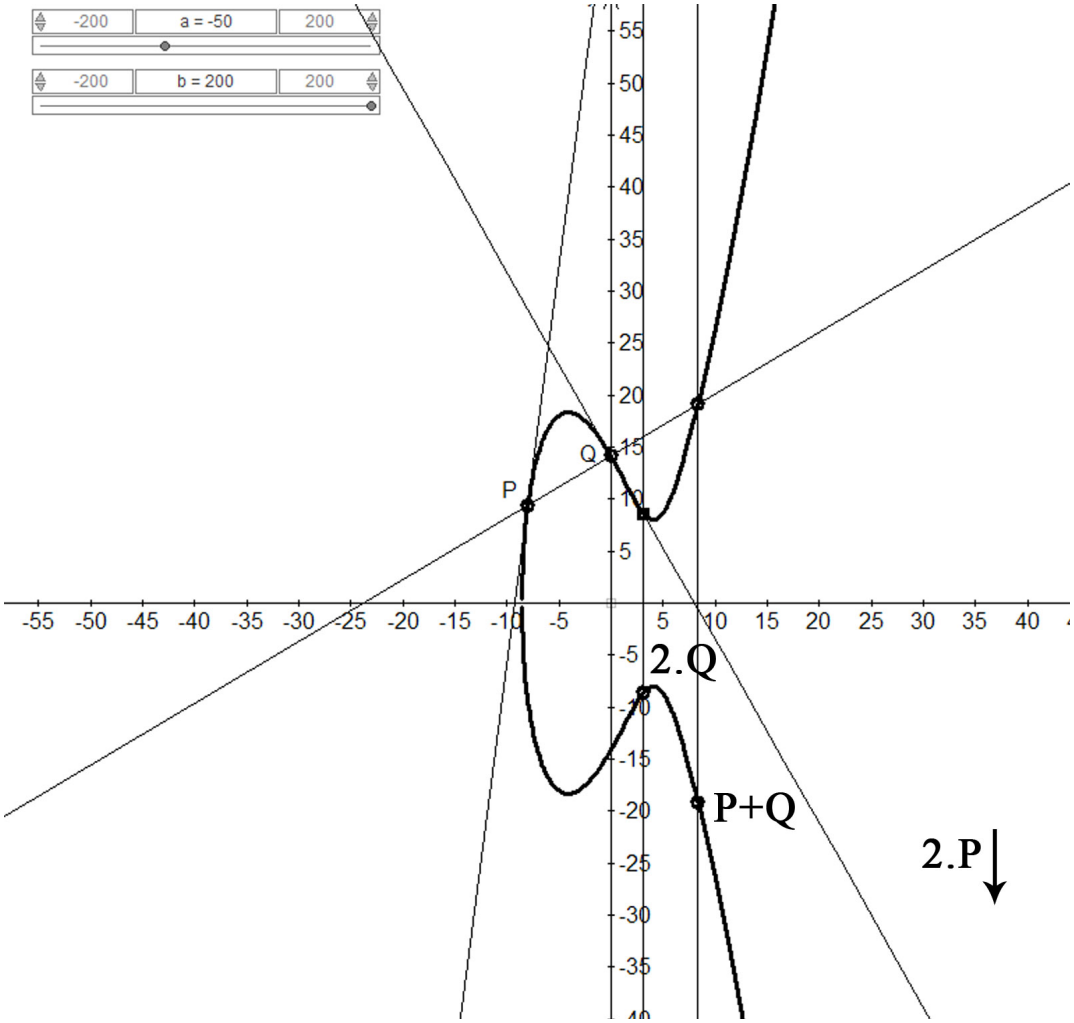


Abbildung 2.9: Skizze *a* Beispiel 2

Beispiel 3: Sei $E : y^2 = x^3 + 10x + 50$ sowie $P = \left(\begin{smallmatrix} 3 \\ \sqrt{107} \end{smallmatrix}\right)$ und $Q = \left(\begin{smallmatrix} 3 \\ -\sqrt{107} \end{smallmatrix}\right)$ gegeben. Berechne P+Q, $2 \cdot P$ und $2 \cdot Q$.

- $P + Q$:Laut Definition der Addition ist das Ergebnis der unendlich entfernte Punkt.

- $2P$:

$$x_3 = (\frac{3 \cdot 9 + 10}{2\sqrt{107}})^2 - 3 - 3 \cong -2,8$$
$$y_3 = (\frac{3 \cdot 9 + 10}{2\sqrt{107}})(3 + 2,8) - \sqrt{107} \cong 0,03$$

$$\underline{2 \cdot P = \left(\begin{smallmatrix} -2,8 \\ 0,03 \end{smallmatrix}\right)}$$

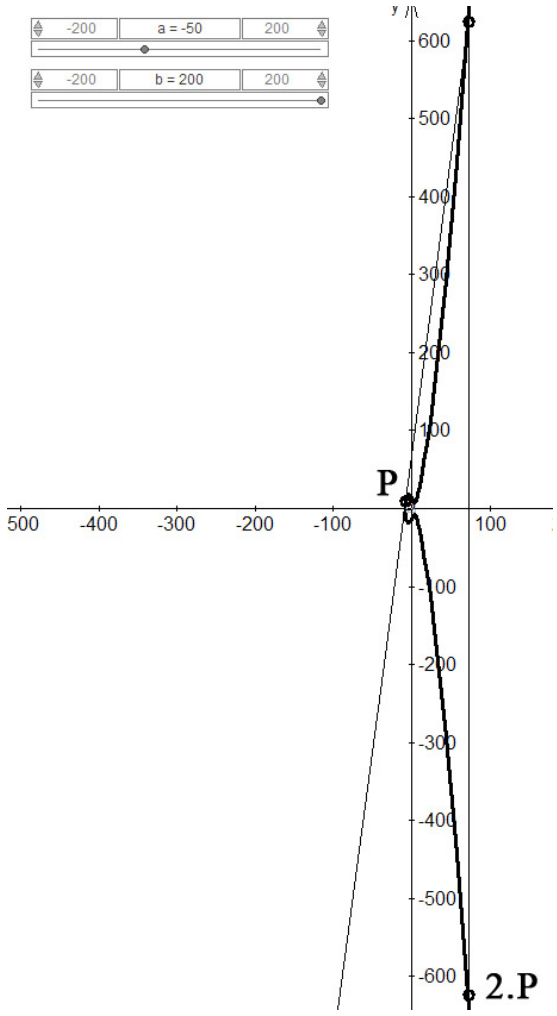


Abbildung 2.10: Skizze *b* Beispiel 2

- $2Q$:

$$x_3 = (\frac{3 \cdot 9 + 10}{2(-\sqrt{107})})^2 - 3 - 3 \cong -2,8$$
$$y_3 = (\frac{3 \cdot 9 + 10}{2(-\sqrt{107})})(3 + 2,8) - \sqrt{107} \cong -0,03$$

$$\underline{2 \cdot Q = \begin{pmatrix} -2,8 \\ -0,03 \end{pmatrix}}$$

Bemerkung: Es fällt auf, dass die Ergebnisse von $2P$ und $2Q$ auch wieder gespiegelte Punkte sind.

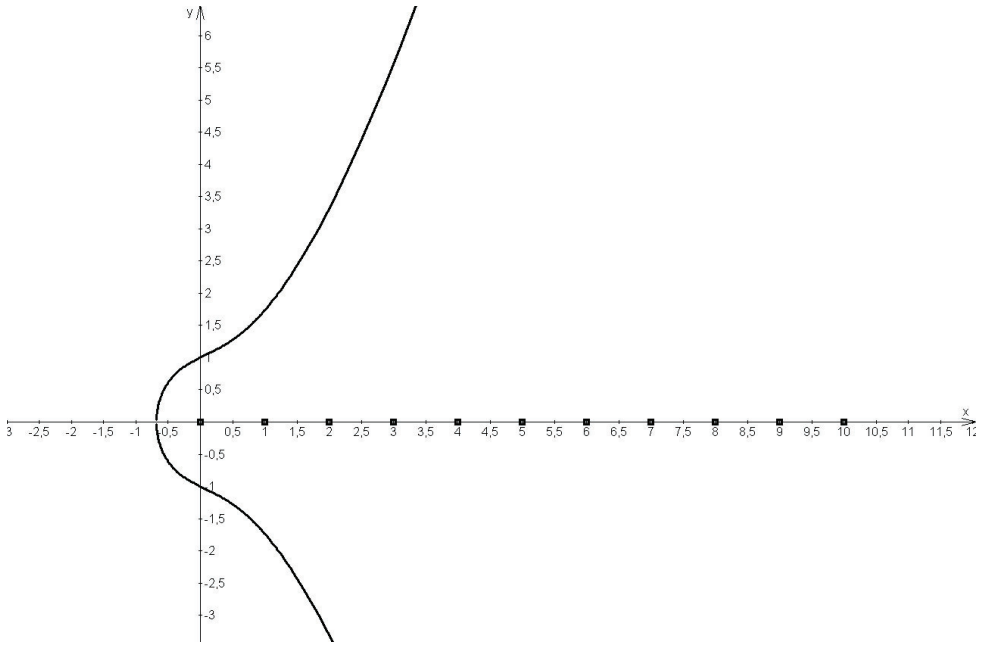


Abbildung 2.11: $y^2 = x^3 + x + 1$ über $\mathbb{R}$

2.7 Elliptische Kurven über $\mathbb{Z}_p$

2.7.1 Grundsätzliches

Wenn wir den stetigen Fall verlassen, also von $\mathbb{R}$ auf $\mathbb{Z}_p$ wechseln, passiert folgendes: Die elliptische Kurvengleichung bleibt die selbe, aber von der x- Achse werden jetzt nur mehr die Elemente aus $\mathbb{Z}_p$ abgebildet. Wir bilden die Gleichung $y^2 = x^3 + x + 1$ zunächst über $\mathbb{R}$ (siehe Abbildung 2.11). Wie sieht die elliptische Kurve $y^2 = x^3 + x + 1$ über dem Körper $\mathbb{Z}_{11}$ aus? Diese Kurve können wir uns jetzt nicht mehr graphisch veranschaulichen, so wie das über $\mathbb{R}$ funktioniert hat. Wir müssen die Punkte, welche die elliptische Kurve bilden, für alle x-Werte, die in Frage kommen, d.h.für die $x^3 + x + 1$ das Quadrat eines y- Wertes aus $\mathbb{Z}_{11}$ ist, berechnen. Wir wollen sehen, ob es für $x = 3$ einen in Frage kommenden y-Wert gibt und diesen berechnen. Dazu setzen wir in die Ellipsengleichung ein und erhalten in $\mathbb{Z}_{11}$, d.h. durch Berechnung mod 11:

$$\begin{aligned} y^2 &= 3^3 + 3 + 1 \\ y^2 &= 31 = 9 \end{aligned}$$

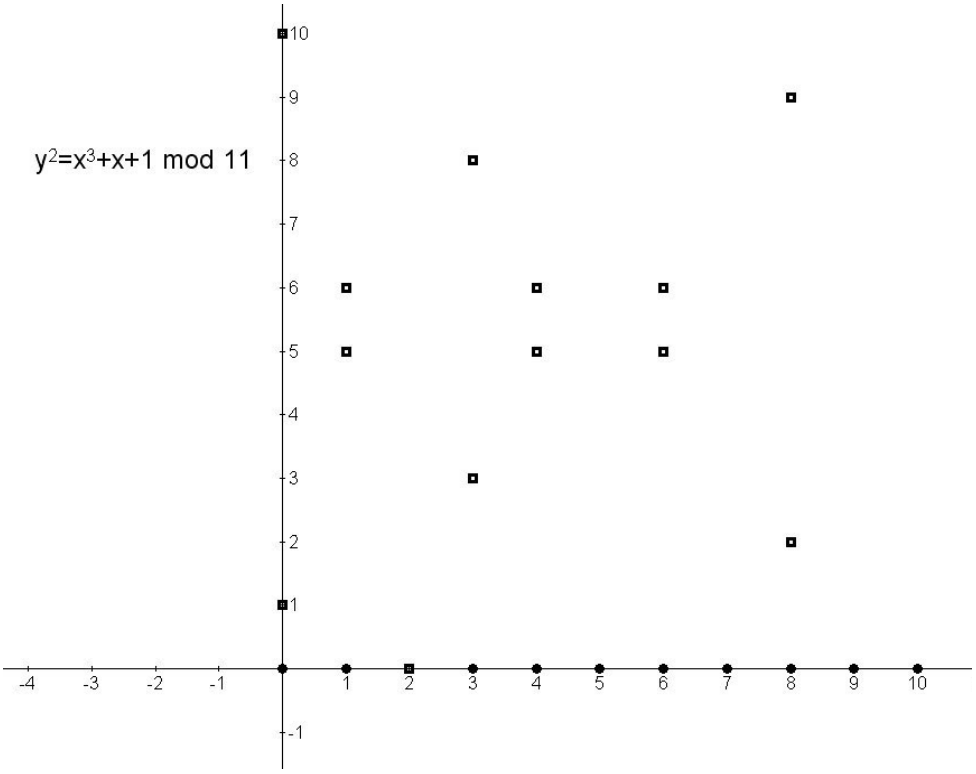


Abbildung 2.12: $y^2 = x^3 + x + 1$ über $\mathbb{Z}_{11}$

$y^2 = 9$ hat in $\mathbb{Z}_{11}$ die Lösung

$$\begin{aligned} y &= \pm 3 \\ y_1 &= 3 \\ y_2 &= -3 \equiv 8 \end{aligned}$$

Aufgabe: Ausrechnen und Einzeichnen aller Punkte der eben verwendeten Kurve (siehe Abbildung 2.12). Was passiert mit den Werten von y^2, für die es keine Wurzel in $\mathbb{Z}_{11}$ gibt wie z.B. $y^2 = 10$ an der Stelle $x = 5$?

Bemerkung. Wie man erkennen kann, liegen die Punkte wieder symmetrisch, diesmal bezüglich der Achse $y = \frac{p}{2}$.

2.7.2 Rechnen mit Punkten einer Elliptischen Kurve E

Wir verwenden die gleichen Rechenoperationen wie bei reellen Zahlen, sie beziehen sich jetzt aber auf $\mathbb{Z}_p$. Für $P, Q \in E$ mit $P = (x_1, y_1) \neq Q = (x_2, y_2)$ gilt daher $P + Q = R = (x_3, y_3) \in E$:

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \mod p$$
$$y_3 = (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1 \mod p$$

sowie für $P = Q = (x_1, y_1)$ gilt daher für $P + Q = 2 \cdot P = 2 \cdot Q = R = (x_3, y_3)$:

$$x_3 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1 \mod p$$
$$y_3 = (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3) - y_1 \mod p$$

Beispiel 1: Wir verwenden wieder die elliptische Kurve $y^2 = x^3 + x + 1$ über $\mathbb{Z}_{11}$. Wir haben schon alle Punkte graphisch veranschaulicht. Es ergibt sich (siehe Abbildung 2.12):
$E = \{\mathcal{O}, \binom{0}{1}, \binom{0}{10}, \binom{1}{5}, \binom{1}{6}, \binom{2}{0}, \binom{3}{3}, \binom{3}{8}, \binom{4}{5}, \binom{4}{6}, \binom{6}{5}, \binom{6}{6}, \binom{8}{2}, \binom{8}{9}\}$.

Aufgabe: Addition von $P_1 = (0, 10)$ und $P_2 = (1, 5)$:

$$x_3 = \underbrace{(\frac{5 - 10}{1 - 0})}_{=6}^2 - 0 - 1 \quad = 36 - 1 = 2$$
$$y_3 = 6 \cdot (-2) - 10 = -22 = 0$$

$$\underline{P_1 + P_2 = (2, 0)}$$

Beispiel 2: Addition von $P_1 = (2, 12)$ und $P_2 = (7, 11)$ sowie berechnen von $2 \cdot P_1$ und $2 \cdot P_2$ der Kurve $y^2 = x^3 - 4x + 1$ über $\mathbb{Z}_{13}$. Die Punkte der Kurve sind (siehe Abbildung 2.13):
$E = \{\mathcal{O}, \binom{0}{1}, \binom{0}{12}, \binom{2}{1}, \binom{2}{12}, \binom{3}{4}, \binom{3}{9}, \binom{4}{6}, \binom{4}{7}, \binom{7}{2}, \binom{7}{11}, \binom{8}{0}, \binom{10}{5}, \binom{10}{8},$
$\binom{11}{1}, \binom{11}{12}, \binom{12}{2}, \binom{12}{11}\}$.

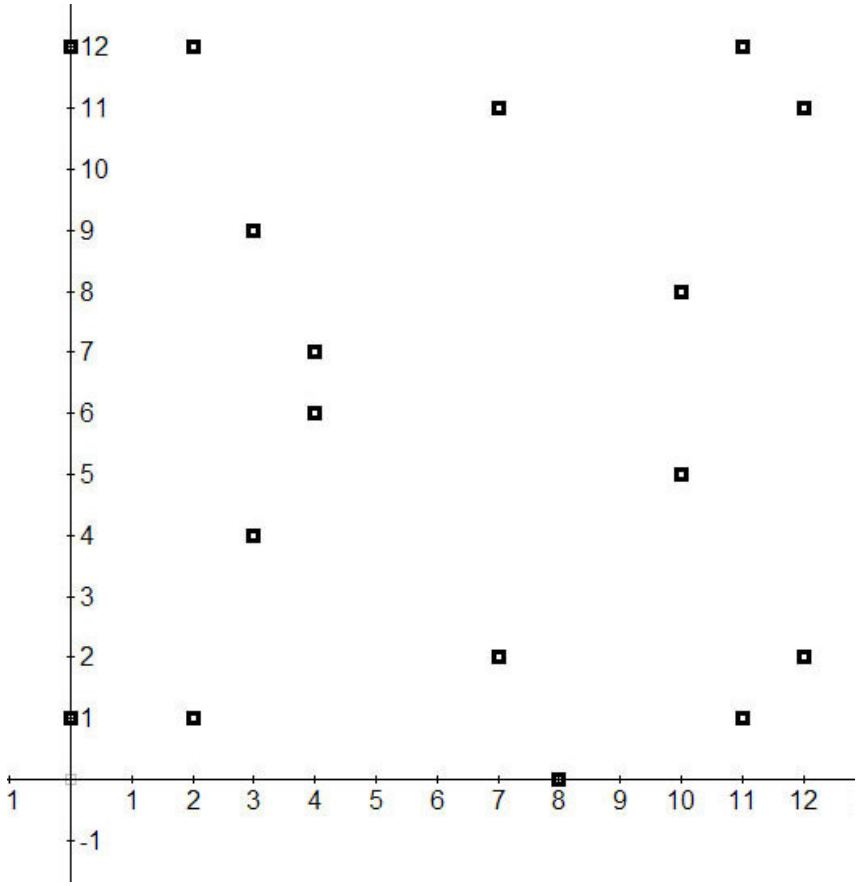


Abbildung 2.13: $y^2 = x^3 - 4x + 1$ über $\mathbb{Z}_{13}$

- Addition von P_1 und P_2:

$$x_3 = (\underbrace{\frac{11-12}{7-2}}_{= -\frac{1}{5} \equiv -8 \bmod 13})^2 - 2 - 7 \; = 55 = 3$$

$$y_3 = (-8) \cdot (2-3) - 12 = 9$$

$$\underline{P_1 + P_2 = (3,9)}$$

- Multiplikation $2 \cdot P_1$:

$$x_3 = \underbrace{(\frac{3 \cdot 2^2 - 4}{2 \cdot 12})}_{=9}^2 - 2 - 2 \; = 3 - 4 = 12$$

$$y_3 = (9) \cdot (2-12) - 12 =, 90 - 12 \; = 2$$

$$\underline{2P_1 = (12,2)}$$

- Multiplikation $2 \cdot P_2$:

$$x_3 = \underbrace{(\frac{3.7^2 - 4}{2.11})}_{=0}^2 - 2 \cdot 7 \quad = -14 = 12$$

$$y_3 = (0) \cdot (7 - 12) - 11 = -11 = 2$$

$$\underline{P_1 + P_2 = (12, 2)}$$

2.7.3 Einsatz von Derive

Diese Beispiele konnte man noch „zu Fuß“rechnen, im folgenden Kapitel macht das Rechnen ohne Computer jedoch keinen Sinn mehr. Es gibt Derive-Programme für das Addieren und das Multiplizieren von Punkten einer elliptischen Kurve über einem endlichen Körper.

Vorüberlegungen

Kryptographie im Allgemeinen bietet sehr gute Möglichkeiten, Computer sinnvoll im Unterricht einzusetzen. Es ist für die Schüler faszinierend und motivierend, wenn der Rechner im Bruchteil einer Sekunde mit hundert- bis zweihundertstelligen Zahlen operiert. Claus erwähnt in [3, 172ff], dass

> in einem anwendungsorientierten Mathematikunterricht der Sekundarstufe II [...] der Computer als Hilfsmittel zum Problemlösen eingesetzt werden [kann].

Weiters schreibt er, dass der Unterricht mithilfe des Computers ergänzt und belebt wird.

Diese Arbeit hält sich an das sogenannte *Blackbox-Whitebox* Prinzip. Zuerst werden sämtliche Rechenschritte per Hand durchgeführt und geübt (Abschnitt 2.2 - 2.6), sodass sie verstanden und beherrscht werden (*Whitebox*). Im Anschluss können sie vom Computer mit gutem Gewissen übernommen werden (sie werden somit zur *Black-Box*), da der Fokus nicht auf dem Rechnen liegen sollte. Nach ausführlicher Beschäftigung mit den Rechenoperationen lagern wir diese auf den Computer aus. Dabei liegt es im Ermessen der Lehrperson, wie die Programme eingeführt werden. Wenn die SchülerInnen schon Programmiererfahrung haben, können die konkreten Programme entwickelt werden (kurze Programmbeschreibungen sind angeführt), andernfalls werden sie vorprogrammiert und von den SchülerInnen einfach benützt. Jedenfalls sollten sie das Anwenden von Programmen beherrschen. Die folgenden Programme sind aus [6] bzw. aus [7].

points

Für kleine Beispiele macht das Programm *points* Sinn, das alle Punkte der Kurve berechnet und anschreibt (siehe Abbildung 2.14).

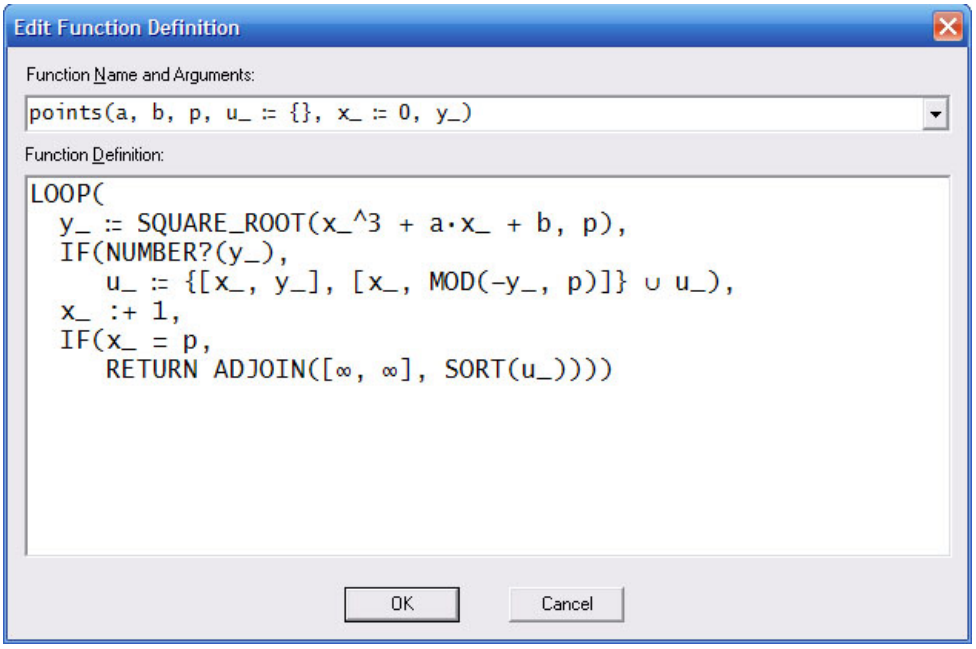


Abbildung 2.14: Das Programm *points*

Programmbeschreibung: a, b und p sind die Freiheiten aus $y^2 = x^3 + ax + b \bmod p$. Die Variablen mit Unterstrich, also u_, x_ und y_ werden nur lokal verwendet. Es beginnt mit einer loop- Schleife, zuerst wird $y_= \sqrt{x^3 + ax + b} \bmod p$ berechnet, wenn diese Zahl eine natürliche Zahl ist, wird der Punkt x_ und y_ in der Menge u_ abgespeichert, sowie x_ und die negative Wurzel -y_ modulo p. Dann wird x_ um 1 erhöht und es beginnt von vorne, solange, bis x_ = p ist. Im letzten Schritt wird die Ausgabe definiert, nämlich die Punktmenge u_ und der Punkt $[\infty, \infty]$, also der oben mit $\mathcal{O}$ bezeichnete Kurvenpunkt, der bei jeder Kurve enthalten ist.

Beispiel: Alle Punkte der Kurve $y^2 = x^3 - 12x + 4 \bmod 17$

$$\text{points}(-12,\ 4,\ 17)' = \begin{bmatrix} \infty & 0 & 0 & 5 & 5 & 7 & 7 & 9 & 9 & 10 & 11 & 11 & 14 & 14 & 16 & 16 \\ \infty & 2 & 15 & 1 & 16 & 5 & 12 & 8 & 9 & 0 & 8 & 9 & 8 & 9 & 7 & 10 \end{bmatrix}$$

add

Das Programm *add* ist streng nach der Definition der Addition gebaut und lässt sich leicht nachvollziehen (siehe Abbildung 2.15).

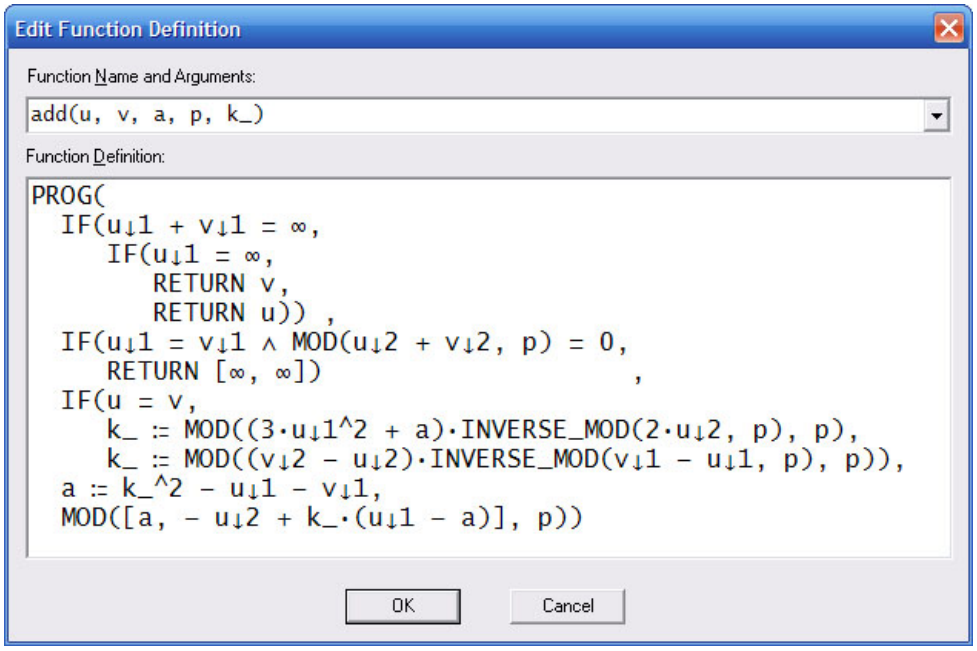


Abbildung 2.15: Das Programm *add*

Programmbeschreibung: u und v sind die beiden Punkte der Kurve, die man addieren möchte, sie sind dem Programm in der Listenform $[u_1, u_2]$ bzw. $[v_1, v_2]$ zu übergeben. a und p sind Parameter der Kurve. Es folgen drei *if*- Schleifen:

- Die erste behandelt den Fall, dass einer der beiden Punkte der Punkt $\mathcal{O}$ ist und bestimmt dann den anderen als Ergebnis.
- Die zweite kommt zur Anwendung, wenn die x-Werte der beiden Punkte gleich sind und die y- Werte addiert modulo $p = 0$ sind. Die Punkte liegen dann auf einer zur y- Achse parallelen Geraden oder sie fallen zusammen als eine 0- Stelle von E. Als Ausgabe wird der Punkt $\mathcal{O}$ definiert.
- In der dritten Schleife werden die beiden Lambdas definiert, hier werden sie mit k_ bezeichnet. Das erste λ kommt zur Anwendung, wenn $u = v$ ist, ansonsten das zweite. Zum Schluss werden die beiden Koordinaten des Ergebnispunktes ausgegeben.

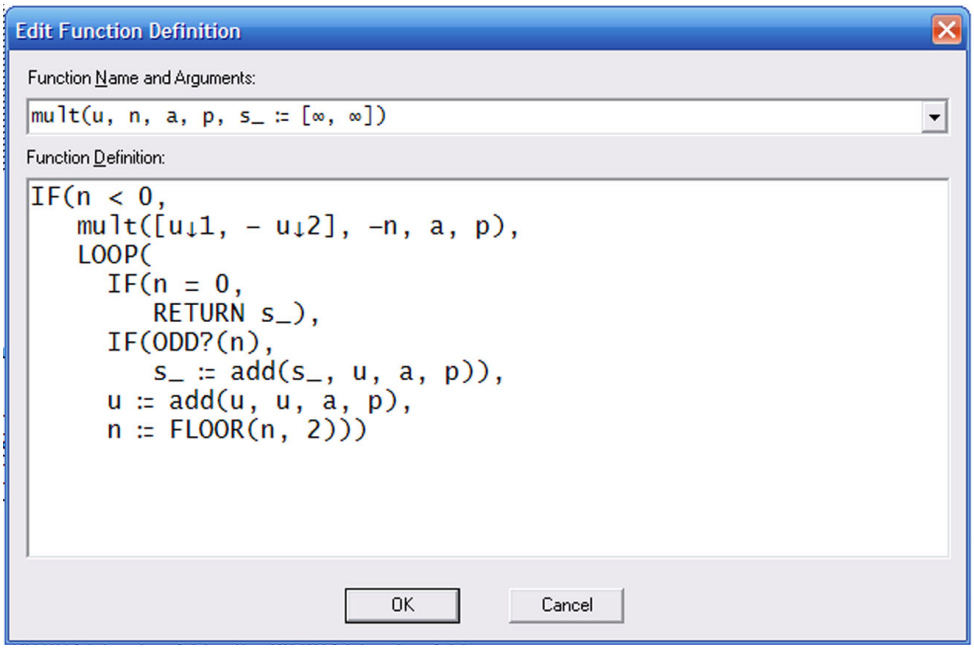


Abbildung 2.16: Das Programm *mult*

Beispiel: Addition der Punkte (5/16) und (9/9) auf der Kurve $y^2 = x^3 - 12x + 4$ über $\mathbb{Z}_{17}$:

```
add([5, 16], [9, 9], -12, 17) = [5, 1]
```

mult

mult verwendet das Programm *add*, n ist der Multiplikator des Punktes $u = [u_1, u_2]$ (siehe Abbildung 2.16)).

Programmbeschreibung: Das Programm *mult* arbeitet wie im Kapitel 2.6.2 beschrieben. Am Beginn wird definiert, dass der andere Punkt mit gleichem x- Wert zu verwenden ist, falls der Multiplikator n negativ sein sollte. In diesem Fall wird mit $|n|$ multipliziert. In der folgenden *loop*-Routine wird n solange halbiert (und abgerundet), bis es Null ist, u wird dabei stets verdoppelt, oder, falls es ungerade sein sollte, wird noch eines dazu addiert. Somit wird die Rechnung $23P$ zu

$$23P = P + 2(11P) = P + 2(P + 2(5P)) = P + 2(P + 2(P + 2(2P)))$$

Beispiel: Multiplikation des Punktes [11,8] mit 13 auf der Kurve $y^2 = x^3 - 12x + 4$ mod 17

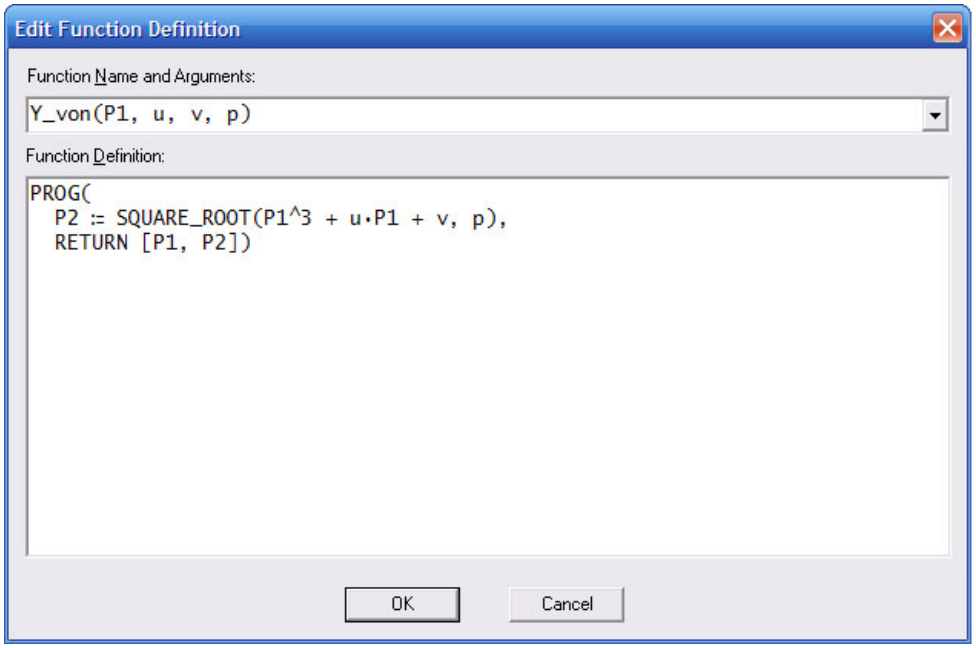


Abbildung 2.17: Das Programm *Y_von*

```
mult([11, 8], 13, -12, 17) = [9, 8]
```

Y_von

Als sehr nützlich hat sich auch das kleine Programm *Y_von* erwiesen (siehe Abbildung 2.17). Es berechnet den zu einem x-Wert gehörigen positiven y-Wert und gibt den Punkt aus. Falls kein y-Wert existiert, steht ein Fragezeichen an der Stelle des y-Wertes.

P_inv

Diese Programm invertiert den Punkt, das heißt der y-Wert wird mit negativem Vorzeichen versehen und dann modulo p gerechnet (siehe Abbildung 2.18).

Zusätzliche Befehle

- *mod*(a, p): berechnet a modulo p.
- *square_root*(a, p): berechnet die positive Quadratwurzel der Zahl $a \in \mathbb{Z}_p$ modulo p, wenn diese existiert. Ansonsten wird ein Fragezeichen ausgegeben. Dieser Befehl ist wichtig zum Berechnen des zu einem x-Wert gehörigen y-Wertes.
- P:=[x,y] : Das definieren eines Punktes wird beim Einsatz größerer Zahlen sehr wichtig.

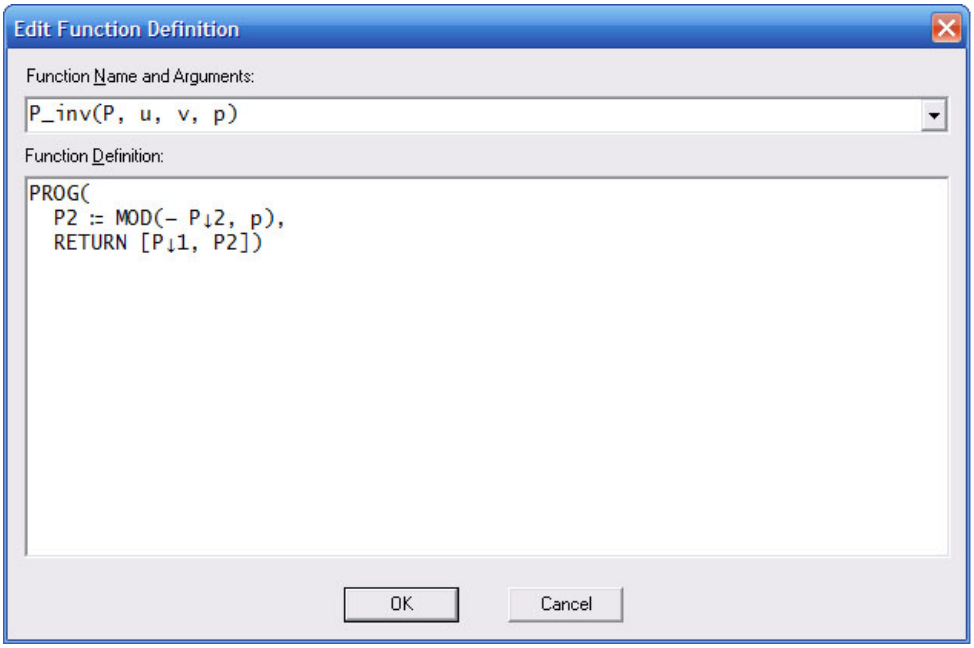


Abbildung 2.18: Das Programm *P_inv*

- *random(v)*: gibt eine Zufallszahl in der Größenordnung von v aus.
- *next_prime(u)*: gibt die nächsthöhere Primzahl von u aus.

Beispiele

Gegeben sei die Kurve $E : y^2 = x^3 - 12x + 4$ über $\mathbb{Z}_{23}$. Berechne mit Hilfe von Derive:

- Die Anzahl der Punkte von E
- Sei $P = \left({}^{1}_{-}\sqrt{y^2} \right), Q = \left({}^{14}_{+}\sqrt{y^2} \right)$. Berechne P+7Q, 12P, 22Q.

2.8 ElGamal über Elliptischen Kurven

Nachdem wir das nötige Werkzeug gesammelt haben, können wir jetzt einen Verschlüsselungsalgorithmus betrachten. Die Grundmenge, auf der wir unsere Rechnungen anstellen, sind die Punkte einer elliptischen Kurve, wir müssen uns also vor jedem Verschlüsselungsakt mit unserem Gegenüber auf eine spezielle Kurve einigen. Die Parameter der Kurve u und v sowie die Primzahl p bilden den ersten Teil des öffentlichen Schlüssels.Als erstes werden somit

- E: $y^2 = x^3 + u \cdot x + v$ über $\mathbb{Z}_p$ und
- $P \in E$ gewählt.

1. Teilnehmer A wählt zufällige ein $a \in (1, ..., p-1)$ und bildet damit $Q = aP$. Dieses Q gibt er nun als seinen öffentlichen Schlüssel bekannt, während a als sein privater Schlüssel geheim bleibt.

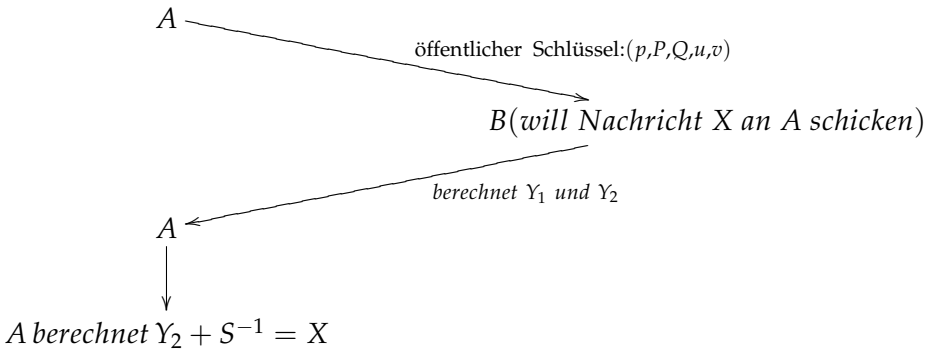
   öffentlicher Schlüssel von Teilnehmer A: (p, u, v, P, Q)

2. Teilnehmer B will an A nun die Nachricht X schicken (die Nachricht wird als Punkt der Kurve codiert, siehe Kapitel 2.8.1).

   Er wählt dazu b zufällig aus $(1, ..., p-1)$ und berechnet damit $Y_1 = bP$ und $Y_2 = X + bQ \ (= X + a \cdot b \cdot P)$

   (Y_1, Y_2) bilden das Chiffrat, das er an A schickt.

3. Um die Nachricht zu entschlüsseln bildet A $S := a \cdot Y_1 = a \cdot P \cdot b$ und das Inverse davon ($S^{-1} = -a \cdot P \cdot b$). Die Nachricht erhält A nun mit $Y_2 + S^{-1}$.



2.8.1 Codierung

Bevor tatsächlich ein Bespiel berechnet werden kann, muss noch besprochen werden, wie man eine Nachricht in die Welt der elliptischen Kurven versetzen kann, also wie man sie als Punkt(e) codiert. Der Text wird zunächst in Blöcke aufgeteilt und als Zahl codiert, wie z.B. mit folgender Tabelle:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
P	Q	R	S	T	U	V	W	X	Y	Z	∪			
16	17	18	19	20	21	22	23	24	25	26	27			

Hallo Welt wird wie folgt codiert:

H	A	L	L	O	∪	W	E	L	T
08	01	12	12	15	27	23	05	12	20

Die Null am Beginn fällt natürlich bei Rechnungen weg. Dieser Fehler ist jedoch schnell behoben, weil die Anzahl der Ziffern immer gerade sein muss.

Jetzt benötigen wir eine elliptische Kurve. Dabei muss der Modul p länger sein als unsere Nachricht, oder wir „zerschneiden“die Nachricht in Blöcke. Seien die Parameter $u = 12$ und $v = 1$ sowie die Zahl
`p:=NEXT_PRIME(RANDOM(2^{64}))`$=$ 16759217722839375653 der Modul für das folgende Beispiel. Das gewählte p ist um eine Stelle länger als unsere Nachricht und wir haben nur einen Block zu codieren. Unser *Hallo Welt* wird nun als x-Koordinate verwendet. Man muss nur den y- Wert berechnen (sofern er existiert, siehe weiter unten):
`SQUARE_ROOT(08011212152723051220^3 + 12*08011212152723051220 + 1, p)` $=$
14118129172583213142. Klarerweise kann man auch `-14118129172583213142 mod p` als y-Koordinate verwenden. An dieser Stelle kann man mit dem Verschlüsseln beginnen.

Anmerkung: Es kann auch passieren, dass der Wert der Nachricht keinen y- Wert auf unserer Kurve hat. In diesem Fall gibt es mehrere Möglichkeiten. Man kann zur Nachricht immer die Zahl Eins dazuaddieren, bis ein y-Wert existiert, oder man verwendet eine andere Kurve. Im ersten Fall muss man sich zusätzlich mit dem Gegenüber ausmachen, wie die Nachricht verändert wird. Im automatischen Betrieb wird diese Information jedoch gleich in den codierten Text eingebaut.

2.8.2 Ein ausführliches Beispiel

Das folgende Beispiel hält sich streng an die Anleitung aus 2.8. Wir benötigen als erstes eine Kurve $E : y^2 = x^3 + ux + v$:

```
                          32
(u := RANDOM(2  )) = u := 1903517484

                          32
(v := RANDOM(2  )) = v := 3426728589

                          80
(p := NEXT_PRIME(RANDOM(2  ))) = p := 640221524322852549361979
```

Weiters suchen wir einen Punkt $P \in E$, der als öffentlicher Schlüssel dient:

```
                                32
(P1 := RANDOM(2  )) = P1 := 4166218209

                          3
(P2 := SQUARE_ROOT(P1  + u·P1 + v, p)) = P2 := 6091059574235820195251

(P := [P1, P2]) = P := [4166218209, 6091059574235820195251]
```

Alternativ kann man Y_von als *BlackBox* verwenden:

```
(P := Y_von(P1, u, v, p)) = P := [4166218209, 6091059574235820195251]
```

Jetzt versetzen wir uns in die Lage von Teilnehmer A. Wir müssen uns eine Geheimzahl a ausdenken. Diese könnte folgendermaßen aussehen:

```
                              50
(a := RANDOM(2  )) = a := 751280673317359
```

Mit dieser berechnen wir unseren öffentlichen Schlüssel Q:

```
(Q := mult(P, a, u, p)) = Q := [545598793106421931783741, 1734038213330380700097]
```

Nun ist Teilnehmer B an der Reihe. Er möchte die Nachricht *Hallo Welt* an A schicken. Wie dieser Text in Zahlen aussieht wissen wir schon, nämlich
0801121215272305122 0. Um einen Punkt zu erhalten, muss er den y- Wert ausrechnen.

```
(N1 := 8011212152723051220) = N1 := 8011212152723051220

                          3
(N2 := SQUARE_ROOT(N1  + u·N1 + v, p)) = N2 := 471451071640959857463359

(N := [N1, N2]) = N := [8011212152723051220, 471451071640959857463359]
```

Alternativ mit *BlackBox*:

```
(N := Y_von(N1, u, v, p)) = N := [8011212152723051220, 471451071640959857463359]
```

Teilnehmer B hatte Glück, die Nachricht hat als x-Wert verwendet eine y-Koordinate auf der Kurve. Auch Teilnehmer B braucht eine Geheimzahl:

```
                              50
(b := RANDOM(2  )) = b := 85264971240790
```

Jetzt kann verschlüsselt werden:

```
(Y1 := mult(P, b, u, p)) = Y1 := [52742395055489647731777, 4071389988431602648148 98]

(Y2 := add(N, mult(Q, b, u, p))) = Y2 := [1601776486097959048421 87, 1826467951513563514318 34]
```

Y1 und Y2 bilden gemeinsam das Chiffrat, welches nun an Teilnehmer A geschickt wird. Dieser entschlüsselt die Nachricht in zwei Schritten. Zuerst berechnet er S^{-1}:

```
(S := mult(Y1, a, u, p)) = S := [372039675694277311599977, 282101597535383398131034]

(Sinv := [S , MOD(- S , p)]) = Sinv := [372039675694277311599977, 358119926787469151230945]
         [1          2    ]
```

Mit P_inv:

```
(Sinv := P_inv(S, u, v, p)) = Sinv := [372039675694277311599977, 358119926787469151230945]
```

Um die Nachricht zu erhalten muss nur noch eine letzte Addition durchgeführt werden:

```
add(Y2, Sinv, u, p) = [8011212152723051220, 471451071640959857463359]
```

Wir sehen, dass wir mit dem x- Wert wieder unsere Nachricht erhalten haben!

Abbildungsverzeichnis

1.1 Vergleich der nötigen Bit-Länge zwischen RSA und ECC 17

2.1 $y^2 = x^3 + x + 1$ 32
2.2 Dynamisch Darstellung einer elliptischen Kurve mit Hilfe von Schiebereglern in dem Programm *DynaGeo*. 33
2.3 Charakteristische Erscheinungsformen von $y^2 = x^3 + ax + b$ 34
2.4 $y^2 = x^3 - 50x + 200$ 36
2.5 Addition geometrisch 37
2.6 mögliche Lösungen einer kubischen Gleichung 38
2.7 Multiplikation auf einer elliptischen Kurve, grafisch 40
2.8 Skizze Beispiel 1 43
2.9 Skizze *a* Beispiel 2 44
2.10 Skizze *b* Beispiel 2 45
2.11 $y^2 = x^3 + x + 1$ über $\mathbb{R}$ 46
2.12 $y^2 = x^3 + x + 1$ über $\mathbb{Z}_{11}$ 47
2.13 $y^2 = x^3 - 4x + 1$ über $\mathbb{Z}_{13}$ 49
2.14 Das Programm *points* 51
2.15 Das Programm *add* 52
2.16 Das Programm *mult* 53
2.17 Das Programm *Y_von* 54
2.18 Das Programm *P_inv* 55

Literaturverzeichnis

[1] Dietmar Dorninger. *Algebraische Methoden in den Computerwissenschaften*, Vorlesung TU Wien, SS2000. (Skriptum hierzu von Christoph Fabianek und Andreas Traxler, Kapitel 2).

[2] Peter Paukowitsch. *Lineare Algebra und analytische Geometrie (für LAK)*, Skriptum zur Vorlesung, 2004/05.

[3] Heinz Jörg Claus. *Einführung in die Didaktik der Mathematik*, Seite 172 ff., Wissenschaftliche Buchgesellschaft Darmstadt, 1995.

[4] Mirbach, Andreas. *Elliptische Kurven, die Bestimmung ihrer Punktezahl und Anwendung in der Kryptographie*, Verlagshaus Monsenstein und Vannerdat, 2003

[5] Alfred Schreiber. *Arithmetik und Algebra*, Kapitel 7: Kongruenzen und Restklassen, www.gefilde.de/ashome/vorlesungen/arithalgebra/skript/kapitel07.pdf, 2005.

[6] Johann Wiesenbauer. Titbits 29, Derive Newsletter #55, Seite 39-56, Dezember 2004.

[7] Eisler Andreas. Elliptische Kurven und ihre Bedeutung in der Kryptographie, Seite 9-11, Diplomarbeit, TU-Wien, 2008.

[8] Bundesministeriums für Unterricht, Kunst und Kultur. *Lehrplan Mathematik der AHS-Oberstufe*, http://www.bmukk.gv.at/medienpool/11884/lp_neu_ahs_29.pdf, Zugriff am 02.03.2010.

[9] Homepage des Standardsetzers IEEE,

http://grouper.ieee.org/groups/1363/, Zugriff am 02.03.2010.

[10] Homepage des Standardsetzers IEEE,

http://grouper.ieee.org/groups/1363/P1363/testvector.txt, Zugriff am 02.03.2010.

Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die aus anderen Quellen entnommenen Stellen als solche gekennzeichnet habe.

Wien, am 19. März 2010

Johannes Hasibeder